UNIVERZA V LJUBLJANI
EKONOMSKA FAKULTETA

ZAKLJUČNA STROKOVNA NALOGA VISOKE POSLOVNE ŠOLE

VARSTVO OSEBNIH PODATKOV IN NOVA UREDBA EU

Ljubljana, julij 2019 ANAMARIJA MALJKOVIĆ

IZJAVA O AVTORSTVU

Podpisana Anamarija Maljković, študentka Ekonomske fakultete Univerze v Ljubljani, avtorica predloženega dela z naslovom Varstvo osebnih podatkov in nova uredba EU, pripravljenega v sodelovanju s svetovalcem izr. prof. dr. Mitjo Kovačem,

I Z J A V L J A M

1. da sem predloženo delo pripravila samostojno;

2. da je tiskana oblika predloženega dela istovetna njegovi elektronski obliki;

3. da je besedilo predloženega dela jezikovno korektno in tehnično pripravljeno v skladu z Navodili za izdelavo zaključnih nalog Ekonomske fakultete Univerze v Ljubljani, kar pomeni, da sem poskrbela, da so dela in mnenja drugih avtorjev oziroma avtoric, ki jih uporabljam oziroma navajam v besedilu, citirana oziroma povzeta v skladu z Navodili za izdelavo zaključnih nalog Ekonomske fakultete Univerze v Ljubljani;

4. da se zavedam, da je plagiatorstvo – predstavljanje tujih del (v pisni ali grafični obliki) kot mojih lastnih – kaznivo po Kazenskem zakoniku Republike Slovenije;

5. da se zavedam posledic, ki bi jih na osnovi predloženega dela dokazano plagiatorstvo lahko predstavljalo za moj status na Ekonomski fakulteti Univerze v Ljubljani v skladu z relevantnim pravilnikom;

6. da sem pridobila vsa potrebna dovoljenja za uporabo podatkov in avtorskih del v predloženem delu in jih v njem jasno označila;

7. da sem pri pripravi predloženega dela ravnala v skladu z etičnimi načeli in, kjer je to potrebno, za raziskavo pridobila soglasje etične komisije;

8. da soglašam, da se elektronska oblika predloženega dela uporabi za preverjanje podobnosti vsebine z drugimi deli s programsko opremo za preverjanje podobnosti vsebine, ki je povezana s študijskim informacijskim sistemom članice;

9. da na Univerzo v Ljubljani neodplačno, neizključno, prostorsko in časovno neomejeno prenašam pravico shranitve predloženega dela v elektronski obliki, pravico reproduciranja ter pravico dajanja predloženega dela na voljo javnosti na svetovnem spletu preko Repozitorija Univerze v Ljubljani;

10. da hkrati z objavo predloženega dela dovoljujem objavo svojih osebnih podatkov, ki so navedeni v njem in v tej izjavi.

V Ljubljani, dne _____ Podpis študentke: _____

KAZALO

UVOD

Varstvo osebnih podatkov je ena izmed temeljnih človekovih pravic in osebnih svoboščin, ki jih v Sloveniji in v večini drugih držav ureja ustava. Zaradi velikega napredka informacijske tehnologije, ki temelji na uporabi interneta je potrebno, da smo zelo pozorni na različne pasti nezakonite uporabe osebnih podatkov in se na njih ustrezno odzivamo. Digitalizacija skoraj vseh aspektov vsakdanjega življenja in uporaba interneta tako v osebnem kot v poslovnem okolju sta pospešili pretok informacij o posameznikih in zelo povečali obseg zbiranja podatkov, ki se lahko uporabijo v različne zakonite ali nezakonite namene. Zaradi tega ker je te informacije in podatke mogoče uporabiti v različne zakonite in včasih tudi nezakonite namene sta Svet Evropske unije in Evropski parlament po večletnih pogajanjih sprejela dogovor, ki bo na ravni celotne Evropske unije zagotavljal usklajeno in enotno ukrepanje v vseh državah članicah in okrepil pravice posameznikov. Končni cilj Evropske unije je s Splošno uredbo o varstvu podatkov omogočiti, da imajo prebivalci večji nadzor nad osebnimi podatki, hkrati pa dvigniti raven varstva osebnih podatkov v EU (Informacijski pooblaščenec, 2017) Prav tako je cilj s Splošno uredbo o varstvu podatkov, ki je neposredno zavezujoča za države članice, oblikovati enoten digitalni trg, in se na ta način izogniti regulatornim posebnostim posameznih držav članic, ki bi zaradi ovirale pretok informacij in posledično delovanje trga Evropske unije (Jamšek, 2019).

Uredba EU 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 2016/679, Ur. l. EU, L 119/1 (v nadaljevanju Splošna uredba o varstvu osebnih podatkov) se je začela uporabljati s 25. 5. 2018 in je z tem prinesla tudi drugačna pravila in obveznosti za podjetja, ki obdelujejo osebne podatke pri svojem poslovanju med ostalim tudi strožji nadzor in omejitve pri uporabi osebnih podatkov pri obiskovalcih na spletnih straneh, ter bo nadomestila določbe dosedanjega Zakona o varstvu osebnih podatkov ZVOP-1 iz leta 2004. Od tega dne dalje morajo subjekti, ki obdelujejo osebne podatke upoštevati pravila Splošne uredbe, ter še tista ostala pravila iz ZVOP-1 zlasti področne ureditve osebnih podatkov biometrija, videonadzor,.. ki bodo ostala v uporabi. Ministrstvo za pravosodje si je močno prizadevalo, da bi vsa vprašanja osebnih podatkov jasno in ustrezno uredilo z novim Zakonom o varstvu osebnih podatkov ZVOP-2, ki pa žal ni bil pravočasno sprejet in je trenutno še v zakonodajnem postopku. Kljub temu da nov Zakon o varstvu osebnih podatkov še ni bil sprejet pa je Splošna uredba o varstvu osebnih podatkov splošno veljavna, zavezujoča in uporabljiva neposredno za vse članice Evropske Unije. Večji del določb obstoječega zakona ZVOP-1 pa se je z uveljavitvijo Splošne uredbe o varstvu podatkov preneha veljati po neobvezujoči oceni Ministrstva za pravosodje. V splošni uporabi pa se je Uredbe prijel vzdevek Evropski zakon.

Zaključna strokovna naloga predstavlja celoten pregled s področja varstva osebnih podatkov in njegovo uvrstitev v pravni red najbolj pa sem se osredotočila na spremembe, ki jih prinaša Splošna uredba o varstvu osebnih podatkov to pa so bistvene spremembe in novosti novega okvirja v Evropi za varstvo osebnih podatkov in so razvidna že iz osnovnih načel Splošne

uredbe, takšna pravna načela pa so tudi vrednostno merilo, ki usmerja vsebinsko opredelitev pravnih pravil in vrsto njihovega izvrševanja. Raziskovalno vprašanje, ki si ga zastavljam v okviru zaključne strokovne naloge, je, kateri so cilji in razlogi za uvedbo nove Splošne uredbe EU o varstvu podatkov. Vsi osebni podatki morajo biti obdelani, zbrani in uporabljeni zakonito na pregleden in pošten način. Zbrani so lahko zgolj za izrecne, določene in zakonite namene, kar pomeni da se zbrani osebni podatki ne smejo uporabljati in obdelovati za kakršnekoli druge namene in načine za katere niso bili pridobljeni. Po uvodu so v prvem delu opisani temeljni pojmi o varstvu podatkov, v drugem delu sem se osredotočala na pravne vire varstva osebnih podatkov in na ZVOP-1, nadalje je v tretjem poglavju opisana Splošna uredba o varstvu podatkov in nameni in razlogi zakonske preureditve in ZVOP-2 na koncu v četrtem poglavju pa so opisane najpomembnejše spremembe novega okvirja varstva osebnih podatkov.

1 TEMELJNI POJMI VARSTVA OSEBNIH PODATKOV

1.1 Osebni podatek in obdelava osebnih podatkov

Osebni podatek pomeni kakršnokoli informacijo v zvezi z določeno ali določljivo fizično osebo posebno pa ime in priimek posameznika, naslov, telefonska številka, EMŠO, davčna številka, itd. Po novem tudi spletni identifikatorji IP naslovi, ID piškotkov ali lokacijski podatki. Strožje zahteve veljajo za varstvo posebne vrste oziroma občutljivih osebnih podatkov kot so politično mnenje, versko prepričanje, rasno ali etično poreklo, spolna usmerjenost, članstvo v sindikatu, zdravstveni podatki in po novem biometrični in genetski podatki. Osebni podatki se lahko nahajajo v različnih zbirkah in evidencah, v računovodskih podatkih, v kadrovskih mapah zaposlenih, v tabelah ki vsebujejo različne podatke o kupcih, v posnetkih videonadzornega sistema, občanih, strankah, pacientih, spletnih straneh zbiranje osebnih podatkov preko elektronske pošte, pogodbenih partnerjev (outsourcing, videonadzor).

Definicija osebnega podatka v ZVOP-1 6. členu navaja osebni podatek kot katerikoli podatek, ki se nanaša na posameznika, ne glede na obliko, v kateri je izražen. Medtem ko Splošna uredba o varstvu osebnih podatkov definira slednjega v četrtem členu kot katero koli informacijo v zvezi z določenim ali določljivim posameznikom. Delovna skupina 29 je analizirala opredelitev osebnega podatka v skladu z Direktivo o varstvu podatkov, ki vsebuje štiri osnovne poglavitne elemente, ki so med seboj tesno prepleteni:

1. katera koli informacija;
2. ki se nanaša;
3. določen ali določljiv;
4. fizična oseba.

1. »Katera koli informacija« prvi element zahteva obširnejšo razlago pojma osebnega podatka ne glede na vsebino, naravo ali tehnično oblikovanje informacije, kar pomeni da je lahko zapis na primer številčni, abecedni, akustični, fotografski, grafični lahko je v računalniku, na papirju ali kot video zapis. Ključno je tudi da pojem osebnih podatkov z vidika narave informacij vključuje vse vrste trditev o osebi in zajema objektivne in subjektivne informacije. Objektivne informacije so (na primer prisotnost kisika v krvi določene osebe), subjektivne informacije pa so vrednostne ocene in mnenja (na primer pri zaposlovanju določena oseba je dober delavec ali pri bančništvu ali je določena oseba zanesljiv posojilojemalec). Za osebni podatek se lahko celo šteje informacija tudi če ni bila nikoli nujno resnična ali dokazana. Se pravi da posamezniku na katerega se podatki nanašajo pravila osebnih podatkov že predvidevajo možnost, da so informacije nepravilne in mu dajejo možnost dostopa do informacij in možnost spodbijanja teh informacij z ustreznimi pravnimi sredstvi. Poleg tega je treba posebej omeniti biometrične podatke, ki jih je mogoče opredeliti kot fiziološke značilnosti, biološke lastnosti, ponavljajoči se dogodki ali žive lastnosti, kadar so ti dogodki ali pojavi za določenega posameznika edinstveni in merljivi, čeprav je možnost da vzorci, ki se v praksi uporabljajo za tehnično merjenje vključujejo določeno mero verjetnosti. Primeri takih biometričnih podatkov so lahko struktura obraza, prstni odtisi, vzorci šarenice, glasovi in pa tudi vzorci žil, geometrija roke ali kakšna druga vedenjska lastnost ali posebno znanje (recimo poseben način govora, lastnoročni podpis, tipkanje itd.) (Prelesnik, 2008, str. 6).
2. »Ki se nanaša« ta opredelitev je zelo bistvena in pomembna, da se čim bolj natančno ugotovi kakšne so povezave oziroma odnosi in kako jih razlikujemo. To so trije različni elementi z katerimi lahko določimo ali se informacija nanaša na določenega posameznika pri tem pa je potrebna opredelitev glede namena, vsebine in rezultata. Kadar se podatki uporabljajo z namenom ocenjevanja se za element » namena « da obstaja lahko šteje ocenjevanje določenih obravnav ali vplivajo na položaj posameznika ali njegov status pri katerem se seveda upoštevajo vse okoliščine, ki vplivajo na tak primer. V primerih kjer je prisoten element » vsebine « je to primer kadar so na voljo informacije o določenem posamezniku ne glede na to kakšen je namen upravljalca podatkov ali vpliv informacij na določenega posameznika ali vpliv tretje stranke na katerega se podatki nanašajo. Pri elementu » rezultata « ni nujno da je vplivna moč določenega rezultata nujno zelo velika dovolj je že da se zaradi obdelave teh podatkov lahko posameznik obravnava drugače od drugih oseb. Te tri elemente je potrebno obravnavati kot alternativo in ne kot komulativne pogoje (Prelesnik, 2008, str. 6).
3. »Določen ali določljiv« posameznik je določljiv, ko ga je mogoče posredno ali neposredno določiti predvsem z navedbo identifikacije, kot je identifikacijska številka, ime, spletni indifikator, podatkih o lokaciji ali pa se lahko identiteto posameznika določi z navedbo enega ali več dejavnikov, ki so za njega značilni genetsko, fizično, duševno, fiziološko, kulturno, gospodarsko ali družbeno. Na splošno velja da je oseba določena ko se v skupini več oseb razlikuje od vseh ostalih v skupini, kar pomeni da je posameznik » določljiv « kadar ga je mogoče identificirati, čeprav to do sedaj še ni bilo storjeno.

