EVA 2020-2030-0006

ZAKON O VARSTVU OSEBNIH PODATKOV NA PODROČJU OBRAVNAVANJA KAZNIVIH DEJANJ (ZVOPPOKD)

I. UVOD

1. OCENA STANJA IN RAZLOGI ZA SPREJEM PREDLOGA ZAKONA

Predlog Zakona o varstvu osebnih podatkov na področju obravnavanja kaznivih dejanj (ZVOPPOKD) 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 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, v Sloveniji pa ustavnosodna presoja 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

[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).

Okvirnega sklepa Sveta 2008/977/PNZ«[3], ki naj bi isto storil še **za ti. policijske oziroma kazensko pravosodne in podobne obdelave.**

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 še nikoli prej ni v takšnem obsegu omogočala obdelave osebnih podatkov za izvajanje dejavnosti, kot so preprečevanje, preiskovanje, odkrivanje ali pregon kaznivih dejanj ali izvrševanje kazenskih sankcij.« (uvodna navedba št. 3 Direktive (EU) 2016/680).

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 prej 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 oziroma 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 navedenega cilja 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

[3] Št. 5833/12, 27.01.2012, Medinstitucionalna oznaka: 2012/0010(COD).
[4] Takrat z vsebino, objavljeno v: Uradni list RS, št. 33/91-I, 42/97, 66/00, 24/03, 69/04 in 68/06.
[5] Direktiva Evropskega parlamenta in Sveta 95/46/ES z dne 24. oktobra 1995 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov, Uradni list EGS, L 281, 23. 11. 1995, str. 0031 – 0050 in Uradni list EU, L 284, 31. 10. 2003, str. 1–53 – Uredba (ES) št. 1882/2003.
[6] Okvirni sklep Sveta 2008/977/PNZ z dne 27. novembra 2008 o varstvu osebnih podatkov, ki se obdelujejo v okviru policijskega in pravosodnega sodelovanja v kazenskih zadevah, Uradni list EU, L 350, 30. 12. 2008, str. 60–71.
[7] Konvencija Sveta Evrope, h kateri lahko pristopijo tudi države izven Evrope. Oznaka Sveta Evrope za Konvencijo: ETS No. 108. Objava: Uradni list RS, št. 11/94 – Mednarodne pogodbe, št. 3/94 in 86/04 – ZVOP-1.
[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.

veljavnega Okvirnega sklepa 2008/977/PNZ iz leta 2008 in da torej sprejetje predlagane Direktive ni potrebno.

Glede vsebine Predloga Splošne uredbe so se ob začetku njenega zakonodajnega obravnavanja pojavili ustavnopravni pomisleki tudi v Zvezni republiki Nemčiji, tako je leta 2012 nemški zvezni ustavni sodnik Johannes Masing objavil članek[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«).

Glede takratnega besedila Predloga Direktive (EU) 2016/680 pa je tudi Informacijski pooblaščenec izrazil negativno stališče na seji Odbora za zadeve Evropske unije Državnega zbora RS z dne 23. 3. 2012, da namreč njeno sprejetje ni potrebno, da zadostuje dosedanja ureditev v slovenski področni zakonodaji in v ZVOP-1 ter dotedanji Okvirni sklep 2008/977/PNZ.

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] 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].

1.2 Razlogi za sprejem zakona

Zaradi navedenih pravnih aktov Evropske unije oziroma Sveta Evrope so potrebne spremembe zakonodaje Republike Slovenije, torej najprej Zakona o varstvu osebnih podatkov na področju obravnavanja kaznivih dejanj (ZVOPPOKD), ki implementira Direktivo[12], nato pa tudi sprejetje Zakona o varstvu osebnih podatkov kot sistemskega zakona Republike Slovenije za področje varstva osebnih podatkov (ZVOP-2), slednjega za izvajanje določenih določb Splošne uredbe o varstvu podatkov iz leta 2016.

Posledično je bilo pripravljeno besedilo predloga novega zakona ZVOPPOKD, 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

[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; v nadaljnjem besedilu: Splošna uredba.

[11] Uradni list EU, L, št. 119/89 z dne 4. 5. 2016, str. 89–131; v nadaljnjem besedilu: Direktiva.

[12] Delno pa vključuje tudi zakonske rešitve določenih pravnih praznin glede implementacije Direktive (EU) 2016/681 – Evidenca letalskih potnikov, ki je v pristojnosti Ministrstva za notranje zadeve, zlasti glede pooblaščenih oseb za varstvo osebnih podatkov pri Enoti za letalske potnike na Policiji, glede dnevnika obdelav za obdelane podatke ipd.

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

od leta 1992[14] dalje ter tudi določbe še veljavne Konvencije o varstvu posameznikov glede na avtomatsko obdelavo osebnih podatkov (v nadaljnjem besedilu: Konvencija št. 108).

Koncept zakona je bil v obdobju 2017–2018 ter v prvem in drugem krogu medresorskega in strokovnega usklajevanja v letu 2019 drugačen, celovit (izvajanje oziroma prenos Splošne uredbe in Direktive v enem zakonu), sedaj je to zaradi preglednosti in lažjega izvajanja razdeljeno na dva zakona. Predloženi ZVOPPOKD tako primarno pomeni implementacijo Direktive.

2. CILJI, NAČELA IN POGLAVITNE REŠITVE PREDLOGA ZAKONA

2.1 Cilji Predloga zakona

Cilji Predloga zakona so:

- zagotoviti na sistemski ravni v ZVOPPOKD izvrševanje določb Direktive,
- določiti ustrezne podlage v ZVOPPOKD za nadaljnje zakonsko urejanje podrobnih obdelav osebnih podatkov v področnih zakonih (zlasti s področja policije in kazenskega pravosodja),
- zagotoviti, da se v ZVOPPOKD v čim večji meri ohrani dosedanja visoka raven varstva osebnih podatkov v Republiki Sloveniji ter tudi na ta način zagotovi uresničevanje osebne človekove pravice do varstva in tajnosti osebnih podatkov iz 38. člena Ustave Republike Slovenije.

2.2. Pravni pristop glede zakonske izvedbe Direktive (EU) 2016/680 na področju varstva osebnih podatkov

Zakonodajna izvedba Direktive, ki se nanaša na področje kaznovalnega delovanja države (kazensko pravosodje in policijsko delovanje), je določena natančno, splošne določbe ter tudi del področnih določb iz predloga zakona veljajo tudi za področne določbe veljavne zakonodaje (npr. policijske, državnotožilske, kazenskoprocesne ipd.).

Pomembno glede zakonodajnih rešitev iz Predloga ZVOPPOKD je, da se upoštevajo relevantne sistemske določbe Konvencije št. 108, ki morajo tudi biti izvedene v tem zakonu.

Ker ima Republika Slovenije že od leta 1990 sicer 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 ZVOPPOKD ali bodočega ZVOP-2 (poleg že navedenih področnih ureditev varstva osebnih podatkov). To je pomembno zlasti z vidika določb o definicijah, pravnih podlagah za obdelave osebnih podatkov, obdelav osebnih podatkov v druge namene, uporabe načel zakona ipd.

Predlog zakona delno sledi prenovljenemu izrazoslovju Direktive: 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). Določeni instituti pa so izjemoma prevzeti celo iz Splošne uredbe, ker so potrebni tudi na področju obravnavanja kaznivih dejanj (npr. institut privolitve).

[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.

Prav tako na dokončnejšo vsebino predloga zakona vpliva dejstvo, da je bila 23. maja 2018 izvedena objava popravkov uradne slovenske inačice besedila Direktive, kar pa velja tudi za večino drugih jezikovnih inačic Direktive (in povezane Splošne uredbe).

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 št. 108, 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 **z vidika preglednosti in lažje uporabe zakonskih določb primerno, da se pripravi nov Zakon o varstvu osebnih podatkov na področju obravnavanja kaznivih dejanj**,

2.3. O zakonodajnih tehnikah predloga zakona

V besedilu določb Predloga ZVOPPOKD je uporabljena kombinacija več zakonodajnih tehnik:

1. tehnika indikacije (sklica), npr. na konkretne pravne podlage iz Direktive (le občasno, npr. pri čezmejnih posredovanjih osebnih podatkov),
2. tehnika določanja nacionalnih posebnosti (npr. sistem povezovanja),
3. tehnika prevzema iz drugega pravnega akta (npr. institut privolitve),
4. tehnika razčlenitve (npr. nadzorni postopki Informacijskega pooblaščenca, določitev/uporaba izraza pristojni organ in ne upravljavec),
5. tehnika prepisa (npr. glede ključnih obveznosti upravljavca in obdelovalca).

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

2.4. Načela predloga zakona

Načelo spoštovanja osebnosti in pravic človeka

Prvo vodilno načelo novega predloga zakona je zakonodajno urejanje v smeri individualnega pristopa, po katerem je treba izhajati iz človeka kot upravičenca (nosilca; naslovnika; subjekta) pravice do varstva osebnih podatkov in torej njemu zagotoviti dejansko uresničevanje te pravice. Prost pretok osebnih podatkov, prenosi osebnih podatkov, čezmejne obdelave osebnih podatkov, posredovanja osebnih podatkov, obdelave osebnih podatkov v druge namene ipd. lahko delujejo le, če je navedeni individualni pristop spoštovan. Pri presoji zakonodajnih ali izvedbenih posegov v pravico do varstva osebnih podatkov je treba izhajati iz ocene vpliva posega v varstvo osebnih podatkov človeka kot subjekta ter opraviti oceno z vidika spoštovanja strogega načela sorazmernosti (2. člen v zvezi s tretjim odstavkom 15. člena Ustave Republike Slovenije).

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 (a) točke prvega odstavka 4. člena 4 Direktive, 8. člena Direktive in (a) točke 5. člena Konvencije. Države članice Evropske unije lahko glede na svojo nacionalno (zlasti ustavno) ureditev vseeno določijo splošne in konkretne 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 določajo v podzakonskih predpisih (kar je nedopustno po ustaljeni ustavnosodni presoji

Ustavnega sodišča Republike Slovenije od leta 1992 dalje[15]). Temu pristopu tako sledita zlasti prvi in drugi odstavek 6. člena predloga zakona. Za delovanje (odločanje, poseganje v pravice, določanje obveznosti) s strani javnega sektorja (javne oblasti) – v tem primeru celo represivnih organov države – lahko velja le strogo načelo zakonitosti.

Načelo stroge sorazmernosti

Pri izvajanju posegov v pravico do varstva osebnih podatkov je treba izhajati iz načela sorazmernosti, kot ga opredeljuje predlog zakona, konkretneje je treba izhajati uporabe strogega testa sorazmernosti po ustaljeni ustavnosodni presoji (predvsem odločba US, št. U-I-60/03, 4. 12. 2003[16], zlasti 30. točka v zvezi s 17. točko odločbe).

Načelo namenske obdelave osebnih podatkov

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 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 prvega in drugega odstavka 9. člena Direktive biti omogočene tudi obdelave osebnih podatkov v druge namene. Tovrstno omejitev omogoča tudi določba tretjega odstavka 15. člena Ustave Republike Slovenije o omejitvah človekovih pravic s pravicami drugih oseb. Vendar pa tudi ta odstop upošteva drugi odstavek 38. člena Ustave – gl. izrecno določen pogoj v prvem odstavku 8. člena predloga zakona v skladu s katerim, lahko te dodatne namene določa le (področni) zakon.

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«[17].

2.5. Poglavitne rešitve iz predloga zakona

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

Tako so nekoliko drugače (v skladu z določbami Direktive) 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 predlog zakona sledi zavezujoči ustavni ureditvi iz drugega odstavka 38. in 87. člena Ustave Republike Slovenije, glede načela sorazmernosti pa 2. členu v zvezi s tretjim odstavkom 15. člena Ustave Republike Slovenije. Glede načela poštenosti (v zvezi z načelom preglednosti) 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).

[15] Odločba US, št. U-I-115/92, 24. 12. 1992; objava: Uradni list RS, št. 3/93 in OdlUS I, 105. Sedaj je relevantna tudi odločba Ustavnega sodišča RS iz leta 2019 o načelu upravne zakonitosti (drugi odstavek 120. člena Ustave Republike Slovenije: »Upravni organi opravljajo svoje delo samostojno v okviru in na podlagi ustave in zakonov.«), št. U-I-26/17, U-I-87/16, U-I-105/16, 24. 10. 2019; objava: Uradni list RS, št. 67/19, kjer je navedeno: »50. Po drugi strani splošnih aktov za izvrševanje javnih pooblastil (kot je tudi Metodologija), ki dopolnjujejo in podrobneje izpeljujejo zakonsko določbo, ni mogoče razumeti kot dejavnik, ki bi omogočal do zakonodajalca blažje razumevanje zahtev načela jasnosti in pomenske določljivosti zakonov. Nasprotno stališče bi ogrozilo zagotavljanje jamstev drugega odstavka 120. člena Ustave. Ni ustavno sprejemljivo, da bi se nerazumljivost in nejasnost zakonov (glede materije, ki mora po Ustavi biti zakonsko urejena) odpravljalo z jasnimi in razumljivimi podzakonskimi akti.«

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

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

Znatno je spremenjena definicija splošne privolitve posameznika za obdelavo njegovih 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 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«.

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 dejansko uporabljajo tudi za njih.

Določena je nova ureditev glede drugih (dosedaj: naknadnih) namenov obdelave osebnih podatkov, po predlagani ureditvi in v skladu z Direktivo so drugi (novi) nameni obdelave osebnih podatkov sedaj širši in je upoštevanje prvotnega namena zbiranja in obdelave osebnih podatkov nekoliko manj pomembno, mora pa biti določen nov namen z zakonom.

Za namene izkazovanja skladnosti obdelave osebnih podatkov sta kot obveznost za upravljavce in obdelovalce poleg izvedbe ocene učinkov določena tudi izvajanje ukrepa ti. notranje sledljivosti posredovanj osebnih podatkov in ukrepa ti. zunanje sledljivosti obdelav osebnih podatkov, podobno kot v dosedanjem tretjem odstavku 22. člena ZVOP-1.

Določena je nova ureditev za osebe, ki znotraj upravljavcev (pristojni državni organi Republike Slovenije) 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 so zahtevane delovne izkušnje (praksa) ali poznavanje zakonodaje s področja varstva osebnih podatkov, določajo se namestniki.

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

Natančno je urejeno uveljavljanje pravic posameznika, na katerega se nanašajo osebni podatki, pred pristojnimi organi, na podlagi klasičnega upravnega postopka z določenimi prilagoditvami obravnavanim zadevam (npr, omejitev vpogleda v spis, preverjanje identitete, zavarovanje osebnih podatkov, ki so predmet nadzornega postopka), ko ima zoper odločitve pristojnih organov možnost vložitve pritožbe na nadzorni organ, to je Informacijski pooblaščenec. Posameznik se lahko tudi neposredno obrne na Informacijskega pooblaščenca zaradi uveljavljanja svojih pravic v zvezi z obdelavo njegovih osebnih podatkov pri pristojnem organu, Informacijski pooblaščenec pa v tem primeru vodi klasični upravni postopek po določbah tega zakona, brez preiskovalnih pooblastil, ki jih ima v primeru inšpekcijskega nadzora.

Posameznik, ki meni da so njegove pravice kršene ima po predlaganem zakonu tudi možnost vložitve neposredne prijave pri Informacijskemu pooblaščencu in je v tem postopku prijavitelj s posebnim položajem in nastopa kot stranka, za razliko od postopka po Zakonu o inšpekcijskem nadzoru, kjer prijavitelj nima položaja stranke v postopku. Informacijski pooblaščenec lahko vodi nadzorne postopke tudi v javnem interesu, ki jih uvede ali na lastno pobudo, na podlagi prijave fizične ali pravne osebe ali na pobudi drugih organov.

Predlog zakona pa glede drugi odstavek 9. člena Direktive ne ureja znanstvenega, zgodovinskega in statističnega raziskovanja in arhivskega delovanja, ampak to prepušča področnim zakonskim ureditvam (ZNPPol, ZDT-1, ZVDAGA …).

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.

Področje kazenskega pravosodja in policije ter izvrševanja kazenskih sankcij zahteva, da so ustrezne specifike in izjeme, tako glede namenov obdelav osebnih podatkov kot tudi obveščanja posameznikov o njihovih osebnih podatkih, glede na določbe Direktive urejene specifično.

V področnih ureditvah obdelav osebnih podatkov so npr. delno prenovljeno razdelane določbe o povezovanju , strokovnem nadzoru ipd.

Kazenske določbe določajo manjši, pa vseeno ustrezni nabor prekrškov, pomen zakona je namreč v izvajanju učinkovitega nadzora.

Glede na drugačne definicije iz Direktive je tudi prišlo do znatne spremembe dosedanjega tradicionalnega izrazoslovja s področja varstva osebnih podatkov (ustaljeno od leta 1984[18]).

Tako so sedanji novi temeljni izrazi zlasti:

- zbirka (do sedaj zbirka osebnih podatkov),
- varnost osebnih podatkov (do sedaj zavarovanje osebnih podatkov),
- upravljavec (do sedaj upravljavec osebnih podatkov),
- obdelovalec (do sedaj pogodbeni obdelovalec),
- posebne vrste osebnih podatkov (do sedaj občutljivi osebni podatki),
- prenos osebnih podatkov (dosedanji iznos osebnih podatkov v tretje države),
- 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 predlog zakona zlasti:

- ukinitev Register zbirk osebnih podatkov in dolžnost notifikacije zbirk Informacijskemu pooblaščencu, kar je nadomeščeno z evidenco dejanj obdelav za upravljalce in obdelovalce osebnih podatkov;
- določa olajšan sistem izbire pooblaščene osebe za varstvo osebnih podatkov, enako tudi glede pogojev za njihovo določitev;
- določa definicijo povezovanja zbirk osebnih podatkov – samo veliki sistemi s tveganimi obdelavami osebnih podatkov bodo potrebovali ureditev v področnem zakonu (sodni register, E-Sociala…), Informacijski pooblaščenec ne bo več izdajal odločb o povezovanju.

2.6. Sprejetje zakona

Zakon bi moral biti uveljavljen že 6. 5. 2018, ko je potekel rok za zakonodajno implementacijo Direktive. Zato mora zakon biti čimprej sprejet in objavljen v Uradnem listu Republike Slovenije.

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

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, saj so bila sredstva zagotovljena že v letih 2018 in 2019, sicer v okviru priprav na takratno sprejetje Zakona o varstvu osebnih podatkov (ZVOP-2) oziroma za izvrševanje Splošne uredbe o varstvu podatkov.

Nadalje je za navesti, da je bilo precej predlaganih zakonskih rešitev že dosedaj del pravnega reda Republike Slovenije in jih sedanji predlog zakona le nekoliko nadgrajuje.

Dodatna sredstva ne bodo potrebna niti 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 novih pravnih aktov Evropske unije glede varstva osebnih podatkov. Povezano sicer s Splošno uredbo o varstvu podatkov (oziroma takratnim Predlogom ZVOP-2) so bila ta sredstva že bila vnaprej zagotovljena v letu 2017 za leti 2018 in 2019 (o tem 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 bila zagotovljena dodatna sredstva v državnem proračunu, ki so bila ustrezna. 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 delovnih izkušenj) - 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 preteklo 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 bila tako zagotovljena finančna sredstva skupaj v višini 359.600,00 EUR, tako za Splošno uredbo kot za Direktivo. Dodatna finančna sredstva niso več potrebna. Prav tako je v letu 2018 država Informacijskemu pooblaščenec zagotovila nove poslovne prostore, kar omogoča učinkovito izvajanje njegovih nalog in pristojnosti, zlasti nadzornih nalog.

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

Predlog zakona predstavlja celovito prilagoditev +-pravu Evropske unije, saj gre za predpis, ki v naš pravni red prenaša Direktivo (EU) 2016/680. Predlagani prenos bo tako omogočil policiji ter organom kazenskega pravosodja in izvrševanja kazenskih sankcij da obdelujejo osebne podatke v skladu z določbami Direktive. Prav tako se s tem predlogom zakona v pravni red Republike Slovenije prenaša pravni red prenaša Direktiva (EU) 2016/681 – direktiva glede Evidenc letalskih potnikov[19], v delu, ki se nanaša na poseben položaj pooblaščene osebe za varstvo osebnih podatkov glede evidence letalskih potnikov, ter glede še nekaterih tehničnih vprašanj (npr. poseben rok za hrambo podatkov iz dnevnikov obdelave).

V nadaljevanju je v primerjalno pravni ureditvi prikazana implementacija Direktive (EU) 2016/680.

5.1 Uvodno o primerjalno pravni ureditvi

Med državami članicami, ki so se odločile da direktivo prenesejo z ločenim izvedbenim zakonom, so med drugimi tudi Kraljevina Danska, Republika Hrvaška, Republika Finska, Republika Latvija, Kraljevina Nizozemska, Italijanska republika, Portugalska republika in Republika Litva, ki so, z izjemo Kraljevine Danske, svoje zakone sprejele šele po pričetku veljave direktive. Trend zakonodajnega urejanja izvedbenih zakonov med naštetimi državami članicami izkazuje jasne namere slediti ciljem Direktive (po posodobitvi predpisov, s kar se da hitro in preprosto implementacijo, olajšanjem uporabe za organe pregona, preiskovanja, preprečevanja kaznivih dejanj, možnostjo prilagajanja uporabi novim tehnologijam in zavezanostjo visokim standardom varstva osebnih podatkov in osnovnih človekovih pravic.

Kot poseben primer gre izpostaviti Kraljevino Dansko, ki je že leta 2017 sprejela izvedbeni zakon, ki je bistvenega pomena za nadaljnje sodelovanje Danske v okviru Europola. V njem so tako strogo ločili obdelavo osebnih podatkov s strani organov pregona za kazenske zadeve in obdelavo osebnih podatkov za civilnopravne zadeve po Zakonu o varstvu osebnih podatkov ter Splošni uredbi o varstvu podatkov (ki je začel veljati leto dni kasneje).

V nadaljevanju so tako predstavljeni že sprejeti danski, hrvaški in finski zakon (torej trije sprejeti zakoni držav članic Evropske unije), delno tudi na način, da se izpostavijo cilji predlagateljev iz uradnih obrazložitev predlogov teh zakonov. Prav tako sta izpostavljeni ureditvi Avstrije in Nemčije, ki pa sta uporabili ti. skupni zakonski pristop – skupno ureditev implementacije v enem zakonu za Splošno uredbo in Direktivo.

5.2 Kraljevina Danska

Kraljevina Danska je 27 aprila 2017 sprejela Zakon o obdelavi osebnih podatkov s strani organov pregona, ki je pričel veljati 1. maja 2017. Ministrstvo za pravosodje Kraljevine Danske je ugotovilo, da

[19] Direktiva (EU) 2016/681 je drugače skoraj v celoti prenesena v Zakonu o nalogah in pooblastilih policije.

bi za uspešno implementacijo Direktive le-ta morala biti, kolikor je to mogoče, opravljena v celovitem zakonu, ki zajema obdelavo podatkov za pristojne danske organe, da bi preprečili, preiskovali, odkrivali ali preganjali kazniva dejanja, ali izvrševali kazenske sankcije, vključno s preprečevanjem groženj javni varnosti. Ta pristop ustvarja višjo stopnjo jasnosti za organe pri uporabi področne zakonodaje in vodi tudi k temu, da tovrstni osebni podatki niso več zajeti v zakonu o osebnih podatkih, kadar sodijo v okvir določb tega zakona.

I. del zakona določa vsa področja obdelave osebnih podatkov, ki se delno ali v celoti obdelujejo z avtomatsko obdelavo podatkov in za drugo neavtomatsko obdelavo osebnih podatkov, ki so ali bodo vsebovani v ustreznih evidencah, ko se obdelava izvaja zaradi preprečevanja, preiskovanja, odkrivanja ali pregona kaznivih dejanj ali izvrševanja kazenskih sankcij, vključno z namenom varovanja ali preprečevanja groženj javni varnosti.

II. del zakona določa pravila obdelave osebnih podatkov, vključno z določbami o razlikovanju med osebami, za katere obstaja utemeljen razlog, da so storile ali bodo storile kaznivo dejanje, osebami, obsojene za kaznivo dejanje, žrtvami kaznivega dejanja ali osebe, za katere določena dejstva vzbujajo prepričanje, da so lahko žrtve kaznivega dejanja, in druge osebe v zvezi s kaznivim dejanjem (na primer osebe, ki so lahko poklicane kot priče v preiskavah v zvezi s kaznivimi dejanji ali v kasnejših kazenskih postopkih, osebe, ki lahko dajo informacije o kaznivih dejanjih itd.).

III. del zakona določa pravice posameznika, vključno s pravico do vpogleda, popravka in izbrisa podatkov, IV. del zakona določa obveznosti obdelovalca in upravljavca podatkov, vključno z vodenjem evidenc o obdelavah in vpogledih, oceni učinka in posvetovanje z nadzornimi organi, VII. del zakona določa pravila izmenjave podatkov z drugimi državami, VIII. del določa vlogo, naloge in pristojnosti nadzornega organa, IX. del pa določa pravna sredstva ter sankcije.

5.3 Republika Hrvaška

Republika Hrvaška je 19. julija 2018 sprejela Zakon o varstvu fizičnih oseb v zvezi z obdelavo in izmenjavo osebnih podatkov zaradi preprečevanja, preiskovanja, odkrivanja ali pregona kaznivih dejanj ali izvrševanja kazenskih sankcij, ki je začel veljati 4. avgusta 2018. Ker bi prenos določb direktive v veljavne predpise zahteval spremembo več zakonov, se je vlada Republike Hrvaške odločila, da že v osnutku zadevo uredi na enoten način. Zakon tako določa, da mora biti vsaka obdelava osebnih podatkov zakonita, poštena in pregledna v odnosu do fizičnih oseb, na katere se nanaša, in se izvaja samo za namene, ki jih določa ta zakon. Fizične osebe bi morale biti seznanjene s tveganji, zaščitnimi ukrepi in pravicami v zvezi z obdelavo svojih osebnih podatkov in s tem, kako lahko uveljavljajo svoje pravice. Osebni podatki morajo biti ustrezni in skladni z namenom, za katerega se obdelujejo. Zlasti je treba paziti, da obseg podatkov, ki se zbirajo in obdelujejo, ne presega namena obdelave teh podatkov in da se ne shranjujejo dlje, kot je potrebno za namene, za katere se obdelujejo. Osebne podatke je treba obdelovati le, če namena obdelave ni mogoče razumno doseči z drugimi sredstvi.

I. del zakona v okvirju splošnih določb vsebuje tudi definicije temeljnih pojmov, ki jih uporablja in ki so namenjeni uporabi v okvirju tega zakona, drugi izrazi, ki se uporabljajo v tem zakonu in nimajo pomena, kot je opredeljen v prvem odstavku tega člena, imajo pomen, določen v Splošni uredbi.

II. del zakona določa načela obdelave podatkov, roke hrambe podatkov, razlikovanje med kategorijami podatkov, razlikovanja podatkov in preverjanjem kakovosti osebnih podatkov, posebne pogoje obdelave in posebne vrste osebnih podatkov ter avtomatizirano obdelavo in odločanje.

III. del določa pravice posameznika v postopku, IV. del določa obveznosti obdelovalca in upravljavca podatkov, vključno z vodenjem evidenc o obdelavah in vpogledih, oceni učinka, predhodno posvetovanje z nadzornimi organi ter poročanje nadzornemu organu, varnost obdelave, V. del določa prenos podatkov tretjim državam ali mednarodnim organizacijam, VI. del določa naloge in pooblastila nadzornega organa, VII. del zakona pa ureja pravno varstvo posameznika.

5.4 Republika Finska

Republika Finska je 5. decembra 2018 sprejela Zakon o obdelavi osebnih podatkov v kazenskih zadevah in v povezavi z ohranjanjem nacionalne varnosti[20], ki je pričel veljati 1. januarja 2019. Podobno kot že omenjeni Danska in Hrvaška se je tudi Republika Finska odločila, da Direktivo prenese v ločen in celovit zakon, z namenom nedvoumne ureditve in hitrejše implementacije. Tako je obdelava osebnih podatkov v kazenskih zadevah povsem izključena iz področja uporabe GDPR. Zakon se tako uporablja za preprečevanje ali preiskovanje kaznivih dejanj, začetek obravnave obtožb, začetek pravnih dejanj, obravnavo kazenskih zadev na sodišču, izvrševanje sankcioniranj ali preprečevanje groženj javni varnosti.

I. del zakona določa vsa področja obdelave osebnih podatkov za področje odkrivanja, pregona, preiskovanja in sankcioniranja kaznivih dejanj ter področja varnosti države, ob tem pa določa tudi uporabo avtomatizirane obdelave osebnih podatkov. V 2. členu ureja razmerje zakona do drugih predpisov. II. del določa pravila, načine in namen obdelave osebnih podatkov, razlikovanje med vrstami osebnih podatkov, verifikacijo in izmenjavo osebnih podatkov, obveznosti do razkritja določenih vrst obdelav osebnih podatkov, avtomatsko odločanje. III. del določa pravila za varovanje osebnih podatkov, obveznosti obdelovalca in upravljavca podatkov, evidentiranje obdelave in dostopov. IV. del določa pravice posameznika, čigar podatki se obdelujejo. V. del še dodatno in podrobneje ureja varovanje osebnih podatkov in postopke poročanja. VI. del ureja pristojnosti in naloge pooblaščenca za varstvo podatkov. VII. del ureja izmenjavo osebnih podatkov in njihovo varovanje za namene izmenjave s tretjimi državami ali mednarodnimi organizacijami. VIII. del določa naloge in pristojnosti nadzornega organa ter določa načine komunikacije in posvetovanja za namene obdelave ali varstva osebnih podatkov.

5.5 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)[21]. Sistemski pristop zakona je, da upošteva obstoječo nacionalno pravno ureditev (ustavnopravno), ustaljene rešitve iz področnih zakonov Nemčije ter tradicionalno prakso varstva osebnih podatkov v Nemčiji.

I. del zakona velja za vsa področja obdelave osebnih podatkov, tako tudi za področje nacionalne varnosti, obrambe in pomeni tudi izvedbo določb Direktive. 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 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 izjemoma določi tudi področna zakonodaja. Na ta način je nadgrajen sistem iz 9. člena Splošne uredbe. Ko gre za obdelavo teh podatkov v druge namene, se po uvodnem delu drugega odstavka upošteva tudi področna zakonodaja. 24. člen določa stroga pravila glede obdelave osebnih podatkov v druge namene, in sicer le za potrebe preprečevanja nevarnosti za državno ali javno varnost ali za kazenski pregon[22] ali če je to potrebno za uveljavljanje, izvajanje ali obrambo civilnopravnih

[20] Suomen säädöskokoelma (SK); Number: 1054/2018; objavljen dne 10. 12. 2018
[21] Zakon z dne 30. junija 2017, Bundesgesetzblatt Teil I, 2097.
[22] Zasebni sektor npr. uporablja videonadzor in bi hotel vložiti kazensko ovadbo, saj je ocenil, da obstaja sum storitve kaznivega dejanja.

zahtevkov, če ne prevladujejo interesi posameznika, na katerega se nanašajo osebni podatki, za izključitev obdelave osebnih podatkov. V 35. členu so določene omejitve pravice do izbrisa osebnih podatkov – če bi bil poseg nesorazmeren ali pa gre le za minimalno korist za posameznika.

III. del zakona implementira Direktivo. Določbe v njem, ki so enake ali podobne tistim, ki so v Splošni uredbi ali v predhodnih delih zakona, in izhajajo iz pristopa (kot je določen že v I. delu zakona), po katerem je nacionalnemu zakonodajalcu prepuščeno, kako bo prenesel določbe Direktive,kar pomeni, da lahko uporabi tudi 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, ki so pristojni za nadzor osebnih podatkov na določenih ti. represivnih področjih.

5.6 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)[23].

Sprejeti zakonski okvir zaradi novelacije sledi dotedanji ureditvi varstva osebnih podatkov v Republiki Avstriji. 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 tradicionalno ureditev (po sodni praksi od leta 1951 dalje) 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 določilo mejna starost 14 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 še ni posegla na področje izrekanja (spornih) visokih glob po Splošni uredbi, glede katerih se v Avstriji zatrjuje kršitev človekovih pravic oziroma neustavnost tudi z vidika, da tako visokih glob ne bi smel izrekati nadzorni organ, ki ni sodišče, ampak bo počakala na odločitev Ustavnega sodišča Republike Avstrije v podobnem primeru (visoke globe, ki jih izreka avstrijski Urad za finančni trg). V zvezi z izrekanjem globa je sicer 20. aprila 2018 sprejela novelo navedenega zakona (sprememba Zakona o varstvu osebnih podatkov z zakonskim nazivom: Zakon o deregulaciji varstva osebnih podatkov - Datenschutz-Deregulierungs-Gesetz 2018, BGBl. I Nr. 24/2018) in v njej določila, da se v primeru predpisanih glob za kršitve po Splošni uredbi najprej izrekajo opozorilne sankcije, šele v primeru ponovljenih kršitev pa globe po Splošni uredbi (spremembe 11. člena), prav tako pa je v isti noveli določila, da nosilci javnih pooblastil niso odgovorni za prekrške po Splošni uredbi (spremembe 35. člena).

