UNIVERZA V LJUBLJANI

EKONOMSKA FAKULTETA

ZAKLJUČNA STROKOVNA NALOGA VISOKE POSLOVNE ŠOLE

PRAVICE POSAMEZNIKOV PRI VAROVANJU OSEBNIH PODATKOV V SPLOŠNI UREDBI O VARSTVU PODATKOV

Ljubljana, 2. julij 2018 URŠA JENKO

IZJAVA O AVTORSTVU

Podpisana Urša Jenko, študentka Ekonomske fakultete Univerze v Ljubljani, avtorica predloženega dela z naslovom Pravice posameznikov pri varovanju osebnih podatkov v Splošni uredbi o varstvu osebnih podatkov, pripravljenega v sodelovanju s svetovalcem doc. dr. Jakom Cepcem.

IZJAVLJAM

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

SEZNAM KRATIC

ang. - angleško

EU - (ang. European Commission) Evropska unija

ES - (ang. European Council) Evropski svet

GDPR - (ang. General Data Protection Regulation) Splošna uredba o varstvu podatkov

ZVOP-1 - Zakon o varstvu osebnih podatkov

IP - (ang. Internet Protocol) internetni protokol

RFID - (ang. Radio Frequency IDentification) Radiofrekvenčna identifikacija

ID - (ang. Identity Document) osebni dokument

IT - (ang. Information technology) informativna tehnologij

UVOD

Informacije in osebni podatki o ljudeh se zbirajo v vsakodnevnem življenju, kot so odpiranje bančnega računa, rezervacija letalske karte, vpis v fitnes, včlanitev v klube, obisk družbenih omrežij, uporaba telefona… Kamorkoli danes pogledamo, lahko vidimo ljudi, ki uporabljajo pametne telefone, na katerih imajo aplikacije, iščejo po internetu, so na družabnih omrežjih. S pomočjo digitalne informacijske tehnologije, ki se je v zadnjih petnajstih letih zelo hitro razvila, je mogoče na daljavo nadzirati že naše domove (pametna hiša). Zaradi digitalizacije pa se je povečalo tudi zbiranje in pospešil pretok informacij o posameznikih (Jamšek, 2018). Ljudem vse lažje sledimo, oblikujemo profile glede na njihove osebne podatke in nato vse te informacije uporabimo v različne namene, zakonite in nezakonite.

Naša zasebnost je postala vse bolj ogrožena, pa se morda tega sploh ne zavedamo. Varstvo osebnih podatkov je v Sloveniji podrobno urejeno z Zakonom o varstvu osebnih podatkov (ZVOP-1-UPB1), Ur. l. RS št. 86/04, 113/2005, 51/2007, 67/2007, 94/2007, ki je usklajen z Direktivo Evropskega parlamenta in Sveta ES/46/95 (v nadaljevanju Direktiva 95/46/ES)[1]. Evropski parlament in Svet Evropske unije sta leta 2016 sprejela Splošno uredbo o varstvu podatkov (v nadaljevanju GDPR)[2], ki je nadomestila Direktivo 95/46/ES in pomembno okrepila varstvo osebnih podatkov v Evropski uniji. GDPR je začel veljati konec aprila 2016, v uporabo pa je stopil 25. maja 2018. Z njim bomo imeli vsi posamezniki v Evropski uniji enotno, usklajeno varstvo osebnih podatkov.

V zaključni nalogi sem se osredotočila na pravno ureditev varstva pravic posameznikov v okviru varovanja njihovih osebnih podatkov, ki jih prinaša GDPR. V prvem delu naloge bom najprej predstavila temelje GDPR, njene glavne cilje in splošna načela. V drugem delu naloge pa bom podrobneje analizirala vsebino pravic posameznikov pri varovanju njihovih osebnih podatkov in analizirala, ali bodo te nove pravice prinesle posameznikom v Sloveniji več pravic, ki so jih imeli pri dosedanji zakonodaji, torej po ZVOP-1. Odgovoriti želim torej na vprašanje: Kakšne spremembe v pravicah posameznikov je prinesla Splošna uredba o varstvu podatkov.