Identifikacija se ponavadi opravi z uporabo več informacij ali tako imenovanih identifikatorjev kot so barva las, višina, funkcija, ime, poklic itd. Oseba je lahko neposredno določena z imenom kar je najpogostejši identifikacijski faktor ali posredno določljiva na primer z številko kartice zdravstvenega zavarovanja, telefonsko številko, številko potnega lista, registrsko številko svojega avtomobila in tudi z ostalimi drugačnimi identifikatorji (Prelesnik, 2008, str. 7).

4. »Fizična oseba« samo fizične osebe imajo osebne podatke in zasebnost, zato lahko o osebnem podatku govorimo zgolj pri fizičnih osebah medtem ko pravne osebe ne posredujejo osebnih podatkov in zato tudi ne morejo pričakovati da bodo imele zasebnost. Pravne osebe imajo svoje podatke javno objavljene v poslovnem registru (naziv podjetja, naslov, davčna številka, matična številka, bančni račun). Pojem fizične osebe obravnava Splošna deklaracija človekovih pravic in v šestem členu določa da ima v skladu z tem vsakdo povsod pravico do priznanja pravne sposobnosti. Pravila Direktive ki ponujajo varstvo se uporablja za fizične osebe se pravi za ljudi, kar pomeni da je pravica do varstva osebnih podatkov univerzalna kar pomeni da ni omejena na državljane ali prebivalce države (Prelesnik, 2008, str. 7).

– **Obdelava osebnih podatkov**

Osebni podatki se lahko obdelujejo kar pomeni da se lahko pridobivajo, zbirajo, shranjujejo, urejajo, sporočajo, razkrivajo, povezujejo ali širijo samo za točno določen namen in v primeru kadar obstaja ustrezna pravna podlaga kot je privolitev posameznika, pogodba ali zakon. Obdelava osebnih podatkov pomeni vsako dejanje ali več dejanj skupaj, ki se izvajajo z osebnimi podatki z avtomatiziranimi sredstvi ali tudi brez njih kot so strukturiranje, spreminjanje ali prilagajanje, vpogled, priklic, beleženje, zbiranje, urejanje, razkritje z posredovanjem, uporaba, omejevanje, razširjanje, uničenje ali izbris. Osebne podatke lahko obdelujemo sami kot upravljalec ali po pogodbi z zunanjim pogodbenim obdelovalcem po naročilu in izključno na podlagi zahteve upravljalca. Splošna uredba o varstvu osebnih podatkov določa da je obdelava osebnih podatkov vsaka dejavnost, ki se izvaja na podatkih o strankah in je zakonita če je izpolnjen eden od naslednjih pogojev:

- Zakonska obveznost: obdelava podatkov je potrebna zaradi izpolnitve zakonske obveznosti, ki obvezuje upravljalca.
- Privolitev: določena oseba na katero se nanašajo osebni podatki je informirano, prostovoljno, izrecno in nedvoumno privolila v obdelavo svojih osebnih podatkov zaradi določenega namena.
- Izvajanje pogodbe: na zahtevo posameznika preden skleni določeno pogodbo je potrebna obdelava podatkov za izvajanje pogodbe ali izvajanje ukrepov.
- Javni interes: obdelava podatkov je potrebna pri izvajanju javne oblasti dodeljene upravljalcu ali za opravljanje naloge v javnem interesu.
- Zakoniti interes: obdelava podatkov je potrebna pri zakonitih interesih pri katerih si prizadeva upravljalec ali neka tretja oseba, razen takrat kadar nad takšnimi zakonskimi interesi prevladajo temeljne pravice ali interesi posameznika.

– Zaščita življenjskih interesov: obdelava podatkov je potrebna za zaščito življenjskih interesov takrat, kadar se osebni podatki nanašajo na določenega posameznika ali katero drugo fizično osebo.

1.2 Pravica do varstva osebnih podatkov

Lahko rečemo da je pravico do varstva osebnih podatkov zelo težko definirati predvsem zaradi tega ker predstavlja le okvir pravic posameznika, ki se nanašajo samo nanj in jih lahko pravica zavaruje. Ena temeljnih človekovih pravic je pravica do zasebnosti, ki jo Ustava Republike Slovenije navaja v petintridesetem členu, v katerem je zagotovljena nedotakljivost človekove telesne in duševne celovitosti, njegove zasebnosti ter osebnostnih pravic. Med to zasebnost in osebnostne pravice lahko uvrstimo pravico do varstva osebnih podatkov. Naprej pa v osemintridesetem členu Ustave Republike Slovenije določa da je zagotovljeno varstvo osebnih podatkov in da je prepovedana uporaba osebnih podatkov v nasprotju z namenom njihovega zbiranja. Zbiranje, obdelovanje, namen uporabe, nadzor in varstvo tajnosti osebnih podatkov določa zakon. Vsakdo ima pravico seznaniti se z zbranimi osebnimi podatki, ki se nanašajo nanj in pravico do sodnega varstva ob njihovi zlorabi. Med drugim je pravica do zasebnosti varovana tudi v mednarodnih aktih v osmem členu Evropske konvencije o varstvu človekovih pravic in temeljnih svoboščin (Ur. l. RS, Mednarodne pogodbe št. 7/94), po katerem ima vsak pravico do spoštovanja svojega osebnega in družinskega življenja, svojega doma in dopisovanja in v šestnajstem členu Pogodbe o delovanju Evropske unije v katerem je določeno, da ima vsakdo pravico do varstva osebnih podatkov, ki se nanašajo nanj. Pravico do varstva osebnih podatkov je treba obravnavati glede na vlogo, ki jo ima v družbi v skladu z načelom sorazmernosti, zaradi tega ker ni absolutna pravica in jo uravnotežiti z drugimi temeljnimi pravicami.

1.3 Področne ureditve

– **Neposredno trženje**

Neposredno trženje pomeni ko lahko upravljavec osebnih podatkov uporablja osebne podatke posameznikov, ki jih je zbral z zakonitim opravljanjem dejavnosti ali iz javno dostopnih virov za namene ponujanja blaga, storitev, zaposlitev, začasnega opravljanja del z uporabo poštnih storitev, telefonskih klicev, elektronske pošte ali drugih telekomunikacijskih storitev. Uporablja lahko le osebno ime, naslov stalnega ali začasnega prebivališča, telefonsko številko, naslov elektronske pošte in številko telefaksa. Upravljalec osebnih podatkov je dolžan obvestiti posameznika o kakršnemkoli posredovanju njegovih osebnih podatkov drugim uporabnikom in za to pridobiti njegovo pisno privolitev. Posameznik lahko tudi kadarkoli zahteva da se njegovi osebni podatki prenehajo uporabljati začasno ali trajno za namen neposrednega trženja in z tem je upravljalec osebnih podatkov dolžan ustrezno preprečiti uporabo osebnih podatkov v roku petnajstih dni, ter o tem

obvestiti posameznika ki je to zahteval. Upravljalec pri takem primeru tudi krije vse nastale stroške (Zakon o varstvu osebnih podatkov (ZVOP-1), Ur. l. RS, št. 94/07).

– **Videonadzor**

Videonadzor se lahko izvaja v javnem in zasebnem sektorju, če je to potrebno za varnost ljudi ali premoženja, zaradi zagotavljanja nadzora vstopa ali izstopa ali če zaradi narave dela obstaja možnost ogrožanja zaposlenih. Izvajalec videonadzora mora objaviti obvestilo, ki mora biti vidno in objavljeno na način, da omogoči posamezniku, da je seznanjen o izvajanju preden se videonadzor začne izvajati in mora vsebovati podatke o nazivu izvajalca in telefonsko številko za pridobitev informacij o shranjevanju posnetkov (ZVOP-1).

– **Biometrija**

Lasnosti posameznika se lahko primerjajo ali ugotavljajo z obdelavo biometričnih značilnosti, tako da lahko preverimo njegovo identiteto oziroma izvršimo njegovo identifikacijo pod pogoji ki jih določa zakon.To so vedenjske, telesne in fiziološke značilnosti, ki določajo vsakega posameznika med katere uvrščamo očesno mrežnico, šarenico, prstne odtise, ušesa, značilna drža, indeoksiribonukleinska kislina (DNK) in posnetek papilarnih črt na prstih (ZVOP-1).

– **Evidenca vstopov in iztopov iz prostorov**

Oseba zasebnega ali javnega sektorja lahko za namene varovanja življenja, premoženja, telesa posameznikov ter zaradi održavanja reda v njenih prostorih zahteva od vsakega posameznika, ki vstopi ali izstopi iz tega prostora da navede vse ali nekatere svoje osebne podatke, ter njihov razlog za vstop in iztop iz prostora. Lahko tudi preveri resničnost teh podatkov z pregledom osebnega dokumenta posameznika. V evidenci vstopov in iztopov se lahko vodijo samo naslednji osebni podatki, ki se lahko zahtevajo od posameznika kot so osebno ime, številka in vrsta osebnega dokumenta, naslov stalnega ali začasnega prebivališča, zaposlitev, datum, uro in razlog zakaj je posameznik vstopil ali izstopil v prostor. Te podatki se lahko hranijo največ tri leta od vpisa v evidence, nato pa se zbrišejo ali uničijo, če z zakonom ni določeno drugače (ZVOP-1).

– **Javne knjige in varstvo osebnih podatkov**

ZVOP-1 v 83. členu navaja: »Osebni podatki iz javne knjige, urejene z zakonom, se lahko uporabljajo le v skladu z namenom, za katerega so bili zbrani ali se obdelujejo, če je zakoniti namen njihovega zbiranja ali obdelave določen ali določljiv.«

– **Povezovanje zbirk osebnih podatkov**

Zbirke osebnih podatkov iz javnih knjig in uradnih evidenc lahko povezujemo samo takrat, ko je tako določeno v zakonu. Vsak upravljavec, ki povezuje zbirke osebnih podatkov je dolžan pisno o tem predhodno obvestiti državni nadzorni organ, predvsem če katerakoli

zbirka osebnih podatkov vsebuje občutljive podatke. Zbirke osebnih podatkov iz prekrškovnih in kazenskih evidenc je prepovedano povezovati z drugimi zbirkami osebnih podatkov, ter podatki o povezanih zbirkah osebnih podatkov iz javnih knjig in uradnih evidenc se v registru vodijo posebej od ostalih zbirk o osebnih podatkih (ZVOP-1).

– **Strokovni nadzor**

Izvajalec strokovnega nadzora lahko obdeluje le tiste osebne podatke nad katerimi ima po zakonu pristojnost do izvajanja nadzora in ima pravico do izpisa, kopiranja, vpogleda ali prepisovanja vseh osebnih podatkov pri njihovi obdelavi za izdelave poročila in za namene strokovnega nadzora, ter je dolžan varovati njihovo tajnost. Vse stroške ki lahko nastanejo pri obdelavi osebnih podatkov krije upravljavec osebnih podatkov (ZVOP-1).