3. del zakona določa varstvo in obdelavo osebnih podatkov kot del izvedbe določb Direktive.

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

Pristop avstrijskega zakonodajalca je v razmerju do začetnih zakonodajnih ambicij (besedilo predloga zakona v razmerju do končno sprejetega zakona leta 2017 in njegove novele iz leta 2018) pokazal, da ne gre ne za unificiran pristop niti ne za (dovolj) harmoniziran pristop, ampak gre ob upoštevanju

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

nespremenjenih določenih sistemskih rešitev ter novih rešitev in rešitev iz področne zakonodaje dejansko za ti. fragmentacijo pravne ureditve.

II. BESEDILO ČLENOV

I. POGLAVJE
SPLOŠNE DOLOČBE

1. člen
(vsebina)

(1) Ta zakon ureja varstvo posameznikov pri obdelavi osebnih podatkov, ki jih državni organi Republike Slovenije, ki so zakonsko določeni kot pristojni za področja preprečevanja, preiskovanja, odkrivanja ali pregona kaznivih dejanj ali izvrševanja kazenskih sankcij (v nadaljnjem besedilu: pristojni organi), obdelujejo za namene izvrševanja teh pristojnosti.

(2) Ta zakon ureja tudi pogoje za zakonito in pošteno obdelave osebnih podatkov, postopke in načine odkrivanja in preprečevanja nezakonitih posegov v pravice posameznikov, na katere se nanašajo osebni podatki, za učinkovito varstvo teh vrednot pa ureja tudi nadzorna pooblastila in nadzorne ukrepe nadzornega organa ter kaznivost za prekrške glede njihovih kršitev.

(3) S tem zakonom se v pravni red Republike Slovenije prenašata 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 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 (UL L št. 127 z dne 23. 5. 2018, str. 20), (v nadaljnjem besedilu: Direktiva), ki ureja varstvo osebnih podatkov na področju obravnavanja kaznivih dejanj in njihovih storilcev ter pravice posameznikov, na katere se nanašajo osebni podatki, ter Direktiva (EU) 2016/681 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o uporabi podatkov iz evidence podatkov o potnikih (PNR) za preprečevanje, odkrivanje, preiskovanje in pregon terorističnih in hudih kaznivih dejanj (UL L št. 119 z dne 4. 5. 2016, str. 132), v delu, ki se nanaša na položaj in naloge pooblaščenih oseb za varstvo osebnih podatkov.

2. člen
(prepoved diskriminacije glede obdelave osebnih podatkov)

Obdelava osebnih podatkov na podlagi nedopustne diskriminacije 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 posameznice ali posameznika (v nadaljnjem besedilu: posameznik) je prepovedana.

3. člen
(področje uporabe)

Določbe tega zakona se uporabljajo 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 izvajajo z avtomatiziranimi sredstvi.

4. člen
(pomen izrazov)

Izrazi, uporabljeni v tem zakonu, 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. »upravljavec« pomeni pristojni organ, ki sam ali skupaj z drugimi določa sredstva obdelave osebnih podatkov; upravljavec je določen z zakonom; zakon določi tudi namen obdelave osebnih podatkov;

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

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

10. »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;

11. »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;

12. »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;

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

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

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

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

17. »nadzornik« pomeni državno nadzornico ali državnega nadzornika za varstvo osebnih podatkov, kot ga določa zakon, ki ureja Informacijskega pooblaščenca;

18. »nadzorne osebe« pomenijo informacijskega pooblaščenca in nadzornike, kadar izvajajo nadzor po določbah tega zakona;

19. »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;

20. »izbris« pomeni trajno odstranitev ali uničenje osebnega podatka, tako da ga ni več mogoče obnoviti;

21. »anonimiziranje« pomeni takšno spremembo osebnih podatkov, da jih ni več mogoče povezati z določenim ali določljivim posameznikom ali je to mogoče le z nesorazmerno velikimi napori, stroški ali porabo časa; tako anonimizirani podatki pa ne veljajo za osebne podatke po tem zakonu;

22. »blokiranje« pomeni takšno označitev ali izločitev osebnih podatkov, da se omeji ali prepreči njihova nadaljnja obdelava, blokirani podatki pa veljajo za osebne podatke po tem zakonu;

23. »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, katere se upravljajo pri enem upravljavcu;

24. »kazenska zadeva sodišča« pomeni kazensko zadevo iz pristojnosti sodišča s splošno pristojnostjo, kot jo določa zakon, ki ureja sodišča, in o kateri odloča sodišče v skladu z zakoni, ki urejajo sodne postopke;

25. »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.

5. člen
(načela varstva osebnih podatkov)

(1) Osebni podatki:

1. se obdelujejo zakonito, pošteno in na pregleden način za posameznika, 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) Pristojni organ je odgovoren za skladnost svojih obdelav osebnih podatkov z določbami prejšnjega odstavka in mora biti to skladnost tudi zmožen izkazati (odgovornost).

6. člen
(zakonitost obdelave)

(1) Obdelava osebnih podatkov za namene iz prvega odstavka 1. člena tega zakona je zakonita le, če je potrebna in v obsegu, v katerem je potrebna za opravljanje nalog pristojnih organov, določenih z zakonom, in če vrste osebnih podatkov, kategorije posameznikov, na katere se ti osebni podatki nanašajo, namen obdelave ter rok hrambe ali rok za reden pregled potrebe po hrambi določa zakon.

(2) Pristojni organi lahko obdelujejo tudi osebne podatke posameznika, ki je podal privolitev za obdelavo svojih osebnih podatkov za enega ali več namenov iz prvega odstavka 1. člena tega zakona, če takšno možnost, namen obdelave in vrste osebnih podatkov, ki naj se obdelujejo, določa zakon.

(3) Pristojni organi lahko za namene iz prvega odstavka 1. člena tega zakona obdelujejo tudi osebne podatke posameznika, če jih posameznik javno objavi ali naredi javno dostopne brez očitnega ali izrecnega namena omejitve dostopa do podatkov na določen ožji krog oseb. Obdelava je dopustna le v okviru posamezne konkretne zadeve.

(4) Pristojni organi lahko ne glede na namene iz prvega odstavka 1. člena tega zakona obdelujejo osebne podatke, ki so nujno potrebni za varovanje življenjskih interesov posameznika, zlasti življenja ali telesa ali zdravja posameznika, na katerega se osebni podatki nanašajo, ali druge osebe. Po izvedeni obdelavi je pristojni organ dolžan napisati poročilo z navedbo razlogov za obdelavo in obsegom obdelanih osebnih podatkov. Poročilo je na razpolago posamezniku, na katerega se nanašajo osebni podatki, in nadzornemu organu.

7. člen
(zakonitost obdelave posebnih vrst osebnih podatkov)

(1) Obdelava posebnih vrst osebnih podatkov s strani pristojnih organov je prepovedana.

(2) Obdelava posebnih vrst osebnih podatkov s strani pristojnih organov je ne glede na določbo prejšnjega odstavka zakonita, če je skladna z določbami prejšnjega člena in če:

1. je nujno potrebna za opravljanje nalog pristojnih organov, določenih z zakonom, in

2. je zagotovljeno ustrezno varstvo človekovih pravic ali temeljnih svoboščin posameznika, na katerega se nanašajo osebni podatki.

8. člen
(obdelava osebnih podatkov za druge namene)

(1) Obdelava osebnih podatkov s strani istega ali drugega pristojnega organa za druge namene obdelave od tistih, za katere so bili podatki pridobljeni, je dovoljena, če ti nameni obdelave spadajo med namene iz prvega odstavka 1. člena tega zakona in če tako določa zakon.

(2) Osebni podatki, ki jih pristojni organi zbirajo za namene iz prvega odstavka 1. člena tega zakona, se ne obdelujejo za druge namene, kot so nameni iz prvega odstavka 1. člena tega zakona, razen če to dovoljuje zakon. V tem primeru za obdelavo veljajo določbe Splošne uredbe o varstvu podatkov oziroma zakona, ki ureja varstvo osebnih podatkov, oziroma drugih zakonov.

9. člen
(avtomatizirano odločanje in oblikovanje profilov)

(1) Odločanje, ki temelji izključno na avtomatizirani obdelavi osebnih podatkov, vključno z oblikovanjem profilov, ki ima lahko negativen pravni učinek na posameznika, na katerega se nanašajo osebni podatki, ali ga lahko bistveno prizadene, je prepovedano, razen če to določeno z zakonom, ki določa zlasti pravico posameznika, da zahteva ponovni in ročni pregled odločitve s strani fizične osebe pri pristojnem organu ter da do odločitve izrazi lastno stališče, ali določa druge ustrezne ukrepe za zagotavljanje ustreznega varstva človekovih pravic in temeljnih svoboščin, ki jih mora izvesti pristojni organ.

(2) Odločitve iz prejšnjega odstavka ne smejo temeljiti na obdelavah 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 avtomatizirano odločanje, mora pristojni predlagatelj zakona izvesti oceno učinka iz 49. člena tega zakona.

(4) Oblikovanje profilov v okviru avtomatizirane ali drugačne obdelave posebnih vrst osebnih podatkov, ki ima za posledico diskriminacijo posameznikov, na katere se nanašajo osebni podatki, je prepovedano.

10. člen
(sodno varstvo)

(1) Posameznik, ki meni, da določena obdelava njegovih osebnih podatkov s strani pristojnega organa ali obdelovalca krši določbe tega zakona ali drugih zakonov, ki urejajo obdelavo ali varstvo osebnih podatkov za namene iz prvega odstavka 1. člena tega zakona, lahko zahteva sodno varstvo svojih pravic ves čas, dokler kršitev traja.

(2) Če je kršitev iz prejšnjega odstavka prenehala, lahko posameznik s tožbo zahteva ugotovitev, da je kršitev obstajala.

(3) Posameznik lahko s sodnim varstvom po določbah tega člena zahteva prenehanje kršitve, vzpostavitev zakonitega stanja oziroma odškodnino.

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

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

(6) Sodišče v postopku odloči najpozneje v šestih mesecih.

11. člen
(zastopanje s strani nevladnih organizacij)

Posameznik, na katerega se nanašajo osebni podatki, lahko pisno pooblasti nevladno organizacijo s področja varstva človekovih pravic in temeljnih svoboščin, ki ima status nevladne organizacije v javnem interesu, da v njegovem imenu glede obdelav njegovih osebnih podatkov uveljavlja sodno varstvo ali vloži pritožbo ali prijavo po določbah tega zakona.

II. POGLAVJE
PRAVICE POSAMEZNIKA, POSTOPEK TER IZVAJANJE NADZORA
1. oddelek – skupne določbe

12. člen
(uveljavljanje pravic pred pristojnim organom, obdelovalcem ali nadzornim organom)

(1) Posameznik, na katerega se nanašajo osebni podatki, lahko uveljavlja svoje pravice iz tega zakona pred pristojnim organom, v primeru iz petega odstavka 42. člena tega zakona pa pred obdelovalcem.

(2) Ne glede na prejšnji odstavek lahko posameznik, na katerega se nanašajo osebni podatki, svoje pravice iz tega zakona uveljavlja tudi pred nadzornim organom, kadar so dostop do osebnih podatkov ali pravica do popravka ali izbrisa omejene na podlagi prvega odstavka 23. člena tega zakona..

13. člen
(omejitve vpogleda v spis)

(1) V postopkih uveljavljanja pravic po prejšnjem členu tega zakona do dokončnosti odločitve posameznik nima pravice do pregledovanja osebnih podatkov ali dokumentacije, ki je predmet zahteve, iz katerih bi se dalo razbrati ali sklepati na vsebino obdelovanih osebnih podatkov, če bi to lahko glede na okoliščine konkretne zadeve škodovalo izvedbi uradnih postopkov ali varstvu ali uresničevanju človekovih pravic in temeljnih svoboščin tretjih oseb..

(2) Po dokončnosti odločitve lahko posameznik pregleda zadevo v obsegu, dovoljenem z odločitvijo pristojnega organa ali odločitvijo nadzornega organa.

14. člen
(preverjanje identitete posameznika)

Če pristojni organ oziroma nadzorni organ opravičeno dvomi o identiteti posameznika, ki je vložil zahtevo, pritožbo ali prijavo, lahko od njega zahteva dodatne informacije, ki so potrebne za potrditev njegove identitete, ali v skladu z 59. členom tega zakona zahteva vpogled v njegov uradni identifikacijski dokument. Osebne podatke, ki jih pridobi pri tem, lahko obdeluje le za ta namen in jih sme hraniti dve leti od zaključka obdelave, za namen izkazovanja skladnosti obdelave s tem zakonom.

15. člen
(zavarovanje osebnih podatkov, ki so predmet postopka)

(1) Pristojni organ od seznanitve z uvedbo postopka po tem poglavju ne sme izbrisati, spremeniti ali odsvojiti zahtevanih osebnih podatkov, ki so predmet postopka, ne glede na potek rokov hrambe, dokler o zadevi ni pravnomočno odločeno.

(2) Nadzorna oseba lahko ob upoštevanju okoliščin konkretnega postopka odredi drugačen način zavarovanja dokazov, zlasti izdelavo kopije osebnih podatkov ali postopkov obdelave.

16. člen
(izvršba)

(1) Izvršba izvršljive odločbe nadzornega organa se opravlja po postopku, kot ga določa zakon, ki ureja splošni upravni postopek, če ta zakon ne določa drugače.

(2) Za izvršbo je pristojen nadzorni organ.

(3) Izvršba se opravi na zahtevo posameznika, na katerega se nanašajo osebni podatki, na podlagi izvršljive odločbe in sklepa o dovolitvi izvršbe, in sicer s prisilitvijo zoper pristojni organ ali drugega upravljavca. Denarna kazen bremeni odgovorno osebo pristojnega organa ali drugega upravljavca, ki ni izvršila odločbe nadzornega organa.

(4) Če je potrebno izvršiti odločbo v inšpekcijskem nadzoru v javnem interesu, nadzorni organ uvede izvršbo po uradni dolžnosti.

(5) Zoper sklep o dovolitvi izvršbe ni dovoljena pritožba, dopusten pa je upravni spor.

2. oddelek – pravice posameznika in postopek pri pristojnem organu

17. člen
(uporaba določb zakona, ki ureja splošni upravni postopek)

Za vprašanja postopka uveljavljanja pravic posameznika, na katerega se nanašajo osebni podatki, po tem oddelku se uporabljajo določbe zakona, ki ureja splošni upravni postopek, če ta zakon ne določa drugače.

18. člen
(uresničevanje pravic na podlagi drugih zakonov)

Kadar drug zakon določa uresničevanje pravic iz 7., 8. in 9. točke prvega odstavka 21. člena ter 22. in 24. člena tega zakona v kazenski zadevi sodišča, posameznik, na katerega se nanašajo osebni podatki, uresničuje te pravice le v obsegu in na način, kot je določeno s tem drugim zakonom.

19. člen
(komunikacija s posameznikom, na katerega se nanašajo osebni podatki)

(1) Pristojni organ posamezniku, na katerega se nanašajo osebni podatki, vse splošne informacije o obdelavi (21. člen tega zakona) ter vsa sporočila v zvezi z uveljavljanjem njegovih pravic (22. do 24. člen tega zakona) zagotovi v jedrnati, razumljivi in lahko dostopni obliki ter jasnem in preprostem jeziku. Pristojni organ lahko te informacije oziroma komunikacije posamezniku posreduje na vse ustrezne načine, vključno z elektronsko obliko, pri čemer jih praviloma posreduje v obliki, v kateri je bila zahteva vložena.

(2) Pristojni organ posamezniku, na katerega se nanašajo osebni podatki, olajša uresničevanje njegovih pravic, zlasti tako, da pripravi obrazce za uveljavljanje pravic.

(3) Pristojni organ posamezniku, na katerega se nanašajo osebni podatki, brezplačno zagotovi:

1. splošne informacije, ukrepe in sporočila iz prvega odstavka tega člena;

2. izvedbo ustreznih ukrepov iz prvega odstavka 9. člena tega zakona;

3. uveljavljanje pravic iz drugega odstavka 12. člena tega zakona;

4. uresničevanje pravic iz 18. člena ter

5. dajanje ustreznih sporočil o kršitvah iz 53. člena tega zakona.

20. člen
(ravnanje z očitno neutemeljeno ali pretirano zahtevo)

(1) Pristojni organ v primeru, da je zahteva posameznika, na katerega se nanašajo osebni podatki, že glede na informacije ali podatke v njej, očitno neutemeljena, zavrne obravnavo zahteve.

(2) Pristojni organ v primeru, da so zahteva ali zahteve posameznika pretirane, zlasti zato, ker se ponavljajo, zavrne obravnavo zahteve ali ne glede na tretji odstavek prejšnjega člena predhodno naloži plačilo materialnih stroškov posredovanja informacij, sporočila ali odgovora oziroma priprave, kopije ali izpisa na zahtevo posameznika.

(3) Pristojni organ plačila stroškov iz prejšnjega odstavka posamezniku ne naloži, če ti ne presegajo 20 eurov (z vključenim davkom na dodano vrednost).

(4) Pristojni organ nosi breme izkazovanja očitne neutemeljenosti ali pretiranosti zahteve ali zahtev ter višine stroškov.

(5) Minister, pristojen za pravosodje, po posvetovanju z nadzornim organom izda pravilnik, s katerim predpiše zaračunavanje materialnih stroškov iz drugega odstavka tega člena, in ga objavi v Uradnem listu Republike Slovenije.

21. člen
(dajanje splošnih informacij)

(1) Pristojni organ da na razpolago najmanj naslednje splošne informacije:

1. naziv in kontaktne podatke pristojnega organa;

2. kontaktne podatke pooblaščene osebe za varstvo osebnih podatkov iz četrtega odstavka 55. člena tega zakona;

3. o namenih obdelave osebnih podatkov;

4. o pravici do vložitve pritožbe in prijave pri nadzornem organu ter njegove kontaktne podatke;

5. o pravici, da od pristojnega organa zahteva dostop do osebnih podatkov in popravek ali izbris osebnih podatkov in omejitev obdelave osebnih podatkov;

6. pravno podlago obdelave;

7. rok hrambe ali rok za reden pregled potrebe po hrambi;

8. če so informacije o tem na razpolago, kategorije uporabnikov osebnih podatkov, vključno z uporabniki v tretjih državah ali mednarodnih organizacijah;

9. če je to potrebno zaradi uresničevanja pravic posameznikov, na katere se nanašajo osebni podatki, še dodatne informacije, zlasti če so bili osebni podatki pridobljeni brez vednosti posameznikov, na katere se nanašajo.

(2) Informacije iz prejšnjega odstavka ne vključujejo podatkov o konkretnih obdelavah osebnih podatkov posameznika.

(3) Pristojni organ informacije iz 1. do 6. točke prvega odstavka tega člena tudi javno objavi.

22. člen
(pravica do dostopa do osebnih podatkov)

(1) Posameznik, na katerega se nanašajo osebni podatki, ima pravico od pristojnega organa na svojo zahtevo prejeti podatek o tem, ali se obdelujejo njegovi osebni podatki, ter kopijo ali izpis teh podatkov.

(2) Če se obdelujejo njegovi osebni podatki, ima posameznik pravico pridobiti tudi konkretne 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 23. člena tega zakona pa se lahko navede le okvirni opis uporabnikov;

4. roku hrambe ali roku za reden pregled potrebe po hrambi;

5. obstoju pravice zahtevati popravek ali izbris podatkov ali omejitev obdelave;

6. obstoju pravice do vložitve pritožbe ali prijave pri nadzornem organu in njegovih kontaktnih podatkih;

7. vseh razpoložljivih informacijah o viru osebnih podatkov, razen če je identiteta vira varovana kot tajna ali zaupna po določbah zakona.

(3) Pristojni organ posamezniku iz razloga po 1. ali 2. točki prvega odstavka 23. člena tega zakona ne zagotovi informacij iz prejšnjega odstavka, kadar bi se s tem razkrila identiteta oseb, zoper katere se izvajajo prikriti preiskovalni ukrepi po zakonu, ki ureja kazenski postopek, ali zoper katere so razpisani ukrepi prikritega evidentiranja in namenske kontrole po zakonu, ki ureja naloge in pooblastila policije.

(4) Pristojni organ o zahtevi odloči brez nepotrebnega odlašanja, najpozneje pa v tridesetih dneh po prejemu zahteve. Odločitev vsebuje tudi pouk o pravici do pritožbe pri nadzornem organu.

23. člen
(omejitve pravice do dostopa do osebnih podatkov)

(1) Pravica posameznika do dostopa do lastnih osebnih podatkov se lahko z zakonom delno ali popolnoma omeji glede posameznih obdelav ali posameznih kategorij obdelav, če in dokler je to nujno in sorazmerno:

1. da se onemogoči oviranje ali vplivanje na uradne postopke, katerih nameni so določeni v prvega odstavka 1. členu tega zakona;

2. da se onemogoči oviranje ali vplivanje na druge uradne postopke, povezane s prejšnjo točko;

3. zaradi zagotavljanja javne varnosti;

4. zaradi zagotavljanja varnosti države ali obrambe države;

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

(2) Pristojni organ brez nepotrebnega odlašanja, najpozneje pa v petnajstih dneh od prejema zahteve, odloči o zavrnitvi ali omejitvi dostopa in razlogih za to. Ta rok lahko organ po potrebi s sklepom podaljša za največ petnajst dni ob upoštevanju zapletenosti zahteve oziroma števila zahtev. Odločba vsebuje tudi pouk o pravici do pritožbe pri nadzornem organu.

(3) Pristojni organ v odločbi iz prejšnjega odstavka ne navede konkretnih razlogov za zavrnitev ali omejitev dostopa, če bi to ogrozilo izvrševanje namena zavrnitve ali omejitve dostopa iz prvega odstavka tega člena.

(4) Pristojni organ z uradnim zaznamkom zabeleži dejansko stanje oziroma pravne razloge, na katerih temelji odločitev iz prejšnjega odstavka, ki mora vsebovati tudi številko zadeve, na katero se nanaša, in podpis uradne osebe. Uradni zaznamek je na podlagi zahteve zaradi opravljanja nalog v konkretni zadevi dostopen pooblaščeni osebi za varstvo osebnih podatkov pristojnega organa in nadzornemu organu

(5) Kadar gre za vprašanje, ali se v zvezi s posameznikom izvajajo ali ne izvajajo prikriti preiskovalni ukrepi iz zakona, ki ureja kazenski postopek, ali ukrepi prikrite in namenske kontrole iz zakona, ki ureja naloge in pooblastila policije, pristojni organ ne razkrije morebitne obdelave osebnih podatkov ali morebitne omejitve dostopa do njih.

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

(1) Posameznik, na katerega se nanašajo osebni podatki, ima pravico od pristojnega organa zahtevati popravek oziroma dopolnitev svojih netočnih oziroma nepopolnih osebnih podatkov. Pristojni organ brez nepotrebnega odlašanja, najpozneje pa v petnajstih dneh od prejema zahteve, popravi netočne osebne podatke ali dopolni nepopolne osebne podatke in o tem obvesti posameznika. Rok se lahko po potrebi s sklepom podaljša za največ petnajst dni ob upoštevanju zapletenosti zahteve in števila zahtev. Če nepopolnih osebnih podatkov ni možno ali dopustno dopolniti, jim lahko pristojni organ priloži dopolnilno izjavo posameznika, na katerega se nanašajo osebni podatki.

(2) Posameznik, na katerega se nanašajo osebni podatki, ima pravico od pristojnega organa zahtevati, da izbriše njegove osebne podatke, če obdelava krši določbe 6., 7. ali 8. člena tega zakona ali če je treba osebne podatke izbrisati za izpolnitev pravne obveznosti, ki velja za pristojni organ. Pristojni organ brez nepotrebnega odlašanja, najpozneje pa v petnajstih dneh od prejema zahteve, izbriše te podatke. Ta rok se lahko po potrebi s sklepom podaljša za največ petnajst dni ob upoštevanju zapletenosti zahteve in števila zahtev.

(3) Pristojni organ v primerih kršitev določb ali izpolnitve pravne obveznosti iz prejšnjega odstavka z odločbo zavrne zahtevo za izbris in omeji obdelavo, če:

1. posameznik, na katerega se osebni podatki nanašajo, izpodbija točnost ali posodobljenost osebnih podatkov in točnosti ali posodobljenosti ni mogoče preveriti ali

2. je treba osebne podatke še nadalje hraniti za namene dokazovanja.

(4) Pristojni organ v odločbi iz prejšnjega odstavka pod pogoji iz prvega, tretjega ali petega odstavka prejšnjega člena ne navede razlogov za zavrnitev. Kadar pristojni organ to omejitev pozneje prekliče, o tem nemudoma obvesti posameznika, na katerega se nanašajo osebni podatki.

(5) Pristojni organ sporoči popravek nepravilnih osebnih podatkov upravljavcu, s strani katerega je prejel te osebne podatke.

(6) V primerih popravka, izbrisa podatkov ali omejitve obdelave pristojni organ obvesti vse uporabnike osebnih podatkov. Uporabniki osebne podatke, ki jih v okviru svojih pristojnosti obdelujejo, nemudoma popravijo, izbrišejo, ustrezno označijo ali omejijo njihovo obdelavo.

(7) Pristojni organ v odločitev po tem členu, s katero ne ugodi zahtevku v celoti, vključi tudi pouk o pravici do pritožbe pri nadzornem organu.

25. člen
(pravna sredstva)

(1) O pritožbi posameznika, na katerega se nanašajo osebni podatki, zoper odločitev pristojnega organa odloča nadzorni organ kot organ druge stopnje.

(2) Zoper odločitev nadzornega organa, s katero se postopek konča, ni pritožbe, je pa dopusten upravni spor. Sklepe, izdane v postopku pred nadzornim organom po tem oddelku, se sme izpodbijati samo v upravnem sporu zoper končno odločitev.

(3) Tožbo v upravnem sporu lahko vložita tako posameznik, na katerega se nanašajo osebni podatki, kot pristojni organ.

3. oddelek – inšpekcijski nadzor

1. pododdelek – skupne določbe

26. člen
(splošna pravila postopka)

V postopkih inšpekcijskega nadzora v interesu prijavitelja s posebnim položajem ter inšpekcijskega nadzora v javnem interesu po tem oddelku se uporabljajo določbe zakona, ki ureja inšpekcijski nadzor, če ta zakon ne določa drugače.

27. člen
(izvajanje postopkovnih dejanj brez prisotnosti)

(1) V postopku inšpekcijskega nadzora lahko nadzorni organ zaslišuje osebe pri pristojnem organu in priče brez prisotnosti prijavitelja, v celoti ali deloma, če je takšna prisotnost v nasprotju z javnim interesom ali interesom tretjih oseb, o čemer obvesti prijavitelja. V takem primeru nadzorni organ tudi ne dovoli prisotnosti pri drugih dejanjih v postopku in mu ne vroča zapisnikov o teh dejanjih.

(2) Nadzorni organ v primerih iz tretjega odstavka 22. člena in petega odstavka 23. člena tega zakona zaslišuje osebe pri pristojnem organu brez prisotnosti prijavitelja in ne dovoli njegove prisotnosti pri drugih dejanjih v postopku ter mu ne vroča zapisnikov o teh dejanjih.

28. člen
(izključitev stranske udeležbe)

V postopku inšpekcijskega nadzora ni dopustna stranska udeležba, kot jo določa zakon, ki ureja splošni upravni postopek.

29. člen
(nadzorna pooblastila v inšpekcijskih postopkih)

(1) Nadzorna pooblastila pri izvajanju inšpekcijskih nadzorov so:

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

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

3. vstop in pregled prostora, zemljišča, prevoznih sredstev ter opreme in sredstev za obdelavo osebnih podatkov (v nadaljnjem besedilu: prostori in oprema), v oziroma s katerimi pristojni organ ali obdelovalec sam ali drug poslovni subjekt ali posameznik po njunem pooblastilu opravlja obdelavo osebnih podatkov, za katero izhaja verjetnost kršitve določb zakona, podzakonskih predpisov ali splošnih aktov za izvrševanje javnih pooblastil za namene iz prvega odstavka 1. člena tega zakona;

4. zavarovanje in pregled elektronskih in z njimi povezanih naprav ter nosilcev elektronskih podatkov, vključno s preko omrežja dosegljivimi informacijskimi sistemi, na katerih so shranjeni podatki (v nadaljnjem besedilu: elektronska naprava), za katere je verjetno, da se na njih nahajajo podatki, glede katerih izhaja verjetnost kršitve določb zakona, podzakonskih predpisov ali drugih splošnih aktov za izvrševanje javnih pooblastil za namene iz prvega odstavka 1. člena tega zakona;

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

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

7. zaseg predmetov ter poslovnih knjig in druge dokumentacije za največ 10 delovnih dni, če je to potrebno za izvedbo postopka, o čemer se izda potrdilo o zasegu, ki vsebuje navedbo zaseženih predmetov in njihov opis, navedbo kraja, kjer so bili najdeni, ter navedbo razloga za zaseg;

8. druga pooblastila, določena z drugim zakonom.

(2) Če pristojni organ ali obdelovalec ne dovoli izvedbe pregleda skritih predelov prostorov in opreme ali zavarovanje in pregled elektronskih naprav, lahko nadzorni organ pregled izvede po predhodni pridobitvi pisne odredbe sodišča. O predlogu za izdajo odredbe iz prejšnjega stavka preiskovalni sodnik pri Okrožnem sodišču v Ljubljani odloči najpozneje v 48 urah od prejema predloga nadzorne osebe.

(3) V primerih iz prejšnjega odstavka, ko pristojni organ ali obdelovalec ne dovoli izvedbe ukrepov pregleda ali zavarovanja, nadzorna oseba odredi začasno zapečatenje oziroma blokiranje ustreznega predela prostorov in opreme ali elektronske naprave, tako da se lahko ohranijo možni dokazi in le za čas, dokler ni izdana ustrezna sodna odredba oziroma do poteka roka za njeno izdajo. Če pristojni organ ali obdelovalec ne dovolita izvedbe ukrepov pregleda ali zavarovanja, morata nadzorni osebi utemeljiti očitno verjetnost, da bi lahko prišlo do posega v pravice do njune prostorske ali komunikacijske zasebnosti. Če nadzorna oseba še pred začetkom izvajanja ukrepa oceni, da bi lahko prišlo do posega iz prejšnjega stavka, to navede v predlogu za izdajo pisne sodne odredbe ter 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 pristojni organ ali obdelovalec kršil ali krši določbe zakona, podzakonskih predpisov ali drugih splošnih aktov za izvrševanje javnih pooblastil za namene iz prvega odstavka 1. člena tega zakona, in je verjetno, da se bodo pri pregledu prostorov in 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 in 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, in

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

(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. Predstavnika pristojnega organa ali obdelovalca 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 se sestavi zapisnik, ki se lahko ne glede na določbe zakonov, ki urejata splošni upravni in inšpekcijski postopek, kadar ne gre za nujne in neodložljive ukrepe, sestavi najpozneje v 10 dneh od dneva opravljenega nadzora ter se vroči pristojnemu organu ali obdelovalcu ali predstavnikom pristojnega organa ali obdelovalca. Zapisnik poleg sestavin iz zakona, ki ureja splošni upravni postopek, vsebuje ugotovljeno dejansko stanje, ki vključuje dejstva in okoliščine, pomembne za odločbo. Pristojni organ ali obdelovalec lahko na zapisnik podata pripombe ter se o ugotovljenih dejstvih in okoliščinah pisno ali ustno izjavita v roku, ki ga določi nadzorni organ in ne sme biti krajši od dveh delovnih dni po vročitvi zapisnika, o čemer se ju v zapisniku izrecno pouči. Določbe prejšnjega stavka ne veljajo za zapisnike, ki vsebujejo vsebine glede nujnih in neodložljivih ukrepov.