1 SPLOŠNA UREDBA O VARSTVU OSEBNIH PODATKOV

Varstvo osebnih podatkov je ena temeljnih pravic v Evropski uniji in je zapisana v Listini o temeljnih pravicah Evropske unije (Ur. l. EU C 83/389). V prvem odstavku 8. člena Listina določa, da ima »vsakdo pravico do varstva osebnih podatkov, ki se nanašajo nanj«. Torej se mora ne glede na državljanstvo ali prebivališče posameznika spoštovati njegove temeljne pravice in svoboščine ter pravico do varstva osebnih podatkov.

[1] Direktiva 95/46/ES Evropskega parlamenta in Sveta z dne 24. oktobra 1995 o varstvu posameznikov pri obdelavi osebnih podatkov in prostem pretoku takih podatkov.
[2] 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.

Osebni podatek je »*katerakoli informacija v zvezi z določenim ali določljivim posameznikom, ki ga je mogoče določiti posredno ali neposredno, zlasti z navedbo identifikatorja (ime, identifikacijska številka, podatki o lokaciji, spletni identifikator) ali z navedbo enega ali več dejavnikov, ki so značilni za fiziološko, genetsko, duševno, gospodarsko, kulturno ali družbeno identiteto posameznika*« (1. odstavek 4. člena GDPR). Trobentar (2017, str. 21) pojasnjuje, da so v posodobljeno opredelitev izraza osebni podatek sedaj uvrščeni tudi spletni identifikatorji (identifikatorji naprav, IP naslovi, RFID oznake, ID piškotkov). S pomočjo spletnih identifikatorjev tržniki lahko analizirajo aktivnosti posameznikov na spletu, jih profilirajo, bolj prilagojeno oglašujejo, izboljšajo svoje iskalne storitve …

Splošna uredba o varstvu podatkov še vedno zasleduje cilje in načela Direktive ES/46/95. Direktiva (GDPR, uvodna izjava 9) v vseh teh letih ni preprečila tveganj za varstvo posameznikov glede spletne dejavnosti, pravne negotovosti, različnega izvajanja in uporabe v državah članicah, kar pa lahko prepreči prosti pretok osebnih podatkov v Evropski Uniji.

Zato Informacijski pooblaščenec (brez datuma) pravi: »*Cilj Splošne uredbe o varstvu osebnih podatkov je omogočiti prebivalcem nadzor nad njihovimi osebnimi podatki in poenotiti ter dvigniti raven varstva osebnih podatkov v Evropski uniji*.«

Kot je zapisano v uvodni izjavi 11 GDPR je po vsej Evropski uniji za učinkovito varstvo osebnih podatkov potrebno »*okrepiti in podrobneje opredeliti pravice posameznikov, na katere se nanašajo osebni podatki, ter obveznosti tistih, ki obdelujejo osebne podatke in določajo obdelavo osebnih podatkov, pa tudi enakovredna pooblastila za spremljanje in zagotavljanje skladnosti s pravili varstva osebnih podatkov ter enakovredne sankcije za kršitve v državah članicah*«. Podjetja se morajo uskladiti z GDPR, da bodo preprečila pridobitev glob in kazenskih postopkov (IT Governance Privacy team, 2017, str.24).

Čeprav je že dosedanja ureditev varovala temeljne pravice in svoboščine posameznikov pri varovanju njihovih osebnih podatkov, evropski zakonodajalec pričakuje, da bo to varstvo z GDPR še bolj zaostreno in poglobljeno.