2 PRAVNI VIRI VARSTVA OSEBNIH PODATKOV IN ZVOP-1

2.1 Zakonska ureditev in razvoj varstva osebnih podatkov

Ustava Republike Slovenije (URS), Ur. l. RS, št. 33/91-I, 42/97 – UZS68, 66/00 – UZ80, 24/03 – UZ3a, 47, 68, 69/04 – UZ14, 69/04 – UZ43, 69/04 – UZ50, 68/06 – UZ121,140,143, 47/13 – UZ148, 47/13 – UZ90,97,99 in 75/16 – UZ70a) je temeljni zakonodajni akt v Republiki Sloveniji, ki zagotavlja varstvo osebnih podatkov in pravico do zasebnosti. Te pravice ima URS določene v 35. členu v katerem navaja da je zagotovljena nedotakljivost človekove telesne in duševne celovitosti, njegove zasebnosti ter osebnostnih pravic in v 38. členu kjer navaja da je zagotovljeno varstvo osebnih podatkov. Vsako zbiranje, obdelovanje, namen uporabe, nadzor in varstvo tajnosti osebnih podatkov določa zakon. Vsakdo pa ima pravico seznaniti se z zbranimi osebnimi podatki, ki se nanašajo nanj in pravico do sodnega varstva ob njihovi zlorabi. Ustavodajalec se glede na navedeno ni odločil za tako imenovani »model zlorabe«, ampak za »obdelovalni model«, kar pomeni, da pravila ni določil na načelih svobode obdelave osebnih podatkov, ampak na urejanju dopustne obdelave osebnih podatkov na zakonski ravni. Izbira takšnega modela pomeni da je ustavno dovoljeno obdelovati le tiste vrste podatkov, ki so nujno potrebni in primerni za uresničenje zakonsko opredeljenega namena, kar v bistvu pomeni, da je prepovedano vse, razen tistega, kar je izrecno dovoljeno z zakonom in popolnoma mora biti jasno, kateri podatki se lahko obdelujejo, zagotovljeno mora biti primerno zavarovanje in točen namen obdelave podatkov (Pirc Musar, 2006a, str. 20).

Svoj prvi zakon s področja varstva osebnih podatkov je Slovenija sprejela leta 1990 in ta predmetni zakon je veljal dokler ni bil 15. 4. 2004 sprejet ZVOP- 1 in začel veljati z 1. 1. 2005. Sprejetje ZVOP-1 je bilo predvsem zelo pomembno zaradi vstopa Slovenije v Evropsko Unijo saj je z tem dobila dolžnost da uskladi varstvo osebnih podatkov z določbami Direktive 95/46/ES. Zakon je predvideval ustanovitev neodvisnega in samostojnega nadzornega organa za varstvo osebnih podatkov, ki ima vse pristojnosti, kot

se za tak nadzorni organ zahteva, zakonodajni okvir pa je bil dokončno dopolnjen z Zakonom o informacijskem pooblaščencu saj se je Direktiva 95/46/ES v celoti prenesla šele z uveljavitvijo tega zakona v slovenski pravni red. Informacijski pooblaščenec pa je bil ustanovljen 1. januarja 2006 (Prelesnik, 2015, str. 3).

Vprašanja, ki so povezana z uveljavljanjem, spoštovanjem in varstvom človekovih pravic in svoboščin so v današnjem svetu pogoj za normalno delovanje vsake države, ki je civilizirana. Te pravice so namreč pridobljene v tisočletnem spopadanju med tistimi ljudmi, ki so bili družbeno močni in ostalimi sloji, ki so bili tej oblasti podrejeni. Zraven večnega argumenta v prid človekovim svoboščinam in pravicam ni nobenega drugega bolj prepričljivega kriterija za razvejanost pravic in presojo sodobne podobe kot je zgodovinska utrjena pot pri njihovem uveljavljanju, oblikovanju in utemeljevanju in prav zaradi takšnega zgodovinskega razvoja smo zavedni z dejstvom, da vprašanja glede človekovih pravic niso le ena izmed mnogih vprašanj posamezne družbene ter politične ureditve, ampak njeno pomembnejše vprašanje od katerega je odvisna njena rešitev celotne politične zgradbe družbe. Se pravi da brez jasne zgodovinske zavednosti o razvijanju človekovih pravic ne bi bilo možno teoretično razpravljati o pravicah, ker bi se ne bi bilo mogoče izogniti določenim oviram, ki jih konstantno postavlja močna ideologizacija in več poskusov nezgodovinske absolutizacije stanja pravic v različnih družbah. Vsa človekova preteklost je zgodovina boja, da bi bil svoboden, saj je svoboda bistvenega pomena za vsakega človeka, ki jo je možno ravno zaradi tega antropološko utemeljiti. Zaradi tega je človekova miselnost, odkar se zavedamo našega obstoja pretkana z idejo o svobodi in enakosti pri katerih so določena zgodovinska dogajanja določala stopnjo utopičnosti in abstraktnosti teh idej. Vsem pa je bilo skupno vprašanje in iskanje odgovora, kakšen je odnos med politično skupnostjo in svobodo posameznika (Jambrek, Perenič & Uršič, 1988, str. 17–19).

Prvi znaki da je varstvo osebnih podatkov ena od temeljnih človekovih pravic, ki ga določa ustava so bili amandmaji sprejeti k republiški ustavi v letu 1989 in so že takrat določali da je zagotovljeno varstvo osebnih podatkov. Slovenija je marca 1990 na podlagi teh amandmajev dobila svoj prvi zakon katerega je bila glavna naloga določitev pravic in urediti varstvo osebnih podatkov, ter ukrepe in načela da se ne bi dogajale zlorabe teh pravic. Pomembna je bila tudi ratifikacija Konvencije o varstvu posameznika, zaradi avtomatske obdelave podatkov, ki je postala standard zakonskega procesiranja, zbiranja in uporabe podatkov. Državni zbor RS je leta 1999 zaradi pritiska in zahtev zaradi približevanja k Evropski uniji sprejel nov Zakon o varstvu osebnih podatkov, ki je že bil usklajen z navedeno direktivo ni pa še imel določene institucije, ki bo nadzirala varstvo osebnih podatkov. V letu 2001 sta bila z Zakonom o spremembah in dopolnitvah zakona o varstvu osebnih podatkov zato ustanovljena Varuh človekovih pravic in Inšpektorat za varstvo osebnih podatkov (Pirc Musar, Bien, Bogataj, Prelesnik & Žaucer, 2006, str. 21–22).

2.2 Viri EU in mednarodne pogodbe

Svet Evrope je mednarodna regionalna organizacija, ki je bila ustanovljena 5. maja 1949 in ima danes iz evropske regije 47 držav članic. Slovenija je postala članica 14. 5. 1993 in z tem sprejela izpolnjevanje smernic, priporočil in načel, ki jih daje Svet Evrope in so obvezne za vse članice. Vsaka država mora za vstop izpolnjevati dva pogoja, ki sta pristop k Evropski konvenciji o varstvu človekovih pravic in temeljnih svoboščin in sprejetje nadzora njenega implementacijskega mehanizma. Evropska konvencija o varstvu človekovih pravic in temeljnih svoboščin je bila sprejeta v Rimu 4. 11. 1950 veljati pa je začela 3. 9. 1953. Slovenija jo je ratificirala v letu 1994 do sedaj pa je bila tudi že večkrat dopolnjena. Osmi člen je eden izmed najpomembnejših in določa da ima vsakdo pravico do svojega zasebnega in družinskega življenja, svojega doma in dopisovanja. V izvrševanje te pravice se javna oblast ne sme vmešavati razen če je to z zakonom določeno in nujno v demokratični družbi zaradi državne varnosti, javne varnosti ali ekonomske blaginje države, zato da se prepreči nered ali zločin, da se zavaruje zdravje ali morala ali da se zavarujejo pravice in svoboščine drugih ljudi (Rovšek, 2005, str. 54).

Konvencijo o varstvu posameznikov glede na avtomatsko obdelavo osebnih podatkov (v nadaljevanju Konvencija št. 108) je bila sprejeta 21. 1. 1981 v Strasbourgu in je začela veljati v letu 1985, Slovenija pa jo je ratificirala v letu 1994. Temeljni namen Konvencije št. 108 je spoštovanje pravic in temeljnih svoboščin posameznika in v njeni določbi prvega člena navaja da je njen namen zagotoviti na ozemlju vsake pogodbenice vsakemu posamezniku, ne glede na državljanstvo in prebivališče, zagotoviti spoštovanje njegovih pravic in temeljnih svoboščin, še posebej do pravice do zasebnosti glede na avtomatsko obdelavo osebnih podatkov, ki se nanašajo na posameznika. Iz samega namena konvencije izhaja da se bo zakonodaja prilagajala avtomatski obdelavi osebnih podatkov in tehnološkemu napredku v 153. členu URS pa je bila v pravni sistem prenesena neposredna uporaba njenih določil, ki določajo, da morajo biti predzakonski akti, zakoni in ostali predpisi usklajeni z ratificiranimi mednarodnimi pogodbami. Konvencija vsebuje več temeljnih načel varstva osebnih podatkov kot so načelo kakovosti podatkov, načelo omejitve obdelave, načelo zavarovanja podatkov ter načelo odprtosti in sodelovanja. Pomen načel je da morajo podatki biti obdelani in pridobljeni zakonito in pošteno, pri posebnih vrstah osebnih podatkov (zdravstveno stanje, versko prepričanje, poreklo) pa ne smejo biti obdelovani podatki, ki jim z nacionalno zakonodajo ni določena posebna zaščita in sprejeti ustrezni ukrepi za zavarovanje osebnih podatkov in tudi da mora vsak posameznik imeti omogočen dostop do vseh informacij, ki so v zvezi z obdelovanjem njegovih osebnih podatkov. Njenim podpisnicam pa daje tudi nalogo da izvršijo primerne pravne ukrepe ob kršenju določb nacionalne zakonodaje s katero se zagotovi uresničitev temeljnih načel zaščite podatkov iz konvencije (Kovačič, 2006, str. 76).

Direktiva o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov (95/46/ES) Ur. EU, L 281/31 je bila sprejeta 24. oktobra 1995 in je osrednji del evropske zakonodaje o področju varstva osebnih podatkov. Države ki so članice so jo morale

implementirati do 24. oktobra 1998 in je za vsako državo članico zavezujoča glede cilja, ki ga je potrebno doseči vendar dovoljuje nacionalnim organom izbiro metod in njene oblike. Sprejeta je bila zaradi zagotovitve ravnovesja med svoboščinami posameznikov in varstvom temeljnih pravic. Direktiva 95/46/ES določa da mora biti obdelovanje osebnih podatkov pošteno in zakonito, podatki morajo biti zbrani na zakonit in za točno določen namen in ne smejo nikoli biti obdelovani za kakršnekoli druge namene, razen če to ni bilo že prej tako določeno. Podatki morajo vedno biti aktualni, neprekomerni in ustrezni, ter so shranjeni v takšni obliki, ki dovoljuje identifikacijo posameznikov le tako dolgo, dokler ni dosežen namen njihove obdelave. Za obdelavo osebnih podatkov mora vedno obstajati soglasje posameznika, na katerega se te podatki nanašajo in tudi vsak posameznik mora biti obveščen o tem kateri podatki in za kakšen namen se zbirajo. Seznanjen mora biti tudi z pravicami do popravkov osebnih podatkov in možnostjo dostopanja do osebnih podatkov. Osebni podatek, njegova obdelava in namen obdelave, zavarovanje in iznašanje osebnih podatkov so postali temelji splošne izobrazbe posameznika in zato je z Direktivo 95/46/ES lahko rečemo da dosežen zelo pomemben premik glede uresničevanja pravic do informacijske zasebnosti. Glede na to da spoznanja in predpisi direktive varstva osebnih podatkov izhajajo iz leta 1995, vendar se je od takrat do danes zgodil velik tehnološki razvoj, ki ga zakonodajalec ni mogel predvidevati in zato predpisi niso mogli več slediti temu napredku in zagotavljati odgovore na praktične sodobne dileme. V današnjem svetu kjer ima tehnologija zelo pomembno vlogo na vseh področjih v življenju in v katerem je pretok osebnih podatkov vedno večji in so se izzivi globalizacije in novih tehnologij izredno povečali in zato zahtevajo novejše rešitve za bolj učinkovito varstvo osebnih podatkov je Direktiva 95/46/ES zelo zastarela, zato je bila reforma v EU glede varstva osebnih podatkov nujno potrebna in je bila tako kot posledica nove zakonodaje o varstvu osebnih podatkov v EU direktiva razveljavljena v maju 2018.