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

30. člen
(inšpekcijski ukrepi)

(1) Kadar se pri opravljanju inšpekcijskega nadzora ugotovi kršitev določb zakona, podzakonskih predpisov ali splošnih aktov za izvrševanje javnih pooblastil za namene iz prvega odstavka 1. člena tega zakona, v delih, ki urejajo varstvo osebnih podatkov, sme nadzorni organ odrediti naslednje inšpekcijske ukrepe:

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

2. odrediti prepoved obdelave osebnih podatkov, če niso zagotovljeni ali se ne izvajajo predpisani ukrepi in postopki za varnost osebnih podatkov;

3. odrediti omejitve obdelave, kot so anonimiziranje, blokiranje ali arhiviranje;

4. odrediti prepoved prenosa osebnih podatkov v tretjo državo ali njihovega posredovanja tujim uporabnikom osebnih podatkov, če se iznašajo ali posredujejo v nasprotju z določbami zakona;

5. odrediti prepoved obdelave osebnih podatkov, kot so tudi brisanje ali uničenje osebnih podatkov;

6. odrediti druge ukrepe, določene z zakonom, ki ureja inšpekcijski nadzor.

(2) Z ukrepi po prejšnjem odstavku se ne sme posegati v kazenske zadeve sodišča in zadeve Ustavnega sodišča Republike Slovenije, kadar obravnava kazenske zadeve sodišča.

2. pododdelek – inšpekcijski nadzor v interesu prijavitelja s posebnim položajem

31. člen
(prijava in prijavitelj s posebnim položajem)

(1) Posameznik, ki pri nadzornem organu vloži prijavo, ker meni, da obdelava osebnih podatkov, ki jo izvaja pristojni organ v zvezi z njim, krši zakon, podzakonske predpise ali druge splošne akte za izvrševanje javnih pooblastil za namene iz prvega odstavka 1. člena tega zakona, je prijavitelj s posebnim položajem.

(2) V postopku pred nadzornim organom ima prijavitelj s posebnim položajem položaj stranke.

(3) Nadzorni organ postopek vodi v interesu prijavitelja s posebnim položajem.

32. člen
(posebna pravila postopka)

(1) V primeru prijave prijavitelja s posebnim položajem nadzorni organ vedno uvede postopek inšpekcijskega nadzora, če prijava vsebuje sestavine, kot jih za vlogo določa zakon, ki ureja splošni upravni postopek.

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

(3) Ne glede na določbo prvega odstavka tega člena nadzorni organ prijavo v roku enega meseca zavrne z odločbo, če je že glede na informacije ali podatke v njej očitno neutemeljena.

(4) Vir prijave ni tajen.

33. člen
(pravice prijavitelja s posebnim položajem)

(1) Nadzorni organ prijavitelja s posebnim položajem na njegovo zahtevo obvešča o svojih ukrepih.

(2) Prijavitelj ima pravico podati pripombe na osnutek odločbe nadzornega organa, razen glede odločbe iz tretjega odstavka prejšnjega člena, do katerih se nadzorni organ opredeli v odločbi. Nadzorni organ prijavitelju s posebnim položajem s sklepom določi primeren rok za podajo pripomb.

34. člen
(položaj pristojnih organov)

(1) Pri izvajanju nadzora nad pristojnim organom ima pristojni organ položaj zavezanca po določbah zakona, ki ureja inšpekcijski nadzor, če ta zakon ne ureja drugače.

(2) Pristojni organ lahko poda pripombe na osnutek odločbe nadzornega organa, do katerih se mora nadzorni organ opredeliti. Nadzorni organ pristojnemu organu s sklepom določi primeren rok za podajo pripomb.

(3) Pristojni organ, njegove odgovorne ali druge pooblaščene osebe morajo v postopku po tem pododdelku govoriti resnico in ne smejo ničesar zamolčati, njihove izjave pa se lahko štejejo kot izjave strank.

(4) Podatki in informacije ter izjave, pridobljene na podlagi prejšnjega odstavka, se ne morejo uporabiti v postopku odločanja o prekršku.

35. člen
(odločba)

(1) Odločba v postopku inšpekcijskega nadzora po tem pododdelku poleg sestavin, ki jih določa zakon, ki ureja splošni upravni postopek, vsebuje:

1. ugotovitev o obstoju ali neobstoju zatrjevane kršitve obdelave osebnih podatkov prijavitelja s posebnim položajem v trenutku vložitve prijave;

2. ukrepe, odrejene pristojnemu organu glede obdelave osebnih podatkov, ki se nanašajo na prijavitelja s posebnim položajem, in rok za njihovo izvedbo;

3. dovoljen obseg pregleda spisa zadeve za prijavitelja s posebnim položajem.

(2) Ne glede na prejšnji odstavek odločba ne obsega razlogov za zavrnitev ali omejitev dostopa, če bi to ogrozilo izvrševanje namena zavrnitve ali omejitve dostopa iz prvega odstavka 23. člena tega zakona. Odločba v skladu s petim odstavkom 23. člena tega zakona tudi ne obsega navedb, s katerimi

bi se potrdilo ali zanikalo izvajanje ali neizvajanje prikritih preiskovalnih ukrepov iz zakona, ki ureja kazenski postopek, ali prikritih in namenskih kontrol iz zakona, ki ureja naloge in pooblastila policije.

(3) Odločba postane izvršljiva z vročitvijo.

(4) Zoper odločbo in sklepe v postopku pred nadzornim organom po tem pododdelku ni pritožbe, je pa dopusten upravni spor zoper odločitve, s katerimi je postopek končan. Tožbo v upravnem sporu lahko vložita tako prijavitelj s posebnim položajem kot zavezanec.

36. člen
(ukrepanje glede obdelav osebnih podatkov drugih posameznikov)

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

3. pododdelek – inšpekcijski nadzor v javnem interesu

37. člen
(uvedba inšpekcijskega nadzora v javnem interesu)

(1) Nadzorni organ inšpekcijski nadzor uvede na lastno pobudo, na pobudo drugih organov iz 38. člena tega zakona, na podlagi prijave fizične ali pravne osebe ali na podlagi prejšnjega člena.

(2) Nadzorni organ postopek vodi v javnem interesu.

38. člen
(uvedba inšpekcijskega nadzora na pobudo drugih organov)

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

(2) Nadzorni organ izvede nadzor po tem členu prednostno, če to ne škoduje izvedbi nadzorov po določbah prejšnjega pododdelka.

III. POGLAVJE
OBVEZNOSTI PRISTOJNIH ORGANOV, OBDELOVALCEV IN SKUPNIH UPRAVLJAVCEV

1. oddelek – splošne obveznosti

39. člen
(odgovornost pristojnega organa za skladnost)

(1) Pristojni organ izvede in dokumentira ustrezne tehnične in organizacijske ukrepe, s katerimi zagotovi skladnost obdelave z zakonom.

(2) Pristojni organ pri izbiri ukrepov iz prejšnjega odstavka upošteva naravo, obseg, okoliščine in namene obdelave, pa tudi tveganja za človekove pravice in temeljne svoboščine, ki so povezana z

obdelavo in se razlikujejo po verjetnosti in resnosti. Kadar je to sorazmerno glede na dejavnosti obdelave, ukrepi vključujejo tudi izvajanje ustreznih politik za varstvo osebnih podatkov.

(3) Pristojni organ ukrepe iz prvega odstavka tega člena po potrebi pregleda in dopolni, zlasti kadar se spremenijo okoliščine obdelave.

(4) Pristojni organ mora biti zmožen izkazati skladnost obdelave z zakonom.

(5) Pristojni organ nadzornemu organu omogoči nemoteno opravljanje njegovih nalog.

40. člen
(vgrajeno in privzeto varstvo osebnih podatkov)

(1) Pristojni organ izvede ustrezne tehnične in organizacijske ukrepe za vgrajeno varstvo osebnih podatkov, kot je psevdonimizacija, s katerimi se že med načrtovanjem obdelave, pa tudi med njenim izvajanjem zagotovi učinkovito izvajanje načel varstva osebnih podatkov ter varstvo pravic posameznikov, na katere se nanašajo osebni podatki.

(2) Pristojni organ pri izbiri ukrepov iz prejšnjega odstavka upošteva stanje najnovejšega tehnološkega razvoja in stroške izvajanja ter naravo, obseg, okoliščine in namene obdelave, pa tudi tveganja za človekove pravice in temeljne svoboščine posameznikov, ki so povezana z obdelavo in se razlikujejo po verjetnosti in resnosti.

(3) Pristojni organ izvede ustrezne tehnične in organizacijske ukrepe, s katerimi vzpostavi sistem privzetega varstva osebnih podatkov, kar vključuje privzeto obdelavo samo tistih osebnih podatkov, ki so potrebni za vsak posamični namen obdelave. Ta obveznost velja za količino zbranih osebnih podatkov, obseg njihove obdelave, rok njihove hrambe in njihovo dostopnost. S temi ukrepi se zagotovi zlasti, da osebni podatki niso samodejno dostopni nedoločenemu številu oseb brez posredovanja pristojne osebe pristojnega organa.

41. člen
(skupni upravljavci)

(1) V primerih, ko dva ali več pristojnih organov ali pristojnih organov in upravljavcev skupaj določijo sredstva obdelave, ti veljajo za skupne upravljavce. Skupni upravljavci na pregleden način z medsebojnim pisnim dogovorom določijo dolžnosti vsakega od njih za izpolnjevanje obveznosti iz tega zakona, zlasti v zvezi z uresničevanjem pravic posameznika, na katerega se nanašajo osebni podatki, ter v zvezi z nalogami vsakega od njih glede dajanja splošnih informacij, razen če in kolikor so te dolžnosti določene že z zakonom. Z dogovorom ali zakonom se lahko določi tudi enotna kontaktna točka za uveljavljanje pravic posameznikov, na katere se nanašajo osebni podatki.

(2) Posameznik, na katerega se nanašajo osebni podatki, lahko ne glede na določbe dogovora oziroma zakona uresničuje pravice, ki jih ima na podlagi tega zakona glede varstva njegovih pravic s področja osebnih podatkov, pri vsakem od skupnih upravljavcev.

42. člen
(obdelovalec)

(1) Pristojni organ sme zaupati izvajanje posamezne obdelave le tistemu obdelovalcu, ki da ustrezna zagotovila za izvedbo ustreznih tehničnih in organizacijskih ukrepov, da bo obdelava potekala v skladu z zakonom in da bo zagotovljeno varstvo pravic posameznika, na katerega se nanašajo osebni podatki.

(2) Obdelovalec lahko izvajanje posamezne obdelave nadalje zaupa drugemu obdelovalcu, ob izpolnjevanju pogojev iz prejšnjega odstavka, le na podlagi predhodnega posebnega pisnega dovoljenja pristojnega organa.

(3) Pristojni organ in obdelovalec s pogodbo določita vsebino in trajanje dejanj obdelave, katerih izvajanje se zaupa obdelovalcu, naravo in namen teh obdelav, vrste osebnih podatkov, ki naj se

obdelujejo, kategorije posameznikov, na katere se nanašajo osebni podatki ter obveznosti in pravice pristojnega organa in obdelovalca. Pogodba poleg tega določa tudi, da obdelovalec:

1. deluje samo po navodilih upravljavca;

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

3. na ustrezen način pomaga pristojnemu organu pri zagotavljanju pravic posameznika, na katerega se nanašajo osebni podatki;

4. v skladu z navodili pristojnega organa po zaključku izvajanja obdelave izbriše ali vrne vse osebne podatke pristojnemu organu ter uniči obstoječe kopije teh osebnih podatkov, vključno z morebitnimi dnevniškimi zapisi in varnostnimi kopijami, razen v primerih, ko zakon predpisuje nadaljnjo hrambo teh osebnih podatkov;

5. da pristojnemu organu na razpolago vse informacije, potrebne za izkazovanje skladnosti obdelave z določbami tega člena;

6. pri najemu drugega obdelovalca zagotovi izpolnjevanje pogojev iz tega odstavka.

(4) Pogodba iz prejšnjega odstavka mora biti sklenjena v pisni obliki.

(5) Če obdelovalec iz prvega ali drugega odstavka tega člena v nasprotju z določbami tega zakona oziroma pogodbe iz tretjega odstavka tega člana samostojno določi druge namene oziroma sredstva obdelave, se ta obdelovalec v zvezi s to obdelavo šteje za upravljavca.

(6) Obdelovalec nadzornemu organu omogoči nemoteno opravljanje njegovih nalog.

43. člen
(dolžnost upoštevanja navodil pristojnega organa)

Vsakdo, ki dela za pristojni organ ali obdelovalca in ima dostop do osebnih podatkov, teh osebnih podatkov ne sme obdelovati brez navodila pristojnega organa, razen če to določa zakon.

44. člen
(evidenca dejavnosti obdelave)

(1) Pristojni organ upravlja evidenco vseh kategorij dejavnosti obdelave osebnih podatkov in skrbi za njeno točnost in posodobljenost.

(2) Evidenca iz prejšnjega odstavka vsebuje:

1. naziv oziroma ime in kontaktne podatke pristojnega organa in njegove pooblaščene osebe za varstvo osebnih podatkov, in kadar obstaja, skupnega upravljavca;

2. namene obdelave;

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

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

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

6. roke za izbris oziroma pregled potrebe po hrambi za posamezne kategorije osebnih podatkov;

7. kadar je ustrezno, splošni opis tehničnih in organizacijskih ukrepov za zagotavljanje varnosti osebnih podatkov.

8. navedbo pravne podlage za dejavnost obdelave, vključno s pravno podlago za prenose;

9. informacijo, ali se pri dejavnosti obdelave oblikuje profile.

(3) Obdelovalec upravlja evidenco vseh kategorij dejavnosti obdelave, ki jih izvaja v imenu pristojnega organa.

(4) Evidenca iz prejšnjega odstavka vsebuje:

1. naziv oziroma ime in kontaktne podatke obdelovalca ali obdelovalcev, posameznih pristojnih organov, v imenu katerih deluje obdelovalec, in kadar jo ima imenovano, tudi naziv oziroma ime in kontaktne podatke pooblaščene osebe za varstvo osebnih podatkov;

2. kategorije obdelav, ki jih izvaja v imenu posameznega pristojnega organa;

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 pristojni organ;

4. kadar je ustrezno, splošni opis tehničnih in organizacijskih ukrepov za zagotavljanje varnosti osebnih podatkov.

(5) Evidenci iz prvega in tretjega odstavka tega člena morata biti v pisni obliki ali z njo enakovredni elektronski obliki.

(6) Pristojni organ in obdelovalec nadzornemu organu na njegovo zahtevo omogočita dostop do evidenc iz prvega in tretjega odstavka tega člena.

45. člen
(vodenje dnevnikov)

(1) Pristojni organi, skupni upravljavci iz 41. člena tega zakona in obdelovalci po tem zakonu vodijo dnevnik obdelave vsaj o naslednjih dejanjih obdelave osebnih podatkov v avtomatiziranih sistemih obdelave osebnih podatkov:

1. zbiranje,

2. spreminjanje,

3. vpogled,

4. razkritje, vključno s prenosi,

5. povezovanje,

6. izbris.

(2) Dnevnik obdelave iz prejšnjega odstavka mora vsaj za dejanja vpogleda in razkritja osebnih podatkov omogočati utemeljitev dejanja obdelave, opredelitev njenega datuma in časa, identifikacijo osebe, ki je izvedla dejanje obdelave, ter identifikacijo uporabnikov osebnih podatkov. Dodatne vsebine dnevnika obdelave določi pristojni organ ob upoštevanju drugega odstavka 39. člena tega zakona.

(3) Dnevnik obdelave se sme uporabljati zgolj za preverjanje zakonitosti obdelave, notranji nadzor, zagotavljanje celovitosti in varnosti osebnih podatkov ter za potrebe predkazenskih in kazenskih postopkov.

(4) Pristojni organi, skupni upravljavci iz 41. člena tega zakona in obdelovalci nadzornemu organu na njegovo zahtevo omogočijo dostop do dnevnika obdelave.

(5) Vsebina dnevnika obdelave se hrani dve leti od zaključka koledarskega leta, v katerem so bila v njih zabeležena dejanja obdelave, če zakon ne določa drugače.

(6) Vsebina dnevnika obdelave, ki ga upravlja Nacionalna enota za informacije o potnikih po zakonu, ki ureja naloge in pooblastila policije, se zaradi obstoja večjega tveganja za človekove pravice in

temeljne svoboščine posameznikov hrani pet let od zaključka koledarskega leta, v katerem so bila v njih zabeležena dejanja obdelave.

46. člen
(preverjanje kakovosti osebnih podatkov)

(1) Pristojni organ sprejme vse razumne ukrepe, da se pred posredovanjem osebnih podatkov ali njihovim dajanjem na voljo preveri njihova točnost, popolnost, zanesljivost in posodobljenost.

(2) Pristojni organ osebnim podatkom, ki se posredujejo ali dajo na razpolago, priloži informacije, na podlagi katerih lahko uporabnik oceni njihovo točnost, popolnost, zanesljivost in posodobljenost, če z njimi razpolaga.

(3) Kadar se izkaže, da so bili posredovani ali dani na razpolago osebni podatki, ki ne ustrezajo zahtevam iz prvega odstavka tega člena, ali so bili posredovani nezakonito, pristojni organ to nemudoma sporoči vsem uporabnikom.

(4) Pristojni organ v primeru iz prejšnjega odstavka nemudoma popravi osebne podatke oziroma jih izbriše ali omeji njihovo obdelavo.

(5) Ob izbrisu osebnih podatkov je zaradi zagotavljanja sledljivosti obdelave osebnih podatkov v skladu s 45. členom 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.

47. člen
(razlikovanje med različnimi kategorijami posameznikov)

Pristojni organ pri obdelavi v največji možni meri in z uporabo razumnih ukrepov razlikuje med osebnimi podatki različnih kategorij posameznikov, na katere se nanašajo osebni podatki, kot so:

1. osumljenci;

2. obdolženci;

3. obtoženci;

4. obsojenci;

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 ali so bile v stiku ali povezane z osebami iz 1. do 5. točke tega člena.

48. člen
(razlikovanje med osebnimi podatki, ki temeljijo na dejstvih, in osebnimi podatki, ki temeljijo na osebnih ocenah)

Pristojni organ pri obdelavi v največji možni meri razlikuje med osebnimi podatki, ki temeljijo na dejstvih, in osebnimi podatki, ki temeljijo na osebnih ocenah. Pristojni organ izvaja redno notranje preverjanje skladnosti teh obdelav in to ustrezno dokumentira. Pri tem osebne podatke, ki temeljijo na osebnih ocenah, v največji možni meri ustrezno označi ter utemelji na način, ki omogoča naknadno preverjanje teh ocen.

2. oddelek – ukrepi pred obdelavo in varnost osebnih podatkov

49. člen
(ocena učinka)

(1) Kadar bi lahko kategorija obdelave, zlasti zaradi uporabe novih tehnologij in ob upoštevanju narave, obsega, okoliščin oziroma namena obdelave, povzročila veliko tveganje za človekove pravice in temeljne svoboščine posameznikov, mora pristojni organ pred začetkom obdelave opraviti oceno učinka predvidenih dejanj obdelave na varstvo osebnih podatkov (v nadaljnjem besedilu: ocena učinka).

(2) Oceno učinka je vedno treba opraviti glede:

1. obdelav, ki vključujejo sistematično in obsežno vrednotenje osebnih podatkov 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. obdelav posebnih vrst osebnih podatkov ali osebnih podatkov v zvezi s kazenskimi obsodbami in prekrški v velikem obsegu;

3. obsežnega in sistematičnega nadzora javno dostopnega območja;

4. povezovanja zbirk podatkov.

(3) Ocene učinka ni treba opraviti glede obdelave, glede katere je bila ocena učinka izvedena že med sprejemanjem zakona, ki je podlaga za obdelavo, vendar le, če se okoliščine obdelave po izdelavi ocene učinka niso v bistvenem spremenile.

(4) Ocena učinka obsega:

1. splošni opis predvidenih dejanj obdelave;

2. oceno tveganj za človekove pravice in temeljne svoboščine posameznikov, na katere se nanašajo osebni podatki;

3. ukrepe, namenjene obvladovanju teh tveganj;

4. zaščitne ukrepe, kot so notranji nadzori;

5. ukrepe za zagotavljanje varnosti obdelave ter

6. mehanizme za zagotavljanje varstva osebnih podatkov in za izkazovanje skladnosti z zakonom, pri čemer se upoštevajo pravice in zakoniti interesi posameznikov, na katere se nanašajo osebni podatki, ter drugih zadevnih oseb.

(5) Pred uvedbo novega sistema za avtomatizirano obdelavo osebnih podatkov za namene iz prvega odstavka 1. člena tega zakona pristojni organ izdela oceno učinka glede ukrepov za zagotavljanje varnosti obdelave po 5. in 6. točki prejšnjega odstavka.

50. člen
(predhodno posvetovanje z nadzornim organom)

(1) Pristojni organ in obdelovalec morata pred začetkom obdelave, ki bo del nove zbirke, izvesti predhodno posvetovanje z nadzornim organom, kadar:

1. iz ocene učinka iz prejšnjega člena izhaja, da bi obdelava povzročila veliko tveganje za človekove pravice ali temeljne svoboščine posameznikov, na katere se nanašajo osebni podatki, če pristojni organ ne bi sprejel ukrepov za zmanjšanje tega tveganja; ali

2. kategorija obdelave, zlasti kadar vključuje uporabo novih tehnologij, mehanizmov ali postopkov, predstavlja veliko tveganje za človekove pravice ali temeljne svoboščine posameznikov, na katere se nanašajo osebni podatki.

(2) Nadzorni organ lahko določi in na svojih spletnih straneh objavi seznam kategorij obdelave, za katere mora pristojni organ v skladu s prejšnjim odstavkom opraviti predhodno posvetovanje.

(3) Pristojni organ in obdelovalec nadzornemu organu na njegovo zahtevo zagotovita dostop do vsebine ocene učinka ter vse druge informacije, ki jih rabi, da oceni skladnost obdelave z zakonom, pri tem še zlasti tveganja za varstvo osebnih podatkov posameznika, na katerega se ti podatki nanašajo, ter s tem povezane zaščitne ukrepe.

(4) Kadar nadzorni organ meni, da bi načrtovana obdelava osebnih podatkov lahko pomenila kršitev zakona, zlasti ker pristojni organ ni ustrezno opredelil tveganja ali ni sprejel ustreznih ukrepov za zmanjšanje tveganja, v roku šestih tednov po prejetju zaprosila za posvetovanje pisno svetuje pristojnemu organu in, kadar je to primerno, obdelovalcu, katere dodatne ukrepe je treba sprejeti. Nadzorni organ lahko ob upoštevanju zapletenosti zadeve rok podaljša za en mesec in o tem obvesti pristojni organ in po potrebi obdelovalca.

51. člen
(varnost obdelave)

(1) Pristojni organi, skupni upravljavci iz 41. člena tega zakona in obdelovalci morajo 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 obdelava izvaja v sistemih za avtomatizirano obdelavo osebnih podatkov, morajo pristojni organi, skupni upravljavci iz 41. člena tega zakona in obdelovalci po izvedeni oceni tveganj iz prejšnjega odstavka izvesti ukrepe, ki:

1. preprečujejo 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 uporabo sistemov za avtomatizirano obdelavo nepooblaščenim uporabnikom, ki do sistemov dostopajo z uporabo komunikacijske opreme (nadzor uporabnikov);

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

6. zagotavljajo, da je mogoče preveriti in ugotoviti, komu so bili ali bi mu lahko bili osebni podatki poslani oziroma komu je bil ali bi lahko bil omogočen dostop do njih prek komunikacijske opreme (nadzor prenosa);

7. zagotavljajo, da je mogoče naknadno preveriti in ugotoviti, katere vrste osebnih podatkov so bile vnesene 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 se osebni podatki, ki jih za pristojni organ obdelujejo njegovi zaposleni oziroma obdelovalec, obdelujejo le v skladu z navodili pristojnega organa (nadzor obdelave);

10. zagotavljajo, da se osebni podatki, ki so zbrani za različne namene, obdelujejo ločeno (ločenost);

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

12. zagotavljajo, da funkcije sistema delujejo in da se morebitne napake v funkcijah sporočijo ustreznim osebam (zanesljivost);

13. zagotavljajo, da se shranjeni osebni podatki ne okvarijo zaradi napak v delovanju sistema (celovitost), in

14. zagotavljajo, da so osebni podatki zaščiteni pred izgubo in uničenjem (razpoložljivost).

52. člen
(obvestilo nadzornemu organu o kršitvi varnosti osebnih podatkov)

(1) V primeru kršitve varnosti osebnih podatkov, za katero je verjetno, da bi povzročila tveganje za človekove pravice in temeljne svoboščine posameznikov, pristojni organ brez nepotrebnega odlašanja, po možnosti pa najpozneje v 72 urah po seznanitvi s kršitvijo, o kršitvi uradno obvesti nadzorni organ. Kadar obvestilo ni podano v 72 urah, obvestilu priloži tudi razloge za zamudo.

(2) Obdelovalec ob seznanitvi s kršitvijo varnosti osebnih podatkov o tem nemudoma obvesti pristojni organ.

(3) Obvestilo iz prvega odstavka tega člena vsebuje vsaj:

1. opis narave kršitve varnosti osebnih podatkov, po možnosti pa tudi kategorije in oceno števila zadevnih posameznikov, na katere se nanašajo osebni podatki, ter vrste in oceno števila zapisov osebnih podatkov, v zvezi s katerimi so se zgodile kršitve;

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

3. opis verjetnih posledic kršitve varnosti osebnih podatkov;

4. opis sprejetih ali predlaganih ukrepov za obravnavanje kršitve varnosti osebnih podatkov, če je to primerno, tudi z ukrepi za zmanjšanje morebitnih škodljivih učinkov kršitve.

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

(5) Pristojni organ dokumentira vsako kršitev varnosti osebnih podatkov iz prvega odstavka tega člena, vključno z dejstvi v zvezi s kršitvijo varnosti osebnih podatkov, njenimi predvidenimi učinki in sprejetimi popravnimi ukrepi, ki jih je sprejel za odpravo kršitve. Dokumentacija je na razpolago nadzornemu organu, kadar preverja skladnost delovanja pristojnega organa z določbami tega člena.

(6) Kadar kršitev varnosti osebnih podatkov vključuje osebne podatke, ki jih je pristojni organ dobil od upravljavca iz druge države članice Evropske unije ali ki jih je poslal upravljavcu iz druge države članice Evropske unije, mora pristojni organ informacije iz tretjega odstavka tega člena brez nepotrebnega odlašanja sporočiti upravljavcu druge države članice Evropske unije.

53. 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, pristojni organ brez nepotrebnega odlašanja sporoči posamezniku, na katerega se nanašajo osebni podatki, da je prišlo do kršitve varnosti osebnih podatkov.

(2) V sporočilu iz prejšnjega odstavka je treba v jasnem in preprostem jeziku opisati naravo kršitve varnosti osebnih podatkov ter navesti vsaj informacije in opis ukrepov iz 2., 3. in 4. točke tretjega odstavka prejšnjega člena.

(3) Sporočilo iz prvega odstavka tega člena ni potrebno, če je izpolnjen kateri izmed naslednjih pogojev:

1. pristojni organ je že pred kršitvijo izvajal ustrezne tehnološke in organizacijske zaščitne ukrepe in so bili ti ukrepi uporabljeni za osebne podatke, v zvezi s katerimi je prišlo do kršitve varnosti osebnih podatkov, zlasti ukrepe, na podlagi katerih so osebni podatki nerazumljivi vsem, ki niso pooblaščeni za dostop do njih, kot na primer šifriranje;

2. pristojni organ je po kršitvi sprejel ukrepe, zaradi katerih ni več verjetno, da bi se veliko tveganje za človekove pravice in temeljne svoboščine, ki je nastalo zaradi kršitve varnosti osebnih podatkov, še lahko uresničilo;

3. obveščanje posameznikov bi zahtevalo nesorazmeren napor, zato se v takšnem primeru objavi javno sporočilo ali izvede podoben ukrep, s katerim so posamezniki, na katere se nanašajo osebni podatki, enako učinkovito obveščeni.

(4) Če pristojni organ posameznika, na katerega se nanašajo osebni podatki, še ni obvestil o kršitvi varnosti osebnih podatkov, mu nadzorni organ to naloži, če oceni, da je verjetno, da bi kršitev lahko povzročila veliko tveganje za človekove pravice in temeljne svoboščine posameznika, pa niso podani pogoji 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 23. člena tega zakona zadrži, omeji ali opusti.

54. člen
(zaupno obveščanje o kršitvah)

(1) Pristojni organ vzpostavi notranje poti obveščanja, ki omogočajo zaupno in hitro seznanitev vodstva pristojnega organa in pooblaščene osebe za varstvo osebnih podatkov o kršitvah določb tega zakona.

(2) Pristojni organ določi ustrezen način ukrepanja glede utemeljenih prijav kršitev.

(3) Pristojni organ in pooblaščena oseba za varstvo osebnih podatkov varujeta tajnost vira prijave. Identiteto prijavitelja lahko razkrijeta le nadzornemu organu ali na podlagi odredbe sodišča.

3. oddelek – pooblaščena oseba za varstvo osebnih podatkov

55. člen
(pooblaščena oseba za varstvo osebnih podatkov)

(1) Pristojni organ izmed zaposlenih določi pooblaščeno osebo za varstvo osebnih podatkov, ki mu na neodvisen način svetuje in pomaga pri zagotovitvi skladnosti obdelav s tem zakonom in drugimi zakoni, ki urejajo obdelavo in varstvo osebnih podatkov.

(2) Sodišču s splošno pristojnostjo ni treba imenovati pooblaščene osebe za varstvo osebnih podatkov v zvezi z obdelavami za namene iz prvega odstavka 1. člena tega zakona glede kazenskih zadev sodišča.

(3) Pristojni organ lahko izmed zaposlenih določi tudi namestnika za čas zadržanosti ali odsotnosti pooblaščene osebe za varstvo osebnih podatkov. Namestnik takrat opravlja naloge pooblaščene osebe za varstvo osebnih podatkov in izvaja vse njene naloge.

(4) Pristojni organ sporoči ime ter službene kontaktne podatke pooblaščene osebe za varstvo osebnih podatkov in njenega morebitnega namestnika (naslov pristojnega organa, telefonska številka, naslov elektronske pošte) nadzornemu organu. Njune kontaktne podatke za namen vzpostavitve stika posameznika s pristojnim organov glede njegovih pravic po tem zakonu tudi javno objavi na svojih spletnih straneh.

(5) Pristojni organ pooblaščeni osebi za varstvo osebnih podatkov zagotovi ustrezna sredstva za nepristransko in učinkovito opravljanje nalog in ustrezna usposabljanja za ohranjanje strokovnega znanja.

(6) Pristojni organ zagotovi, da je pooblaščena oseba za varstvo osebnih podatkov ustrezno in pravočasno vključena v vse zadeve v zvezi z varstvom osebnih podatkov.

(7) Pristojni organ zagotovi, da pooblaščena oseba za varstvo osebnih podatkov v zvezi s svojim delom ne prejema nobenih navodil, da zaradi opravljanja svojih nalog ne sme biti razrešena ali kaznovana ter da neposredno poroča predstojniku pristojnega organa.

56. člen
(pogoji za določitev pooblaščene osebe za varstvo osebnih podatkov)

(1) Pristojni organ lahko za pooblaščeno osebo za varstvo osebnih podatkov in njenega namestnika določi posameznika, ki izpolnjuje naslednje pogoje:

1. je državljan Republike Slovenije,

2. aktivno obvlada slovenski jezik,

3. je poslovno sposoben,

4. je zaposlen pri pristojnem organu,

5. ima znanja oziroma praktične izkušnje s področja varstva osebnih podatkov,

6. ni bil pravnomočno obsojen zaradi naklepnega kaznivega dejanja, ki se preganja po uradni dolžnosti, in da ni bil obsojen na nepogojno kazen zapora v trajanju več kot šest mesecev;

7. zoper njega ni vložena pravnomočna obtožnica zaradi naklepnega kaznivega dejanja, ki se preganja po uradni dolžnosti.

(2) Več pristojnih organov lahko ob upoštevanju njihove organizacijske strukture in velikosti določi skupno pooblaščeno osebo za varstvo osebnih podatkov ali njenega namestnika.

(3) Pristojni organ lahko za pooblaščeno osebo za varstvo osebnih podatkov iz prvega odstavka tega člena določi osebo, ki je že imenovana za pooblaščeno osebo za varstvo osebnih podatkov na drugih pravnih podlagah.