Za razliko od direktive, ki je sredstvo za harmonizacijo pravnega reda in nacionalnemu zakonodajalcu služi kot podlaga za ureditev pravnega področja, ki je zajeto z direktivo (Cepec & Kovač, 2012, str. 75), je GDPR sredstvo za unifikacijo pravnih pravil. Uredbe se v skladu s PDEU[3] neposredno uporabljajo v vseh državah članicah, kar pomeni, da pravila iz uredb veljajo tako za države članice kot za njene pravne in fizične osebe od trenutka veljavnosti uredbe dalje. Državam članicam besedila uredbe ni treba prenašati v nacionalni pravni red, v skladu z interpretacijo Sodišča Evropske Unije je implementiranje besedila uredbe v nacionalno zakonodajo celo prepovedano, saj bi prenašanje besedila uredbe v nacionalno zakonodajo lahko povzročilo neenakosti med uredbo in kasnejšo ureditvijo v

[3] Pogodba o Evropski uniji in pogodba o delovanju Evropske unije

nacionalni pravni zakonodaji, kar pa bi onemogočilo poenotenje prava med državami članicami (Cepec & Kovač, 2012, str. 74).

Uvodna izjava 5 GDPR opisuje, da se je čezmejni prenos osebnih podatkov občutno povečal zaradi gospodarskega in socialnega povezovanja, zato pravo Evropske unije izraža željo, da države članice sodelujejo med seboj in si izmenjujejo osebne podatke. Izmenjava osebnih podatkov se je znatno povečala zaradi hitrega tehnološkega razvoja in globalizacije. Posameznikovi osebni podatki so tako rekoč na voljo že na globalnem nivoju, zato se mora omogočiti lažji pretok in visoka raven varstva osebnih podatkov v Evropski uniji, v tretje države in mednarodne organizacije (GDPR, uvodna izjava 6).

GDPR v 2. členu določa, da se uredba uporablja za obdelavo osebnih podatkov v celoti ali delno z avtomatiziranimi sredstvi. Podatki, ki so del zbirke ali namenjeni oblikovanju le te, so namenjeni za drugačno obdelavo, kakor z avtomatiziranimi sredstvi. Osebni podatki pravnih oseb in družb, ki so ustanovljene kot pravne osebe, se ne obdelujejo, ampak se obdelujejo le osebni podatki posameznikov.

Osebne podatke s strani institucij, organov, uradov in agencij Evropske unije obdelujejo v skladu z Uredbo (ES) št. 45/2001[4], ki je prilagojena pravilom in načelom GDPR (3. odstavek 2. člena GDPR).

GDPR (2. odstavek 2. člena) se za obdelavo osebnih podatkov ne uporablja, kadar:

- imamo delovanje zunaj področja uporabe prava Evropske unije (nacionalna varnost),
- države članice izvajajo aktivnosti v zvezi s skupno zunanjo in varnostno politiko Evropske unije,
- fizične osebe izvajajo osebne, domače dejavnosti, ki nimajo povezave s poklicno dejavnostjo,
- pristojni organi obdelujejo osebne podatke za odkrivanje, preiskovanje, preprečevanje, pregon kaznivih dejanj in izvrševanje kazenskih sankcij, vključno z varovanjem pred grožnjami javni varnosti in njihovem preprečevanjem. Vse to je že urejeno v posebnem aktu Evropske unije (Direktiva EU 2016/680[5]).

Glede na 4. odstavek 2. člena GDPR ne posega v uporabo Direktive o elektronskem poslovanju[6] in njenih pravil o odgovornosti posrednih ponudnikov, katere cilj (uvodna izjava 8) je zagotoviti prosti tok storitev informacijske družbe (prodaja blaga, prenos podatkov,

[4] Uredba (ES) št. 45/Evropskega parlamenta in Sveta z dne 18. decembra 2000 o varstvu posameznikov pri obdelavi osebnih podatkov v institucijah in organih Skupnosti in o prostem pretoku takih podatkov.
[5] 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.
[6] Direktiva 2000/31/ES Evropskega parlamenta in Sveta z dne 8. junija 2000 o nekaterih pravnih vidikih storitev informacijske družbe, zlasti elektronskega poslovanja na notranjem trgu.

dostop do podatkov, oglaševanje na spletu) med državami članicami Evropske unije in prispevati k pravilnem delovanju notranjega trga.