Organizacija združenih narodov je bila ustanovljena 26. oktobra 1945 in je mednarodna organizacija katere Ustanovna listina predstavlja njen temelj delovanja in kjer sta bila obravnavana in sprejeta dva pomembnejša akta in to sta Splošna deklaracija človekovih pravic in Mednarodni pakt o državljanskih in političnih pravicah. V mednarodni teoriji človekovih pravic je pravica do varstva osebnih podatkov uvrščena pod bolj širok pojem pravic do spoštovanja zasebnosti. Splošna deklaracija človekovih pravic je bila sprejeta leta 1948 in vse njene določbe so zakonsko obvezne za vse države, ki imajo vneseno njeno vsebino v svojih ustavah. Pomemben je 12. člen, ki se navezuje na pravico do zasebnosti in pravi da se ne sme nikogar nadlegovati z samovoljnim vmešavanjem v njegovo družino in zasebnost, v njegovo dopisovanje in stanovanje kot tudi da ni dovoljeno napadati posameznikovo ugled in čast in poleg tega določa da ima vsak posameznik pravico do varstva zakona pod takšnimi pogoji. Mednarodni pakt o državljanskih in političnih pravicah je bil sprejet leta 1966 in začel veljati naslednjo leto v marcu, ter pravi da je dosegljiva idealna človeška svoboda, če so le zato omogočeni pogoji, ki vsakemu dajejo možnost da uživa v svojih političnih in državljanskih pravicah ter v svojih kulturnih, socialnih in ekonomskih pravicah. V njegovem 17. členu je določeno da se nihče ne sme nikomur nezakonito in samovoljno vmešavati v njegovo zasebno in družinsko življenje, v

dopisovanje in stanovanje ali nezakonito napadati posameznikovo čast in ugled, ter da ima vsak posameznik pravico do zakonskega varstva pred takimi napadi. Mednarodna organizacija dela je ena izmed najstarejših agencij Združenih narodov njena naloga pa je izvajanje aktivnosti na izboljšavi socialnih pravic in statusa ki ga imajo delavci. V okviru te organizacije je bil leta 1997 sprejet Kodeks ravnanja o varstvu osebnih podatkov delavcev in sicer da se osebni podatki o delavcih zbirajo, uporabljajo in shranjujejo namensko in zakonito.

2.3 Zakon o varstvu osebnih podatkov

V Republiki Sloveniji je na področju varovanja osebnih podatkov to bil prvi Zakon o varstvu osebnih podatkov in je začel veljati 24. 3. 1990, vendar ko je Slovenija leta 2004 vstopila v EU kot njena članica je zato 15.7. 2004 sprejet nov ZVOP-1, ki je začel veljati 1.1.2005. ZVOP- 1 določa načela, pravice, ukrepe in obveznosti z katerimi se preprečuje neustavno, nezakonito in neupravičeno poseganje v dostojanstvo in zasebnost posameznikov pri obdelavi osebnih podatkov. Namen in vsebina tega zakona sta opredeljena v prvem členu ZVOP- 1 katerega je izhodišče da je varstvo osebnih podatkov del širokega področja o varstvu zasebnosti. Na področju nadzora veliko obveznost ZVOP- 1 dodeljuje Informacijskemu pooblaščencu, ki nadzira da se zakon izvaja pravilno in je neodvisni nadzorni organ. Tako ZVOP-1 preprečuje nezakonite in neustavne posege v dostojanstvo in zasebnost posameznika.

Prepoved nezakonitih dejanj pa ne velja samo za kršitve ZVOP- 1, ampak tudi za kršenje drugih specialnih zakonov, ki z določbami ZVOP- 1 in v skladu z 38. členom Ustave RS obdelujejo osebne podatke na različnih področjih. Poznamo tudi izjemne primere, ko določbe ZVOP- 1 ne veljajo in jih ne uporabljamo. Prvi takšen primer je ko se osebni podatki posameznika obdelujejo izključno za osebne ali družinske namene, takrat ni potrebno da uporabljamo ZVOP-1. Drugi primer, kjer se ZVOP- 1 ne upošteva so osebni podatki, ki se obdelujejo za člane verskih skupnosti, sindikatov, političnih strank in društev v tem primeru ima upravljalec osebnih podatkov dolžnost, da vzpostavi katalog kjer so zbrani vsi osebni podatki, ter je zadolžen poročati državnemu nadzornemu organu za varstvo osebnih podatkov in tudi o njih se ne sme objavljati podatkov v drugih registrih, kjer so zbrani drugi osebni podatki. Tretji primer so osebni podatki, ki se uporabljajo v medijih za obveščanje javnosti za katere velja enako kot v drugem primeru in ne rabijo uporabljati določb zakona o iznosu osebnih podatkov iz države (Čebulj & Žurej, 2005, str. 31).

V celotnem postopku ravnanja z osebnimi podatki ZVOP-1 določa temeljna načela, ki jih moramo vedno upoštevati, poleg tega pa so ta načela vsebovana tudi v Mednarodnih pravnih aktih in v Ustavi. Najpomembnejša med njimi so: načelo sorazmernosti, načelo zakonitosti in poštenosti in načelo prepovedi diskriminacije. Zakonodajalec želi z njimi poskrbeti da bi se minimalno posegalo v zasebnost posameznika pri obdelavi njegovih osebnih podatkov. Z splošnimi načeli se razlaga zakonske določbe in se jih pravno argumentira, ter so vodilo

pravni ureditvi in zakonskim garancijam. Zelo pomembno pri tem zakonu je da so naslovniku pravne norme določila razumljiva v aspektu pravnih načel, ki jih zakonodajalec poudari kot ureditveni razlog (Pavčnik, 1999, str. 21).

3 SPLOŠNA UREDBA EU O VARSTVU PODATKOV

3.1 Namen in razlogi zakonske preureditve in ZVOP-2

Zelo široka uporaba in razvoj komunikacijske in informacijske tehnologije sta začela zelo močno vplivati na vsa področja človekovega delovanja in življenja. Temu lahko rečemo digitalizacija našega gospodarstva in družbe. Govorimo lahko o četrti industrijski revoluciji, pri kateri ne gre za menjavo fizičnega dela ljudi z stroji, ampak gre za nadomestitev in izboljšavo človeških miselnih opravil in ravnanje z visokimi računskimi in avtomatiziranimi procesi. Digitalizacija je prinesla nove do sedaj še nepredstavljive možnosti, ne samo v industriji, ampak tudi v storitvenih dejavnostih. Razvijanje programskih oprem in informacijske tehnologije je omogočilo uporabo mobilnih aplikacij in razvijanje algoritmov za razvoj umetne inteligence, senzorje in zmogljivejše robote, ki so čedalje cenejši in manjši, kar omogoča vedno bolj širše uporabljanje proizvodnje in novih tehnik, pod kar spada tudi 3D tiskanje, najpomembnejša pa je možnost povezave v kiberfizične sisteme, pri katerih naprave lahko izmenjujejo podatke med seboj in proces poteka deloma avtonomno. Nastane zelo veliko podatkovje, ki mu rečemo big data, ki ga je možno analizirati in podatke ki smo jih z tem pridobili uporabimo v poslovnih procesih, tako imenovanih smart data. Mobilni internet ne povezuje več samo ljudi med sabo, ampak je ustvaril internet storitev in stvari, tehnološki razvoj oblaka (angl. cloud technology), uveljavil pa je tudi digitalne platforme (Senčur Peček, 2017, str. 6).

Pri obdelovanju osebnih podatkov z modernimi tehnologijami je veliko pomanjkanje pravnih norm, saj takšna tehnologija že dolgo ni več znanstvena fantastika to so trojanski konji, internet stvari, brezpilotni letalniki, nove oblike biometrije, avtomatska prepoznava tablic, še pametnejši telefoni in aplikacije, neskončne možnosti avtomatiziranega odločanja in profiliranja so povod za spreminjanja zakona o varstvu osebnih podatkov na ravni EU. Ker je bila tako Direktiva 95/46/ES kot na njenem temelju sprejet ZVOP-1 odsev časa, je povsem jasno da sodobnemu načinu življenja, ki so ga ustvarile sodobne tehnologije ta pravna podlaga ne ustreza več. Te tehnologije veliko dajejo a istočasno v zameno želijo pridobiti veliko več naših podatkov (Prelesnik, 2017, str. 3).

V letu 2010 je Evropska komisija predstavila Svetu in Evropskemu parlamentu sporočilo z katerim sta se obe institucije strinjali in na temeljih tega sporočila je leta 2012 Komisija pripravila predlog za reformo varstva osebnih podatkov. Predlog se je sprejemal po rednem zakonodajnem postopku, Evropski parlament in Svet pa sta zraven odločala kot sozakonodajalca. V prvi obravnavi je marca 2014 Evropski parlament sprejel vidik za predlog uredbe, ki služi kot iztočnica za nadaljnja pogajanja med institucijami. Splošna

uredba o varstvu osebnih podatkov je bila sprejeta in usklajena 27. aprila 2016, ko se je končal celoten proces in je bila potrebna le še objava v Uradnem listu Evropske Unije v katerem je bila objavljena 4. maja 2016.

Sprejetje predloga ZVOP- 2 po nujnem postopku je predlagala vlada RS 12. 4. 2018, vendar neuspešno, saj je velika večina poslanskih skupin predlog zavrnila in je posledično prišlo do razpustitve parlamenta, tako da do sprejema zakona nikoli ni prišlo, ampak neodvisno od nesprejetja ZVOP-2 se je začela Splošna uredba o varstvu osebnih podatkov neposredno uporabljati z 25. 5. 2018. Ne glede na to da ZVOP-2 še vedno ni bil sprejet moramo vedeti, da se Splošna uredba o varstvu osebnih podatkov uporablja neposredno, zato so vse določbe v nacionalnih zakonih, trenutno je to v RS ZVOP-1, ki nasprotujejo Splošni uredbi o varstvu osebnih podatkov neveljavne. Novi evropski ureditvi pa se morajo prilagoditi podjetja ne glede na to da RS še ni sprejela ZVOP-2. Nov osnutek predloga Zakona o varstvu osebnih podatkov ZVOP-2 je že bil objavljen 6. 3. 2019, rok za uveljavitev zakona pa naj bi bil določen julij 2019.

Cilji predloga ZVOP-2 je zagotavljanje izvrševanj Direktive in Splošne uredbe v pravnem redu RS, tako da bi čim več vprašanj bilo rešeno ali urejeno v sistemskem zakonu o varstvu osebnih podatkov in tako zagotovljena uresničitev posameznikove človekove pravice do varstva osebnih podatkov, kot je navedeno v 38. členu Ustave RS. Predvsem je treba zagotoviti spoštovanje pravne varnosti, da bi bila vsebina določb ZVOP-2 najbolje kar se da v pomoč posameznikom na katere se osebni podatki nanašajo, ter zagotoviti ljudem na katere se osebni podatki nanašajo ter poslovnim subjektom in javnopravnim organom, da so sistemske norme pojasnjevalno predpisane ali čimbolj povezane, tako da je omogočen čimvečji koherenten pristop k izvedbi varovanja pravic in izvedbi uresničevanja s področja varstva osebnih podatkov. Predvsem pa zagotovitev da se ohrani do sedaj dosežena višja stopnja varovanja osebnih podatkov v čimvečji meri. V predlogu ZVOP-2 so kot del novosti uporabljene zakonodajne tehnike kot so: tehnika indikacije, tehnika prepisa, tehnika povzetka in tehnika združitve določb iz Splošne uredbe in Direktive. Načela predloga ZVOP-2 pa so: načelo spoštovanja osebnosti in pravic človeka, načelo zakonitosti, načelo stroge sorazmernosti, načelo namenske obdelave osebnih podatkov in delno relevantno načelo, kar pomeni da je prepovedano vse kar ni izrecno dovoljeno. Glede na dosedanji Zakon o varstvu podatkov (ZVOP-1) se poglavitne zakonodajne spremembe nanašajo na splošne določbe, kot tudi na posebne določbe, ter tudi na področne ureditve. Nekoliko drugače so določena načela poštenosti, zakonitosti in sorazmernosti, kar precej je spremenjena definicija splošne privolitve posameznika za obdelavo njegovih osebnih podatkov. Potem so na novo razdelane obdelave in definicije v povezanosti z posebnimi vrstami osebnih podatkov, glede drugih namenov obdelave osebnih podatkov je določena nova ureditev v skladu z Splošno uredbo in nova ureditev za osebe ki znotraj obdelovalcev ali upravljalcev jamčijo za varstvo osebnih podatkov, posebno ko gre za množične ali tvegane obdelave osebnih podatkov. Bolj natančno je definiran tudi postopek uveljavljanja pravic posameznikov posebno pa je poudarjen pomen svobode izražanja v odnosu do varstva

osebnih podatkov. Po določbi ZVOP-2 ostaja enotni nadzorni organ za varstvo osebnih podatkov RS Informacijski pooblaščenec, kot je veljalo tudi do sedaj, v posebnem delu ZVOP-2 (IX. del) pa je urejeno področje pravosodja, policije, izvrševanje kazenskih sankcij in obrambe in varnosti države. V posebnem delu ZVOP-2 so tudi urejene področne ureditve obdelave osebnih podatkov delno prenovljeni sta določbi o videonadzoru in biometriji. Upravne globe se bo določbi Splošne uredbe obravnavajo kot prekrški tako določajo kazenske določbe, prekrškovni organ pa je Informacijski pooblaščenec. Nujno so morale biti izvedene tudi velike spremembe dosedanjega tradicionalnega izrazoslovja na področju varstva osebnih podatkov, ker je bilo to nujno potrebno urediti glede na drugačno definicijo iz Splošne uredbe in Direktive. Predlog zakona ZVOP-2 pa določa tudi večje število rešitev z vidika administrativnih poenostavitev ali razbremenitev, vključno z gospodarstvom (Predlogi k osnutku Zakona o varstvu osebnih podatkov (EVA: 2018-2030-0045), 2019, str. 4).