57. člen
(naloge in upravičenja pooblaščene osebe za varstvo osebnih podatkov)

(1) Pooblaščena oseba za varstvo osebnih podatkov opravlja naslednje naloge v zvezi z obdelavami osebnih podatkov, ki jih izvaja pristojni organ, pri katerem je določena:

1. obveščanje pristojnega organa in njegovih zaposlenih, ki izvajajo obdelavo, o njihovih obveznostih v skladu z zakonom in drugimi predpisi, ki urejajo varstvo osebnih podatkov, ter svetovanje o teh obveznostih;

2. spremljanje skladnosti obdelav z zakoni in politikami pristojnega organa, ki urejajo varstvo osebnih podatkov, vključno z dodeljevanjem nalog, ozaveščanjem in usposabljanjem osebja, vključenega v dejanja obdelave, ter izvajanjem ustreznih nadzorov;

3. svetovanje glede ocene učinka v zvezi z varstvom osebnih podatkov in spremljanje njenega izvajanja v skladu s tem zakonom;

4. sodelovanje z nadzornim organom glede vzpostavljanja tehničnih pogojev za izvedbo nadzorov ter neposredno obveščanje vodstva pristojnega organa in nato nadzornega organa o kršitvah zakona glede določb o osebnih podatkih v zakonu;

5. delovanje kot kontaktna točka za nadzorni organ pri vseh vprašanjih v zvezi z obdelavo osebnih podatkov pri pristojnem organu, pomoč pri izvajanju posvetovanj ali pridobivanju mnenj po določbah tega zakona;

6. posvetovanje o drugih vprašanjih, politikah ali obdelavah osebnih podatkov pri pristojnem organu ali glede sodelovanja z drugimi subjekti glede teh vprašanj.

(2) Pooblaščena oseba za varstvo osebnih podatkov ima dostop do vsebine vseh osebnih podatkov, ki jih obdeluje pristojni organ, kadar izvršuje svoje naloge.

58. člen
(pooblaščena oseba za varstvo osebnih podatkov pri Nacionalni enoti za informacije o potnikih)

(1) Pooblaščena oseba za varstvo osebnih podatkov po zakonu, ki ureja naloge in pooblastila policije, mora izpolnjevati pogoje in opravlja naloge, kot jih določata ta zakon in zakon, ki ureja naloge in pooblastila policije.

(2) Generalni direktor policije za Nacionalno enoto za informacije o potnikih določi osebo, ki je že določena za opravljanje nalog pooblaščene osebe za varstvo osebnih podatkov pri policiji, ali drugo osebo znotraj policije.

IV. POGLAVJE
POSEBNE DOLOČBE

1. oddelek – preverjanje identitete

59. člen
(preverjanje identitete posameznika)

(1) Če pristojni organ opravičeno dvomi v identiteto posameznika, lahko ob obravnavi njegove zahteve ne glede na določbe drugih zakonov, ki urejajo pravico do vpogleda v posamezne osebne dokumente ali njihove kopije, preveri točnost osebnih podatkov posameznika z vpogledom v njegov uradni identifikacijski dokument, z uporabo sredstev elektronske identifikacije ali z uporabo drugih sredstev informacijske tehnologije. Če tako določa drug zakon, se lahko preverjanje točnosti izvede tudi ob zajemu posameznikovih osebnih podatkov, njihovi spremembi ali dopolnitvi.

(2) Za potrebe izvajanja določb tega zakona velja za uradni identifikacijski dokument vsak uradno izdani dokument, ki vsebuje fotografijo imetnika in ga je izdal državni organ, kar so: osebna izkaznica, potni list, obmejna prepustnica, vozniško dovoljenje oziroma orožni list in uradni identifikacijski dokumenti drugih držav ali mednarodnih organizacij.

2. oddelek – povezovanje

60. člen
(uporaba povezovalnih znakov)

(1) Pri pridobivanju osebnih podatkov iz zbirk osebnih podatkov s področja zdravstva, policije, obveščevalno-varnostne dejavnosti države, obrambe države, sodstva in državnega tožilstva, probacije ter iz kazenske evidence in prekrškovnih evidenc pristojni organ ne sme uporabljati povezovalnega znaka, na način, da bi se za pridobitev osebnega podatka uporabil izključno ta znak.

(2) Ne glede na prejšnji odstavek se lahko izjemoma uporabi en povezovalni znak za pridobivanje osebnih podatkov, če je to podatek v konkretni zadevi, ki lahko omogoči, da se prepreči, odkrije, preišče ali preganja kaznivo dejanje, ki se preganja po uradni dolžnosti. O tem se brez odlašanja napravi uradni zaznamek ali drug ustrezen zapis.

61. člen
(povezovanje uradnih evidenc in javnih knjig)

(1) Zbirke pristojnih organov se lahko povezujejo med seboj ali drugimi uradnimi evidencami, javnimi knjigami ali drugimi zbirkami, v katerih se obdelujejo posebne vrste osebnih podatkov, osebni podatki v zvezi s kazenskimi obsodbami in prekrški, podatki o dohodkih v skladu z zakonom, ki ureja dohodnino, podatki o premoženju posameznika v skladu z zakonom, ki ureja uveljavljanje pravic iz javnih sredstev, podatki o nepremičninah v lasti posameznika v skladu z drugimi zakoni, podatki oziroma informacije o kreditni sposobnosti v skladu z zakonom, ki ureja centralni kreditni register, in zakonom, ki ureja preprečevanje pranja denarja in financiranja terorizma, samo če takšno povezovanje izrecno določa zakon.

(2) Povezovanje zbirk v skladu s prejšnjim odstavkom 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.

(3) Najpozneje 30 dni pred začetkom povezovanja zbirk iz prvega odstavka tega člena mora pristojni organ oziroma obdelovalec poslati obvestilo nadzornemu organu, v katerem navede, da namerava izvesti povezovanje v skladu s tem členom, ga podrobno opisati zlasti z navedbo pravnih podlag, tehničnih rešitev in zaščitnih ukrepov ter priložiti oceno učinka, razen če ocene učinka v skladu z določbo tretjega odstavka 49. člena tega zakona ni treba izdelati.

3. oddelek – strokovni nadzor

62. člen
(strokovni nadzor)

Če drug zakon ne določa drugače, se določbe tega oddelka uporabljajo za obdelavo osebnih podatkov pri notranjem strokovnem nadzoru, ki ga opravljajo pristojni organi.

63. člen
(splošne določbe)

(1) Organ, ki izvaja strokovni nadzor znotraj pristojnega organa (v nadaljnjem besedilu: izvajalec strokovnega nadzora), sme za namen izvedbe strokovnega nadzora obdelovati vse osebne podatke, ki jih obdeluje pristojni organ, ki so potrebni za izvedbo posameznega strokovnega nadzora.

(2) Izvajalec strokovnega nadzora mora pri izvajanju strokovnega nadzora in izdelavi poročila ali ocene ob zaključku strokovnega nadzora varovati zaupnost osebnih podatkov, s katerimi se seznani v okviru strokovnega nadzora. 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.

64. člen
(obveščanje posameznika in pridobivanje podatkov)

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

(2) Posameznik iz prejšnjega odstavka lahko posreduje izvajalcu strokovnega nadzora za namene izvajanja strokovnega nadzora kontaktne osebne podatke drugega posameznika (osebno ime, zaposlitev, številke ali naslove službenih komunikacijskih sredstev ter navedbo povezave z zadevo nadzora), 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.

65. člen
(posebne vrste osebnih podatkov)

Če se pri izvajanju strokovnega nadzora obdelujejo posebne vrste osebnih podatkov ali podatki iz kazenskih evidenc ali prekrškovnih evidenc, izvajalec strokovnega nadzora o tem naredi uradni zaznamek.

4. oddelek – posredovanje osebnih podatkov

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

(1) Posredovanje osebnih podatkov s strani pristojnega organa drugi osebi javnega sektorja ali s strani druge osebe javnega sektorja pristojnemu organu je dovoljeno, če je za posredovanje podana pravna podlaga v skladu s 6., 7. in 8. členom tega zakona. Pristojni organ oziroma druga oseba javnega sektorja, ki se ji podatki posredujejo, sme osebne podatke obdelovati samo za namen, za katerega so ji bili posredovani.

(2) Posredovanje osebnih podatkov od pristojnega organa k pravnim ali fizičnim osebam zasebnega sektorja je dovoljeno, če je to potrebno za uveljavljanje, izvajanje ali obrambo pravnih zahtevkov. Pravna ali fizična oseba zasebnega prava sme posredovane osebne podatke obdelovati samo za namen, za uresničevanje katerega se ji posredujejo.

(3) Posredovanje iz prvega odstavka tega člena je brezplačno.

(4) 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 in postopke za izvajanje varnosti osebnih podatkov s pravilnikom predpiše minister, pristojen za notranje zadeve.

67. člen
(posredovanje osebnih podatkov, ki ga izvedejo osebe zasebnega sektorja)

(1) Posredovanje osebnih podatkov s strani osebe zasebnega sektorja pristojnemu organu je dovoljeno, če je za posredovanje podana pravna podlaga v skladu s 6., 7. in 8. členom tega zakona.

(2) Pristojni organ osebne podatke pridobi z zahtevo iz prvega odstavka 68. člena tega zakona, razen če drug zakon določa drugače.

(3) Posredovanje podatkov iz prvega odstavka tega člena je brezplačno.

68. člen
(postopek posredovanja osebnih podatkov)

(1) Posredovanje osebnih podatkov po tem oddelku se izvede na podlagi zahteve, ki vsebuje:

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

2. pravno podlago za pridobitev zahtevanih osebnih podatkov;

3. namen obdelave osebnih podatkov;

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 vlagatelju zahteve, če zakon ne določa drugačnega roka, 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 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 ali pristojni organ 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.

V. POGLAVJE
PRENOS OSEBNIH PODATKOV TRETJIM DRŽAVAM ALI MEDNARODNIM ORGANIZACIJAM

69. člen
(splošna pravila za prenos osebnih podatkov)

(1) Pristojni organ sme vsak prenos osebnih podatkov, ki se obdelujejo ali so namenjeni obdelavi po prenosu v tretjo državo ali mednarodno organizacijo, vključno z nadaljnjimi prenosi v drugo tretjo državo ali mednarodno organizacijo, izvesti le, če so upoštevane določbe tega zakona in:

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

2. se osebni podatki posredujejo upravljavcu v tretji državi ali mednarodni organizaciji, ki je pristojen za izpolnitev enega od namenov iz prvega odstavka 1. člena tega zakona;

3. v primeru, ko se prenašajo ali dajejo na razpolago osebni podatki iz druge države članice Evropske unije in je ta država članica v skladu s svojim nacionalnim pravom dala predhodno soglasje za prenos oziroma čezmejno obdelavo;

4. je Evropska komisija sprejela sklep o ustreznosti ravni varstva osebnih podatkov v tretji državi ali mednarodnih organizaciji iz tretjega odstavka 36. člena Direktive ali, če tak sklep ne obstaja, v tretji državi ali mednarodni organizaciji obstajajo ustrezni zaščitni ukrepi v skladu s 71. 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 72. členom tega zakona uporabiti izjeme za določene primere in

5. tretja država ali mednarodna organizacija soglaša, da bo osebne podatke naprej prenesla drugi tretji državi ali drugi mednarodni organizaciji le na podlagi predhodnega dovoljenja pristojnega organa Republike Slovenije, ki je izvedel prvotni prenos, in ob primernem upoštevanju vseh tehtnih meril, vključno z resnostjo 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 drugi tretji državi ali drugi mednarodni organizaciji.

(2) Prenos se v primerih iz 3. točke prejšnjega odstavka lahko izvede tudi brez podaje predhodnega soglasja druge države članice Evropske unije, če je prenos nujno potreben za preprečitev neposredne in resne grožnje javni varnosti Republike Slovenije ali tretje države ali za varstvo ustavne ureditve, bistvenih varnostnih, političnih in gospodarskih interesov Republike Slovenije, predhodnega soglasja pa ni bilo mogoče pravočasno pridobiti. O tem se brez nepotrebnega odlašanja obvesti organ druge države članice Evropske unije, pristojen za dajanje predhodnega soglasja.

70. 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 s sklepom iz tretjega odstavka 36. člena Direktive odločila, da ta tretja država oziroma eden ali več specifičnih sektorjev v tej tretji državi ali zadevna mednarodna organizacija zagotavlja ustrezno stopnjo varstva osebnih podatkov.

(2) Če je sklep iz tretjega odstavka 36. člena Direktive razveljavljen, spremenjen ali začasno odložen, se lahko prenosi nadaljujejo, če je za to podana katera od drugih pravnih podlag iz tega poglavja.

71. člen
(prenos osebnih podatkov z uporabo ustreznih zaščitnih ukrepov)

(1) Če ne obstaja sklep Evropske komisije iz tretjega odstavka 36. člena Direktive, je prenos osebnih podatkov v tretjo državo ali mednarodno organizacijo dopusten, če:

1. so v pravnem aktu, ki obvezuje tretjo državo ali mednarodno organizacijo, določeni ustrezni zaščitni ukrepi za varstvo osebnih podatkov ali

2. je pristojni organ po oceni vseh okoliščin, ki so pri prenosu pomembne, ugotovil, da v tretji državi ali mednarodni organizaciji dejansko obstajajo ustrezni ukrepi za varstvo osebnih podatkov.

(2) Pristojni organ obvesti nadzorni organ o kategorijah prenosov, ki jih izvaja na podlagi prejšnjega odstavka.

(3) Pristojni organ mora izpolnjevanje pogojev iz prvega odstavka tega člena dokumentirati, kar vključuje zlasti datum in uro prenosa, podatke o prejemniku oziroma uporabniku, utemeljitev prenosa in prenesene osebne podatke. Dokumentacijo hrani pet let od zaključka koledarskega leta, v katerem je bil izveden prenos. Dokumentacijo mora na podlagi zahteve dati na razpolago nadzornemu organu.

(4) Če nadzorni organ ugotovi neskladnost ukrepov za varstvo osebnih podatkov v zadevni tretji državi ali mednarodni organizaciji s tem zakonom, lahko z odločbo odredi ustavitev oziroma prepoved prenosa osebnih podatkov.

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

(6) Nadzorni organ o odločbi obvesti Evropsko komisijo in jo objavi na svoji spletni strani.

72. člen
(izjeme za posamezne primere)

(1) V primerih, ko ne obstaja sklep o ustreznosti iz tretjega odstavka 36. člena Direktive in niti ustrezni zaščitni ukrepi v skladu s prejšnjim členom, je prenos osebnih podatkov tretji državi ali mednarodni organizaciji dopusten, kadar je prenos potreben:

1. za varovanje življenjskih interesov posameznika, zlasti življenja ali telesa ali zdravja posameznika, na katerega se osebni podatki nanašajo, ali druge osebe;

2. za varovanje zakonitih interesov posameznikov, na katere se nanašajo osebni podatki, in je to določeno v zakonu;

3. za preprečitev neposredne in resne nevarnosti za javno varnost države članice Evropske unije ali tretje države ali za varstvo ustavne ureditve, bistvenih varnostnih, političnih in gospodarskih interesov Republike Slovenije;

4. v posameznem primeru za namene iz prvega odstavka 1. člena tega zakona ali

5. v posameznem primeru za uveljavljanje, izvajanje ali obrambo pravnih zahtevkov v povezavi z nameni iz prvega odstavka 1. člena tega zakona.

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

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

73. člen
(posebni prenosi določenim uporabnikom v tretjih državah)

(1) Pristojni organi smejo v posameznih posebej utemeljenih primerih izvesti posebni prenos osebnih podatkov v tretjo državo tudi tako, da jih neposredno prenesejo uporabniku, ustanovljenem v tretji državi, ne glede na to, ali je ta uporabnik v skladu s pravom tretje države pristojen za obdelavo osebnih podatkov za namene iz prvega odstavka 1. člena tega zakona ter ne glede na določbe mednarodnih pogodb s področja pravosodnega sodelovanja v kazenskih zadevah in policijskega sodelovanja s tretjo državo, če:

1. so upoštevane druge zahteve tega zakona;

2. je prenos nujno potreben za izvajanje za namene iz prvega odstavka 1. člena tega zakona;

3. v tem posameznem primeru pristojni organ ugotovi, da človekove pravice in temeljne svoboščine posameznika, na katerega se nanašajo osebni podatki, ne prevladajo nad javnim interesom za prenos;

4. bi bil prenos v skladu z drugimi določbami tega poglavja zakona neučinkovit ali neprimeren, zlasti ker ga ne bi bilo mogoče izvesti pravočasno;

5. je pristojni organ tretje države o tem brez nepotrebnega odlašanja obveščen, razen če to ne bi bilo učinkovito ali primerno, in

6. pristojni organ obvesti uporabnika iz tretje države o določenem namenu ali namenih, izključno za katere sme obdelati osebne podatke, pod pogojem, da je takšna obdelava potrebna.

(2) Pristojni organ obvesti nadzorni organ o prenosih, ki jih izvede na podlagi prejšnjega odstavka.

(3) Pristojni organ mora izpolnjevanje pogojev iz prvega odstavka tega člena dokumentirati, kar vključuje zlasti datum in uro prenosa, podatke o prejemniku oziroma uporabniku, utemeljitev prenosa in prenesene osebne podatke. Dokumentacijo hrani pet let od zaključka koledarskega leta, v katerem je bil izveden prenos. Dokumentacijo mora na podlagi zahteve dati na razpolago nadzornemu organu.

VI. POGLAVJE
NADZORNI ORGAN

74. člen
(določitev nadzornega organa)

(1) Informacijski pooblaščenec je neodvisni in samostojni nadzorni organ, ki izvaja nadzor nad spoštovanjem določb tega zakona ter glede obdelav osebnih podatkov za namene iz prvega odstavka 1. člena tega zakona.

(2) Nadzorni organ skrbi za enotno uresničevanje ukrepov na področju varstva osebnih podatkov po določbah tega zakona, tako da se zaščitijo človekove pravice in temeljne svoboščine posameznikov v zvezi z obdelavo osebnih podatkov ter omogoči prosti pretok osebnih podatkov med državami članicami Evropske unije v skladu z določbami tega zakona.

75. člen
(pristojnosti nadzornega organa)

(1) Nadzorni organ:

1. izvaja nadzore nad izvajanjem določb tega zakona ter drugih zakonov, podzakonskih predpisov ali drugih splošnih aktov glede obdelav osebnih podatkov s področij iz prvega odstavka 1. člena tega zakona;

2. odloča v pritožbenem postopku in v postopkih inšpekcijskih nadzorov po tem zakonu;

3. daje predhodna mnenja ministrstvom, državnemu zboru, organom samoupravnih lokalnih skupnosti, drugim državnim organom ter nosilcem javnih pooblastil o usklajenosti določb predlogov zakonov ter ostalih predpisov z zakoni in drugimi predpisi, ki urejajo osebne podatke;

4. izvaja predhodno posvetovanje v skladu s tem zakonom;

5. daje pristojnim organom ter posameznikom, na katere se nanašajo osebni podatki, neobvezna mnenja, pojasnila in stališča o vprašanjih glede varstva osebnih podatkov v zvezi zakoni in povezanimi predpisi na področju obravnavanja kaznivih dejanj, določenem s prvim odstavkom 1. člena tega zakona;

6. spodbuja ozaveščenost in razumevanje javnosti o tveganjih, pravilih, zaščitnih ukrepih in pravicah v zvezi z obdelavo;

7. spodbuja ozaveščenost pristojnih organov in obdelovalcev o njihovih obveznostih na podlagi tega zakona;

8. sodeluje pri delovanju Evropskega odbora za varstvo osebnih podatkov;

9. pripravi letno poročilo o izvajanju tega zakona, v skladu z določbami zakonov, ki urejata informacijskega pooblaščenca oziroma varstvo osebnih podatkov;

10. obvesti pristojno sodišče o kršitvah zakona in na lastno pobudo sodišču v sodnem postopku posreduje mnenje o ugotovljenih kršitvah;

11. izvaja druge naloge, določene s tem zakonom.

(2) Inšpekcijski nadzor po tem zakonu izvajajo nadzorne osebe, pri nadzoru pa lahko sodeluje strokovno osebje nadzornega organa s področja informacijskih in komunikacijskih tehnologij ter namestniki informacijskega pooblaščenca.

76. člen
(omejitve pri izvajanju nadzorov)

Ne glede na določbe prejšnjega člena nadzorni organ ni pristojen za inšpekcijski in prekrškovni nadzor glede:

1. obdelav osebnih podatkov, ki se obdelujejo v kazenski zadevi sodišča, izvedenih v okviru 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, izvedenih v okviru neodvisnega sodniškega odločanja Ustavnega sodišča Republike Slovenije v zadevah iz prejšnje točke.

77. člen
(medsebojna pomoč)

(1) Nadzorni organ pristojnim nadzornim organom drugih držav članic Evropske unije na njihovo zahtevo zagotovi ustrezne informacije in medsebojno pomoč glede konkretne zadeve, ki jo potrebujejo za dosledno izvajanje in uporabo njihove zakonodaje, s katero s svoj pravni red prenašajo Direktivo.

(2) Informacije in medsebojna pomoč iz prejšnjega odstavka obsega zlasti zahteve za informacije in nadzorne ukrepe, kot so zahteve za posvetovanja, preglede in preiskave.

(3) Zahteva za pomoč mora vsebovati vse potrebne informacije, vključno z namenom in obrazložitvijo zahteve. Izmenjane informacije se uporabljajo samo za namen, za katerega so bile zahtevane.

(4) Nadzorni organ obvesti nadzorni organ, ki je zahtevo poslal, o rezultatih oziroma po potrebi o stanju zadeve ali ukrepih, sprejetih v odziv na zahtevo.

(5) Nadzorni organ zahteve ne sme zavrniti, razen če:

1. ni pristojen za vsebino zahteve ali za izvršitev zahtevanih ukrepov ali

2. bi izpolnitev zahteve kršila zakon.

(6) Nadzorni organ zavrnitev zahteve obrazloži.

(7) Nadzorni organ zahtevane informacije praviloma posreduje z elektronskimi sredstvi v standardizirani obliki.

(8) Nadzorni organ medsebojno pomoč zagotovi brezplačno in brez nepotrebnega odlašanja, najpozneje pa en mesec po prejemu zahteve.

(9) Ne glede na prejšnji odstavek se nadzorni organi lahko dogovorijo o pravilih o vzajemnih nadomestilih za posebne izdatke, nastale zaradi zagotavljanja medsebojne pomoči v izjemnih okoliščinah.

(10) Nadzorni organ lahko zahteva pomoč nadzornih organov drugih držav članic Evropske unije. Zahteva za pomoč mora vsebovati vse potrebne informacije glede konkretne zadeve, vključno z namenom in obrazložitvijo zahteve. Pridobljene informacije se uporabljajo samo za namen, za katerega so bile zahtevane.

VII. POGLAVJE
KAZENSKE DOLOČBE

78. člen
(splošne kršitve s strani pristojnega organa)

Z globo od 100 do 5.000 eurov se kaznuje za prekršek odgovorna oseba pristojnega organa, če:

1. obdeluje osebne podatke brez podlage v zakonu ali brez privolitve posameznika, na katerega se nanašajo osebni podatki (prvi in drugi odstavek 6. člena);

2. po izvedeni obdelavi ne napiše poročila z navedbo razlogov za obdelavo in obsegom obdelanih osebnih podatkov (četrti odstavek 6. člena);

3. obdeluje posebne vrste osebnih podatkov brez podlage v zakonu, pa to ni nujno potrebno za opravljanje nalog pristojnih organov, določenih z zakonom (1. točka 7. člena);

4. če ne opravi ponovnega in ročnega pregleda odločitve, ki temelji izključno na avtomatizirani obdelavi osebnih podatkov in ki ima lahko negativen pravni učinek na posameznika, na katerega se nanašajo osebni podatki, ali ki tega posameznika lahko bistveno prizadene, pa je posameznik pregled zahteval (prvi odstavek 9. člena);

5. če po seznanitvi z uvedbo postopka izbriše, spremeni ali odsvoji zahtevane osebne podatke, ki so predmet postopka, dokler o zadevi ni pravnomočno odločeno (prvi odstavek 15. člena).

6. če ravna v nasprotju z odredbo nadzorne osebe o načinu zavarovanju dokazov (drugi odstavek 15. člena);

7. javno ne objavi splošnih informacij iz prvega odstavka 21. člena (tretji odstavek 21. člena);

8. če ne vodi dokumentacije, iz katere izhaja, da je zagotovljena skladnost obdelav z zakonom (prvi odstavek 39. člena);

9. če ne upravlja evidence vseh kategorij dejavnosti obdelav osebnih podatkov (prvi odstavek 44. člena);

10. dnevnik obdelave uporabi za druge namene od tistih, določenih v tretjem odstavku 45. člena tega zakona;

11. ne sporoči nemudoma vsem uporabnikom, da so jim bili posredovani ali dani na razpolago osebni podatki, ki ne ustrezajo zahtevam iz prvega odstavka 36. člena ali so bili posredovani nezakonito (tretji odstavek 46. člena), oziroma takšnih podatkov nemudoma ne popravi, jih izbriše ali omeji (četrti odstavek 46. člena);

12. ne izvaja predpisanih ukrepov varnosti obdelave iz 1. do 10. točke drugega odstavka 51. člena tega zakona;

13. ne dokumentira vseh kršitev varnosti osebnih podatkov (peti odstavek 52. člena);

14. uporablja povezovalni znak v nasprotju s 60. členom tega zakona;

79. člen
(kršitve s področja pogodbene obdelave)

(1)) Z globo od 400 do 20.000 eurov se za prekršek kaznuje pravna oseba, ki:

1. zaupa obdelavo drugemu obdelovalcu brez predhodnega posebnega pisnega dovoljenja pristojnega organa (drugi odstavek 42. člena);

2. ne deluje samo po navodilih pristojnega organa kot upravljavca (1. točka tretjega odstavka 42. člena);

3. ne zagotovi, da so osebe pri obdelovalcu, ki so pooblaščene za obdelavo osebnih podatkov, zavezane k zaupnosti ali jih k zaupnosti zavezuje ustrezen zakon (2. točka tretjega odstavka 42. člena);

4. po zaključku izvajanja obdelave ne izbriše ali vrne vseh osebnih podatkov pristojnemu organu ali ne uniči obstoječih kopij teh osebnih podatkov (4. točka tretjega odstavka 42. člena);

5. v nasprotju z določbami tega zakona samostojno določi druge namene oziroma sredstva obdelave (peti odstavek 42. člena);

6. ne upravlja evidence vseh kategorij dejavnosti obdelave, ki jih izvaja v imenu pristojnega organa (tretji odstavek 44. člena)

7. povezuje zbirke podatkov brez pravne podlage v zakonu (prvi odstavek 61. člena).

(2) Z globo od 200 do 10.000 eurov se za prekršek iz prejšnjega odstavka kaznuje, samostojni podjetnik posameznik ali posameznik, ki samostojno opravlja dejavnost.

(3) Z globo od 100 do 5.000 eurov se za prekršek iz prvega odstavka tega člena kaznuje odgovorna oseba pogodbenega obdelovalca, ki je pravna oseba, samostojni podjetnik posameznik ali posameznik, ki samostojno opravlja dejavnost

(4) Z globo od 40 do 5.000 eurov se za prekršek iz prvega odstavka kaznuje posameznik.

80. člen
(kršitve s področja prenosov osebnih podatkov tretjim državam ali mednarodnim organizacijam)

Z globo od 100 do 5.000 eurov se kaznuje za prekršek odgovorna oseba pristojnega organa, če:

1. Izvede prenos osebnih podatkov v tretjo državo ali mednarodno organizacijo v nasprotju z določbami prvega odstavka 71. člena tega zakona;

2. izvede prenos osebnih podatkov v tretjo državo ali mednarodno organizacijo v nasprotju z določbami prvega odstavka 72. člena tega zakona;

3. izvede posebni prenos osebnih podatkov v tretjo državo v nasprotju z določbami prvega odstavka 73. člena tega zakona;

4. ne dokumentira izpolnjevanja pogojev iz prvega odstavka 71. člena, prvega odstavka 72. člena ali prvega odstavka 73. člena tega zakona (tretji odstavek 71. člena, tretji odstavek 72 člena ter drugi odstavek 73. člena).

81. člen
(izrek globe)

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

VIII. POGLAVJE
PREHODNE IN KONČNE DOLOČBE

82. člen
(rok za izdajo pravilnikov)

(1) Minister, pristojen za notranje zadeve, izda pravilnik, s katerim določi ukrepe in postopke za izvajanje varnosti osebnih podatkov iz četrtega odstavka 66. člena tega zakona, v treh mesecih od uveljavitve tega zakona.

(2) Minister, pristojen za pravosodje, izda pravilnik iz petega odstavka 20. člena tega zakona v treh mesecih od uveljavitve tega zakona.

83. 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) 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.

84. člen
(končna določba)

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

III. OBRAZLOŽITVE ČLENOV

I. poglavje

SPLOŠNE DOLOČBE

Prvo poglavje predloga zakona ureja splošne določbe predloga zakona za policijo in določene druge državne organe. Vsebuje določbe, ki so sistemske narave, npr. glede nediskriminacije, sodnega varstva, obdelave posebnih vrst osebnih podatkov, definicij temeljnih izrazov. Navedene določbe bodo tudi v podobni ali isti vsebini del prihodnjega povezanega sistemskega zakona o varstvu osebnih podatkov (ZVOP-2).

1. člen (vsebina):

Predlagani 1. člen v prvem odstavku najprej vsebinsko določa domet (uporabo) zakona. Pri tem sledi vsebinskemu dometu, ki ga za obdelavo osebnih podatkov na področju policije in drugih državnih organov določa 1. člen Direktive. Izhaja najprej iz formalnega koncepta, po katerem je za domet (uporabo) tega zakona bistveni kriterij kaznivo dejanje, nato pa je kriterij jurisdikcijske narave - državni organi Republike Slovenije, ki so zakonsko določeni kot pristojni za področja preprečevanja, preiskovanja, odkrivanja ali pregona kaznivih dejanj ali izvrševanja kazenskih sankcij.

Kriterij kaznivega dejanja (koncept kaznivega dejanja po določbah Kazenskega zakonika – 16. člen ter nato določena konkretna kazniva dejanja od 100. člena dalje) pomeni, da domet tega zakona ni tudi področje prekrškov (kot del širšega koncepta kaznivih ravnanj), ta formalni kriterij pomeni, da je pri vsaki obdelavi osebnih podatkov treba zagotoviti, da je jasno, da se izvaja glede konkretnega kaznivega dejanja ali kaznivih dejanj iz Kazenskega zakonika, ne pa zaradi kakšnega drugega namena (izjema je le v drugem odstavku 8. člena predloga zakona). Kriterij državnih organov, ki so zakonsko določeni kot pristojni za področja preprečevanja, preiskovanja, odkrivanja ali pregona kaznivih dejanj ali izvrševanja kazenskih sankcij, pa pomeni, da je vključeno delovanje policije, preiskovalnega sodstva, kazenskega sodstva, državnega tožilstva, izvrševanja kazenskih sankcij in probacije, vse z vidika delovanja glede kaznivih dejanj. Gre torej za zaključeni krog državnih organov (v povezavi s prej navedenim formalnim kriterijem).

Nameni iz prvega odstavka so bistveni za uporabo določb tega zakona, v veliko primerih je določeno sklicevanje na prvi odstavek 1. člena – tako da je jasen domet določb zakona in vpliv na uporabo tega zakona glede določb drugih zakonov.

Predlagani drugi odstavek napoveduje urejanje posebej pomembnega področja, ki se nanaša na nadzorna pooblastila in nadzorne ukrepe Informacijskega pooblaščenca, ter tudi kaznivosti za prekrške, vse z namenom, da se zagotavljata zakonita in poštena obdelava osebnih podatkov ter odkrivajo in preprečujejo nezakoniti posegi v pravice posameznikov, na katere se nanašajo osebni podatki. Določba torej navaja, da so zagotovljena nujno potrebna učinkovita preiskovalna in kaznovalna orodja za državni nadzorni organ, z namenom, da se zagotovi jamstvena funkcija glede varstva osebnih podatkov – jamstvo, da bodo človekove pravice posameznikov in posameznic, na katere se nanašajo osebni podatki, spoštovane, ko se bo v njih posegalo z obdelavo osebnih podatkov. Nadzorna pooblastila in nadzorni ukrepi po predlogu zakona morajo zato biti učinkoviti, da se zagotavlja poštena in zakonita obdelava osebnih podatkov. Predlagana norma z vidika varovanih vrednot opravičuje določitev preiskovalnih pooblastil (nadzorna pooblastila) v 29. členu predloga zakona.