Glede na 3. člen GDPR se le ta uporablja, če imata upravljavec in obdelovalec v okviru svojih dejavnosti sedež v Evropski uniji, četudi sama obdelava osebnih podatkov v Evropski uniji poteka ali ne.

Kadar upravljavci, ki nimajo svojega sedeža v Evropski uniji, posameznikom znotraj Evropske unije nudijo blago, storitve ali spremljajo njihovo vedenje (oblikovanje profila posameznika), torej obdelujejo njihove osebne podatke, morajo upoštevati GDPR. Uredbo prav tako uporabljajo upravljavci, ki nimajo svojega sedeža v Evropski uniji, vendar se pravo države članice uporablja na podlagi mednarodnega javnega prava (3. odstavek 3. člena GDPR).

2 NAČELA OBDELAVE PODATKOV

Temeljna načela pri obdelavi osebnih podatkov so urejena v 5. členu GDPR. V skladu z 2. odstavkom 4. člena GDPR je obdelava podatkov »*vsako dejanje ali niz dejanj, ki se izvaja v zvezi z osebnimi podatki ali nizi osebnih podatkov z avtomatiziranimi sredstvi ali brez njih*«, na primer zbiranje, urejanje, beleženje, strukturiranje, shranjevanje, spreminjanje, priklic, vpogled, uporaba, razkritje s posredovanjem, razširjanje ali drugačno omogočanje dostopa, prilagajanje, kombiniranje, omejevanje, izbris ali uničenje …

Temeljna načela predstavljajo osnovo celotne ureditve varstva osebnih podatkov v GDPR in predstavljajo vodilna oziroma nosilna sporočila varstva.

Temeljna načela GDPR so (točke a do f 1. Odstavka 5. člena GDPR): (a) zakonitost, pravičnost in transparentnost, (b) zbiranje osebnih podatkov zgolj za določene, izrecne in zakonite namene, (c) podatki se lahko zbirajo zgolj v obsegu, potrebnem za dosego namena, (d) osebni podatki so točni in posodobljeni, (e) hranjenje osebnih podatkov toliko časa, kot se obdelujejo, (f) obdelava podatkov je varna.

V nadaljevanju podrobneje predstavljam posamezna temeljna načela.

2.1 Zakonitost, poštenost, transparentnost

– **Zakonitost**

GDPR v 6. členu definira, da je obdelava podatkov zakonita, ko je vsaj eden od naslednjih pogojev izpolnjen:

a) **Soglasje:** posameznik privoli v obdelavo njegovih osebnih podatkov za določen namen ali namene.

b) **Pogodba:** obdelava je potrebna za izvajanje ali sklenitev pogodb.
c) **Pravna obveznost:** obdelava je potrebna, da se izpolni zakonska obveznost upravljavca, brez pogodbenih obveznosti.
d) **Življenjski interesi:** obdelava je potrebna, da se zaščitijo življenjski interesi posameznika.
e) **Javni interes:** obdelava je potrebna, da upravljavec v skladu s pravno obveznostjo opravlja naloge v javnem interesu ali izvaja javno oblast (na podlagi prava Evropske unije ali države članice), na primer za humanitarne namene, spremljanje epidemij, naravnih nesreč ali nesreč povzročenih zaradi človeka.
f) **Zakoniti interesi:** obdelava je potrebna zaradi zakonitih interesov upravljavca ali tretje osebe (če ne prevladajo temeljne pravice in svoboščine posameznika). Sem štejemo obdelovanje osebnih podatkov za direktno trženje, preprečevanje zlorab…