3.2 Ocena učinka v zvezi z varstvom podatkov

Splošna uredba daje zelo velik značaj preventivnim dejanjem v sklopu novega temeljnega načela odgovornosti, ki zahteva in istočasno poudarja proaktivno in preventivno ravnanje obdelovalcev in upravljalcev podatkov. Ocena učinka v zvezi z varstvom podatkov so opredeljene v 35. členu Uredbe in zastopajo enega od bistvenih konceptov načela odgovornosti in orodje za pravočasno analizo, identifikacijo in zmanjšanje tveganj v zvezi z nezakonitimi ravnanji z osebnimi podatki. Kadar je mogoče, da bi lahko vrsta obdelave povzročila večje tveganje za svoboščine in pravice posameznikov, zlasti zaradi uporabe novih tehnologij in ob upoštevanju okoliščin, narave, obsega in namenov obdelovanja podatkov, takrat upravljalci pred obdelavo opravijo oceno učinka predvidenega dejanja in se ocena lahko navezuje in izvrši za več procesov ali za posamezen proces obdelave osebnih podatkov. Ocena zajema vsaj oceno sorazmernosti in potrebnosti dejanj obdelovanja podatkov glede na njihov namen, sistematičen opis predpostavljenih namenov in dejanj obdelave, oceno tveganj za svoboščine in pravice posameznikov na katere se navezujejo osebni podatki in ukrepi za obravnavo tveganj, zaščitnih ukrepov, ter varnostnih ukrepov. Ocena učinka je zasnovana za upravljanje s tveganji in njihovi čimvečji minimizaciji in ima tudi druge pozitivne vplive. Vedno je izvedena pred obdelavo osebnih podatkov in se ponavlja redno predvidoma na vsaj tri leta. Informacijski pooblaščenec priporoča da se ocena učinka izvede v štirih fazah in sicer prva je opredelitev konteksta, kjer so našteti vsi podatki, njihov namen obdelave, način pridobitve podatkov, udeleženi subjekti, kakšna sredstva se uporabljajo pri obdelavi in koliko časa se podatki hranijo. Druga faza je analiza tveganj in obsega identificiranje predvidenih tveganj v tej fazi je potrebno določiti raven resnosti in raven verjetnosti izbira orodij in metodologije pa je prepuščena upravljalcem. Ocena tveganja se opravi po temeljnih načelih varstva osebnih podatkov, ki jih določa 5. člen Uredbe in to so: zakonitost, poštenost in preglednost, najmanjši obseg podatkov, omejitev namena, omejitev shranjevanja, točnost in celovitost in zaupnost. Tretja faza so ukrepi za obvladovanje tveganj njihov namen pa je odpravljanje ali vsaj ublaževanje prepoznanih

tveganj na raven ki je spremenljiva. Četrta faza pa je priprava poročila ocene učinka, če so vse prve tri faze izvedene ustrezno imamo zapise, ki se sistematično uredijo v poročilo v katerem mora biti razvidno, da so bili upoštevani vsi kriteriji, ki so zahtevani, da je ocena učinka ustrezna. Priporočeno je da ima poročilo zaključek in da je vedno na razpolago nadzornemu organu, kadar zahteva poročilo. Z nadzornim organom se morajo upravljalci posvetovati v primeru, kadar iz ocene učinka lahko razberemo, da bi obdelovanje lahko povzročilo večje tveganje, če upravljalec ne bi hotel sprejeti ukrepa za zmanjšanje tveganja. Predhodno posvetovanje ni potrebno, če je tveganje ublaženo na spremenljivi ravni (Informacijski pooblaščenec, 2019).

3.3 Privolitev

Splošna uredba o varstvu podatkov določa da je privolitev posameznika ena od šestih pravnih veljavnih podlag za zakonito obdelavo podatkov in da je potrebno pridobiti veljavno privolitev na način, ki daje posamezniku pravo moč odločitve pod kakšnimi pogoji in komu bo posameznik dovolil obdelavo svojih osebnih podatkov. Privolitev mora vedno biti informirana, prostovoljna, specifična in nedvoumna. Če obdelava osebnih podatkov ni nujno potrebna za dosežek pogodbene obveznosti, potem ni dovoljeno pogojevanje privolitve z izvajanjem pogodbe. Vsak namen obdelave podatkov potrebuje ločeno privolitev in vsak posameznik ima pravico, da lahko privolitev kadarkoli prekliče. Splošna uredba o varstvu podatkov v 4. členu opredeljuje privolitev posameznika na katerega se navezujejo osebni podatki, kot vsako konkretno, prostovoljno, nedvoumno in informirano izkazano voljo posameznika z katero se z jasno potrditvijo ali izjavo posameznik izrazi da soglaša z obdelavo osebnih podatkov, ki se navezujejo na njega. Včasih je potrebno pridobiti izrecno privolitev posameznika do tega pa ponavadi pride v določenih primerih ko je potreba po nadzoru nad osebnimi podatki večja in ko obstaja veliko tveganje da bi podatki lahko bili zlorabljeni. Vedno je potrebno pridobiti izrecno privolitev, ko se obdelujejo posebne vrste podatkov, ko odločanje temelji izključno na avtomatizirani obdelavi podatkov in ko se osebni podatki prenašajo v tretje države. Splošna uredba o varstvu podatkov predpisuje, da je za veljavno privolitev potrebno jasno in pritrdilno postopanje, pri izrecni privolitvi pa so zahteve postavljene nekoliko višje in sicer izrecno na kakšen način je bila privolitev izražena, priporočeno je da je v pisni obliki lahko pa je tudi v obliki izpolnjenega spletnega obrazca ali kot skeniran dokument z podpisom ali dokument podpisan z elektronskim podpisom. Posebno varstvo osebnih podatkov pa potrebujejo predvsem otroci, saj se manj zavedajo posledic, tveganj in zaščitnih ukrepov pri svojih pravicah. Splošna uredba za varstvo podatkov privolitev otrok ureja v 8. členu, kjer navaja da morata biti izpolnjena dva pogoja in sicer da obdelava temelji na privolitvi otroka in da je obdelava, ki se ponuja neposredno otroku povezana preko storitev informacijske družbe. Takšno posebno varstvo bi moralo vplivati predvsem na uporabo osebnih podatkov otrok za ustvarjanje uporabniških profilov ali v namene trženja. Splošna uredba za varstvo podatkov določa da storitve informacijske družbe, ki so ponujane neposredno otroku in obdelujejo osebne podatke otroka so zakonite samo takrat, kadar je otrok star vsaj 16 let. Ko bo potrjen predlog ZVOP-2 bo

privolitev zakonita, če jo bo posredovala mladoletna oseba, ki je stara 15 let ali več. Pri privolitvah za znanstveno raziskovanje mora posameznik imeti možnost dati privolitev le na določenih področjih znanstvenega raziskovanja ali le pri delu projekta, privolitev pa mora vedno biti dobro informirana, namen obdelave mora biti dobro določen, opisan in jasen, kar pomeni da morajo biti določeni že od samega začetka. V primeru da to ni možno so opisi lahko bolj generalni, razen če gre za posebne vrste osebnih podatkov pri katerih Splošna uredba v 9. členu določa pri takih primerih več skrbnosti. Pri projektu ki napreduje iz ene stopnje v drugo stopnjo, mora privolitev za to naslednjo stopnjo biti dana vnaprej še preden se lahko projekt nadaljuje. Ustrezne zaščitne ukrepe kot so anonimizacija in psevdonimizacija pa Splošna uredba navaja v svojem 89. členu. Čeprav obdelava podatkov temelji na privolitvi, to ne opravičuje prekomernega zbiranja osebnih podatkov glede na določene namene (Informacijski pooblaščenec, 2019).

3.4 Pogodbena obdelava

Pogodba je potrebna zaradi tega, ker morata obe stranki poznati svoje odgovornosti in obveznosti, ki iz te pogodbe izhajajo. Upravljalci imajo odgovornost za skladnost z Splošno uredbo in zato lahko imenujejo le tiste obdelovalce, ki so zmožni zagotoviti zadostno jamstvo, da so zagotovljene zahteve Splošne uredbe in da se tudi pravice posameznikov ustrezno varujejo. Obdelovalci lahko z osebnimi podatki ravnajo le na osnovi dokumentiranih navodil upravljalca in imajo po Splošni uredbi določeno neposredno odgovornost, ki je lahko predmet za samostojno sankcijo. Splošna uredba v 28. členu določa minimalen obseg sestavin pogodbe o pogodbeni obdelavi in da so pogodbe v pisni obliki, kar zagotavlja da se in upravljalec in obdelovalec zavedata svojih obveznosti in pravic. Uporabljanje pisnih pogodb pa tudi dviguje posameznikovo zaupanje, da so njegovi osebni podatki obdelovani varno in zakonito. V pogodbah mora biti popolnoma razvidno kateri in čigavi podatki, ter za koliko časa in kakšen namen bodo obdelovani in razviden domet pravic in obveznosti, ki jih ima upravljalec z osebnimi podatki. Splošna uredba predpisuje da obdelovalec zagotovi da so osebe, ki so pooblaščene za obdelovanje osebnih podatkov zavezane k zaupnosti ali jih k temu zavezuje določen zakon. Obdelovalec mora sprejeti vse ukrepe, ki so potrebni za varnost osebnih podatkov in jih je dolžan opisati v internem pravilniku o varnosti osebnih podatkov, ter lahko zaposli nekega drugega obdelovalca le, če je pred tem dobil splošno ali posebno pisno dovoljenje upravljalca, ter mora zagotoviti da velja med obdelovalcem in pod-obdelovalcem enaka obveznost kot med obdelovalcem in upravljalcem in da je med njima podpisana pisna pogodba. Obdelovalec pomaga upravljalcu pri izpolnitvi njegovih obveznosti, da poda odgovor na zahteve za uresničitev pravic posameznika na katerega se osebni podatki nanašajo in pomaga tudi pri zagotovitvi varnosti obdelave in uradnih obveščanjih o oceni učinkov in kršitvah za varstvo osebnih podatkov. Po zaključitvi obdelave se vrne ali izbriše vse osebne podatke upravljalcu in iz 28. člena Splošne uredbe izhaja da obdelovalec zagotovi upravljalcu na dostop vse informacije, ki so potrebne za dokazovanje izpolnitve obveznosti in upravljalcu omogoči izvedbo revizij in da pri njih tudi sam sodeluje. Vsak obdelovalec je po Splošni uredbi neposredno odgovoren da:

sodeluje z nadzornimi organi, ne zaposluje pod- obdelovalcev brez predhodnega pisnega dovoljenja upravljalca, vodi evidenco dejavnosti obdelav, zagotovi varnost obdelave osebnih podatkov, po potrebi določi pooblaščeno osebo za varstvo osebnih podatkov, upravljalca obvešča o kršitvah, kadar je potrebno imenuje predstavnika znotraj EU. Če obdelovalec v neskladnosti z pogodbo, ki jo ima z upravljalcem ne izpolni svojih obveznosti kakor jih določa Splošna uredba lahko odgovarja za to odškodninsko v razmerju do posameznikov in upravljalca, lahko pa je tudi izpostavljen popravljalnim ukrepom nadzornega organa in globam. Splošna uredba dovoli uporabo standardnih pogodbenih določil, ki jih sprejme Informacijski pooblaščenec ali jih določi Evropska komisija, saj nova še niso določena, kar pomeni da so še vedno v veljavi obstoječe standardne pogodbene klavzule Evropske komisije in tako bo ostalo vse do njihove nadomestitve, spremembe ali razveljavitve. Če pa želimo osebne podatke prenašati v tretje države na osnovi veljavnih standardnih pogodbenih klavzul ni za to več potrebno dobiti posebnega dovoljenja od Informacijskega pooblaščenca, lahko pa se zaščitni ukrepi zagotavljajo tudi z drugimi pogodbenimi določili, vendar je v takem primeru potem potrebno dobiti dovoljenje od Informacijskega pooblaščenca (Informacijski pooblaščenec, 2019).