Predlagani tretji odstavek navaja pravna akta Evropske unije, ki se izvajata z ZVOPPOKD, namreč Direktiva ter tudi Direktivo (EU) 2016/681[24] v delu, ki se nanaša na pooblaščeno osebo za varstvo osebnih podatkov glede Evidence podatkov o potnikih (PNR).

2. člen (prepoved diskriminacije glede obdelave osebnih podatkov):

Predlagani 2. člen določa prepoved nedopustne diskriminacije glede varstva osebnih podatkov – natančneje: prepoved nedopustne diskriminacije, kadar se izvaja obdelava osebnih podatkov. Pri tem je pomembna opredelitev, da gre za človekovo pravico, da je osredotočeni naslovnik pravic posameznik, na katerega se nanašajo osebni podatki, ter glede razlagalne »moči« glede drugih zakonov ipd.. V 2. členu so glede na 14. člen Ustave Republike Slovenije ter glede na druge ustaljene formulacije pravnega reda Republike Slovenije (npr. prvi odstavek 131. člena Kazenskega zakonika[25] ter prvi odstavek 1. člena Zakona o varstvu pred diskriminacijo[26]) navedene prepovedane okoliščine diskriminacije. Določbe so nekoliko posodobljene – dodana je spolna identiteta po prvem odstavku 1. člena Zakona o varstvu pred diskriminacijo, dodana je genska (ne genetska) predispozicija, beseda »barva« iz dosedanjega 4. člena ZVOP-1 je spremenjena v »barvo kože«, omenjeno je tudi zdravstveno stanje.

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 pomembna kriterija državljanstvo in prebivališče, tudi glede na 1. člen Konvencije o varstvu posameznikov glede na avtomatsko obdelavo osebnih podatkov[27] (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 (ZVOPPOKD ali področni zakon) glede na formulacijo o »nedopustnosti« možnost izvajanja profiliranja glede obdelave osebnih podatkov, avtomatiziranega odločanja pod zakonsko določenimi pogoji in jamstvi (npr. pravica do ugovora).

3. člen (področje uporabe):

V navedenem členu je določena materialna veljava tega zakona, tj. za katere obdelave velja.

Tako je določeno (glede na drugi odstavek 2. člena Direktive), da določbe ZVOPPOKD veljajo za popolnoma ali delno avtomatizirano obdelavo osebnih podatkov ter za drugačne obdelave (ti. ročne oziroma papirnate obdelave) osebnih podatkov, ki so vključeni ali so namenjeni vključitvi v zbirko osebnih podatkov. Konkretno to pomeni, da lahko imamo osebne podatke, glede katerih se izvaja avtomatizirana obdelava, osebne podatke, glede katerih se izvaja ročna obdelava, osebne podatke, glede katerih se delno izvaja avtomatizirana, delno pa ročna obdelava, in ti podatki so vsi namenjeni vključitvi v zbirko. Gre tudi za vzpostavitev ti. materialne jurisdikcije za delovanje nadzornega organa – osredotočenje na nadzorovanje glede obdelav osebnih podatkov, in ne neposredno na zbirke.

Zbirka podatkov je zbirka, ki je opredeljena v zakonu (običajna poimenovanja: zbirka osebnih podatkov, zbirka podatkov, evidenca, register, javna knjiga, spis …). Med zbirke podatkov po tem zakonu ne sodijo pripomočki, to so priročne manjše zbirke, ki si jih ustvarijo uslužbenci za to, da lažje opravijo svoje delo v okviru posamezne zadeve. Gre za zbirke, katerih namen obstoja in uporabe je podpora procesu notranjega odločanja/razmišljanja (ti. »*deliberative process*«). Če takšna zbirka ni začasna in preraste okvir posamezne zadeve, gre za zbirko podatkov po tem zakonu.

Avtomatizirana sredstva so vsa sredstva, ki omogočajo avtomatizacijo uporabe, to so strojna in programska oprema, ki se uporablja za obdelavo podatkov. Gre lahko za individualne programe, ki

[24] Uradni list EU, L 119, 4. 5. 2016, str. 132–149.
[25] Uradni list RS, št. 50/12 – uradno prečiščeno besedilo, 6/16 – popr., 54/15, 38/16 in 27/17.
[26] Uradni list RS, št. 33/16.
[27] Uradni list RS, št. 11/94 – Mednarodne pogodbe, št. 3/94 in 86/04 – ZVOP-1.

tečejo na delovnih postajah posameznih uporabnikov, ali za večje namenske aplikacije, ki tečejo na strežniku, do njih pa dostopajo uporabniki.

4. člen (pomen izrazov):

Predlagani 4. člen najprej določa, da za varstvo osebnih podatkov veljajo bistveni izrazi (»pojmi« po 3. členu Direktive), torej definicije osebnega podatka, obdelave osebnih podatkov, zbirke ipd.

Izrazi so tudi delno popravljeni, tako je npr. definicija osebnega podatka podana v ednini, tudi definicija upravljavca je prilagojena pravnemu redu Republike Slovenije (upravljavci – državni organi za uradna delovanja ne smejo samostojno določati namenov obdelave) ter tudi določbi prvega odstavka 6. člena. Je pa dopuščeno, da si pristojni organi (upravljavci so po ZVOPPOKD pretežno samo pristojni organi) sami določijo sredstva obdelave.

Bistvena je definicija osebnega podatka, ki je dokaj široka – vsevključujoča[28] in pomeni katerokoli informacijo v zvezi z določenim ali določljivim posameznikom, na katerega se nanašajo osebni podatki, določljiv posameznik pa 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.

V 4. členu predloga zakona so določeni tudi nekateri izrazi, ki so dodani zaradi potreb učinkovitega izvrševanja predloga zakona. Med najpomembnejšimi je 10. točka, namreč institut privolitve posameznika za obdelavo njegovih osebnih podatkov, ki pa ni določen v Direktivi (razen posredno omenjen v 37. točki uvodnih navedb). Institut privolitve se tako glasi:

»»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.«[29]

Določba o institutu privolitve je tudi povezana z drugim odstavkom 6. člena predloga zakona, po kateri pristojni organi lahko obdelujejo tudi osebne podatke posameznika, ki je podal privolitev za obdelavo svojih osebnih podatkov za enega ali več namenov iz prvega odstavka 1. člena tega zakona, vendar le, če takšno možnost določa zakon (glede na bistveni pomen urejanja obdelav osebnih podatkov v zakonih, upoštevaje drugi odstavek 38. člena Ustave Republike Slovenije, ter kot je tudi določeno v prvem odstavku 6. člena predloga zakona).

Privolitev je z vidika kaznivih dejanj relevantna glede določenih delovanj po Zakonu o kazenskem postopku – drugi odstavek 219.a člena (preiskava elektronskih naprav), prvi odstavek 143.a člena (dajanje potrdil, da oseba ni v kazenskem postopku glede kaznivega dejanja), Zakonu o nalogah in pooblastilih policije – 48. člen (poligrafski postopek) ipd.

---

[28] Gl.: odločba US, št. U-I-152/17, 4. 7. 2019; objava: »25. Iz MKVP [Konvencija o varstvu posameznikov glede na avtomatsko obdelavo osebnih podatkov], Direktive 2016/680 in Zakona o varstvu osebnih podatkov (Uradni list RS, št. 94/07 – uradno prečiščeno besedilo – v nadaljevanju ZVOP-1), ki so sprejeli široko, vsevključujočo opredelitev, izhaja, da je osebni podatek katerakoli informacija v zvezi z določenim ali določljivim posameznikom; določljiv posameznik pa je tisti, ki ga je mogoče neposredno ali posredno določiti. (op. št. 20 odločbe US: Prim. z a) točko prvega odstavka 2. člena MKVP, 1. točko 3. člena Direktive 2016/680 in s 1. točko 6. člena ZVOP-1. Gl. tudi mnenje št. 4/2007 Delovne skupine 29 o opredelitvi pojma osebnega podatka.)«

[29] Definicija privolitve je sicer povzeta iz 11. točke 4. člena Splošne uredbe o varstvu podatkov, pri čemer je upoštevan Popravek Splošne uredbe o varstvu podatkov (UL L št. 127 z dne 23. 5. 2018, str. 2). V povezavi s Splošno uredbo o varstvu podatkov in njenim delnim oziroma posrednim vplivom na področje notranjih zadev je z vidika, da je možno privolitev za obdelavo osebnih podatkov po določbi tretjega odstavka člena 7 Splošne uredbe o varstvu podatkov kadarkoli umakniti, Zvezno ministrstvo za notranje zadeve Zvezne republike Nemčije v smernicah za izvajanje novega nemškega zakona (opr. št. V II 4 - 20108/24#27, 31. 8. 2017) opozarja: »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).«

V 16. točki je nadalje opredeljeno, da nadzorni organ po predlogu zakona pomeni Informacijskega pooblaščenca, določenega z Zakonom o Informacijskem pooblaščencu[30], nadzornik pomeni državnega nadzornika za varstvo osebnih podatkov, kot ga določa Zakon o Informacijskem pooblaščencu, nadzorne osebe pa pomenijo informacijskega pooblaščenca in nadzornike, kadar izvajajo nadzor po določbah predloga zakona.

V 20. točki je določen institut izbrisa, ki pomeni trajno odstranitev ali uničenje osebnega podatka, tako da ga ni več mogoče obnoviti (torej ni možno tega opraviti z blokiranjem, anonimizacijo, ločevanjem podatkov ipd.).

Po 21. točki anonimiziranje pomeni takšno spremembo osebnih podatkov, da jih ni več mogoče povezati z določenim ali določljivim posameznikom ali je to mogoče le z nesorazmerno velikimi napori, stroški ali porabo časa; tako anonimizirani podatki pa ne veljajo za osebne podatke po tem zakonu.

Po 22. točki blokiranje pomeni takšno označitev ali izločitev osebnih podatkov, da se omeji ali prepreči njihova nadaljnja obdelava, blokirani podatki pa veljajo za osebne podatke po predlogu zakona.

Po 23. točki 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, katere se upravljajo pri enem upravljavcu. Konkretno gre za enotno matično številko občana (EMŠO), davčno številko, ZZZS številko, ne pa npr. za številke upravne ali sodne zadeve.

V 24. točki je opredeljena kazenska zadeva sodišča, ki pomeni kazenske zadeve iz pristojnosti sodišča s splošno pristojnostjo, kot jih določata I. in I.a točka 101. člena Zakona o sodiščih[31] ter o njih odločajo kazenska sodišča v skladu z zakoni, ki urejajo sodne postopke, zlasti Zakon o kazenskem postopku. Po vsebini gre za zadeve sodne preiskave ter kazenskega sojenja (gl. uvodno navedbo št. 49 Direktive). Določba je pomembna, da se prepreči poseganje nadzornega organa preko inšpekcijskih postopkov nadzora v materijo neodvisnega sodnega odločanja kazenskega sodstva (npr. izjeme v 18. členu, drugem odstavku 30. člena, prvem odstavku 55. člena predloga zakona). Določba izhaja iz spoštovanja temeljnega načela vsake pravne in demokratične države, namreč neodvisnosti sodstva,

25. točka zaradi pomena zakonitosti obdelave osebnih podatkov po drugem odstavku 38. člena Ustave Republike Slovenije (določanje obdelav in osebnih podatkov s področnimi zakoni) določa, da »zakon« pomeni ZVOPPOKD, druge zakone Republike Slovenije (npr. Zakon o kazenskem postopku, Zakon o nalogah in pooblastilih policije, Zakon o izvrševanju kazenskih sankcij …), obvezujoče mednarodne pogodbe, ki zavezujejo Republiko Slovenijo (torej mednarodne pogodbe, ratificirane z zakonom – ker vsebujejo originarne norme), ter pravne akte ali odločitve Evropske unije, katerih določbe so enakovredne zakonom in neposredno uporabljive ali neposredno učinkovite (npr. uredbe Evropske unije, občasno tudi določene določbe direktiv, ki se uporabljajo neposredno).

Izraz »zakon« pomeni torej glede na 4. in 8. člen Direktive ter z vidika izvrševanja 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 (glede na drugi odstavek 38. člena Ustave Republike Slovenije in z njim povezano ustaljeno ustavnosodno presojo Ustavnega sodišča Republike Slovenije od leta 1992 dalje[32] ter glede na določbe 87. in 153. člena Ustave Republike Slovenije). Predlagana določba upošteva tudi

[30] Uradni list RS, št. 113/05 in 51/07 – ZUstS-A.
[31] 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, 23/17 – ZSSve, 22/18 – ZSICT in 16/19 – ZNP-1.
[32] Odločba US, št. U-I-115/92, 24. 12. 1992; objava: OdlUS I, 105 in Uradni list RS, št. 3/93.

najnovejšo precedenčno odločbo Ustavnega sodišča Republike Slovenije[33], ki je še okrepila pomen podrobne zakonske podlage za vse obdelave osebnih podatkov – v tem primeru glede množičnih (neciljanih) obdelav osebnih podatkov posameznikov (kot je bila sicer razvijana že v ustavnosodni presoji Ustavnega sodišča Republike Slovenije od leta 1992 dalje).

5. člen (načela varstva osebnih podatkov):

Predlagani člen v prvem odstavku določa temeljna načela varstva osebnih podatkov, s čimer prenaša določbe prvega oziroma četrtega odstavka 4. člena Direktive. Najbolj bistvena so načela poštenosti in zakonitosti (1. točka prvega odstavka), sorazmernosti[34] (3. točka prvega odstavka), prav tako pa je pomembno načelo namensko omejene obdelave osebnih podatkov[35] (2. točka prvega odstavka), ki je z vidika vsebine zakona povezano tudi z določanjem pravnih podlag za obdelavo osebnih podatkov v zakonih (prvi odstavek 6. člena predloga zakona).

V 4. točki prvega odstavka so določene obveznosti upravljavca, da mora zagotavljati točnost in posodobljenost osebnih podatkov, v 5. točki prvega odstavka je določeno, da mora biti hramba osebnih podatkov časovno zamejena (povezava z določanjem rokov hrambe v zakonih po prvem odstavku 6. člena predloga zakona) ali pa se (podrejeno) v zakonu vsaj določi rok za preverjanje potrebnosti hrambe (prvi odstavek 6. člena predloga zakona). V zadnji, 6. točki prvega odstavka, pa so postavljena splošna pravila glede varnosti osebnih podatkov.

V drugem odstavku je določeno, da je pristojni organ (v funkciji upravljavca) odgovoren za skladnost svojih obdelav osebnih podatkov z določbami prejšnjega odstavka in mora biti to skladnost tudi zmožen vedno izkazati – določen je torej poseben koncept odgovornosti upravljavca.

6. člen (zakonitost obdelave):

V predlaganem 6. členu so določene temeljne pravne podlage za zakonito obdelavo osebnih podatkov, ki izhajajo iz načela zakonitosti. Podobne določbe so vsebovane tudi v veljavnem 9. členu ZVOP-1.

Določbe predlaganih štirih odstavkov 6. člena je treba šteti za najpomembnejše za dejansko učinkovanje ZVOPPOKD, njihov pomen pa izhaja tudi iz tega, da pomenijo zakonsko izvedbo ustavnih norm iz najprej 38. člena, nato pa tudi 87., drugega odstavka 120. in 153. člena Ustave Republike Slovenije.

Prvi odstavek 6. člena določa, da je obdelava osebnih podatkov za namene iz prvega odstavka 1. člena ZVOPPOKD zakonita le, če je potrebna in v obsegu, v katerem je potrebna za opravljanje nalog pristojnih organov, določenih z zakonom, in če vrste osebnih podatkov, kategorije posameznikov, na katere se ti osebni podatki nanašajo, ter rok hrambe ali rok za reden pregled potrebe po hrambi določa področni zakon. Predlagana formulacija izhaja iz strogega spoštovanja načela zakonitosti obdelave osebnih podatkov po drugem odstavku 38. člena Ustave Republike Slovenije, po katerem se smejo obdelava konkretnih osebnih podatkov določati le z zakoni.

Načelo zakonitosti v predlogu zakona torej 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 (a) točke prvega odstavka 4. Direktive, 8. člena Direktive in a. točke 5. člena Konvencije št. 108. Glede na to da predlog zakona pomeni izvajanje Direktive, države članice Evropske unije glede na svojo nacionalno (zlasti ustavno) ureditev

[33] Odločba US, št. U-I-152/17, 4. 7. 2019, zlasti 32. točka; objava: Uradni list RS, št. 46/19.
[34] Načelo sorazmernosti po ustaljeni ustavnosodni presoji Ustavnega sodišča Republike Slovenije izhaja iz 2. člena v zvezi s tretjim odstavkom 15. člena Ustave Republike Slovenije.
[35] Gl. tudi drugi odstavek 38. člena Ustave Republike Slovenije.

določijo pravne podlage za konkretne vrste obdelav konkretnih osebnih podatkov v sistemskem ali v področnih zakonih.

V Republiki Sloveniji je že najpozneje od leta 1992[36] ustaljena oziroma zahtevana vsebina zakonov, ki urejajo obdelavo osebnih podatkov, ustaljeno opredeljena v naslednji ustavnopravni vsebini (po 38. členu Ustave Republiki Sloveniji), npr. v odločbi Ustavnega sodišča Republike Slovenije iz leta 2019:

»V zakonu mora biti določno opredeljeno, kateri podatki se smejo zbirati in obdelovati, za kakšen namen jih je dovoljeno uporabiti, predvidena morata biti nadzor nad zbiranjem, obdelovanjem in uporabo osebnih podatkov ter varstvo tajnosti zbranih osebnih podatkov. Namen zbiranja osebnih podatkov mora biti ustavno dopusten. Drugi odstavek 38. člena Ustave zahteva jasno, konkretno in določno opredelitev (ustavno dopustnega) namena obdelave osebnih podatkov. Zbirati se smejo le podatki, ki so primerni in nujno potrebni za uresničitev zakonsko opredeljenega namena. Ko gre za obdelavo osebnih podatkov za namene policijskega dela, mora zakonodajalec še posebej skrbno pretehtati težo ukrepa, s katerim brez privolitve posameznika posega v občutljivo območje njegove zasebnosti. To velja tudi za obdelavo osebnih podatkov v drugih državnih organih za potrebe obrambe države, nacionalne varnosti in ustavne ureditve.«[37]

V Republiki Sloveniji to pomeni, tudi po predlaganem prvem odstavku 6. člena, da se lahko konkretne obdelave konkretnih osebnih podatkov določajo le v (področnih) zakonih (naloge pristojnih organov, vrste osebnih podatkov, kategorije posameznikov, na katere se ti osebni podatki nanašajo, namen obdelave ter rok hrambe ali rok za reden pregled potrebe po hrambi).

Ni pa dopustno določati vrst osebnih podatkov, obdelave, namena obdelave, roka hrambe, kroga posameznikov, katerih osebni podatki se bodo obdelovali, ipd. v podzakonskih predpisih (kar je nedopustno po ustaljeni ustavnosodni presoji Ustavnega sodišča Republike Slovenije že od leta 1992 dalje[38]).

Ob tem je pomembno tudi navesti, da navedba splošne (okvirne) naloge pristojnega organa v zakonu ne pomeni[39] določitve konkretne obdelave osebnih podatkov, ne pomeni določitve osebnih podatkov, ki naj bi se obdelovali, niti ne namena obdelave osebnih podatkov, potrebna je dodatna konkretizacija v zakonu, kot je navedeno v prejšnjih odstavkih obrazložitve prvega odstavka 6. člena predloga zakona.

Definicija pojma »zakon« pa je vsebovana v 25. točki 4. člena, podobno ureditev ima Republika Avstrija v drugem odstavku 1. in 38. členu Zveznega zakona, s katerim se spreminja Zakon o varstvu osebnih podatkov iz leta 2000 (Zakon o prilagoditvi varstva osebnih podatkov 2018).

---

[36] Odločba US, št. U-I-115/92, 24. 12. 1992; objava: Uradni list RS, št. 3/93 in OdlUS I, 105. Eden prvih področnih zakonov neodvisne Republike Slovenije, v katerem so bile pretežno upoštevane prej navedene zahteve iz 38. člena Ustave Republike Slovenije glede področnega urejanja osebnih podatkov v zakonih, je bil s področja notranjih zadev – Zakon o evidencah s področja javne varnosti (Uradni list RS, št. 8/93).

[37] Odločba US, št. U-I-152/17, 4. 7. 2019, 33. točka odločbe; objava: Uradni list RS, št. 48/19.

[38] Odločba US, št. U-I-115/92, 24. 12. 1992; objava: Uradni list RS, št. 3/93 in OdlUS I, 105. V novejšem obdobju je relevantna tudi odločba Ustavnega sodišča RS iz leta 2019 o načelu upravne zakonitosti (drugi odstavek 120. člena Ustave Republike Slovenije: »Upravni organi opravljajo svoje delo samostojno v okviru in na podlagi ustave in zakonov.«), št. U-I-26/17, U-I-87/16, U-I-105/16, 24. 10. 2019; objava: Uradni list RS, št. 67/19, kjer je med drugim navedeno: »50. Po drugi strani splošnih aktov za izvrševanje javnih pooblastil (kot je tudi Metodologija), ki dopolnjujejo in podrobneje izpeljujejo zakonsko določbo, ni mogoče razumeti kot dejavnik, ki bi omogočal do zakonodajalca blažje razumevanje zahtev načela jasnosti in pomenske določljivosti zakonov. Nasprotno stališče bi ogrozilo zagotavljanje jamstev drugega odstavka 120. člena Ustave. Ni ustavno sprejemljivo, da bi se nerazumljivost in nejasnost zakonov (glede materije, ki mora po Ustavi biti zakonsko urejena) odpravljalo z jasnimi in razumljivimi podzakonskimi akti.«

[39] Gl. tudi: dr. Miroslav Žaberl, Mile Nunič, mag. Tatjana Bobnar, mag. Robert Ferenc, mag. Gregor Hudrič, Alojz Senčar (ur.: Mile Nunič), *Zakon o nalogah in pooblastilih policije s komentarjem*, GV Založba, Ljubljana, 2015, str. 41-42: »Prvi odstavek 4. člena zakona pa ni samostojen temelj, ki bi policiji zapovedoval dolžnost določenega delovanja. Gre za pravno normo, katere predmet je okvirno določanje nalog policije in ki je splošna. (opomba št. 2 knjige: Tako tudi VS, sodba št. 755/2005 in 181/2010). […] Edina izjema, ki pa velja za policijo in ki je vezana na odločitev ministra, bi bila v primeru uporabe generalne policijske klavzule (gl. komentar k 10. členu).«

Po drugem odstavku lahko pristojni organi obdelujejo tudi osebne podatke posameznika, ki je podal privolitev za obdelavo svojih osebnih podatkov za enega ali več namenov iz prvega odstavka 1. člena tega predloga zakona, če takšno možnost in namen obdelave (ter ostale vsebine glede na prvi odstavek) določa področni zakon. Razlaga pomena in uporabnosti instituta privolitve je bila že podana v obrazložitvi 4. člena.

Po predlaganem tretjem odstavku lahko pristojni organi za namene iz prvega odstavka 1. člena predloga zakona obdelujejo tudi osebne podatke posameznika, če jih je posameznik javno objavil ali naredil javno dostopne brez očitnega ali izrecnega namena omejitve dostopa do njih za določen ožji krog oseb (zaprti krog oseb). To velja tako za posebne vrste osebnih podatkov (dosedanji občutljivi osebni podatki) kot za ti. navadne osebne podatke. Predlagana določba izhaja iz (c) točke 10. člena Direktive, kjer je to določeno za posebne vrste osebnih podatkov, in se torej pri določanju te pravne podlage izhaja iz sklepanja po argumentu *a maiore ad minus*. Konkretno to tudi pomeni, da na primer policija ne sme obdelovati podatkov, ki jih je posameznik objavil na družbenem omrežju in jih delil z zaprto skupino uporabnikov (na primer samo s svojimi prijatelji), lahko pa obdeluje podatke, ki jih je objavil tako, da so vidni vsem ali večjemu številu uporabnikom tega omrežja. Obdelava je dopustna v okviru posamezne zadeve, podatkov, ki jih uporabniki (posamezniki in posameznice, na katere se nanašajo osebni podatki) javno objavijo, pristojni organi ne smejo zbirati oziroma obdelovati »na zalogo«.

Po predlaganem četrtem odstavku pristojni organi lahko ne glede na namene iz prvega odstavka 1. člena tega zakona obdelujejo osebne podatke, ki so nujno potrebni (strogi test sorazmernosti) za varovanje življenjskih interesov posameznika, zlasti življenja ali telesa ali zdravja posameznika, na katerega se osebni podatki nanašajo, ali druge osebe (tudi za varovanje njenih življenjskih interesov). Dodana je tudi varovalka, po kateri je pristojni organ po izvedeni obdelavi osebnih podatkov dolžan napisati poročilo z navedbo razlogov za obdelavo in obsegom obdelanih osebnih podatkov. Poročilo je na razpolago posamezniku, na katerega se nanašajo osebni podatki, in nadzornemu organu.

Predlagana določba četrtega odstavka 6. člena izhaja iz (b) točke 10. člena Direktive, kjer je to določeno sicer le za posebne vrste osebnih podatkov, je pa glede na njeno besedilo jasno, da se tukaj lahko izjemoma izstopi iz namenov same Direktive (vezanost na koncept kaznivega dejanja)[40].

Predlagana določba tudi pomeni se ta obdelava izven namenov iz prvega odstavka 1. člena predloga zakona nadalje obravnava v skladu s pravili iz Splošne uredbe o varstvu podatkov (četrti odstavek 6. člena).

Pomembno je tudi navesti, da kadar se oblikujejo manjše priročne zbirke, ki ne štejejo za zbirke podatkov po tem zakonu (3. člen), ne gre za obdelavo osebnih podatkov po tem zakonu.

Kadar gre za obdelave, ki se izvajajo za namen dela na konkretni zadevi in so priročne in začasne narave, takšne obdelave ni treba in ni mogoče vnaprej predpisati v zakonu. Začetno poizvedovanje glede informacij v zvezi s storjenimi kaznivimi dejanji ali njihovimi storilci oziroma soudeleženci je del spoznavnega procesa – zato ni mogoče zajeti vseh življenjskih situacij, vseh vrst (osebnih) podatkov in vseh obdelav, ki so potrebne za poizvedovanje glede konkretnega kaznivega dejanja.

7. člen (zakonitost obdelave posebnih vrst osebnih podatkov):

Predlagani 7. člen v prvem odstavku določa, da je obdelava posebnih vrst osebnih podatkov (dosedanje poimenovanje občutljivi osebni podatki) prepovedana. Posebne vrste osebnih podatkov pa so opredeljene v 12. točki 4. člena predloga zakona.

[40] Gl. tudi ureditev v Republiki Avstriji: § 38 Zveznega zakona, s katerim se spreminja Zakon o varstvu osebnih podatkov iz leta 2000 (Zakon o prilagoditvi varstva osebnih podatkov 2018), ki se glasi: »**Razen če je treba zaščititi življenjske interese posameznika, je obdelava zakonita** le, če je določena z zakoni ali z neposredno veljavnimi pravnimi določbami, ki imajo v Avstriji položaj zakonov in je to potrebno ter sorazmerno za izpolnjevanje naloge, ki jo izvaja pristojni organ za namene iz prvega odstavka 36 §.« (poudarilo Ministrstvo za pravosodje).

V drugem odstavku pa so določene izjeme, namreč, da je obdelava posebnih vrst osebnih podatkov s strani pristojnih organov ne glede na določbo prejšnjega odstavka zakonita, če je skladna z določbami 6. člena ter če je nujno potrebna za opravljanje nalog pristojnih organov, določenih z zakonom (nameni iz prvega odstavka 1. člena predloga zakona) in če je zagotovljeno ustrezno varstvo človekovih pravic ali temeljnih svoboščin posameznika, na katerega se nanašajo osebni podatki. Pogoji morajo biti izpolnjeni kumulativno.

8. člen (obdelava osebnih podatkov za druge namene):

8. člen določa pogoje za obdelavo osebnih podatkov v druge namene, pri tem izhaja iz 9. člena Direktive. V prvem odstavku je določeno splošno pravilo, po katerem je obdelava osebnih podatkov s strani istega ali drugega pristojnega organa za druge namene obdelave od tistih, za katere so bili podatki pridobljeni, dovoljena le, če ti novi nameni obdelave spadajo med namene iz prvega odstavka 1. člena predloga zakona in če tako določa področni zakon. V drugem odstavku pa je kot izjema določeno, da se osebni podatki, ki jih pristojni organi zbirajo za namene iz prvega odstavka 1. člena predloga zakona, ne obdelujejo za druge namene, kot so nameni iz prvega odstavka 1. člena tega zakona, razen če to dovoljuje področni zakon (npr. zakoni s področja javne varnosti, vključno s prekrškovno zakonodajo). V tem primeru (če to dovoljuje zakon) pa za obdelavo veljajo pravila iz Splošne uredbe o varstvu podatkov oziroma zakona, ki ureja varstvo osebnih podatkov (trenutno ZVOP-1, v prihodnosti - ZVOP-2), oziroma drugih področnih zakonov.

Določena izjema takšne vrste je že določena v predlogu zakona in se neposredno uporablja, namreč četrti odstavek 6. člena predloga zakona o varstvu življenjskih interesov.

9. člen (avtomatizirano odločanje in oblikovanje profilov):

V 9. členu so določena pravila glede avtomatiziranega odločanja pri obdelavi osebnih podatkov, ki sledijo 11. členu Direktive. Po prvem odstavku je odločanje, ki temelji izključno na avtomatizirani obdelavi osebnih podatkov, vključno z oblikovanjem profilov, ki ima lahko negativen pravni učinek na posameznika, na katerega se nanašajo osebni podatki, ali ga lahko bistveno prizadene, prepovedano. Določena je izjema, da to lahko določa drug zakon, ki pa mora določiti zlasti pravico posameznika, da kot ustrezni ukrep za varovanje njegovih pravic zahteva ponovni in ročni pregled odločitve s strani fizične osebe (običajno uradne osebe) pri pristojnem organu ter da lahko posameznik, na katerega se nanašajo osebni podatki, do odločitve izrazi lastno stališče, oziroma zakon lahko tudi določa, da pristojni organ izvaja druge (nadomestne) ustrezne ukrepe za zagotavljanje ustreznega varstva človekovih pravic in temeljnih svoboščin (npr. obvezno preverjanje ali primerjava rezultatov odločanja s strani nadrejene uradne osebe, posebne enote …). Po drugem odstavku odločitve iz prvega odstavka ne smejo temeljiti na obdelavah posebnih vrst podatkov, razen če zakon določa (sistemske in podrobne) ustrezne ukrepe za varstvo človekovih pravic in temeljnih svoboščin ter zakonitih interesov posameznika, na katerega se nanašajo osebni podatki. Po tretjem odstavku mora pristojni organ kot pripravljavec področnega zakona (lahko tudi poslanec, če gre za poslanski zakon), ki bi vseboval avtomatizirano odločanje, izvesti oceno učinka iz 49. člena predloga zakona. V četrtem odstavku je določena še ena prepovedna norma, da je namreč oblikovanje profilov v okviru avtomatizirane ali drugačne (ročne) obdelave posebnih vrst osebnih podatkov, ki ima za posledico diskriminacijo posameznikov, na katere se nanašajo osebni podatki, prepovedano.

Pri avtomatiziranem odločanju glede obdelav osebnih podatkov torej predlog zakona izhaja iz sistema prepovedi, saj izhaja iz spoštovanja subjektivitete človeka (o človeku naj se ne odloča na avtomatizirani način), nato pa so določene izjeme, ki pa so pogojene z varovalnimi ukrepi (običajno bi bil ustrezni ukrep: predpisana in izvedena naknadna človeška intervencija).

Avtomatizirani sistem obdelave osebnih podatkov sicer pomeni informacijski oziroma računalniški sistem, sestavljen iz enega ali več med seboj povezanih računalnikov, na katerih teče posebna programska oprema. Avtomatizirani sistem obdelave je namenjen sistemski avtomatski obdelavi in hrambi večje količine podatkov (zbirke podatkov). Pri tem ne gre za posamezne manjše uporabniške

programe, ki jih uporabljajo pri svojem delu policija (preiskovalci, forenziki, …), tožilci, preiskovalni sodniki (izvedenci …) ali ko ustvarjajo nove pripomočke (zbirke podatkov za enkratno uporabo ob delu na posamezni zadevi). Avtomatizirana obdelava je obdelava, pri kateri človeški posegi niso potrebni, razen v začetku (sproženje obdelave) in koncu (predčasna ustavitev obdelave) ter pri oceni rezultatov obdelave.