Ko naj bi upravljavec obdeloval osebne podatke posameznika za nek drug namen, kot za tistega, za katerega so bili podatki zbrani, mora najprej oceniti, ali lahko sploh obdeluje te podatke. Ali je drug namen združljiv s prvotnim namenom. Upoštevati mora možno povezavo med enim in drugim namenom obdelave osebnih podatkov; v kakšnih okoliščinah so bili osebni podatki zbrani (še posebej, kar se tiče razmerja med posameznikom teh osebnih podatkov in upravljavcem); naravo osebnih podatkov (posebne vrste podatkov); katere so možne posledice nadaljnje obdelave osebnih podatkov; obstoj zaščitnih ukrepov (šifriranje, psevdonimizacija[7]) pri prvotnih in nadaljnjih obdelavah podatkov (4. odstavek 6. člena GDPR).

– **Poštenost**

Upravljavec pridobi osebne podatke od posameznika in jih obdeluje »*pošteno*« (točka a prvega odstavka 5. člena GDPR) na način, ki ga želi posameznik. Osebni podatki ne smejo biti nikoli obdelovani na način, ki škodi posamezniku. Glede svoje identitete mora biti upravljavec vedno odprt in pošten (IT Governance Privacy team, 2017, str. 93).

– **Transparentnost**

Upravljavec mora glede na točko a prvega odstavka 5. člena GDPR obdelati podatke na »*pregleden način*«, torej jasno in odkrito obrazložiti posamezniku kako bo obdeloval njegove osebne podatke. Na primer, da želi podjetje uporabiti posameznikove osebne podatke za nek drug namen, mora upravljavec o tem obvestiti posameznika in mu namen razložiti (IT Governance Privacy team, 2017, str. 94).

[7] »*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 te zanje veljajo tehnični in organizacijski ukrepi za zagotavljanje, da se osebni podatki ne pripišejo določenemu ali določljivemu posamezniku.*« (5. točka 4. člena GDPR).

2.2 Omejitev namena zbiranja podatkov

V skladu s točko b prvega odstavka 5. člena se osebni podatki posameznika vedno zbirajo za določene, izrecne in zakonite namene. Pri tem mora posameznik pridobiti nedvoumne informacije o obdelavi njegovih osebnih podatkov (pogoji, obvestila o zasebnosti, obrazci za privolitev).

Načelo določenega zbiranja podatkov je prekršeno v trenutku, ko so osebni podatki uporabljeni za namen, za katerega niso bili zbrani. Na primer podjetje, ki je zbralo določene informacije o posameznikih in le te posreduje drugemu podjetju, da jih bodo uporabili za nek drug namen, je prekršilo to načelo (IT Governance Privacy team, 2017, str. 101).

»*Nadaljnja obdelava v namene arhiviranja v javnem interesu, v znanstveno ali zgodovinsko raziskovalne namene ali statistične namene v skladu s prvim odstavkom 89. člena GDPR ne velja za nezdružljivo s prvotnimi nameni*« (točka b prvega odstavka 5. člena GDPR). Torej upravljalec pri obdelavi osebnih podatkov posameznika za zgoraj naštete namene ne potrebuje njegove dodatne privolitve. Posameznik ne more nasprotovati obdelavi njegovih podatkov in ga tudi ni potrebno obvestiti o postopkih obdelave.

2.3 Minimizacija podatkov

Pri obdelovanju osebnih podatkov za nek namen moramo imeti čim bolj bistvene in ustrezne podatke. Torej le tiste podatke, ki so nujno potrebni za obdelavo (točka c prvega odstavka 5. člena GDPR). Čeprav so podjetja v sektorju finančnih storitev in v zdravstveni industriji nagnjena k posredovanju več informacij kot druga podjetja (IT Governance Privacy team, 2017, str. 102).