3.5 Evidenca dejavnosti obdelave

Glede evidentiranja dejavnosti obdelave osebnih podatkov vsebuje Splošna uredba izrecne določbe. Dejavnosti obdelav, ki se izvajajo v organizaciji so vse obdelave osebnih podatkov kot na primer hramba, posredovanje podatkov za določen namen, izbris, itd. Potrebno jih je voditi v pisni obliki in na takšen način, da se jih lahko na zahtevo Informacijskega pooblaščenca predloži v pregled. Tako obdelovalci kot upravljalci imajo vsak svoje dokumentacijske odgovornosti. Srednje velika in majhna podjetja, ki imajo do 250 zaposlenih imajo obveznost dokumentiranja procesov la za specifične vrste dejavnosti obdelave, posebno tam kjer gre za bolj tvegane obdelave kot so obdelave iz kazenskih evidenc ali pri zdravstvenih podatkih. Evidenco večinoma organizacij vodi v elektronski obliki in jih ažurira sproti, da evidence izkazujejo trenutno stanje dejavnosti obdelav. Z dokumentiranjem imajo upravljalci in obdelovalci vsak svoje obveznosti pri organizacijah, ki zaposlujejo več kot 250 ljudi je potrebno evidentirati vse dejavnosti obdelav osebnih podatkov, tiste ki jih zaposlujejo manj pa imajo omejene obveznosti in evidentirajo le tiste dejavnosti obdelav, ki predstavljajo tveganje za svoboščine in pravice posameznikov na katere se navezujejo osebni podatki ali niso občasne ali pa vključujejo posebne vrste osebnih podatkov. Splošna uredba v 30. členu določa, da vsak upravljalec vodi evidenco dejavnosti obdelave osebnih podatkov v sklopu svoje lastne odgovornosti. Vsaka evidenca mora imeti naslednje informacije: ime ali naziv, ter kontaktne podatke upravljalca, namen obdelave, opis kategorij posameznikov na katere se navezujejo osebni podatki in kategorije uporabnikov, kadar je potrebno informacije o prenosih osebnih podatkov v mednarodno organizacijo ali v tretjo državo in če je mogoče splošni opis organizacijskih in tehničnih varnostnih ukrepov in predvidene roke za izbris različnih vrst podatkov. Za izkazovanje skladnosti z Splošno uredbo je priporočeno in koristno, da se pregledno vodijo tudi zbirke

pridobljenih privolitev, pravne podlage za vsako evidentirano dejavnost, seznam obdelav in pogodbenih obdelovalcev, zbirko poročil o izvedbi ocen učinkov za varstvo osebnih podatkov, seznam obvestil o kršitvah, interni pravilnik o varovanju osebnih podatkov, evidenco uveljavljanja pravic posameznikov, ter druga dokumentacija kot so pripoznani kodeksi in pridobljeni certifikati. Dokumentiranje se izvaja z notranjo revizijo in drugimi postopki, ki zagotavljajo skladnost poslovanja in pomagajo ugotoviti katere osebne podatke organizacija obdeluje in kje se ti podatki nahajajo. Lahko se izvaja preko vprašalnikov, ki so pripravljeni za različne dele organizacije in pregledom postopkov, pogodb, politik in dogovorov, ter z beleženjem ugotovitev, ki so v pisni obliki in ustrezno strukturirane, da omogočajo lažje pregledovanje. Ugotovitve se uporabijo na način, da se dokumentacija, ki definira področje varstva osebnih podatkov konstantno osvežuje in prilagaja potrebam in dejanski praksi (Informacijski pooblaščenec, 2019).

3.6 Prijava kršitve varnosti

Če je verjetnost da bi bile z kršitvijo ogrožene svoboščine in pravice posameznikov Splošna uredba navaja dolžnost obveščanja nadzornega organa o morebitnih zaznanih kršitvah varnosti osebnih podatkov, obvestilo pa je potrebno podati takoj ko se zazna kršitev najkasneje v roku 72 ur. Kadar je velika možnost, da kršitev varnosti osebnih podatkov lahko povzroči preveliko tveganje za svoboščine in pravice posameznikov, takrat je potrebno da upravljalec obvesti posameznika, da je prišlo do kršitve njegovih osebnih podatkov. Priporočeno je da imajo organizacije vnaprej dokumentiran in vzpostavljen učinkovit sistem za zaznavo in sporočanje kršitev, kar bi zagotovilo tudi skladnost z Splošno uredbo in zelo pomagalo pri preprečevanju posledic za posameznike in preprečilo nepotrebne sankcije zaradi kršenja obveznosti uradnega obveščanja. Priporočeno je tudi da organizacije beležijo in hranijo vse zaznane kršitve varstva osebnih podatkov, ne glede na to ali je potreba po uradnem obveščanju. Splošna uredba v svojem 33. in 34. členu navaja kršitev varstva osebnih podatkov kot kršitev, ki vodi do nezakonitega uničenja, spremembe, izgube, nepooblaščenega dostopa do osebnih podatkov, kršitev pa je lahko napravljena nehote recimo iz malomarnosti ali pa je naklepna oziroma načrtovana. Na splošno je ta kršitev kot varnostni incident, ki ogroža celovitost, zaupnost in dostopnost osebnih podatkov. V praksi so lahko kršitve varnosti osebnih podatkov: posredovanje osebnih podatkov napačnemu naslovniku, dostopanje do podatkov z strani nepooblaščene osebe, kraja ali izguba računalniške opreme, ki vsebuje osebne podatke, spreminjanje osebnih podatkov brez potrebnih dovoljenj, nepooblaščeno uničevanje baz z osebnimi podatki, izguba dostopa do osebnih podatkov, kot je na primer izguba opreme, ki omogoča dešifriranje ali izguba gesla. V primeru kadar so zaznane katerekoli kršitve je treba oceniti dva ključna faktorja in sicer resnost in verjetnost posledic za svoboščine in pravice posameznikov. Resnost je povezana z škodo, verjetnost pa z možnostjo nastanka posledic, ki jo kršitev lahko povzroči posamezniku. Opozorilo uvodne določbe 85 Splošne uredbe se glasi, da lahko vsako kršenje varnosti osebnih podatkov, če se ti podatki ne obravnavajo pravočasno in ustrezno posameznikom povzroči premoženjsko ali nepremoženjsko in fizično škodo, kot je omejitev

njihovih pravic, izguba nadzora nad njihovimi osebnimi podatki, zloraba ali kraja identitete, diskriminacija, okrnitev ugleda, finančna izguba, izguba zaupnosti osebnih podatkov zaščitenih z poklicno skrivnostjo, neodborena reverzija psevdominizacije ali kakršnakoli druga znatna socialna ali gospodarska škoda. Za posameznika so torej lahko negativne posledice, kot je čustvena prizadetost ali duševna bolečina, kot tudi premoženjska in fizična škoda. Nekatere kršitve na posameznike močno vplivajo, medtem ko druge morda ne bodo presegale niti mogočih manjših neugodnosti za posameznika. Če se v organizaciji zaznajo kršitve se morajo oceniti tveganja za nastanek posledic, ki pa so vsakič odvisna od konkretnih okoliščin in ravno od te ocene je odvisno ali bo potrebno o kršitvi sporočiti Informacijskemu pooblaščencu. Upravljalca so obdelovalci dolžni obvestiti o vsaki kršitvi takoj, ko je ta bila zaznana in dostaviti vse potrebne informacije, da se lahko oceni tveganje posledice kršitve, ki bo pomagalo določiti ali mora upravljalec predložiti o kršitvi uradno obvestilo nadzornemu organu. Informacije, ki jih mora vsebovati uradno obvestilo o kršitvah so: opis kakšna vrsta kršitve je bila storjena, kategorije in kakšno število posameznikov na katere se navezujejo osebni podatki, vrste in približno število koliko evidenc osebnih podatkov, vse kontaktne informacije pooblaščene osebe za varstvo podatkov, opis verjetnosti posledic kršitve varnosti osebnih podatkov in opis ukrepov, ki jih je sprejel upravljalec ali pa predvidene ukrepe za blaženje tveganj za kršitve. Zahteve kaj mora uradno obvestilo o kršitvi vsebovati navaja 33. člen Splošne uredbe. V primeru da se o kršitvi ne obvesti nadzornega organa, ko je to potrebno in zahtevano se to smatra kot neukrepanje in neobveščanje nadzornega organa in je to po Splošni uredbi samostojna kršitev in je za njo predpisana globa do 10 milijonov evrov oziroma do 2 % letnega prometa organizacije. Upravljalec lahko dobi kazen, če ni izpolnil zahteve po obveščanju in kazen za kršitev. Nadzorni organ pa lahko naloži upravljalcu skladno z 58. členom tudi popravljalne ukrepe, ki jih mora upravljalec izpolniti in ravno zaradi tega morajo organizacije zagotoviti učinkovit interni postopek javljanja kršitev, ki lahko omogoči pravočasno zaznavanje kršitev in sporočanje teh kršitev z vsemi potrebnimi informacijami in podatki o varnostnem incidentu (Informacijski pooblaščenec, 2019).

4 NAJPOMEMBNEJŠE SPREMEMBE NOVEGA OKVIRJA VARSTVA OSEBNIH PODATKOV

4.1 Temeljna načela in spremembe v primerjavi z obstoječim zakonom

Bistvene spremembe in novosti novega okvirja varstva osebnih podatkov so pregledna iz osnovnih načel Splošne uredbe o varstvu osebnih podatkov, saj so takšna pravna načela kot vrednostna merila, ki uravnavajo vsebinsko opredelitev pravnih pravil in način njihove izvršitve. Osebni podatki se morajo zbirati, obdelovati in uporabljati pošteno, zakonito in na pregleden način in se lahko zbirajo samo za izrecne, določene in zakonite namene, kar pomeni da se osebni podatki ne smejo obdelovati na način ki ni skladen z namenom za katerega so bili zbrani in jih je prepovedano obdelovati za katerekoli druge namene za katere

niso bili pridobljeni. Glede na dosedanji ZVOP-1 se temeljne zakonodajne spremembe navezujejo na splošne in posebne določbe, ter tudi na področne ureditve in nekoliko drugače so določena načela poštenosti, zakonitosti in sorazmernosti. Na novo so razčlenjene obdelave in definicije o posebnih vrstah osebnih podatkov h katerim so vključene tudi pravne podlage za obdelavo in so sedaj ločene od posebnih vrst osebnih podatkov. To so pravne podlage za obdelave osebnih podatkov o kaznih za prekrške in kazenskih obsodbah, ampak ostajajo enaka pravila, kot veljajo za posebne vrste osebnih podatkov. Dokaj je tudi spremenjena definicija splošne privolitve posameznika za obdelavo njegovih osebnih podatkov, ki se sedaj imenuje privolitev posameznika in pomeni da vsako informirano, prostovoljno, nedvoumno in konkretno ravnanje v obliki jasnega aktivnega delovanja ali izjave iz katerega je razvidna želja posameznika in se nanj navezujejo osebni podatki, ter se strinja z obdelavo njegovih osebnih podatkov. Kot obveznost za obdelovalce in upravljalce pri namenu izkazovanja skladnosti obdelave osebnih podatkov se poleg izvedbe ocene učinkov izvaja tudi ukrep zunanje in notranje sledljivosti obdelav osebnih podatkov, ter je določena tudi nova ureditev za posameznike, ki zagotavljajo varstvo osebnih podatkov znotraj obdelovalcev in upravljalcev, še posebno ko gre za množične ali tvegane obdelave osebnih podatkov. Bolj podrobno je urejen postopek uveljavljanja pravic posameznikov in zaradi koristi zgodovinskega, znanstvenega, arhivskega in statističnega raziskovanja je bolj podrobno razdelano tudi razmerje nasproti varstvu osebnih podatkov in se zato v veljavno arhivsko zakonodajo ne posega. Pomen svobode izražanja na področju varstva osebnih podatkov je posebej poudarjen, tako da je v okviru pravnega reda RS zagotovljeno zadržanje uresničevanje svobode izražanja na isti ravni kot do sedaj. Kot je bil to do sedaj enotni nadzorni organ za varstvo osebnih podatkov RS še vedno ostaja tudi v predlogu ZVOP-2 Informacijski pooblaščenec, področje policije in pravosodja, ter obrambe in izvrševanje kazenskih sankcij pa je urejeno v posebnem delu ZVOP-2 (IX. del). V posebnem delu ZVOP-2 so urejene tudi področne ureditve obdelave osebnih podatkov, kot je biometrija in videonadzor. Izvedene so morale biti tudi ključne spremembe tradicionalnega izrazoslovja z področja varstva osebnih podatkov, ki smo ga uporabljali do sedaj in večje število rešitev z vidika administrativnih poenostavitev ali razbremenitev vključno z gospodarstvom, kot je ukinitev Registra zbirk osebnih podatkov, neposredno trženje, določen je olajšan sistem in določena je definicija povezovanja zbirk osebnih podatkov (Predlogi k osnutku Zakona o varstvu osebnih podatkov (EVA: 2018-2030-0045), 2019, str. 8–10).