10. člen (sodno varstvo):

Predlagani 10. člen ureja sistem splošnega sodnega varstva pravic posameznikov, na katere se nanašajo osebni podatki, konkretneje določa posebno upravnosodno presojo kot samostojno pravno sredstvo. Predlagano sodno varstvo sledi dosedanji ureditvi iz 34. člena ZVOP-1 (tudi upravnosodna presoja), je pa vključeno v predlog zakona na podlagi 54. člena Direktive.

Sodno varstvo po 10. členu je samostojno pravno sredstvo (samostojno sodno varstvo) in ni pogojeno s predhodnim izčrpanjem kateregakoli drugega pravnega sredstva ali pravice po ZVOPPOKD.

Po predlaganem prvem odstavku lahko vsak posameznik, na katerega se nanašajo osebni podatki in ki meni, da določena obdelava njegovih osebnih podatkov s strani pristojnega organa ali obdelovalca krši določbe ZVOPPOKD ali drugih (področnih) zakonov, ki urejajo obdelavo ali varstvo osebnih podatkov za namene iz prvega odstavka 1. člena ZVOPPOKD, zahteva sodno varstvo svojih pravic ves čas, dokler kršitev traja (kriterij trajajoče kršitve).

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

Tretji odstavek določa, da lahko posameznik s sodnim varstvom po določbah 10. člena zahteva prenehanje kršitve, vzpostavitev zakonitega stanja (npr. izbris, popravek) oziroma odškodnino, določene so torej materialne podlage zahtevka.

V četrtem odstavku so določene temeljne postopkovne določbe, tako da v postopku po prvem, drugem in tretjem odstavku 10. člena odloča Upravno sodišče Republike Slovenije z uporabo določb Zakona o upravnem sporu po postopku za tožbo zaradi kršitve človekovih pravic in temeljnih svoboščin, tožnik pa lahko v tožbo vključi tudi odškodninski zahtevek.

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

Po šestem odstavku sodišče v zadevah upravnih sporov po predlaganem členu odloči najpozneje v šestih mesecih.

11. člen (zastopanje s strani nevladnih organizacij):

V predlaganem 11. členu je določeno, kdo lahko poleg splošnih pravil o pooblaščanju (npr. odvetniki, drugi pooblaščenci) glede na zahteve iz 55. člena Direktive zastopa posameznike, na katere se nanašajo osebni podatki. Predlagano je, da lahko vsak posameznik, na katerega se nanašajo osebni podatki, pisno pooblasti nevladno organizacijo s področja varstva človekovih pravic in temeljnih svoboščin, ki ima status nevladne organizacije v javnem interesu[41], da v njegovem imenu glede obdelav njegovih osebnih podatkov uveljavlja sodno varstvo po 10. členu predloga zakona ali vloži pritožbo ali prijavo po določbah ZVOPPOKD. Določba glede kvalifikacij nevladne organizacije je torej ne vključuje samo nevladnih organizacij za varstvo osebnih podatkov ali zasebnosti, ampak vse nevladne organizacije s področja varstva človekovih pravic in temeljnih svoboščin, ki imajo status nevladne organizacije v javnem interesu. Pri tem se upošteva, da ni primerno zahtevati, da bi bile

[41] Za definicijo nevladnih organizacij gl. 2. člen Zakona o nevladnih organizacijah (Uradni list RS, št. 21/18).

nevladne organizacije specializirane samo ali pretežno za varstvo samo ene ali dveh človekovih pravic.

II. poglavje

PRAVICE POSAMEZNIKA, POSTOPEK TER IZVAJANJE NADZORA

V tem poglavju se urejajo pravice posameznika, na katerega se nanašajo osebni podatki, določajo postopkovna vprašanja glede zagotavljanja pravic posameznikov in izvajanje nadzora nad uresničevanjem pravic ter zakonitostjo obdelav. Poglavje ureja pet vrst postopkov, in sicer:

- urejen je poseben postopek uveljavljanja določenega kroga pravic neposredno pred Informacijskim pooblaščencem,

- postopek pred pristojnim organom, pred katerim posameznik, na katerega se nanašajo osebni podatki, uveljavlja pravice iz tega in drugih zakonov (18. člen predloga ureja primere, ko drug zakon določa uresničevanje določenih pravic v kazenski zadevi sodišča, posameznik uresničuje te pravice le v obsegu in na način, kot je določeno s tem drugim zakonom),

- pritožbeni postopek pred nadzornim organom, povezan s prejšnjim postopkom uveljavljanja pravic pred pristojnim organom,

- inšpekcijski postopek v interesu prijavitelja s posebnim položajem in

- inšpekcijski postopek v javnem interesu (na podlagi prijave kogarkoli ali po uradni dolžnosti).

1. oddelek – skupne določbe

V tem oddelku so urejene skupne določbe, ki veljajo za celotno II. poglavje oziroma za vse tri vrste postopkov, ki posamezniku omogočajo uveljavljanje svojih pravic. Določbe se nanašajo na posebno ureditev, ki v določenem delu odstopa od sistemske, ki je urejena v Zakonu o splošnem upravnem postopku (v nadaljnjem besedilu: ZUP) in v Zakonu o inšpekcijskem nadzoru (v nadaljnjem besedilu: ZIN).

12. člen (uveljavljanje pravic pred pristojnim organom, obdelovalcem ali nadzornim organom)

Pravice pred pristojnimi organi (organi, pristojni za področja preprečevanja, preiskovanja, odkrivanja ali pregona kaznivih dejanj ali izvrševanja kazenskih sankcij, torej policija, državno tožilstvo, Uprava za izvrševanje kazenskih sankcij, Uprava za probacijo in sodišče v delu, ki se nanaša na sodno preiskavo) se uveljavljajo na podlagi tega zakona. V postopku se uporablja ZUP, kolikor niso s tem zakonom posamezna vprašanja urejena drugače. Obdelovalec, ki je samostojno določil druge namene oziroma sredstva obdelave, postane upravljavec, s tem pa prevzame tudi obveznosti, ki gredo upravljavcem (peti odstavek 42. člena tega zakona). Posamezniki lahko v tem primeru svoje pravice uveljavljajo tudi pred obdelovalcem. Pritožbe in inšpekcijske prijave oziroma pobude obravnava nadzorni organ (to je Informacijski pooblaščenec).

13. člen (omejitve vpogleda v spis)

Predlagani 13. člen ureja izjemo od splošnih določb ZUP, ki v 82. členu ureja pravico pregledovanja spisa, ko postopek še teče. Ker lahko spis vsebuje podatke in dokumentacijo, ki je predmet postopka, posamezniku vpogleda v spis ni mogoče dovoliti do dokončne odločitve. Odločitev vsebuje tudi odločitev o dovoljenem obsegu pregleda zadeve.

14. člen (preverjanje identitete posameznika)

Predlagani 14. člen ureja preverjanja identitete posameznika, na katerega se nanašajo osebni podatki, kadar pristojni organ oziroma nadzorni organ opravičeno dvomi o identiteti posameznika, ki je vložil

zahtevo, pritožbo ali prijavo. Od posameznika se lahko zahtevajo dodatne informacije za potrditev njegove identitete, in če tudi dodatne informacije ne odpravijo dvoma, se lahko od posameznika zahteva vpogled v uradni identifikacijski dokument ali se identifikacija izvede s pomočjo sredstev elektronske identifikacije (59. člen predloga zakona). Tako pridobljene podatke pristojni organ hrani dve leti od zaključka obdelave za namen izkazovanja skladnosti obdelave (skladnosti v smislu zakonitosti obdelave osebnih podatkov po določbah tega in drugih – področnih – zakonov).

15. člen (zavarovanje osebnih podatkov, ki so predmet postopka)

Predlagani 15. člen ureja posebni upravni ukrep – obveznost pristojnih organov, da zavarujejo vsebino in obliko osebnih podatkov, ki so predmet zahteve. Podatki, ki so predmet zahteve, se ne smejo izbrisati, spremeniti ali odsvojiti, dokler o zadevi ni pravnomočno odločeno, saj v nasprotnem primeru o njih ne bi bilo mogoče ugotavljati zakonitosti obdelave. Nadzorna oseba (nadzornik ali informacijski pooblaščenec) lahko v posameznem postopku glede na okoliščine posameznega primera določi tudi drugi način zavarovanja osebnih podatkov, ki so predmet zahteve. Zavarovanje traja do dokončne in pravnomočne odločitve, v primeru tožbe v upravnem sporu, do pravnomočnosti odločitve sodišča. Namen določbe drugega odstavka je predvsem preprečevanje potrebe po posegih v obstoječe aplikacije, v katerih se obdelujejo osebni podatki in ki ne omogočajo zavarovanja osebnih podatkov znotraj same aplikacije.

16. člen (izvršba)

Predlagani 16. člen določa, da se izvršba izvaja po postopku upravne izvršbe s prisilitvijo, kot jo določa ZUP v 298. členu – z dodano posebno ureditvijo, ki je določena v tem predlogu zakona. Za izvedbo izvršbe je pristojen Informacijski pooblaščenec kot nadzorni organ (*sui generis* določba). Denarna kazen bremeni odgovorno osebo pristojnega organa ali upravljavca, ki ni izvršila odločbe nadzornega organa. Gre za odstop od ureditve v ZUP, ki govori zgolj o zavezancu za storitev, opustitev ali ravnanje, ki je določeno v odločitvi (prvi odstavek 298. člena ZUP). Zoper sklep o dovolitvi izvršbe ni dovoljena pritožba, kot jo ureja ZUP v 292. členu, ker ni drugostopenjskega organa, ki bi lahko o njej odločil.

Četrti odstavek določa, da se lahko izvršba po tem členu uporablja tudi za izvršitev odločb, izdanih v inšpekcijskem nadzoru po določbah tega zakona.

2. oddelek – pravice posameznika in postopek pri pristojnem organu

Drugi oddelek ureja postopkovne določbe in materialne pravice, ki jih posamezniki uveljavljajo pred pristojnim organom, ter pravico do pritožbe, o kateri odloča Informacijski pooblaščenec. Predlog zakona določa okrepljeno odgovornost pristojnih organov 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 pristojnim organom, upravljavcem, Informacijskim pooblaščencem oziroma pred sodišči.

17. člen (uporaba določb zakona, ki ureja splošni upravni postopek)

Predlog zakona v 17. členu določa subsidiarno uporabo določb Zakona o splošnem upravnem postopku (ZUP). Ta zakon posamezne določbe ZUP ureja drugače, najprej v skupnih določbah, ki veljajo za vse tri že omenjene postopke po tem zakonu, torej tudi za postopek po tem oddelku. To so omejitve vpogleda v spis, preverjanje identitete posameznika in zavarovanje osebnih podatkov, ki so predmet postopka ter izvršbe.

Po tem oddelku se za uresničevanje pravic posameznika drugače ureja še komunikacija s posameznikom in ravnanje z očitno neutemeljeno ali pretirano zahtevo.

18. člen (uresničevanje pravic na podlagi drugih zakonov)

Predlog 18. člena ureja uporabo zakona na področju kazenske zadeve sodišča za uresničevanje pravic v zvezi z dajanjem splošnih informacij, dostopa do osebnih podatkov ter pravice do popravka, izbrisa in do omejitve obdelave, v primeru, ko drugi, področni zakoni, navedene pravice urejajo drugače. Če pravice iz tega predloga zakona ureja drug zakon, jih posameznik uveljavlja po tem

drugem zakonu (npr. Zakon o državnem tožilstvu), če pa drugi zakon tega ne ureja, pa lahko posameznik pravice uveljavlja po ZVOPPOKD.

19. člen (komunikacija s posameznikom, na katerega se nanašajo osebni podatki)

V predlaganem 19. členu je urejena pravica posameznika, da od pristojnih organov, ki obdelujejo njegove osebne podatke, pridobi splošne informacije ali odgovore glede dostopa do kopije osebnih podatkov, pravice do popravka, izbrisa ali omejitve teh pravic, in sicer v jasnem in preprostem ter razumljivem jeziku. Informacije se prilagodijo potrebam posameznikov, so enostavno dostopne, tudi preko spletnih strani pristojnega organa.

V prvem odstavku je določen tudi način posredovanja informacij posamezniku, ki se posredujejo praviloma v obliki, v kateri je bila zahteva vložena, tudi elektronski obliki.

Drugi odstavek pristojne organe zavezuje, da uresničevanje pravic posameznika čim bolj olajša, tudi tako, da za zahtevo pripravi obrazce.

Tretji odstavek nalaga pristojnim organom, da z namenom čim lažjega uresničevanja pravic posameznika, le-te posamezniku zagotovijo brez nepotrebnega odlašanja in brezplačno.

20. člen (ravnanje z očitno neutemeljeno ali pretirano zahtevo)

Predlagani 20. člen ureja načine postopanja v primeru, ko so zahteve posameznikov očitno neutemeljene ali pretirane, zlasti ker se ponavljajo, na primer, ko posameznik, na katerega se nanašajo osebni podatki, nerazumno in neprestano zahteva informacije ali zlorabi svojo pravico do informacij, na primer z navajanjem napačnih ali zavajajočih informacij pri oddaji zahteve. V teh primerih ima pristojni organ možnost zaračunati razumne materialne stroške, če bodo presegali 20 eurov (z vključenim DDV) ali zahtevo zavrniti, očitno neutemeljenost pa mora pristojni organ utemeljiti.

Predlagani člen, ki določa ravnanje z očitno neutemeljenimi ali pretiranimi zahtevami in dokazno breme pristojnega organa v zvezi s tem, izhaja iz uvodne navedbe št. 40 Direktive, kjer je med drugim navedeno:

»[…] Če so poleg tega zahteve očitno neutemeljene ali pretirane, kot v primeru, ko posameznik, na katerega se nanašajo osebni podatki, nerazumno in neprestano zahteva informacije ali zlorabi svojo pravico do informacij, na primer z navajanjem napačnih ali zavajajočih informacij pri oddaji zahteve, bi moral upravljavec imeti možnost zaračunati razumno pristojbino ali pa zavrniti ukrepanje v zvezi s to zahtevo.«

Minister za pravosodje bo izdal pravilnik, ki bo posebej urejal zaračunavanje materialnih stroškov, morebitno plačilo predujma za posredovanje zahtevanih podatkov v primeru pretiranih zahtev in ga objavil v uradnem listu.

21. člen (dajanje splošnih informacij)

Predlagani 21. člen določa, katere so tiste splošne informacije, ki jih pristojni organi tudi javno objavijo na svojih spletnih straneh (identiteta upravljavca, podatke pooblaščene osebe, namen obdelave, pravica do vložitve pritožbe in prijave pri nadzornem organu ter njegove kontaktne podatke, pravica do dostopa, popravka, izbrisa ali omejitve ter tudi pravne podlage za obdelavo osebnih podatkov[42]). Posamezniku se dajejo na razpolago tudi podatki o roku hrambe ali roku za reden pregled potrebe po hrambi, kategorije uporabnikov osebnih podatkov vključno z uporabniki v tretjih državah ali mednarodnih organizacijah in če so osebni podatki bili pridobljeni brez vednosti posameznika, na katerega se nanašajo.

22. člen (pravica do dostopa do osebnih podatkov)

[42] Določba o javnosti informacije o pravni podlagi za obdelavo osebnih podatkov izhaja iz drugega odstavka 38. 87, drugega odstavka 120. in 153. člena Ustave Republike Slovenije, ker v Republiki Sloveniji ne sme biti tajnih zakonov oziroma drugih predpisov.

Prvi odstavek predlaganega 22. člena določa pravico posameznika, da od pristojnega organa prejme potrditev o tem, ali se v zvezi z njim obdelujejo osebni podatki, ter prejeti kopijo teh podatkov, če se o njem osebni podatki obdelujejo.

Drugi odstavek določa pravico posameznika, da prejme konkretne informacije o tem, kateri osebni podatki se obdelujejo v zvezi z njim, in sicer: podatke o namenih in pravnih podlagah obdelave, vrstah osebnih podatkov, ki se obdelujejo, uporabnikih, zlasti tistih v tretjih državah ali mednarodnih organizacijah, razen če gre za omejitve iz prvega odstavka 23. člena tega zakona, vendar tudi v teh primerih vsaj okvirni opis uporabnikov, rokih hrambe ali roku za reden pregled potrebe po hrambi, pravici zahtevati popravek, izbris ali omejitev obdelave. S tem posameznik lahko preveri točnost in zakonitost obdelave, podatek pa prejme v obliki kopije osebnih podatkov. Prav tako se posameznika seznani s pravico do pritožbe ali prijave pri nadzornem organu ter njegovih kontaktnih podatkih in o vseh razpoložljivih informacijah o viru osebnih podatkov, kolikor identiteta vira ni varovana kot tajna ali zaupna.

Tretji odstavek določa, da v primerih, ko bi dostop do podatkov oviral ali vplival na uradne postopke, mu pristojni organ zaradi varovanja identitete oseb, zoper katere se izvajajo prikriti preiskovalni ukrepi po zakonu, ki ureja kazenski postopek, ali zoper katere so razpisani ukrepi prikritega evidentiranja in namenske kontrole po zakonu, ki ureja naloge in pooblastila policije, ta dostop omeji.

Četrti odstavek določa rok za odločanje pristojnega organa, ki je trideset dni po prejemu zahteve.

23. člen (omejitve pravice do dostopa do osebnih podatkov)

Prvi odstavek določa, da je pravice posameznika do dostopa do osebnih podatkov mogoče popolnoma ali delno omejiti, kadar je to določeno z zakonom (ta pravila v tem primeru prevladajo: npr. Zakon o nalogah in pooblastilih policije, zakoni, ki urejajo sodne postopke, omejitev pa mora biti skladna tudi z Listino o temeljnih pravicah Evropske unije in Evropsko konvencijo o človekovih pravicah, kot ju razlaga sodna praksa Sodišča Evropske unije in Evropskega sodišča za človekove pravice, zlasti glede vsebine teh človekovih pravic in temeljnih svoboščin, predvsem 8. člena Evropske konvencije o človekovih pravicah) in ob upoštevanju načela sorazmernosti (2. člen v zvezi s tretjim odstavkom 15. člena Ustave Republike Slovenije) v vsakem konkretnem primeru posebej, in sicer: da se onemogoči oviranje ali vplivanje na postopke v zvezi z nalogami in nameni pristojnih organov iz tega zakona, vključno s pridobivanjem in prenosi osebnih podatkov, zaradi javne varnosti, varnosti ali obrambe države in zaradi varstva pravic in svoboščin tretjih oseb. Torej je treba v vsakem konkretnem primeru omejevanja pravic posebej preveriti, da je takšno omejevanje v tem primeru resnično nujno in obenem sorazmerno v razmerju do razloga za omejevanje. Ta določba pomeni prenos določb tretjega odstavka 13. člena Direktive.

Drugi odstavek določa roke za odločitev o zavrnitvi ali omejitvi dostopa in razlogih zanje. Prisojni organ mora odločiti o navedenem brez nepotrebnega odlašanja, najpozneje pa v petnajstih dneh, ta rok pa pristojni organ lahko zaradi zapletenosti in števila zadev s sklepom podaljša največ za petnajst dni. Skupni rok za določitev je tako lahko največ 30 dni. Pristojni organ posameznika seznani z možnostjo pritožbe pri Informacijskem pooblaščencu zoper zavrnitev ali omejitev dostopa do osebnih podatkov.

Tretji odstavek določa, da pristojni organ v odločbi iz prejšnjega odstavka ne navede razlogov za zavrnitev ali omejitev dostopa, če bi to ogrozilo izvrševanje namena zavrnitve ali omejitve dostopa iz prvega odstavka tega člena. Obrazložitev mora biti razvidna iz uradnega zaznamka, ki ga ureja četrti odstavek. Odločba in uradni zaznamek skupaj omogočata preizkus odločitve pri Informacijskem pooblaščencu.

Četrti odstavek ureja zapis uradnega zaznamka o dejanskem stanju in razlogih za zavrnitev ali omejitev dostopa (t.i. dokumentiranje), kadar bi razlogi za zavrnitev v odločbi lahko ogrozili izvrševanje namena zavrnitve ali omejitve. V uradni zaznamek lahko vpogledata pooblaščena oseba za varstvo osebnih podatkov in informacijski pooblaščenec, vendar le v okviru opravljanja naloge, ki se nanaša na konkretno zadevo (npr. svetovanje, nadzor).

Peti odstavek ureja, da pristojni organ v okviru ne poda same potrditve ali zanikanja obdelave osebnih podatkov, kadar gre za izvajanje prikritih preiskovalnih ukrepov ali prikrite in namenske kontrole na podlagi konkretnih področnih zakonov, zaradi javne varnosti in oviranja ali vplivanja na postopke pristojnih organov. V takih primerih torej pristojni organ obdelava osebnih podatkov niti ne potrdi in niti ne zanika posamezniku, v zvezi s katerim se obdelujejo podatki, niti posamezniku, v zvezi s katerim se podatki ne obdelujejo.

Predlagano pa je, da vsi posamezniki – ne glede na položaj (ali so nadzorovani preko ukrepov; ali so se v njih slučajno znašli; ali pa sploh niso nadzorovani) – dobijo od pristojnega organa enak odgovor, iz katerega ni mogoče sklepati, ali se v zvezi z njimi osebni podatki obdelujejo ali ne. Namen določbe je zavarovati integriteto in učinkovitost preiskovalnih ukrepov.

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

Prvi odstavek ureja pravico posameznika od pristojnega organa zahtevati popravek oziroma dopolnitev svojih netočnih oziroma nepopolnih podatkov. Odstavek določa tudi roke za popravek, in sicer: petnajst dni od prejema zahteve, ta rok pa pristojni organ lahko zaradi zapletenosti in števila zadev s sklepom podaljša za največ petnajst dni. V primeru, če nepopolnih osebnih podatkov ni možno ali dopustno dopolniti, jim lahko pristojni organ priloži dopolnilno izjavo posameznika, na katerega se nanašajo osebni podatki; takrat torej pristojni organ podatkov ne spremeni, ampak jim le priloži uradni zaznamek o izjavi.

Drugi odstavek ureja izbris podatkov, če obdelava krši določbe o zakonitosti obdelave osebnih podatkov ali posebnih vrst osebnih podatkov ali določbe o obdelavi podatkov za drug namen (6., 7. in 8. člen tega zakona) ali pa je treba osebne podatke izbrisati zaradi izpolnitve pravne obveznosti, ki velja za pristojni organ (na podlagi zakona ali po pravnomočni sodni odločbi, odločbi Ustavnega sodišča RS, mednarodno zavezujočih aktov, sporazumov…). Odstavek določa tudi roke za izbris, in sicer petnajst dni, ta rok pa pristojni organ lahko zaradi zapletenosti in števila zadev s sklepom podaljša največ za petnajst dni.

Tretji odstavek določa omejitev obdelave namesto izbrisa iz že omenjenih razlogov, torej če netočnih ali nepopolnih podatkov in te netočnosti ali posodobljenosti ni mogoče preveriti (v tem primeru mora posameznika, na katerega se nanašajo osebni podatki, obvestiti ob preklicu omejitve), ter iz razloga, da je treba osebne podatke še vedno hraniti za namen dokazovanja.

V takšnem primeru bi bilo treba omejene podatke obdelovati le za namen, ki je preprečil njihov izbris. Metode za omejitev obdelave osebnih podatkov bi lahko med drugim zajemale prenos izbranih podatkov v drug sistem za obdelavo, na primer za namene arhiviranja, ali onemogočenje dostopnosti izbranih podatkov. Pri avtomatiziranih zbirkah bi bilo treba omejitev obdelave načeloma zagotoviti s tehničnimi sredstvi. V zbirki bi moralo biti jasno navedeno dejstvo, da je obdelava osebnih podatkov omejena.

Po četrtem odstavku mora pristojni organ posameznika, na katerega se nanašajo osebni podatki, s odločbo o zavrnitvi popravka, izbrisa osebnih podatkov ali o omejitvi obdelave obvestiti o razlogih za zavrnitev ter o možnosti vložitve pritožbe pri Informacijskem pooblaščencu in o njegovih kontaktnih podatkih. Če so podane okoliščine iz prvega, tretjega ali petega odstavka 23. člena, pa ne navede razlogov za zavrnitev in ravna enako kot po predlaganem 23. členu.

Po petem in šestem odstavku mora pristojni organ v primerih popravka, izbrisa podatkov ali omejitve obdelave obvestiti vse uporabnike osebnih podatkov. Uporabniki so zavezani osebne podatke, ki so v njihovi pristojnosti, nemudoma popraviti, izbrisati, ustrezno označiti ali omejiti njihovo obdelavo in torej prenehati širiti.

25. člen (pravna sredstva)

Predlagani 25. člen določa pravna sredstva, ki so na voljo posamezniku za uveljavljanje pravic po tem oddelku. O pritožbi zoper odločitev pristojnega organa odloča Informacijski pooblaščenec kot organ druge stopnje.

Drugi odstavek določa pravna sredstva zoper odločitve Informacijskega pooblaščenca, s katerimi se postopek konča (odločba, sklep o zavrženju zahteve, sklep o ustavitvi postopka itd.). Sklepe v zvezi z izvedbo postopka (postranska vprašanja za izvedbo upravnega postopka), zoper katere je po ZUP možna posebna pritožba, je po tem zakonu dopustno izpodbijati le v upravnem sporu zoper končno odločitev.

Tretji odstavek določa aktivno legitimacijo za vložitev tožbe v upravnem sporu, ki jo priznava tako stranki v postopku kot tudi pristojnemu organu.

3. oddelek – inšpekcijski nadzor

Tretji oddelek ureja inšpekcijski nadzor in inšpekcijska pooblastila ter ukrepe, ki jih uporablja nadzorni organ za nadzor po tem oddelku.

1. pododdelek – skupne določbe

Poleg skupnih določb, ki so v predlogu zakona urejene v prvem oddelku II. poglavja (uveljavljanje pravic pred pristojnim organom, obdelovalcem in nadzornim organom, omejitve vpogleda v spis, preverjanje identitete posameznika, zavarovanje osebnih podatkov, ki so predmet postopka, izvršba), prvi pododdelek ureja dodatne skupne določbe glede pravil postopka, ki jih Informacijski pooblaščenec uporablja pri izvajanju inšpekcijskega nadzora v interesu prijavitelja s posebnim položajem in pri izvajanju inšpekcijskega nadzora v javnem interesu.

26. člen (splošna pravila postopka)

Predlagani 26. člen določa, da Informacijski pooblaščenec v postopkih inšpekcijskega nadzora subsidiarno uporablja ZIN, če določbe tega zakona posamezne institute ne urejajo drugače.

27. člen (izvajanje postopkovnih dejanj brez prisotnosti)

Predlagani 27. člen določa, da lahko v postopku inšpekcijskega nadzora Informacijski pooblaščenec zaslišuje osebe pri pristojnem organu in priče brez prisotnosti prijavitelja, v celoti ali deloma, če je takšna prisotnost v nasprotju z javnim interesom ali interesom tretjih oseb. V takem primeru se tudi ne dovoli prisotnosti pri drugih dejanjih v postopku in mu ne vroča zapisnikov o teh dejanjih. Gre za odstop od načela kontradiktornosti postopka, ki pa je nujen za zagotavljanje integritete postopkov pristojnih organov, v zvezi s katerimi bi razkritje osebnih podatkov posamezniku postopke lahko oviralo ali celo onemogočilo. Informacijski pooblaščenec prijavitelja obvesti o izvajanju postopkovnih dejanj brez njegove prisotnosti.

Drugi odstavek določa obligatorno izključitev prisotnosti prijavitelja in vročanje pisanj, v primerih, ko bi se s tem razkrila identiteta oseb, zoper katere se izvajajo prikriti preiskovalni ukrepi po Zakonu o kazenskem postopku ali prikrita in namenska kontrola iz Zakona o nalogah in pooblastilih policije.

28. člen (izključitev stranske udeležbe)

Predlagani 28. člen v inšpekcijskih postopkih pred Informacijskim pooblaščencem izključuje stransko udeležbo. ZIN izrecno določa, da prijavitelj ni stranka v postopku, s tem zakonom pa je določeno, da ima prijavitelj, na katerega se nanašajo osebni podatki, položaj stranke v postopku (drugi odstavek 31. člena), s čimer so pravice posameznika ustrezno zaščitene tudi brez instituta stranske udeležbe.

29. člen (nadzorna pooblastila v inšpekcijskih postopkih)

Predlagani 29. člen ureja nadzorna pooblastila nadzornikov. Na enem mestu so taksativno zajeta pooblastila, ki jih deloma določajo že ZIN, ZVOP-1 in katere zahteva Direktiva (47. člen).

Prvi odstavek določa temeljna nadzorna (preiskovalna) pooblastila. V 1. točki je določen pregled dokumentacije, v 2. točki pregled poslovnih knjig, v 3. točki vstopi in pregledi prostorov ipd., v 4. točki zavarovanje in pregled elektronskih in z njimi povezanih naprav ter nosilcev elektronskih podatkov, v 5. točki odvzem ali pridobitev ustrezne kopije osebnih podatkov ali druge dokumentacije, v 6. točki je določen izjemni ukrep zapečatenja ustreznega dela prostorov in opreme ipd., v 7. točki zaseg

predmetov ter poslovnih knjig ipd., v 8. točki pa je podano posebno pooblastilo, da se lahko uporabijo tudi druga pooblastila, določena z drugim zakonom (npr. ZIN) – seveda le v primeru, če določenega pooblastila ne ureja predlog tega zakona.

Poudariti je treba, da je v naslednjih odstavkih določeno, da se tudi v inšpekcijskih postopkih do določenih vsebin osebnih podatkov (v poslovnih prostorih, elektronski dokumentaciji) lahko dostopa le na podlagi predhodne sodne odredbe, kot to zahtevata 36. člen (hišna zasebnost) in 37. člen Ustave Republike Slovenije. Možnost oziroma potrebnost tovrstnih posegov utemeljuje določba drugega odstavka 1. člena, ki kaže na pomembnost varovanja ustavne pravice do varstva osebnih podatkov (38. člen Ustave Republike Slovenije). Pri tem se izhaja iz odločbe Ustavnega sodišča Republike Slovenije iz leta 2013[43].

Člen torej določa varovalke pri uporabi inšpekcijskih pooblastil, v zvezi z njimi pa je treba opozoriti tudi na 37. člen ZIN, ki določa odgovornost države za škodo.

30. člen (inšpekcijski ukrepi)

Predlagani 30. člen ureja inšpekcijske ukrepe Informacijskega pooblaščenca v primeru kršitve določb predpisov, ki urejajo varstvo osebnih podatkov na področju uporabe tega zakona. Poleg ukrepov, določenih v tem členu, lahko Informacijski pooblaščenec odredi tudi druge ukrepe, ki jih določa ZIN. Namen inšpekcijskih postopkov je doseči skladnost obdelave osebnih podatkov z veljavno zakonodajo.

6. točka prvega odstavka 30. člena tudi določa možnost uporabe ukrepov ali pooblastil iz drugih zakonov (zlasti ZIN), vendar v primeru razlike prevladajo določbe ZVOPPOKD (npr. kadar ZVOPPOKD v 29. členu določa odreditev predhodne sodne odredbe za določene nadzorne posege).

Predlagani drugi odstavek določa splošno prepoved, da bi nadzorni organ z inšpekcijskimi ukrepi posegal v kazenske zadeve sodišča (definicija je v 24. točki 4. člena). Na ta način je varovana neodvisnost kazenskega sodstva ter Ustavnega sodišča Republike Slovenije, kadar gre za odločanje glede kazenskih zadev (npr. presoja ustavnosti s področja dokaznega prava). Določba izhaja iz spoštovanja temeljnega načela vsake pravne in demokratične države, namreč neodvisnosti sodstva.[44]

2. pododdelek – inšpekcijski nadzor v interesu prijavitelja s posebnim položajem

Drugi pododdelek ureja položaj in pravice prijavitelja s posebnim položajem ter posebna pravila postopka. Poleg skupnih določb, ki so v predlogu zakona urejene v prvem oddelku II. poglavja (uveljavljanje pravic pred pristojnim organom, obdelovalcem in nadzornim organom, omejitve vpogleda v spis, preverjanje identitete posameznika, zavarovanje osebnih podatkov, ki so predmet postopka, izvršba), se za postopek po tem pododdelku uporabljajo tudi določbe prejšnjega pododdelka (skupne določbe).

31. člen (prijava in prijavitelj s posebnim položajem)

V predlaganem 31. členu je definiran prijavitelj s posebnim položajem. Posebnost položaja je v dejstvu, da ima lastnost stranke v postopku, kar je odstop od določb ZIN, ki izrecno določajo, da prijavitelj ni stranka v postopku. Položaj in pravice stranke v postopku ureja ZUP. Z določbami tega pododdelka se določene pravice stranke v postopku omejujejo ali dopolnjujejo. Inšpekcijski postopek se v tem primeru ne vodi v javnem interesu, temveč v interesu prijavitelja.