2.4 Točnost podatkov

Vsi osebni podatki morajo biti točni in posodobljeni. Podatki posameznika, ki se obdelujejo in niso točni, se morajo brez odlašanja popraviti ali zbrisati (točka d prvega odstavka 5. člena GDPR).

Po navadi podjetja stremijo k tem, da imajo točne in ažurne podatke posameznikov, saj lahko tako posameznike ščitijo pred različnimi grožnjami, npr. kraja identitete (IT Governance Privacy team, 2017, str. 104).

2.5 Hranjenje podatkov

Osebni podatki se hranijo le toliko časa, kolikor se osebni podatki obdelujejo za nek namen. Točka e prvega odstavka 5. člena GDPR navaja, da so osebni podatki »*hranjeni v obliki, ki dopušča identifikacijo posameznikov, na katere se nanašajo osebni podatki*«.

Za znanstveni, statistični, znanstveno raziskovalni namen ali namen arhiviranja v javnem interesu se lahko osebnih podatki shranjujejo dlje časa. V tem primeru moramo izvajati organizacijske in tehnične ukrepe, da zaščitimo pravice in svoboščine posameznika teh osebnih podatkov (točka e prvega odstavka 5. člena GDPR).

2.6 Celovitost in zaupnost

Varnost je zagotovljena pri obdelovanju osebnih podatkov posameznika. S tehničnimi ali organizacijskimi ukrepi so osebni podatki zaščiteni pred »*nezakonito in nedovoljeno obdelavo, nenamerno izgubo, uničenjem ali poškodbo*« (točka f prvega odstavka 5. člena GDPR).

2.7 Odgovornost

Odgovornost nosi upravljavec posameznikovih osebnih podatkov, saj je odgovoren za ujemanje zgoraj naštetih načel v zvezi z obdelavo osebnih podatkov. Skladnost načel mora biti zmožen tudi dokazati (2. odstavek 5. člena GDPR).

Upravljavec mora zagotoviti, da so vsi zunanji partnerji in ljudje znotraj podjetja s pogodbenimi in zavezujočimi poslovnimi pravili zavezani k spoštovanju načel GDPR. Kulturo odgovornosti se hrani od zgoraj navzdol – ozaveščanje vseh zaposlenih o dolžnostih in odgovornostih v zvezi z zasebnostjo in varstvom podatkov (IT Governance Privacy team, 2017, str. 110).

3 SPREMEMBE PRAVIC POSAMEZNIKOV

GDPR priznava posamezniku določene pravice. Te mu omogočajo seznanjenje v najlažje dostopni obliki, preprostem in jasnem jeziku ter ažurnost in točnost njegovih osebnih podatkov. Glavne pravice omogočajo posamezniku tudi poseganje v vsebino, obdelavo, obstoj osebnih podatkov in pravico do obveščenosti. Te pravice pozna že Zakon o varstvu osebnih podatkov, a jih GDPR še bolj poudarja in razširja (Trobentar, 2017, str.27).

Za posameznikove osebne podatke skrbi upravljavec, ki jih pridobi od posameznika z jasno privolitvijo oz. soglasjem. Upravljavec mora obveščati posameznika o zaznavnih kršitvah varstva osebnih podatkov (34. člen GDPR). V primeru kršenja posameznikovih osebnih podatkov ima posameznik pravico vložiti pritožbo pri nadzornem organu. »*Nadzorni organ zaščiti temeljne pravice in svoboščine posameznikov v zvezi z obdelavo in olajša prost pretok osebnih podatkov v Evropski uniji*« (51. člen GDPR).

Pravice posameznikov opisane v ZVOP-1 so pravica do seznanitve, pravica do dopolnitve, popravka, blokiranja, izbrisa in ugovora. Z GDPR posameznik pridobi tri nove pravice, in

sicer pravico do pozabe, prenosljivosti in omejitve podatkov. Ključni novi pravici za posameznika sta pravica do prenosljivosti podatkov in pravica do pozabe.