Temeljna načela predloga ZVOP-2 so:

– **Načelo spoštovanja osebnosti in pravic človeka** pomeni zakonodajno urejanje na način individualnega pristopa pri katerem je treba izvirati iz posameznika kot upravičenca pravice do varstva osebnih podatkov, ki mu je potrebno dejansko zagotoviti uresničitev te pravice in je prvo glavno načelo novega predloga ZVOP-2. Načelo velja pri prenosu in posredovanju osebnih podatkov, pri prostem pretoku osebnih podatkov, pri čezmernih obdelavah osebnih podatkov, pri obdelavah osebnih podatkov za druge namene, ipd. in lahko deluje le takrat ko je določeni individualni pristop popolnoma upoštevan. Pri

preudarku na izvedbenih ali zakonodajnih procesih v pravice varstva osebnih podatkov je potrebno izvirati iz ocene vpliva posega na posameznika kot subjekta in narediti oceno z aspekta spoštovanja načela stroge sorazmernosti.

- **Načelo zakonitosti** izvira iz 38. in 87. člena Ustave Republike Slovenije pri katerih prvi določa » zbiranje, obdelovanje, namen uporabe, nadzor in varstvo tajnosti osebnih podatkov določa zakon« in pri drugem, ki določa da so obveznosti in pravice lahko urejene samo z zakonom. To načelo izvira tudi iz uvodne temeljne navedbe 39. Splošne uredbe iz več različnih točk in členov.
- **Načelo namenske obdelave osebnih podatkov** te določbe izvirajo tudi iz 38. člena Ustave Republike Slovenije, kar pomeni kadar se obdelovanje osebnih podatkov določa z zakonom po navodilih Splošne uredbe, Ustave ali Direktive mora biti vsak namen njihovega obdelovanja tudi točno določen v zakonu. V prvem odstavku 38. člena Ustave Republike Slovenije je tudi določeno da je »prepovedana je uporaba osebnih podatkov v nasprotju z namenom njihovega zbiranja«.
- **Načelo stroge sorazmernosti** v predlogu ZVOP-2 za to načelo velja da pri izvajanju kakršnihkoli posegov v pravico do varstva osebnih podatkov je potrebno izvirati iz načela sorazmernosti oziroma bolj podrobno po ustavnosodni presodi z uporabljanjem strogega testa sorazmernosti.
- **Delno relevantno načelo » prepovedano vse, kar ni izrecno dovoljeno «** to načelo še vedno velja pri represivnih posegih države v posameznikove temeljne svoboščine ali pravice. Pri zasebnem sektorju pa veljajo pri tem načelu omejitve, ki so usklajene z določbami v ZVOP-2.

V predlogu ZVOP-2 je delna novost tudi zakonodajna tehnika, glede na potrebo implementacije določb Direktive in delne implementacije določb Splošne uredbe in drugih pravnih aktov, zaradi dejstva da se veliko določb Splošne uredbe koristi neposredno in glede na primarno uporabo je potrebno zagotoviti upoštevanje pravne varnosti predvsem zaradi bolj učinkovitega uresničitve osebne posameznikove pravice do varstva osebnih podatkov po možnosti čim več na enem mestu. Zato so bile zato uporabljene nove zakonodajne tehnike: tehnika indikacije, tehnika povzetka, tehnika prepisa in tehnika združitve določb iz Direktive in Splošne uredbe (Predlogi k osnutku Zakona o varstvu osebnih podatkov (EVA: 2018-2030-0045), 2019, str. 6).

4.2 Pravice posameznikov

Vsak od nas se z pravico do varstva zasebnosti praktično srečuje vsak dan pa se tega niti ne zavedamo, niti kakšne so naše pravice, niti ali so te pravice bile kršene. Ker tehnološki razvoj zelo hitro narašča z internetom in napredkom na področju pametnih naprav postaja varovanje zasebnosti pomembna dobrina, ki se jo je potrebno predvsem zavedati in jo znati tudi ko je to potrebno uporabiti. Na te navedbe nakazuje tudi enotna evropska uredba, ki bo zagotovila enoten pristop k zagotovitvi te pravice za vsakega posameznika v EU. Splošna uredba o varstvu osebnih podatkov preudarno določa, da uredba varuje temeljne svoboščine in pravice

posameznikov še posebej njihovo pravico do varstva osebnih podatkov in daje velik poudarek na sam pomen posameznika. Splošna uredba v uvodni določbi tudi določa, da morajo osebni podatki biti obdelani in oblikovani tako, da služijo ljudem in je tudi namen varovanja osebnih podatkov tak da varuje pravice posameznika na katerega se podatki navezujejo.

Eden izmed ciljev Splošne uredbe je poenotenje pravic posameznika na področju obdelave osebnih podatkov, tako mora vsaka organizacija skladno z obveznostjo obveščanja vsakega posameznika informirati in obvestiti o njegovih pravicah, kar pomeni da če se posameznik, ki je dobro seznanjen z svojimi pravicami obrne na organizacijo lahko zahteva naslednje: dostop do osebnih podatkov, ki jih organizacija obdeluje, kopijo osebnih podatkov v pisni obliki, na kakšen način so osebni podatki shranjeni, dostop do seznama pogodbenih obdelovalcev, ki obdelujejo posameznikove osebne podatke, pravno podlago na kateri se obdelujejo posameznikovi osebni podatki in pojasnilo o namenu obdelovanja, informacijo o obdobju koliko časa se osebni podatki hranijo, informacijo o tem ali lahko organizacija pridobiva posameznikove osebne podatke tudi od drugih organov, informacije o avtomatiziranem odločanju oziroma profiliranju, informacije o kakršnihkoli kršitvah v zvezi z varovanjem osebnih podatkov in informacije kakšni so varnostni ukrepi pri obdelavi osebnih podatkov (minimiziranje, anonimizacija, šifriranje).

Vse te zahteve ima posameznik pravico zahtevati, zato mora vsaka organizacija v tem primeru imeti odgovore. Pravice posameznikov, ki jih uvaja Splošna uredba o varstvu podatkov so:

– **Pravica do seznanitve**

V praksi so nameni do seznanitve z osebnimi podatki zelo različni in večinoma popolnoma legitimni, saj želijo na takšen način posamezniki pogosto preveriti ali upravljalec njihove osebne podatke obdeluje zakonito (na primer ali je izvor podatkov zakonit, ali so podatki točni, ali so bili podatki posredovani uporabnikom, ki niso bili upravičeni do njih). Podatki se ponavadi potrebujejo zaradi obstoječega ali bodočega upravnega, sodnega ali kakšnega drugega pravnega postopka (na primer da se mora dopolniti pomanjkljiva vloga, da se dokaže določeno dejstvo, da se jih vloži v strokovno presojo) ali so podatki potrebni za domačo uporabo (na primer videonadzorni posnetek nekega dogodka), ali so podatki potrebni za ugotavljanje dejstev, ki so relevantna za njihove dolžnosti, pravni položaj ali pravice (na primer da se presodi ali je upravljalec podal odškodninsko obveznost), ali so podatki potrebni zaradi izgubljenih dokumentov (na primer upravna vloga, zavarovalna polica, kreditna pogodba), ker želijo dokazati in preveriti ali upravljalec razpolaga z osebnimi podatki ali ne ali hočejo preveriti vsebinsko ujemanje med podatki, ki jih imajo sami in ki jih ima upravljalec. Upravljalec oziroma organizacija mora ustrezno ukrepati, da zagotovi posamezniku na katerega se navezujejo osebni podatki vse informacije, ki so povezane z obdelovanjem posameznikovih osebnih podatkov v preglednem, razumljivem, jedrnatem, ter preprostem in jasnem jeziku, kar drži še posebej za vse informacije, ki so

namenjene otrokom. Informacije se lahko posredujejo ali v pisni obliki ali na kakšen drug način, lahko tudi preko elektronske pošte (Brulc, 2016, str. 9).

– **Pravica do izbrisa**

Če posameznik zahteva preklic svoje privolitve mora upravljalec nemudoma prenehati obdelovati posameznikove osebne podatke oziroma mora takoj preprečiti dostop do njih. Tudi če so bili osebni podatki posameznika posredovani katerim drugim upravljalcem se bo moral upravljalec, ki je sprejel zahtevo zelo potruditi, da bodo te podatki izbrisani tudi povsod drugod. Vpliv na uveljavitev te pravice sta imeli predvsem sodbi Sodišča EU Manni in Google Spain. Ta pravica je dokaj omejena predvsem za primere, ko so v mladosti bile objavljene kakšne nespametne objave podatkov na družbenih omrežjih, ki lahko kasneje v življenju škodijo posamezniku ali pa izbris podatkov, ki so bili zbrani nezakonito. Če za hranjenje teh podatkov zahteva ali določa zakon ali pa za njihovo objavo obstaja javni interes, potem posameznik praviloma izbrisa ne bo mogel doseči (Burnik, 2012, str. 11).

– **Pravica do ugovora**

Posameznik ima pravico ugovora, če so njegovi osebni podatki uporabijo zaradi statističnih, znanstvenih ali raziskovalnih namenov ali če se njegovi osebni podatki obdelujejo za namene neposrednega trženja. Upravičen razlog za ugovor je na primer, da po nakupu vstopnice za ogled neke gledališke igre še vedno od ponudnika dobivamo oglasna sporočila v zvezi z igrami te gledališke skupine.

– **Pravica glede profiliranja in avtomatiziranega sprejemanja odločitev**

Avtomatizirano sprejemanje odločitev pomeni da se odločitve sprejemajo povsem z tehnološkimi sredstvi brez vpliva človeškega faktorja, Splošna uredba o varstvu osebnih podatkov pa posamezniku dovoljuje pravico, da zanj odločitev ni veljavna, če je utemeljena samo z avtomatiziranimi sredstvi. Pri profiliranju pa gre za to, da se na podlagi določenih značilnosti, kot so barva las, spol, teža oblikujejo določene kategorije. Ta pravica je značilna predvsem za bančni sektor na primer pri ocenah kreditnih sposobnosti. Kljub temu pa Splošna uredba o varstvu osebnih podatkov redko dovoli odločitve, ki so utemeljene samo na avtomatizirani obdelavi. To dovoljuje samo v primeru da je takšna odločitev nujna, ker ni nobenega drugega načina, da pridemo do enakega cilja, da lahko sklenemo pogodbo oziroma je posameznik sam izrecno privolil. Posamezniku pa mora biti tudi zagotovljeno, da se izjasni o odločitvi, ki jo je sprejel na osnovi avtomatizirane obdelave in je zaželeno da čimprej poda prošnjo za osebno pojasnilo, ki mu jo mora oseba, ki je zato zadolžena tudi čimprej predložiti.

– **Pravica do popravka**

Posameznik na katerega se navezujejo osebni podatki ima popolno pravico zahtevati, da v primeru da so v zvezi z njim njegovi osebni podatki napačni, da mora upravljalec njegovih

osebnih podatkov brez nepotrebnega odlašanja to napako takoj popraviti.