[43] Odločba US, št. U-I-40/12, 11. 4. 2013, OdlUS XX, 5 in Uradni list RS, št. 39/13.
[44] Za starejšo ustavnosodno presojo glede neposeganja nadzornega organa v upravne zadeve (pred sprejetjem Splošne uredbe o varstvu podatkov) glejte: odločba US, št. U-I-92/12, 10. 10. 2013; objava: Uradni list RS, št. 89/13.

32. člen (posebna pravila postopka)

Predlagani 32. člen določa, da je za razliko od ZIN, kjer ima inšpekcijski organ diskrecijsko pravico glede odločitve o uvedbi inšpekcijskega postopka, po tem zakonu uvedba postopka obligatorna. Prijava mora vsebovati vse sestavine, kot jih določa ZUP.

ZIN ne določa roka za izvedbo inšpekcijskega nadzora, zato bi v tem primeru obveljal splošen rok, ki ga določa ZUP (1 mesec za enostavne oziroma 2 meseca za zahtevnejše postopke). Ker je vsebina nadzora zahtevna, zakon določa daljši rok (3 mesece) z možnostjo podaljšanja za dodaten mesec.

Tretji odstavek določa, da lahko očitno neutemeljene prijave Informacijski pooblaščenec zavrne, to pa mora storiti v roku enega meseca.

Četrti odstavek določa, da vir prijave ni tajen, kar je nuno potreben odstop od ZIN, ker se postopek vodi v interesu prijavitelja in ne v javnem interesu. Prijavitelj je stranka v postopku.

33. člen (pravice prijavitelja s posebnim položajem)

Predlagani 33. člen določa, da nadzorni organ prijavitelja na njegovo zahtevo, izraženo v prijavi ali v naknadni komunikaciji, obvešča o svojih ukrepih. Kot izhaja iz skupnih določb, je kontradiktornost postopka omejena, prijavitelj je lahko izključen od sodelovanja v postopkovnih dejanjih in od vpogleda v spis. Obveščanje daje prijavitelju možnost, da se seznani s stanjem postopka.

Drugi odstavek določa, da se prijavitelj lahko vključi v postopek, ko je izdan osnutek odločbe nadzornega organa, in nanj poda pripombe, razen kadar je izdana odločba o zavrnitvi obravnave očitno neutemeljene prijave (tretji odstavek predlaganega 32. člena).

34. člen (položaj pristojnih organov)

Predlagani 34. člen določa, da ima pristojni organ položaj zavezanca, kot ga določa ZIN. Posamezne izjeme so določene v nadaljnjih odstavkih.

Drugi odstavek določa, da lahko pristojni organ na osnutek odločbe (kot tudi prijavitelj na podlagi predlaganega drugega odstavka 33. člena) poda pripombe, do katerih se mora nadzorni organ opredeliti. S tem se zagotavlja kontradiktornost postopka v delu, ki se nanaša na odločbo in vse okoliščine, ki so pomembne za odločitev.

Tretji odstavek določa izjemo od ZIN in podobno kot ZUP določa obveznost pristojnega organa, njegove odgovorne ali druge pooblaščene osebe, da v postopku govorijo resnico in ne smejo ničesar zamolčati. Njihove izjave se lahko štejejo kot izjave strank. Enaka obveznost po ZUP velja tudi za prijavitelja.

Četrti odstavek ureja omejitev prehajanja podatkov iz inšpekcijskega postopka v morebitni prekrškovni postopek. V prekrškovnem postopku bo treba izvesti ločen ugotovitveni postopek in ugotavljati dejstva in okoliščine, ki predstavljajo znake prekrška.

35. člen (odločba)

Predlagani 35. člen določa vsebino odločbe izdane v inšpekcijskem nadzoru po tem pododdelku. Poleg sestavin po ZUP mora vsebovati še sestavine iz te določbe. Posebno pozornost je treba nameniti dovoljenemu obsegu pregleda spisa.

Obveznost obrazložitve odločbe pa od pravil ZUP odstopa v primeru, ko bi navedba razlogov za zavrnitev ali omejitev dostopa ogrozila izvrševanje namena zavrnitve ali omejitve dostopa iz prvega odstavka 23. člena tega zakona. Prav tako odločba v skladu s petim odstavkom 23. člena tega zakona ne obsega navedb, s katerimi bi se potrdilo ali zanikalo izvajanje ali neizvajanje prikritih preiskovalnih ukrepov iz zakona, ki ureja kazenski postopek, ali prikritih in namenskih kontrol iz zakona, ki ureja naloge in pooblastila policije.

Ker v inšpekcijskem nadzoru pred Informacijskim pooblaščencem ni drugostopenjskega organa, ki bi odločal o pritožbi, postane odločba izvršljiva z vročitvijo prijavitelju in zavezancu.

36. člen (ukrepanje glede obdelav osebnih podatkov drugih posameznikov)

Predlagani 36. člen določa, da če nadzorni organi v postopku inšpekcijskega nadzora po tem pododdelku zazna sum kršitve varstva pravic glede osebnih podatkov, ki bi lahko vplivale na druge posameznike, lahko poleg že tekočega postopka, iz katerega izvirajo ugotovitve, uvede tudi inšpekcijski nadzor v javnem interesu. Postopek po prijavi prijavitelja s posebnim položajem se torej nadaljuje v skladu z določbami tega zakona, nadzorni organ pa se lahko odloči, da uvede sočasni nadzor (predvidoma glede širšega kroga posameznikov) v javnem interesu.

3. pododdelek – inšpekcijski nadzor v javnem interesu

Poleg skupnih določb, ki so v predlogu zakona urejene v prvem oddelku II. poglavja (uveljavljanje pravic pred pristojnim organom, obdelovalcem in nadzornim organom, omejitve vpogleda v spis, preverjanje identitete posameznika, zavarovanje osebnih podatkov, ki so predmet postopka, izvršba), se za postopek po tem pododdelku uporabljajo tudi določbe prvega pododdelka (skupne določbe) in določbi tega pododdelka, ki urejata uvedbo postopka.

37. člen (uvedba inšpekcijskega nadzora v javnem interesu)

Predlagani 37. člen določa, da Informacijski pooblaščenec vedno uvede postopek inšpekcijskega nadzora v javnem interesu (*ex offo*) na lastno pobudo, na podlagi pobude drugih organov (državni organi, nadzorne javne agencije Republike Slovenije in nadzorni organ za varstvo osebnih podatkov države članice Evropske unije in Sveta Evrope) in na podlagi pobude fizične ali pravne osebe ter na podlagi ugotovljenega suma kršitve varstva pravic glede osebnih podatkov, ki bi lahko vplivale na druge posameznike, pri obravnavi prijave prijavitelja s posebnim položajem (36. člen predloga).

38. člen (uvedba inšpekcijskega nadzora na pobudo drugih organov)

Predlagani 38. člen v prvem odstavku našteva uradne pobudnike (dejansko predlagatelje) za uvedbo inšpekcijskega nadzora v javnem interesu in v drugem odstavku določa, da se takšen nadzor izvede prednostno, če to ne škoduje izvedbi nadzorov v interesu prijavitelja.

III. poglavje

OBVEZNOST PRISTOJNIH ORGANOV, OBDELOVALCEV IN SKUPNIH UPRAVLJAVCEV

39. člen (odgovornost pristojnega organa za skladnost)

Predlagani 39. člen določa posebno vrsto pristojnosti – dejansko odgovornosti – pristojnega organa za zagotavljanje skladnosti obdelave osebnih podatkov.

Po prvem odstavku mora pristojni organ izvesti (dejanska izvedba) in dokumentirati (stalna razpoložljiva in posodabljana dokumentacija) ustrezne tehnične in organizacijske ukrepe, s katerimi zagotovi skladnost obdelave z zakonom (ne samo varnost osebnih podatkov, tudi sledljivost, dnevniki obdelave …).

Po drugem odstavku pristojni organ pri izbiri ukrepov iz prvega odstavka tega člena upošteva naravo, obseg, okoliščine in namene obdelave, pa tudi tveganja za človekove pravice in temeljne svoboščine, ki so povezana z obdelavo in se razlikujejo po verjetnosti in resnosti. Kadar je to sorazmerno glede na dejavnosti obdelave, ukrepi vključujejo tudi izvajanje ustreznih politik za varstvo osebnih podatkov.

Po tretjem odstavku pristojni organ ukrepe iz prvega odstavka tega člena občasno (po potrebi) pregleda in dopolni, zlasti kadar se spremenijo okoliščine obdelave.

Po četrtem odstavku mora biti pristojni organ vedno zmožen izkazati skladnost obdelave z ZVOPPOKD. Običajno bo to izkazal Informacijskemu pooblaščencu pri opravljanju nadzorov po tem zakonu, pooblaščeni osebi za varstvo osebnih podatkov, sistemu notranje kontrole, lahko pa tudi pred Upravnim sodiščem Republike Slovenije v konkretnem sodnem postopku.

Predlagani člen tako ureja eno ključnih novosti Direktive v primerjavi s prejšnjih Okvirnim sklepom – po vzoru iz Splošne uredbe vsebuje novo obveznost upravljavca, da ves čas izvajanja obdelav skrbi za skladnost teh obdelav s pravili ZVOPPOKD oziroma področnih zakonov 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 do sedaj veljalo zgolj za ukrepe za zavarovanje osebnih podatkov oziroma za (pogodbeno) obdelavo – drugi odstavek 25. člena oziroma 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 oziroma za obdelavo podatkov, določitev odgovornih oseb za posamezne zbirke osebnih podatkov ter pravila za izvajanje revizij. Primerne postopek, 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 ali pridobi ustrezno in za to namenjeno programsko opremo.

Pristojni organ mora Informacijskemu pooblaščencu omogočiti nemoteno opravljanje njegovih nalog. To pomeni, da mu mora zlasti omogočiti pregled dokumentacije, vsebine zbirk, opraviti razgovore z uradnimi osebami, posredovati zahtevana pojasnila in odgovore na vprašanja in podobno.

40. člen (vgrajeno in privzeto varstvo osebnih podatkov)

Predlagani 40. člen predstavlja implementacijo 20. člena Direktive. V prvem odstavku in v drugem odstavku so določena pravila glede vgrajenega varstva osebnih podatkov. V tretjem odstavku pa so določena pravila glede privzetega varstva osebnih podatkov.

Po prvem in drugem odstavku ima upravljavec obveznost, da že pri načrtovanju novih obdelav preveri, katere podatke dejansko 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 po tretjem odstavku svoje obdelave v čim večji meri zasnovati tudi tako, da se v vsakem posamičnem primeru pridobijo in obdelajo samo tiste podatki, ki so potrebni v tem primeru. To pri obdelavah, ki se izvajajo s sredstvi informacijske tehnologije, zlasti pomeni, da se pred začetkom vsake obdelave ne naložijo vsi podatki, ki bi bili potrebni za tipično obdelavo te vrste, ampak, kolikor je le mogoče, zgolj tisti podatki, ki jih potrebuje ta konkretna obdelava (privzeto varstvo osebnih podatkov).

41. člen (skupni upravljavci)

Predlagani 41. člen za primere, ko dva ali več pristojnih organov ali pristojnih organov in upravljavcev skupaj določijo sredstva obdelave, določa obveznost, da ti organi svoje medsebojne odnose glede sredstev obdelave uredijo s pisnim dogovorom. Ne morejo pa samostojno določati namenov obdelave, nameni so lahko določeni le z zakonom (prvi odstavek 6. člena predloga zakona). Prav tako ta člen določa, da se lahko posamezniki, katerih osebni podatki se pri tem obdelujejo, glede svojih pravic obrnejo na kateregakoli od teh skupnih upravljavcev.

42. člen (obdelovalec)

Predlagani 42. člen ureja možnost zaupanja izvedbe posameznih dejanj obdelave zunanjemu subjektu (obdelovalcu).

Tako kot že do sedaj lahko upravljavec posamezna opravila v zvezi z obdelavo osebnih podatkov pogodbeno preda (zaupa) obdelovalcu (dosedanjemu »pogodbenemu obdelovalcu«). Podobno kot po veljavni ureditvi mora njuna medsebojna razmerja še vedno urediti v pisni pogodbi ali v drugem pisnem dogovoru, pri čemer pa mora ta pogodba ali dogovor zdaj zagotoviti izvajanje vseh obveznosti po tem zakonu, ne zgolj obveznosti varstva (zavarovanja) obdelave. 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 oziroma 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 to 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 sme 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 do sedaj, je pa podrobnejša (tretji odstavek).

V petem odstavku 42. člen, ki je z vidika dejanskega uresničevanja pravic posameznikov, na katere se nanašajo osebni podatki, en najpomembnejših členov predloga zakona, je določeno, da če obdelovalec v nasprotju z določbami ZVOPPOKD oziroma pisne pogodbe ali pisnega dogovora samostojno določi druge namene oziroma sredstva obdelave, se ta obdelovalec v zvezi s to obdelavo šteje za upravljavca. Ta določitev seveda ne pomeni, da obdelovalec ne velja za kršitelja določb ZVOPOKD.

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).

Obdelovalec (vključno z obdelovalcem, ki po petem odstavku 42. člena predloga izjemoma velja za upravljavca) mora Informacijskemu pooblaščencu omogočiti nemoteno opravljanje njegovih nalog. To pomeni, da mu mora zlasti omogočiti pregled dokumentacije, zbirk podatkov, opraviti razgovore z uradnimi osebami, posredovati zahtevana pojasnila in odgovore na vprašanja in podobno.

43. člen (dolžnost upoštevanja navodil pristojnega organa)

Predlagani 43. člen na podlagi 23. člena Direktive določa, da nihče (vsak zaposleni, vsaka uradna oseba ali drugače pooblaščena oseba), ki dela za pristojni organ ali obdelovalca in ima dostop do osebnih podatkov, teh osebnih podatkov ne sme obdelovati brez navodila pristojnega organa, razen če to določa zakon (npr. delovanje na podlagi sodne odredbe – predložitev osebnih podatkov ali dokazov sodišču, delovanje na podlagi dostopa do informacij javnega značaja).

44. člen (evidenca dejavnosti obdelave)

Predlagani 44. člen na podlagi 24. člena Direktive 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 omejeno in je zato evidenca obdelav podrobneje določena (ni pa javna), 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 obdelovalce.

45. člen (vodenje dnevnikov)

Predlagani 45. člen določa obveznost vodenja dnevnikov obdelave, na podlagi 25. člena Direktive. Obveznost je določena za pristojne organe, upravljavce iz 41. člena ZVOPPOKD ter za obdelovalce iz 42. člena ZVOPPOKD.

V prvem odstavku so določene tipične dejanja, ki se morajo zabeležiti (evidentirati) v dnevniku obdelave, dejanja so našteta enumerativno in vključujejo: zbiranje, spreminjanje, vpogled, razkritje, vključno s prenosi, povezovanje, izbris.

V drugem odstavku je določena posebna sledljivost glede obdelav, v zvezi s spoštovanjem namenov iz prvega odstavka 1. člena ZVOPPOKD ter namenov iz področnih zakonov.

Tretji odstavek določa, da se smejo podatki iz dnevnika obdelave uporabljati zgolj za preverjanje zakonitosti obdelave, notranji nadzor, zagotavljanje celovitosti in varnosti osebnih podatkov ter za potrebe predkazenskih in kazenskih postopkov.

Četrti odstavek določa, da morajo pristojni organi, skupni upravljavci in obdelovalci nadzornemu organu na njegovo zahtevo omogočijo dostop do dnevnika obdelave.

Po petem odstavku se vsebina dnevnika obdelave hrani dve leti od zaključka koledarskega leta, v katerem so bila v njih zabeležena dejanja obdelave, če drug zakon ne določa drugače (npr. šesti odstavek tega člena). Namen dvoletnega roka hrambe je zagotovitev sledljivosti po drugem odstavku.

Predlagani šesti odstavek določa, da se vsebina dnevnika obdelave, ki ga upravlja Nacionalna enota za informacije o potnikih po Zakonu o nalogah in pooblastilih policije, zaradi obstoja večjega tveganja za človekove pravice in temeljne svoboščine posameznikov hrani pet let od zaključka koledarskega leta, v katerem so bila v njih zabeležena dejanja obdelave. Tu gre za prenos šestega odstavka 13. člena Direktive (EU) 2016/681.

46. člen (preverjanje kakovosti podatkov)

Predlagani 46. člen določa, da pristojni organ sprejme vse razumne ukrepe, da se pred posredovanjem osebnih podatkov ali njihovim dajanjem na voljo preveri njihova točnost, popolnost, zanesljivost in posodobljenost. Na ta način se implementira 7. člen Direktive.

Po drugem odstavku pristojni organ osebnim podatkom, ki se posredujejo ali dajo na razpolago, priloži dodatne informacije, na podlagi katerih lahko uporabnik oceni njihovo točnost, popolnost, zanesljivost in posodobljenost, če z njimi razpolaga.

Po tretjem odstavku se v situacijah, kadar je izkazano, da so bili posredovani ali dani na razpolago (npr. vpogled) osebni podatki, ki ne ustrezajo zahtevam iz prvega odstavka tega člena, ali so bili posredovani nezakonito, pristojni organ to nemudoma sporoči vsem uporabnikom.

Po četrtem odstavku pristojni organ v situaciji iz tretjega odstavka nemudoma popravi osebne podatke oziroma jih izbriše ali omeji njihovo obdelavo.

Po petem odstavku je v primeru izbrisa osebnih podatkov zaradi zagotavljanja sledljivosti obdelave osebnih podatkov v skladu s 45. členom ZVOPPOKD 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. Določba je konkretna izpeljava 20. točke 4. člena ZVOPPOKD, ki določa institut izbrisa.

47. člen (razlikovanje med različnimi kategorijami posameznikov)

Predlagani 47. člen izhaja iz posebne potrebe za zagotovitev točnosti osebnih podatkov v kontekstu prvega odstavka 1. člena Direktive ter prvega odstavka 1. člena ZVOPPOKD. Določeno je razlikovanje med različnimi kategorijami posameznikov, na katere se nanašajo osebni podatki, kot to zahteva 6. člen Direktive. Določena so pravila, po katerih pristojni organ pri obdelavi osebnih podatkov v največji možni meri in z uporabo razumnih ukrepov razlikuje med osebnimi podatki različnih kategorij posameznikov, na katere se nanašajo osebni podatki, kot so:

1. osumljenci;

2. obdolženci,

3. obtoženci,

4. obsojenci;

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 ali so bile v stiku ali povezane z osebami iz prejšnjih točk (omrežja presumptivnih sodelavcev, operativne informacije).

Kategorije oseb od 1. do 6. so naštete enumerativno, posebej odprta je kategorija pod 6. točko. Določbe omogočajo, da jih pristojni organ v praksi glede na dejanske okoliščine razširi, torej določi dodatne kategorije posameznikov glede na njihov drugačen položaj.

48. člen (razlikovanje med osebnimi podatki, ki temeljijo na dejstvih, in osebnimi podatki, ki temeljijo na osebnih ocenah)

Predlagani 48. člen določa, da pristojni organ pri obdelavi osebnih podatkov v največji možni meri razlikuje med osebnimi podatki, ki temeljijo na dejstvih, in osebnimi podatki, ki temeljijo na osebnih ocenah. Pri tem osebne podatke, ki temeljijo na osebnih ocenah, v največji možni meri ustrezno označi ter utemelji na način, ki omogoča naknadno preverjanje teh ocen. Predlagani člen predstavlja implementacijo 7. člena Direktive.

2. oddelek – ukrepi pred obdelavo in varnost osebnih podatkov

49. člen (ocena učinka)

Predlagani 49. člen določa obveznost izdelave ocene učinka v zvezi z načrtovano obdelavo osebnih podatkov, kadar bi lahko kategorija obdelave zlasti zaradi uporabe novih tehnologij in ob upoštevanju narave, obsega, okoliščin oziroma namena obdelave povzročila veliko tveganje za človekove pravice in temeljne svoboščine posameznikov.

Drugi odstavek določa okoliščine, ko je treba oceno učinka vedno opraviti, tretji odstavek pa določa izjemo, ko ocene ni treba pripraviti – to je kadar je oceno učinka že izdelal predlagatelj zakona, ki je podlaga za obdelavo. Kljub izjemi je treba oceno učinka opraviti, če so se okoliščine (tehnološke, varnostne) po izdelavi ocene učinka v zakonodajnem postopku bistveno spremenile.

Četrti odstavek določa sestavine ocene učinka.

Peti odstavek določa obveznost, da pristojni organ vedno, ne glede na izjemo v tretjem odstavku, pred uvedbo novega sistema za avtomatizirano obdelavo osebnih podatkov izdela oceno učinka glede ukrepov za zagotavljanje varnosti obdelave, ki obsega ukrepe za zagotavljanje varnosti obdelave in mehanizme za zagotavljanje varstva osebnih podatkov – torej, da načrtuje varnost sistema.

50. člen (predhodno posvetovanje z nadzornim organom)

Predlagani 50. člen določa obveznost, da se pristojni organ in obdelovalec pred začetkom obdelave, ki bo del nove zbirke, o tem predhodno posvetujeta z Informacijskim pooblaščencem. Takšno posvetovanje je treba vedno izvesti, ko iz ocene učinka izhaja, da bi obdelava povzročila veliko tveganje za človekove pravice ali temeljne svoboščine posameznikov, če pristojni organ ne bi sprejel ukrepov za zmanjšanje tega tveganja, ali kadar se bodo pri obdelavi uporabljale nove tehnologije, mehanizmi in postopki, kar bi lahko predstavljalo veliko tveganje za človekove pravice ali temeljne svoboščine posameznikov.

Informacijski pooblaščenec na svojih spletnih straneh objavi seznam kategorij obdelave, za katere mora pristojni organ v skladu s prejšnjim odstavkom opraviti predhodno posvetovanje. Informacijski pooblaščenec skrbi, da je seznam vedno posodobljen in vsebuje kategorije obdelave, ki so po njegovi oceni takšne, da je v zvezi z njimi potrebno predhodno posvetovanje.

V okviru predhodnega posvetovanja morata pristojni organ in obdelovalec informacijskemu pooblaščencu omogočiti vpogled v oceno učinka in druge informacije, ki jih ta rabi, da lahko ustrezno svetuje.

Informacijski pooblaščenec v šestih tednih izdela pisno mnenje, v katerega vključi nasvete pristojnemu organu in, kadar je to primerno, obdelovalcu, katere dodatne ukrepe v zvezi z načrtovano obdelavo je treba sprejeti. Rok za izdelavo mnenja se lahko podaljša za en mesec ob upoštevanju zapletenosti zadeve.

51. člen (varnost obdelave)

Predlagani člen ureja ukrepe za zagotavljanje varnosti obdelav podatkov v informacijskih sistemih.

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

Namen določbe je zagotoviti, da so podatki obdelani na način, ki zagotavlja ustrezno raven varnosti in zaupnosti, vključno s preprečevanjem nedovoljenega dostopa do osebnih podatkov in opreme za obdelavo ali njihove uporabe, in ki upošteva razpoložljive tehnološke ravni in tehnologije, stroške izvajanja glede na tveganja in na naravo osebnih podatkov, ki jih je treba varovati (uvodna navedba št. 28 Direktive).

Varnost obdelav osebnih podatkov je treba zagotavljati za podatke v mirovanju, podatke v prenosu in za podatke v uporabi. Varnost se zagotavlja z uporabo primernih ukrepov na področjih, ki so navedena v seznamu drugega odstavka. Konkretni ukrepi so odvisni od ocene tveganj. Ocena tveganj je lahko pripravljena že v okviru ocene učinkov, sicer pa kot del načrtovanja ukrepov za zagotavljanje varnosti obdelave.

52. člen (obvestilo nadzornemu organu o kršitvi varnosti osebnih podatkov)

Predlagani člen ureja ti. »obvestilo o kršitvi« ("*breach notification*"), po vzoru Zakona o elektronskih komunikacijah[45] (81. člen) ter tudi Zakona o informacijski varnosti[46] (npr. tretji odstavek 31. člena). Gre za pravilo, da morajo upravljavci v primeru odkritih varnostnih napadov oziroma 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 varnostnem incidentu (ali sumu na varnostni incident), ampak zgolj o tistih, za katere je verjetno, da so oziroma še bodo povzročili tveganje za posege v človekove pravice in temeljne svoboščine posameznikov. Ključno je predvsem, ali so napadalci lahko dostopali do podatkov. Konkreten primer takšne kršitve bi bila na primer izguba šifriranega nosilca podatkov (npr. USB-ključa). Ni verjetno, da bi v takšnem primeru nastala tveganja za človekove pravice, ker šifriranih podatkov brez gesla ni mogoče prebrati. V primerih napadov na dosegljivost informacijskega sistema (ti. »*availability napadi*«, med njimi zlasti napadov za onemogočanje dosegljivosti [»*distributed denial of service attack*« – DDOS]), kjer sicer gre za varnostni incident, ni pa nujno, da je prišlo tudi do kršitve varstva osebnih podatkov, Informacijskega pooblaščenca ni potrebno obveščati; v primeru napada z zlorabo ranljivosti strežnika z vrivanjem SQL-stavkov (»*SQL injection*«), za katere je značilno, da napadalec pridobi dostop do podatkov na strežniku, pa je takšno obvestilo potrebno.

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. Namen roka je dati Informacijskemu pooblaščencu možnost čim prej odrediti morebitne ukrepe za zagotovitev varnosti osebnih podatkov, kot tudi, 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, da lahko ti izvedejo ustrezne ukrepe 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 iz informacijsko-varnostne sfere, saj bi čakanje na dokončno raziskanost incidenta lahko povzročilo znatno dodatno škodo posameznikom zaradi zlorab njihovih podatkov v vmesnem času.

Posamezne vidike notifikacijske dolžnosti je že obravnavala Delovna skupina po členu 29 Direktive 95/46/ES, in o tem izdala ustrezne smernice[47].

Tretji odstavek določa vsebino poročila Informacijskemu pooblaščencu, pri tem pa ni treba že v začetku posredovati vseh informacij, če pristojni organ z njimi ne razpolaga – četrti odstavek določa možnost postopnega obveščanja.

Dodatna novost je še v tem, da mora upravljavec takoj po odkritju varnostne grožnje pristopiti k zavarovanju dokazov o dogodku, zato da bo kasneje možno ugotavljati okoliščine in dometa vdora.

53. člen (sporočilo posamezniku o kršitvi varnosti osebnih podatkov)

Predlagani 53. člen v primerih suma hujših varnostnih incidentov glede kršitve varnosti osebnih podatkov upravljavca obvezuje, da o incidentu obvesti tudi posameznike, na katere se nanašajo osebni podatki, zato da lahko izvedejo ustrezne zaščitne ukrepe, še zlasti ukrepe za preprečitev kraje identitete.

Člen ureja vsebino sporočila posameznikom in pogoje, ko obveščanje posameznikov ni potrebno.

---

[45] Uradni list RS, št. 109/12, 110/13, 40/14 – ZIN-B, 54/14 – odl. US, 81/15 in 40/17.
[46] Uradni list RS, št. 30/18.
[47] Gl.: WP250 z dne 3.10.2017, Guidelines on Personal data breach notification under Regulation 2016/679.

Obveščanje posameznikov ni potrebno, ko:

1. je pristojni organ v zvezi s podatki, v zvezi s katerimi je prišlo do kršitve, izvajal ustrezne ukrepe, na podlagi katerih so osebni podatki nerazumljivi vsem, ki niso pooblaščeni za dostop do njih. Konkreten primer takšnih ukrepov je šifriranje trdega diska, na katerem se nahajajo osebni podatki. V primeru izgube ali kraje takšnega diska, podatki niso razumljivi nikomur, ki ni pooblaščen za dostop (ima geslo za dešifriranje diska);

2. je pristojni organ je po kršitvi sprejel ukrepe, zaradi katerih ni več verjetno, da bi se veliko tveganje še lahko uresničilo. Konkreten primer takšnih ukrepov v primeru, ko nepooblaščena oseba dostopa do podatkov o uporabniških imenih in geslih, je zamenjava gesel in uvedba spremljanja in obveščanja posameznikov o prijavah v informacijski sistem, s čimer se možnost zlorabe gesel zmanjša.

3. bi obveščanje posameznikov zahtevalo nesorazmeren napor, ker je posameznikov, ki jih je prizadela kršitev preveč, ali pa ko ni jasno, kateri posamezniki so bili s kršitvijo prizadeti. V tem primeru se objavi javno sporočilo ali izvede podoben ukrep, s katerim so posamezniki, na katere se nanašajo osebni podatki, enako učinkovito obveščeni.

Če se pristojni organ sam ne odloči za objavo, mu jo lahko naloži tudi Informacijski pooblaščenec (inšpekcijski ukrep). Dolžnost objave se lahko zadrži, omeji ali opusti iz enakih razlogov, kot se lahko omeji dostop posameznikov do lastnih osebnih podatkov.

54. člen (zaupno obveščanje o kršitvah)

Predlagani 54. člen določa obveznost pristojnih organov, da vzpostavijo notranje poti za obveščanje o kršitvah določb tega zakona. S kršitvami morajo biti seznanjeni tako vodstvo organa kot tudi pooblaščena oseba za varstvo podatkov. Notranje poti za obveščanje morajo sprejemati tako prijave notranjih deležnikov kot tudi zunanjih. Prijave kršitev je treba obravnavati zaupno in hitro. Določeni so tudi ukrepi za zaščito prijavitelja.

3. oddelek – pooblaščena oseba za varstvo osebnih podatkov

Tretji oddelek poglavja o obveznostih pristojnih organov, obdelovalcev in skupnih upravljavcev ureja določitev pooblaščene osebe za varstvo osebnih podatkov s strani pristojnih organov, pogoje za njeno določitev, naloge, prav tako pa v povezavi z Zakonom o nalogah in pooblastilih policije določa tudi naloge in pogoje za določitev pooblaščene osebe za varstvo osebnih podatkov pri nacionalni enoti za informacije o potnikih.

55. člen (pooblaščena oseba za varstvo osebnih podatkov)

Predlagani prvi odstavek 55. člena pristojnim organom nalaga dolžnost določitve pooblaščene osebe za varstvo osebnih podatkov izmed zaposlenih pri organu. To je neodvisna oseba, ki naj pristojnemu organu na neodvisen način pomaga pri sistematičnem obvladovanju tveganj oziroma kršitev varstva osebnih podatkov. Z njenim imenovanjem pristojni organ izkaže, da se vprašanj varstva osebnih podatkov loteva sistematično in z ustreznimi kadrovskimi in finančnimi vložki.

Drugi odstavek, ne glede na to, da se zakon sicer nanaša tudi na obdelave osebnih podatkov, ki jih za namene iz prvega odstavka 1. člena izvajajo sodišča (preiskovalni postopek itd.), določa, da so sodišča izvzeta iz obveznosti imenovanja pooblaščene osebe po tem zakonu glede kazenskih zadev sodišča (določba ne vpliva na imenovanje take osebe po Splošni uredbi).

Tretji odstavek daje pristojnim organom možnost določitve namestnika pooblaščene osebe za čas njene odsotnosti ali zadržanosti, ki ima v tem primeru vsa pooblastila, ki jih ima pooblaščena oseba.

Četrti odstavek določa, da je službene kontaktne podatke pooblaščene osebe in morebitnega namestnika treba sporočiti Informacijskemu pooblaščencu, ki vodi seznam kontaktnih oseb z

namenom hitrejše komunikacije v primeru kršitev in izvajanja drugih nalog, kontaktni podatki pa se objavijo tudi na spletnih straneh pristojnega organa.

Peti odstavek določa, da mora pristojni organ pooblaščeni osebi za varstvo podatkov in namestniku zagotoviti ustrezna sredstva za nepristransko in učinkovito opravljanje nalog ter omogočiti ustrezno strokovno usposabljanje. S tem se dodatno zagotavlja njeno neodvisno in strokovno delo in onemogoča vpliv na morebitne ugotovitve glede skladnosti obdelav pri pristojnem organu.

Šesti odstavek določa, da mora pristojni organ zagotoviti, da je pooblaščena oseba za varstvo osebnih podatkov vedno in trajno ustrezno ter pravočasno vključena v vse zadeve v zvezi z varstvom osebnih podatkov, ki se izvajajo v okviru dejavnosti pristojnega organa.