4.3 Pooblaščena oseba za varstvo podatkov

Splošna uredba o varstvu osebnih podatkov določa pooblaščeno osebo za varstvo podatkov, kot nadzorni organ, ki bo izvajal vse nadzorne in svetovalne naloge na področju varstva osebnih podatkov. Določitev pooblaščene osebe lahko olajša uskladitev z določbami Splošne uredbe, podjetjem pa pomaga zagotoviti konkurenčno prednost in določa kriterij, da podjetje ali institucija samo presodi ali je potrebno imenovanje pooblaščene osebe, saj ta obveznost ni vezana na število zaposlenih v podjetju. Glavne naloge pooblaščene osebe so svetovanje obdelovalcem in upravljalcem o njihovih obveznostih, spremljanje skladnosti z Splošno uredbo, svetovanje pri izvedbi ocene učinka glede varstva podatkov, ter ozaveščanje in izobraževanje zaposlenih. Pooblaščena oseba mora biti na razpolago tako posameznikom, katerih podatke obdeluje, kot nadzornemu organu in deluje kot notranji revizor za varovanje osebnih podatkov. Imeti mora aktivno podporo z strani vodstva in mora biti neodvisna, ter vedno pravočasno seznanjena z vsemi zadevami v zvezi z varovanjem osebnih podatkov. Pooblaščena oseba mora tudi poznati poslovne procese v podjetju in mora imeti strokovno znanje o evropski in nacionalni zakonodaji in imeti prakso na področju varstva podatkov. Splošna uredba o varstvu osebnih podatkov določa v 37. členu kdo lahko imenuje pooblaščeno osebo to so: javni organi in telesa, podjetja pri katerih je njihov temelj dejavnosti dejanje obdelave, pri katerih je potrebno zaradi njihovega obsega, narave ali namenov posameznike sistematično in redno obsežno spremljati. Pod to kategorijo sodijo na primer zavarovalnice, banke, trgovci z klubi zvestobe, operaterji elektronskih komunikacij, kadrovske agencije, IT podjetja in spletne trgovine, ki izgrajujejo rešitve za obdelavo osebnih podatkov ali institucije, ki izvajajo veliko obdelavo občutljivih in zdravstvenih podatkov ali tako imenovanih posebnih vrst podatkov, kot jih imajo recimo klinike in bolnišnice ali socialno varstveni in zdravstveni zavodi. Temeljno vodilo pri izvedbi nalog pooblaščene osebe mora biti neodvisnost, saj institut zahteva bolj celovit pristop in neodvisen kolegijski organ z vodjo ali neodvisnega posameznika, kar predvsem pomeni da v organizaciji pooblaščena oseba ne more imeti položaja, ki bi ji omogočal storitev obdelave osebnih podatkov ali opredelitev namenov. Nasprotujoči si položaji splošno gledano lahko v organizaciji vključujejo položaje vodstva, kot so: operativni direktor, izvršni direktor, finančni direktor, vodja oddelka za trženje, vodja zdravstvene službe, vodja oddelkov za informacijsko tehnologijo ali vodja službe za človeške vire lahko pa vključujejo tudi druge položaje na nižji ravni organizacije, če takšne vloge ali položaji vodijo v določitev sredstev in namenov obdelave. Dobre prakse pa so: vključitev razlage nasprotnih interesov, opredelitev nezdružljivih položajev, oblikovanje notranjih pravil, da bi lahko preprečili nasprotja interesov, vključitev ustreznih klavzul v razpise za pooblaščeno osebo in izjavo, da pooblaščena oseba ni v nasprotju interesov. Splošna uredba o varstvu osebnih podatkov zahteva, da se kontaktne podatke pooblaščene osebe objavi in sporoči nadzornim organom in morajo vključevati: ime in priimek pooblaščene osebe, telefonsko številko, poštni naslov in elektronski poštni naslov, da lahko posamezniki na katere se navezujejo osebni podatki

čimbolj preprosto vzpostavijo komunikacijo. Za pooblaščeno osebo se lahko imenuje tudi svoj zaposleni v kolikor ne pride do nasprotij interesov in zanj ni potrebno ustvarjati novega delovnega mesta, lahko pa se imenuje za pooblaščeno osebo tudi zunanjega pogodbenega sodelavca (Informacijski pooblaščenec, 2019). Moj doprinos – je podati sistematičen pogled na ravni EU usklajeno pravno ureditev varstva osebnih podatkov, z vidika posameznika in podjetja. Prav tako je prispevek podatki najpomembnejše cilje in razloge za implementacijo Splošne uredbo EU o varstvu podatkov z ekonomskega vidika podjetja, da podjetje prepreči kršenje obveznosti in morebitne posledice sankcij.

SKLEP

Skozi pregled literature sem ugotovila, da smo z razvojem digitalne tehnologije lahko ljudje bolj-izpostavljeni nezakonitim namenom uporabe osebnih podatkov na družbenih omrežjih in zaradi tega je lahko pogosteje kršena naša pravica do osebnih svoboščin in zasebnosti. Razvoj tehnologije nam je tako prinesel širše možnosti pretoka informacij, kar je pozitivno z ekonomskega vidika za poslovanje podjetja na trgu. Hkrati pa razvoj tehnologije prinaša tudi probleme uporabe osebnih podatkov v nezakonite namene. Te probleme je bilo potrebno reševati sistematično in vključiti v zakonodajo, zato smo nujno potrebovali odgovore, ki nam jih je omogočila Evropska unija z Splošno uredbo o varstvu osebnih podatkov, ki se je začela uporabljati z 25. 5. 2018 in je bila zelo potrebna, saj je poenotila varstvo osebnih podatkov v Evropski uniji. Cilj in razlog za uvedbo Splošne uredbe EU o varstvu podatkov je zagotoviti poenoteno in usklajeno ukrepanje z vidika okrepitve pravic posameznikov v vseh državah članicah Evropske unije. Prav tako bi morali sprejeti predpise za varstvo podatkov na nacionalni ravni, ki bi urejali področja, ki jih ne ureja Splošna uredba o varstvu osebnih podatkov. V Sloveniji nam ni uspelo sprejeti takšnega zakona do datuma, ko se je začela uporabljati Splošna uredba o varstvu osebnih podatkov, zato mora biti po predlogu ZVOP-2 zakon objavljen in sprejet v Uradnem listu Republike Slovenije in uveljavljen v mesecu juliju 2019. ZVOP-2 bo zagotavljal izvrševanje določb Splošne uredbe o varstvu osebnih podatkov v pravnem redu Republike Slovenije, da bo čim več vprašanj rešeno in urejeno, ter z tem zagotovljena uresničitev osebne človekove pravice do varovanja osebnih podatkov in zagotovljeno upoštevanje pravne varnosti. Izhodišče zakonodajne ureditve so ljudje in njihove pravice in da bi bil posameznikom na katere se navezujejo osebni podatki čimbolj v pomoč.

Digitalizacija poslovnih procesov nam omogoča hiter prenos podatkov, zaradi česar pride do povečanega obsega zbranih osebnih podatkov in posledično podjetja zaradi tega ne morejo obvladovati oziroma nimajo preglednosti nad osebnimi podatki, kar lahko dokaj hitro vodi v napake in kršitve pri posredovanju osebnih podatkov. Zaradi tega Splošna uredba o varstvu osebnih podatkov zagotavlja več indikatorjev za večjo varnost pri uporabi osebnih podatkov kot je uvedba evidenc obdelave, ocene učinkov, visoka globa za kršitve ali revizijske sledi vpogleda v podatkovne baze. Tehnološki razvoj je povečal pojav široke uporabe interneta, uporabe družbenih omrežij, praktično na vseh področjih življenja širom

Evropske unije, zato je nova Splošna uredba EU o varstvu podatkov odziv na zagotavljanje zakonite uporabe osebnih podatkov posameznika. Podjetjem in državnim organom narekuje potrebo po sprejetju novih internih aktov in uvedbo postopkov zbiranja, uporabe in hrambe podatkov, da se na ta način prepreči zbiranje podatkov v nezakonite namene ter plačila sankcij za hujše kršitve, in posameznikom zagotovi boljše varstvo osebnih podatkov. Organizacije oziroma podjetja bodo morala imenovati pooblaščeno osebo za varstvo podatkov, ki bo pri upravljalcih in obdelovalcih zagotavljala skladnost z predpisi. Njegovo delovanje bo neodvisno in mu bo omogočeno neposredno poročanje vodstvu in bo poleg tega imel tudi komunikacijo z posamezniki katerih se njihovi osebni podatki v obdelavi v organizaciji. Pooblaščena oseba za varstvo podatkov ne bo smela prejemati nobenih navodil in ne bo mogla biti kaznovana ali razrešena zaradi opravljanja svojih nalog.

Za nas kot posameznike je z vidika preprečevanja zlorab osebnih podatkov zaradi krepitve digitalnega marketinga in pomanjkanja informacij na trgu, zelo pomembno, da smo dobro seznanjeni z uporabo naših osebnih podatkov in njihovo obdelavo, ter da se zavedamo da nas pri tem varuje zakonodaja in da imamo svoje pravice. Eden izmed ciljev Splošne uredbe o varstvu osebnih podatkov je bilo ravno poenotenje pravic posameznikov v zvezi z obdelavo njihovih osebnih podatkov, zato mora vsaka organizacija skladno z obveznostjo informirati in obveščati posameznike o njihovih pravicah.

LITERATURA IN VIRI

1. Brulc, U. (2016). Do kot seže pravica seznanitve z lastnimi osebnimi podatki? *Pravna praksa, 35*(47), 9.
2. Burnik, J. (2012). Prenovljen okvir za varstvo osebnih podatkov v EU. *Pravna praksa, 34*(19), 10–12.
3. Čebulj, J. & Žurej, J. (2005). *Varstvo osebnih podatkov in informacije javnega značaja* Ljubljana: Nebra, d. o. o.
4. Informacijski pooblaščenec. (2017). *Kaj prinaša nova Splošna uredba (EU)o varstvu podatkov?* Pridobljeno 16. julija 2019 iz https://www.ip-rs.si/fileadmin/user_ upload/Pdf/pripombe/Splosna_uredba_o_varstvu_podatkov-letak_maj_2017
5. Informacijski pooblaščenec. (2019). *Ocena učinka v zvezi z varstvom podatkov*. Pridobljeno 16. julija 2019 iz https://www.ip-rs.si
6. Jambrek, P., Perenič, A. & Uršič, M. (1988). *Varstvo človekovih pravic; razprave, eseji in dokumenti*. Ljubljana: Mladinska knjiga.
7. Jamšek, B. (2019). *Pregled posledic: kaj je prinesel GDPR?* Pridobljeno 16. julija 2019 iz https://mladipodjetnik.si/novice-in-dogodki/novice/pregled-posledic-kaj-je-prinesel-gdpr
8. Kovačič, M. (2006). *Nadzor in zasebnost v informacijski družbi*. Ljubljana: Fakulteta za družbene vede.
9. Pavčnik, M. (1999). *Teorija prava*. Ljubljana: Cankarjeva založba.

10. Pirc Musar, N. (2006). Dostop do informacij javnega značaja kot pravica in dolžnost. Tehnični in vsebinski problemi klasičnega in elektronskega arhiviranja. *5. zbornik referatov dopolnilnega izobraževanja s področij arhivistike, dokumentalistike in* informatike (str. 20–25). Maribor: Pokrajinski arhiv.
11. Pirc Musar, N., Bien, S., Bogataj, J., Prelesnik, M. & Žaucer, A. (2006). *Zakon o varstvu osebnih podatkov z komentarjem.* Ljubljana: GV Založba.
12. Prelesnik, M. (2008). Pojem osebnega podatka, kot ga razume delovna skupina 29, ali kaj vse je osebni podatek. *Pravna praksa, 27*(45), 6–8.
13. Prelesnik, M. (2015). Prvih deset let Zakona o varstvu osebnih podatkov. *Pravna praksa, 34*(6), 3.
14. Prelesnik, M. (2017). Varovanje osebnih podatkov in transparentnosti pred pomembnimi izzivi. *Pravna praksa, 36*(22), 3–7.
15. Rovšek, J. (2005). *Zasebno in javno v medijih*. Ljubljana: Mirovni inštitut.
16. Senčur Peček, D. (2017). Vpliv informacijske tehnologije na delovna razmerja. *Podjetje in delo, 43*(6–7), 1170.