Sedmi odstavek nadalje določa, da pooblaščena oseba v zvezi z njenim delom ne sme prejemati nobenih navodil, zaradi opravljanja njenih nalog pa ne sme biti razrešena ali kaznovana. Pooblaščena oseba ima po istem odstavku določeno tudi možnost neposrednega poročanja predstojniku pristojnega organa, da se omogoči zlasti učinkovito ukrepanje v primeru kršitve varnosti ali drugih ugotovitev glede skladnosti obdelave.

56. člen (pogoji za določitev pooblaščene osebe za varstvo osebnih podatkov)

Predlagani prvi odstavek 56. člena določa pogoje za določitev pooblaščene osebe za varstvo podatkov in njenega namestnika. Prvi odstavek taksativno našteva pogoje, ki so deloma povzeti iz 88. člena Zakona o javnih uslužbencih, ki določa pogoje za imenovanje v naziv. Poseben je le pogoj dodatnega znanja oziroma praktičnih izkušenj s področja varstva osebnih podatkov, glede na to, da gre za specifično področje, na katerem mora pooblaščena oseba opravljati delovne naloge.

Drugi odstavek določa možnost, da več pristojnih organov določi skupno pooblaščeno osebo, odvisno od organizacijske strukture in velikosti pristojnih organov.

Tretji odstavek določa možnost, da pristojni organ določi za pooblaščeno osebo tisto, ki je pri pristojnem organu že imenovana za pooblaščeno osebo na drugi pravni podlagi (npr. na podlagi Splošne uredbe, Zakona o nalogah in pooblastilih policije).

57. člen (naloge in upravičenja pooblaščene osebe za varstvo osebnih podatkov)

Predlagani 57. člen določa naloge in upravičenja pooblaščene osebe za varstvo podatkov. Pri tem je posebej poudarjeno, da so naloge pooblaščene osebe omejene zgolj na obveščanje, svetovanje in pomoč pristojnemu organu glede njegovih obveznosti in da torej ne pomenijo prevzema odgovornosti za zagotavljanje skladnosti obdelav osebnih podatkov. Za zagotavljanje skladnosti obdelave osebnih podatkov z določbami Direktive in področnih zakonov se pristojni organi odgovornosti za kršitve skladnosti ne morejo rešiti s sklicevanjem na neustrezno delo pooblaščene osebe.

Med nalogami pooblaščene osebe je tudi sodelovanje z Informacijskim pooblaščencem in vzpostavljanje tehničnih pogojev za izvedbo nadzora, deluje kot kontaktna točka, to pomeni z ene točke pridobivanje informacij za morebitno izvedbo nadzora pri pristojnem organu, kar omogoča hitrejše in preglednejše pridobivanje informacij. Med pomembnimi nalogami pooblaščene osebe za varstvo osebnih podatkov je tudi obveščanje vodstva pristojnega organa in nato nadzornega organa o kršitvah zakona glede določb, ki se nanašajo na osebne podatke.

Za učinkovito opravljanje nalog mora pooblaščena oseba za varstvo osebnih podatkov imeti dostop vsebine osebnih podatkov, ki jih obdeluje pristojni organ (drugi odstavek 57. člena).

Objavljeni kontaktni podatki pooblaščene osebe so namenjeni tudi vzpostavitvi stika posameznika s pristojnim organom glede njegovih pravic (četrti odstavek 55. člena).

58. člen (pooblaščena oseba za varstvo osebnih podatkov pri nacionalni enoti za informacije o potnikih)

Predlagani 58. člen določa, da mora pooblaščena oseba za varstvo podatkov pri nacionalni enoti za informacije o potnikih, za imenovanje katere ima generalni direktor policije podlago v 112.d členu Zakona o nalogah in pooblastilih policije, izpolnjevati pogoje za določitev pooblaščene osebe, kot jih določata ta zakon in Zakon o nalogah in pooblastilih policije, ter opravlja naloge, kot jih določata ta zakona. Z Zakonom o nalogah in pooblastilih policije je bila v pravni red Republike Slovenije v določenem delu prenesena Direktiva (EU) 2016/681 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o uporabi podatkov iz evidence podatkov o potnikih (PNR) za preprečevanje, odkrivanje, preiskovanje in pregon terorističnih in hudih kaznivih dejanj (UL L št. 119 z dne 4. 5. 2016, str. 132), vendar ne v delu, ki ureja pogoje in naloge pooblaščene osebe za varstvo podatkov. S tem zakonom so pooblaščene osebe za varstvo osebnih podatkov za pristojne organe enotno urejene.

IV. poglavje – posebne določbe

To poglavje vsebuje področne ureditve, ki neposredno veljajo.

1. oddelek – preverjanje identitete

1. oddelek IV. poglavja določa pravila za preverjanje identitete posameznika, na katerega se nanašajo osebni podatki.

59. člen (preverjanje identitete posameznika)

Predlagani 59. člen ureja način preverjanja identitete posameznika, na katerega se nanašajo osebni podatki. Pri tem se upošteva, da bo v konkretnih postopkih treba identificirati tako državljane Republike Slovenije kot tudi tuje državljane, tiste, ki se nahajajo na ozemlju Republike Slovenije, in tiste, ki so v tujini. Predlagani člen omogoča različne načine identifikacije, tako z vpogledom v osebni dokument, če je posameznik fizično prisoten ob izvajanju postopka, ali vpogled v kopijo dokumenta, ki ga posameznik pošlje po (elektronski) pošti, z uporabo elektronskega podpisa ali z uporabo drugih sredstev informacijske tehnologije (npr. z uporabo video klica). Predlagani člen je povezan tudi s 14. členom predloga zakona.

2. oddelek – povezovanje

2. oddelek IV. poglavja določa pravila glede povezovanja.

60. člen (uporaba povezovalnih znakov)

V 60. členu je določena uporaba povezovalnih znakov (definicija povezovalnih znakov je v 23. točki 4. člena ZVOPPOKD). V prvem odstavku je predlagano, da se pri pridobivanju osebnih podatkov iz zbirk osebnih podatkov s področja zdravstva, policije, obveščevalno-varnostne dejavnosti države, obrambe države, sodstva in državnega tožilstva, probacije ter iz kazenske evidence in prekrškovnih evidenc ne sme uporabljati povezovalni znak, na način, da bi se za pridobitev osebnega podatka uporabil izključno ta znak. Prepovedna norma velja za pristojne organe, spoštovati pa jo morajo tudi obdelovalci.

Predlagani drugi odstavek je izjema od prvega odstavka in določa, da se lahko izjemoma uporabi en povezovalni znak (zlasti EMŠO) za pridobivanje osebnih podatkov, če je to podatek v konkretni zadevi, ki lahko omogoči, da se prepreči, odkrije, preišče ali preganja kaznivo dejanje, ki se preganja po uradni dolžnosti. O tem se brez odlašanja napravi uradni zaznamek ali drug ustrezen zapis.

S tem členom se glede povezovalnih znakov (EMŠO, davčna številka, ZZZS številka) ohranjajo obstoječe tradicionalne sistemske omejitve iz 20. člena ZVOP-1 pri povezovanju z nekaterimi zbirkami osebnih podatkov (evidence), in sicer tako, da je treba poleg EMŠO-a oziroma 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 60. člena so bile vsebovane že v četrtem odstavku 8. člena Zakona o varstvu osebnih podatkov iz leta 1999 ter so v veljavnem prvem odstavku 20. člena ZVOP-1, v navedena zakona pa so bile v povezavi s sprejemanjem Zakona o centralnem registru prebivalstva[48] leta 1998 vključene kot varovalka glede na takratne ideje, 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.

61. člen (povezovanje uradnih evidenc in javnih knjig)

Predlagani 61. člen določa posebna pravila glede povezovanja uradnih evidenc in javnih knjig, določa torej eno od posebnih dejanj obdelave osebnih podatkov, predstavlja nadgradnjo obstoječe ureditve povezovanja zbirk osebnih podatkov iz 84. člena ZVOP-1. Glavna vsebina ureditve ostaja enaka kot do sedaj, in sicer da se omejuje vsako količinsko oziroma 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.

Pri tem se ureditev najbolj tveganih povezovanj ureja 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 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 razgaljenost posameznika in s tem možnosti profiliranja 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 za 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[49], 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.

[48] Izvirno: Uradni list RS, št. 1/99.
[49] Afero je razkril in kritiziral francoski časopis: Le Monde, Boucher, Philippe, *SAFARI ou la chasse aux Français*, 21. 3. 1974.

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 je v primerih, ko se povezujejo zbirke osebnih podatkov z občutljivimi osebnimi podatki ali se uporablja povezovalni znak, potrebna odločitev nadzornega organa za varstvo osebnih podatkov Helenske republike glede ustreznosti povezovanja.

Definicija povezovanja je zdaj urejena v samem členu (drugi odstavek), pri čemer je po novem določena tehnološko nevtralno oziroma bolj splošno, tako da lahko vključuje različne tehnične načine izvajanja povezovanja zbirk, ki so se pojavili 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 oziroma brez zahteve uporabnika (npr. da informacijski sistemi medsebojno čez noč posodabljajo osebne podatke ob spremembah kot v primeru Centralnega registra prebivalstva) ali pa na zahtevo uporabnika (primer eSociala, kjer sistem na zahtevo uporabnika z uporabo različnih centralnih gradnikov pridobi osebne podatke posameznika iz 44 zbirk). Posledice pa so v praksi iste. Prav tako je vseeno, ali se prejeti podatki združijo šele pri uporabniku ali na kakšnem mestu pred njim (primer rešitve ti. »Pladenj«). Prav tako se kot povezovanje šteje tudi vodenje različnih zbirk pri istem upravljavcu ali obdelovalcu, razen če so organizacijsko in tehnično ustrezno ločene, saj bi sicer kršitev pravil varstva osebnih podatkov na eni od povezanih zbirk lahko imela posledice še za ostale povezane zbirke. Smiselno enako velja tudi v primeru, če isti pogodbeni obdelovalec vodi različne zbirke za različne upravljavce. Če te zbirke niso ustrezno ločene, je tudi treba govoriti o povezovanju.

Tako kot do sedaj pa se za povezovanje ne štejejo primeri, ko se pooblaščeni uporabnik v okviru upravnega ali drugega individualnega postopka prijavi v zbirko osebnih podatkov, iz katere je pooblaščen pridobiti osebne podatke posameznika (primeri aplikacij za posamične poizvedbe v centralnih registrih, kot je e-RISK v primeru Centralnega registra prebivalstva ali e-Poizvedbe na področju zdravstvenega zavarovanja). V takšnem primeru ni posebej povečanih tveganj za človekove pravice in temeljne 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 pristojni organ (po prvem odstavku) od zakonodajalca v zakonu dobiti izrecno odobritev (določitev v zakonu)[50], 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).

Po tretjem odstavku pa ne bo več treba pridobiti dovoljenja Informacijskega pooblaščenca (upravna odločba), zadostovalo bo, da pristojni organ, ki bi izvedel povezovanje, o tem predhodno (rok 30 dni)

[50] Gl. 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 določba 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. […]«

obvesti Informacijskega pooblaščenca, ki pa lahko v tej predhodni fazi oceni, da je treba izvesti ti. »tematski« (svetovalni) nadzor.

Zaradi lažjega razumevanja nove ureditve podajamo nekaj širših primerov 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;
- 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.

3. oddelek – strokovni nadzor

3. oddelek IV. poglavja določa strokovni nadzor.

62. člen (strokovni nadzor)

Predlagani 62. člen določa, da za pristojne organe glede strokovnega nadzora veljajo pravila iz tega oddelka, če drug zakon ne določa drugače. S predlaganim oddelkom se upošteva potreba zapolnitve pravne praznine na tem področju, kadar veljavni področni zakoni ne vsebujejo določb o obdelavi osebnih podatkov pri opravljanju strokovnega nadzora. Predlagano poglavje pride v poštev predvsem

na področju policije in državnih tožilstev (5.–11. člen Zakona o organiziranosti in delu v policiji[51] in 173.–175. člen Zakona o državnem tožilstvu[52]), saj nekateri zakoni običajno določajo le pristojnost oziroma obveznost opravljanja strokovnega nadzora, ni pa tudi 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 prvim odstavkom 6. člena predloga zakona (sistemsko načelo zakonitosti glede obdelave osebnih podatkov).

63. člen (splošne določbe)

V 63. členu so ponovljene dosedanje konkretne določbe o obdelavi osebnih podatkov v okviru strokovnega nadzora, kot je to določeno že v 88. členu ZVOP-1.

64. člen (obveščanje posameznika in pridobivanje podatkov)

V 64. členu je določeno obveščanje posameznika (prvi odstavek) in dodatna obdelava osebnih podatkov v okviru strokovnega nadzora (drugi odstavek), kot je to določeno v dosedanjem 89. členu ZVOP-1.

65. člen (posebne vrste osebnih podatkov)

V 65. členu so določeni strokovni nadzor in obdelava posebnih vrst osebnih podatkov, kot je to določeno v dosedanjem 90. členu ZVOP-1.

4. oddelek – posredovanje osebnih podatkov

4. oddelek IV. poglavja določa pravila glede posredovanja osebnih podatkov

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

Predlagani 66. člen ureja posredovanje osebnih podatkov s strani pristojnega organa drugemu subjektu javnega sektorja in obratno.

Izhodiščno pravilo 66. člena za posredovanje je, da mora iti zgolj za eno od oblik obdelave osebnih podatkov in da mora torej zanjo obstajati veljavna pravna podlaga, ki pristojni organ 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 (originatorju) osebnih 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.

67. člen (posredovanje osebnih podatkov, ki ga izvedejo osebe zasebnega sektorja)

Predlagani 67. člen je neke vrste »zrcalna slika« 66. člena – zasebni sektor posreduje določene podatke uporabnikom iz javnega sektorja ali celo iz zasebnega sektorja, če gre za nalogo javnega sektorja po prvem odstavku 66. člena. V tretjem odstavku je določen institut brezplačnosti

[51] Uradni list RS, št. 15/13, 11/14, 86/15, 77/16, 77/17, 36/19 in 66/19 – ZDZ.
[52] Uradni list RS, št. 58/11, 21/12 – ZDU-1F, 47/12, 15/13 – ZODPol, 47/13 – ZDU-1G, 48/13 – ZSKZDČEU-1, 19/15, 23/17 – ZSSve in 36/19.

posredovanja osebnih podatkov (bistveni interes pravne države iz 2. člena Ustave Republike Slovenije).

68. člen (postopek posredovanja osebnih podatkov)

68. člen določa pravila glede postopka posredovanja osebnih podatkov. Pomembno je, da so v šestem odstavku tega člena določena pravila glede ti. »zunanje sledljivosti« obdelave osebnih podatkov, namreč glede posredovanj osebnih podatkov s strani upravljavcev (pristojnih organov) uporabnikom. Upravljavec mora za vsako posredovanje osebnih podatkov zagotoviti, da je mogoče pozneje ugotoviti, kateri osebni podatki so bili posredovani, komu, kdaj in po kateri pravni podlagi, za kateri namen oziroma iz katerih razlogov oziroma za potrebe katerega postopka, razen če drug zakon za posredovanje posameznih vrst podatkov ne določa drugače. Ureditev je podobna kot v dosedanjem tretjem odstavku 22. člena ZVOP-1. Predlagana določba je tako izvedba ukrepov varnosti obdelave, obveščanja o kršitvah varstva osebnih podatkov in olajšanje izvajanja vgrajenega in privzetega varstva osebnih podatkov.

Ta člen tudi določa, da določbe 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, odrejene ali izdane na podlagi in v mejah zakona.

V. poglavje –prenos osebnih podatkov tretjim državam ali mednarodnim organizacijam

V. poglavje ureja prenose osebnih podatkov v tretje države ali mednarodne organizacije in pri tem upošteva specifike področja Direktive, zlasti občasno potrebnost hitrega policijskega sodelovanja.

69. člen (splošna pravila za prenos osebnih podatkov)

Predlagani člen ureja splošna pravila za prenos osebnih podatkov ter glede čezmejne obdelave (za posredovanja osebnih podatkov med državami članicami Evropske unije in mednarodnim organizacijam), vključno z nadaljnjimi prenosi iz teh držav ali mednarodnih organizacij v tretje države ali mednarodne organizacije.

Prenos je dopusten, če so upoštevane določbe tega dela zakona in:

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

2. se osebni podatki posredujejo upravljavcu v tretji državi ali mednarodni organizaciji, ki je pristojen za izpolnitev enega od namenov iz prvega odstavka 1. 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, dala predhodno soglasje za prenos;

4. je Evropska komisija sprejela sklep o ustreznosti ali, če tak sklep ne obstaja, so bili predloženi oziroma obstajajo ustrezni ukrepi v smislu 71. člena tega zakona ali je, če ne obstaja sklep o ustreznosti, možno v skladu z 72. členom tega zakona uporabiti izjeme za določene primere in če je

5. 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 drugem odstavku je prenos brez prehodne odobritve v skladu s 3. točko prejšnjega odstavka dovoljen le, če je prenos nujno potreben za preprečitev neposredne in resne grožnje javni varnosti Republike Slovenije ali tretje države ali za varstvo ustavne ureditve, bistvenih varnostnih, političnih in gospodarskih interesov Republike Slovenije, predhodnega soglasja pa ni bilo mogoče pravočasno pridobiti. O tem je treba nemudoma obvestiti organ, pristojen za podelitev predhodnega soglasja.

70. člen (prenos osebnih podatkov na podlagi sklepa o ustreznosti varstva osebnih podatkov)

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 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 z 71. ali 72. členom tega zakona, niti ne vpliva na obveznosti iz področnih mednarodnih pogodb.

71. člen (prenos osebnih podatkov z uporabo ustreznih zaščitnih ukrepov)

Predlagani člen dopušča prenos osebnih podatkov z uveljavljanjem ustreznih ukrepov varstva osebnih podatkov, če ne obstaja Sklep Evropske komisije iz tretjega odstavka 36. člena Direktive, če:

1. so v ustreznem pravnem aktu, ki je pravno obvezujoč (predpis z učinkom zakona), določeni ustrezni ukrepi za varstvo osebnih podatkov ali

2. je pristojni organ 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 mora upravljavec o teh kategorijah prenosov obvestiti Informacijskega pooblaščenca, ki lahko odredi prepoved prenosa osebnih podatkov.

Po tretjem odstavku je treba prenose v skladu s celotnim prvim odstavkom ustrezno dokumentirati, dokumentacijo, ki vključuje datum in uro prenosa, podatke o prejemniku ali uporabniku, utemeljitev prenosa in navedbo prenešenih osebnih podatkov, pa je treba na zahtevo dati na razpolago Informacijskemu pooblaščencu. Dokumentacija se zaradi razloga naknadne kontrole in zaradi preverjanja spoštovanja zakonitosti ter glede na to, da gre za posebno izjemo, hrani pet let.

72. člen (izjeme za posamezne primere)

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 zakona.

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. za varovanje zakonitih interesov posameznikov, na katere se nanašajo osebni podatki (obramba pred tožbo);

3. za preprečitev 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 prvem odstavku 1. člena ZVOPPOKD, ali

5. v posameznem primeru za uveljavljanje, izvajanje ali obrambo pravnih zahtevkov v povezavi z nameni, navedenimi v prvem odstavku 1. člena ZVOPPOKD (npr. odškodninska tožba).

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 človekovih pravic in temeljnih svoboščin posameznikov, na katere se osebni podatki nanašajo.

Po tretjem odstavku za prenose v skladu s prvim odstavkom veljajo določbe tretjega odstavka 71. člena ZVOPPOKD (obveznosti dokumentiranja ter preverjanja).

73. člen (posebni prenosi določenim uporabnikom v tretjih državah)

S predlaganim členom se prenaša 39. člen 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 – zgolj po tem členu, kjer gre v bistvu za ti. »tiktakajoča bomba« situacijo (ti. »*ticking bomb situation*«). Prvi odstavek v uvodnem besedilu definira prenosnike osebnih podatkov kot pristojne organe (ne morejo torej to biti obdelovalci). 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 6. točki so določeni kumulativni pogoji, ki omogočajo tovrsten izjemni prenos, s tem da 6. točka določa, da mora upravljavec (pristojni 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 o teh prenosih obvesti Informacijskega pooblaščenca. Tretji odstavek pa določa obveznost dokumentiranja prenosov.

VI. poglavje – nadzorni organ

To poglavje določa nadzorni organ Republike Slovenije (Informacijski pooblaščenec), njegove pristojnosti in naloge.

74. člen (določitev nadzornega organa)

Predlagani prvi odstavek določa, da je Informacijski pooblaščenec neodvisni in samostojni nadzorni organ, ki izvaja nadzor nad spoštovanjem določb tega zakona ter glede obdelav osebnih podatkov za namene iz prvega odstavka 1. člena tega zakona. Pri tem izhaja iz podobne sistemske formulacije v uvodnem besedilu prvega odstavka 2. člena Zakona o informacijskem pooblaščencu[53]. Določba je sistemske narave, določa, da ima Republika Slovenija le en nadzorni organ za varstvo osebnih podatkov ter zagotavlja njegovo pravnoorganizacijsko samostojnost ter neodvisnost odločanja po ZVOPPOKD.

Po drugem odstavku nadzorni organ skrbi za enotno uresničevanje ukrepov na področju varstva osebnih podatkov po določbah tega zakona, tako da se zaščitijo človekove pravice in temeljne svoboščine posameznikov v zvezi z obdelavo osebnih podatkov ter omogoči prosti pretok osebnih podatkov med državami članicami Evropske unije v skladu z določbami tega zakona.

[53] Uradni list RS, št. 113/05 in 51/07 – ZUstS-A.

75. člen (pristojnosti nadzornega organa)

Informacijski pooblaščenec kot nadzorni organ za varstvo osebnih podatkov ima po 75. členu predloga zakona naslednje pristojnosti:

1. izvaja nadzore nad izvajanjem določb tega zakona ter drugih zakonov, podzakonskih predpisov ali drugih splošnih aktov glede obdelav osebnih podatkov s področij iz prvega odstavka 1. člena tega zakona;

2. odloča v pritožbenem postopku in v postopkih inšpekcijskih nadzorov po tem zakonu;

3. daje predhodna mnenja ministrstvom, državnemu zboru, organom samoupravnih lokalnih skupnosti, drugim državnim organom ter nosilcem javnih pooblastil o usklajenosti določb predlogov zakonov ter ostalih predpisov z zakoni in drugimi predpisi, ki urejajo osebne podatke;

4. izvaja predhodno posvetovanje v skladu s tem zakonom;

5. daje pristojnim organom ter posameznikom, na katere se nanašajo osebni podatki, neobvezna mnenja, pojasnila in stališča o vprašanjih glede varstva osebnih podatkov v zvezi zakoni in povezanimi predpisi na področju obravnavanja kaznivih dejanj, določenem s prvim odstavkom 1. člena tega zakona;

6. spodbuja ozaveščenost in razumevanje javnosti o tveganjih, pravilih, zaščitnih ukrepih in pravicah v zvezi z obdelavo;

7. spodbuja ozaveščenost pristojnih organov in obdelovalcev o njihovih obveznostih na podlagi tega zakona;

8. sodeluje pri delovanju Evropskega odbora za varstvo osebnih podatkov;

9. pripravi letno poročilo o izvajanju tega zakona, v skladu z določbami zakonov, ki urejata informacijskega pooblaščenca oziroma varstvo osebnih podatkov;

10. obvesti pristojno sodišče o kršitvah zakona in na lastno pobudo sodišču v sodnem postopku posreduje mnenje o ugotovljenih kršitvah;

11. in izvaja druge naloge, določene s tem zakonom.

Po drugem odstavku inšpekcijski nadzor po tem zakonu izvajajo nadzorne osebe (le Informacijski pooblaščenec in državni nadzorniki), pri nadzoru pa lahko sodeluje strokovno osebje nadzornega organa s področja informacijskih in komunikacijskih tehnologij ter namestniki informacijskega pooblaščenca.

76. člen (omejitve pri izvajanju nadzorov)

76. člen določa omejitve glede izvajanja inšpekcijskih in prekrškovnih nadzorov glede obdelav osebnih podatkov, ki se obdelujejo v kazenski zadevi sodišča, izvedenih v okviru 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, ter obdelav osebnih podatkov, izvedenih v okviru neodvisnega sodniškega odločanja Ustavnega sodišča Republike Slovenije v kazenskih zadevah (zlasti postopek ustavne pritožbe, lahko tudi spori o pristojnosti). Ustavno sodišče je posebej navedeno, ker ne gre za sodišče s splošno pristojnostjo, niti ni specializirano sodišče.

77. člen (medsebojna pomoč)

77. člen določa, kako Informacijski pooblaščenec pristojnim nadzornim organom drugih držav članic Evropske unije na njihovo zahtevo zagotovi ustrezne informacije in medsebojno pomoč glede konkretne zadeve, ki jo potrebujejo za dosledno izvajanje in uporabo njihove zakonodaje, s katero s

svoj pravni red prenašajo Direktivo, določa pa tudi omejitve (peti odstavek), če ni pristojen za vsebino zahteve ali za izvršitev zahtevanih ukrepov (lahko pristojen kak drug nadzorni organ) ali pa bi izpolnitev zahteve kršila zakon (npr. poseg v kazenske zadeve).

Po desetem odstavku lahko Informacijski pooblaščenec zahteva pomoč nadzornih organov drugih držav članic Evropske unije, zahteva za upravno pomoč pa mora vsebovati vse potrebne informacije glede konkretne zadeve, vključno z namenom in obrazložitvijo zahteve. Pridobljene informacije se uporabljajo samo za namen, za katerega so bile zahtevane, na njih nadzorni organ ni vezan (odloča po ZVOPPOKD).

VII. POGLAVJE – KAZENSKE DOLOČBE

Sistematika določanja prekrškov v tem zakonu sledi namenu zakona, to je zagotoviti zakonitost obdelav osebnih podatkov. V primeru kršitev se namen doseže z (inšpekcijskim) nadzorom informacijskega pooblaščenca in uveljavljanjem inšpekcijskih pooblastil in ukrepov. Kadar namena ne bi bilo mogoče doseči z nadzorom, ker ga pristojni organ ali pogodbeni obdelovalec aktivno onemogočata, je predvidena prekrškovna sankcija kot zadnja možnost, ki jo ima informacijski pooblaščenec (*ultima ratio*).

78. člen (splošne kršitve s strani pristojnega organa)

Predlagani 78. člen določa kaznivost za prekrške in ustrezne kazni (globo) za kršitve določb ZVOPPOKD, ki jih stori odgovorna oseba pristojnega organa. Z globo se kaznuje odgovorna oseba pristojnega organa, če

1. obdeluje osebne podatke brez podlage v zakonu ali brez privolitve posameznika, na katerega se nanašajo osebni podatki. Pri tem je treba upoštevati tudi četrti in peti odstavek, ki določata pravno podlago, za obdelavo v primeru, ko je posameznik, na katerega se nanašajo osebni podatki, sam javno objavil osebne podatke brez očitnega ali izrecnega namena, da omeji namen njihove obdelave ali je obdelava potrebna za varovanje življenjskih interesov. Gre za kolektivni prekršek.

2. po izvedeni obdelavi ne napiše poročila z navedbo razlogov za obdelavo in obsegom obdelanih osebnih podatkov.

3. obdeluje posebne vrste osebnih podatkov brez podlage v zakonu, pa to ni nujno potrebno za opravljanje nalog pristojnih organov, določenih z zakonom. Materialna določba ima tri pogoje, ki morajo biti določeni kumulativno (skladnost s 6. členom, nujno potrebno za opravljanje nalog in naloge so določene z zakonom). Prekršek je samo obdelava podatkov kljub temu, da niso nujno potrebni za opravljane nalog pristojnega organa. Gre za kolektivne prekrške.

4. če ne opravi ponovnega in ročnega pregleda odločitve, ki temelji izključno na avtomatizirani obdelavi osebnih podatkov in ki ima lahko negativen pravni učinek na posameznika, na katerega se nanašajo osebni podatki, ali ki tega posameznika lahko bistveno prizadene, pa je posameznik pregled zahteval. Navedeni pogoji morajo biti izpolnjeni kumulativno.

5. če po seznanitvi z uvedbo postopka izbriše, spremeni ali odsvoji zahtevane osebne podatke, ki so predmet postopka, dokler o zadevi ni pravnomočno odločeno. Pri tem je treba upoštevati, da lahko prekrška po 5. in 6. točki nastaneta skupaj.

6. če ravna v nasprotju z odredbo nadzornika o načinu zavarovanju dokazov. Pri tem je treba upoštevati, da lahko prekrška po 5. in 6. točki nastaneta skupaj.

7. javno ne objavi splošnih informacij iz prvega odstavka 21. člena. Pri tem mora prekrškovni organ upoštevati, da je lahko objava omejena pod pogoji iz tretjega odstavka 21. člena.

8. če ne vodi dokumentacije, iz katere izhaja, da je zagotovljena skladnost obdelav z zakonom.

9. če ne upravlja evidence vseh kategorij dejavnosti obdelav osebnih podatkov.

10. dnevnik obdelave uporabi za druge namene od tistih, določenih v tretjem odstavku 45. člena.

11. ne sporoči nemudoma vsem uporabnikom, da so jim bili posredovani ali dani na razpolago osebni podatki, ki ne ustrezajo zahtevam iz prvega odstavka 36. člena ali so bili posredovani nezakonito, oziroma takšnih podatkov nemudoma ne popravi, jih izbriše ali omeji.

12. ne izvaja predpisanih ukrepov varnosti obdelave iz 1. do 10. točke drugega odstavka 51. člena tega zakona. Gre za kolektivne prekrške.

13. ne dokumentira vseh kršitev varnosti osebnih podatkov.

14. uporablja povezovalni znak v nasprotju s 60. členom tega zakona.

79. člen (kršitve s področja pogodbene obdelave)

Predlagani 79. člen določa globo za prekrške, ki jih stori odgovorna oseba pogodbenega obdelovalca, ki je pravna oseba, samostojni podjetnik posameznik ali posameznik, ki samostojno opravlja dejavnost. Oseba, ki stori prekršek, je zunanji, pogodbeni obdelovalec. Večina kršitev pogodbene obdelave je prepuščena ureditvi s pogodbo med pristojnim organom in pogodbenim obdelovalcem, ta člen pa ureja le tiste, za katere se šteje, da lahko negativno vplivajo na izvedbo nadzornih postopkov po tem zakonu (zlasti kršitve iz drugega in tretjega odstavka 42. člena, in tudi prvega odstavka 61. člena predloga zakona – v tem primeru za kršitev glede izvajanja povezovanja zbirk podatkov s strani obdelovalca – če za to ni izrecne zakonske določbe (dovoljenja)). V tretjem odstavku je tudi določena kaznivost odgovornih oseb obdelovalca za tovrstne kršitve.

80. člen (kršitve s področja prenosov osebnih podatkov tretjim državam ali mednarodnim organizacijam)

Predlagani 79. člen določa globo za prekrške v zvezi s prenosi osebnih podatkov tretjim državam ali mednarodnim organizacijam.

81. člen (izrek globe)

Predlagani 81. člen določa, da se sme v hitrem prekrškovnem postopku po tem zakonu izreči globa, ki je višja od najnižje predpisane globe. Gre za izjemo od tretjega odstavka 52. člena Zakona o prekrških, ki določa, da se v hitrem postopku storilcu izreče globa v znesku, v katerem je predpisana, če je predpisana v razponu, pa se izreče najnižja predpisana mera globe. Navedeni člen določa možnost, da drug zakon določa drugače.

VIII. POGLAVJE - PREHODNE IN KONČNE DOLOČBE

82. člen (rok za izdajo pravilnikov)

Predlagani 82. člen določa rok za izdajo pravilnika o ukrepe in postopke za izvajanje varnosti osebnih podatkov, ki ga izda minister, pristojen za notranje zadeve. Rok je tri mesece od uveljavitve zakona. Enak rok je določen tudi za izdajo pravilnika o ceniku in način plačila stroškov postopka, ki ga sprejme minister pristojen za pravosodje po posvetovanju z Informacijskim pooblaščencem.

83. člen (prehodne določbe glede delovanja nadzornega organa)

Predlagani 83. člen določa, da se prekrškovni postopki, ki so se začeli pri Informacijskem pooblaščencu ali na sodiščih pred uveljavitvijo tega zakona, 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.

Drugi odstavek določa, da z uveljavitvijo zakona preneha delovati Register zbirk osebnih podatkov. Vsebino registra se preda Arhivu Republike Slovenije v roku enega leta. Vsebina Registra se hrani kot trajno arhivsko gradivo.

84. člen (končna določba)

Predlagani 84. člen določa, da zakon začne veljati trideseti dan po objavi v Uradnem listu Republike Slovenije.