3.1 Soglasje kot temeljna podlaga za zbiranje osebnih podatkov

GDPR je določil zelo visok standard za pridobitev soglasja, saj je eno od zakonitih podlag za obdelovanje podatkov, izrecno soglasje pa dokazuje istovetnost uporabe posebnih podatkov (INFO HIŠA, svetovanje in izobraževanje, d.o.o., brez datuma b, str. 3).

Soglasje oziroma privolitev je po 11. točki 4. člena GDPR »*vsaka prostovoljna, izrecna, informirana in nedvoumna izjava volje posameznika, na katerega se nanašajo osebni podatki, s katero z izjavo ali jasnim pritrdilnim dejanjem izrazi soglasje*«. Posamezniki s privolitvijo pridobijo resnično izbiro in nadzor nad svojimi osebnimi podatki.

Jasno je, da mora biti navedba soglasja nedvoumna in vključevati jasno potrditveno dejanje (opt-in[8]), vendar pa prav tako zahteva ločene oz. granularne možnosti soglasja za različne postopke obdelave. To pomeni, da ima posameznik pravico, da privoli v vsak namen obdelave posebej. Dolžnost upravljavca je, da zaprosi za soglasje posameznika, ko za obdelovanje njegovih osebnih podatkov nima nobenega drugega temelja (na primer pogodba, zakon, zakoniti interes…). Če upravljavec združi več namenov obdelave podatkov v eno samo možnost, privolitev posameznika ne velja, ker ni svobodna (INFO HIŠA, svetovanje in izobraževanje, d.o.o., brez datuma a, str.2).

V uvodni izjavi 32 je zapisano, da je soglasje lahko dano pisno, ustno ali s pomočjo elektronskih sredstev. »*Molk, vnaprej označena okenca ali nedejavnost zato ne pomenijo privolitve*«. Na primer: posameznik označi okence, ko obišče spletno stran, izbere tehnične nastavitve ali izjavo, s katero sprejema obdelavo svojih osebnih podatkov.

Tržniki se velikokrat poslužujejo e-poštnega trženja, kar pomeni, da ljudje prejemajo promocijski material nekega podjetja. Zaradi GDPR morajo posamezniki fizično potrditi, da želijo biti kontaktirani, kot je na primer prostovoljna označitev okenca, ki pomeni, da želijo prejemati e-poštne novice. Okence ne sme biti označeno že vnaprej. Posamezniki lahko tudi kadarkoli upravljajo svoje e-poštne nastavitve, na primer možnost odjave določene elektronske pošte v skladu s pravico do pozabe osebnih podatkov (MacDonald, 2018). Veliko podjetij bo moralo ravno zaradi poostrenih ukrepov preveriti soglasja, ki so jih že dobili in preveriti, ali izpolnjujejo standard GDPR. V kolikor je standard GDPR izpolnjen, podjetja ne potrebujejo novega soglasja posameznika (Information Commissioner's Office, brez datuma).

[8] »*Opt-in je izrecno dovoljenje stranke ali prejemnika pošte, elektronske pošte ali drugega neposrednega sporočila, ki trgovcu omogoča pošiljanje blaga, informacij ali sporočil. Ta metoda je uporabljena v večini marketinških podjetij, ponudnikov informacij, naročniških publikacij*« Opt-in (brez datuma).

V skladu s 7. členom GDPR ima posameznik pravico privolitve enako enostavno dati kot tudi preklicati. Upravljavec mora obvestiti posameznika o tej pravici in mu ponuditi enostaven način preklica soglasja.

7. točka 4. člena GDPR pravi, da je upravljavec fizična ali pravna oseba (podjetje, družba), ki določi za kaj se bodo osebni podatki posameznika obdelovali (namen) in katera sredstva se bodo uporabila pri obdelovanju. Osebne podatke lahko zbira neposredno od posameznika. Osebo, prav tako fizična ali pravna, ki obdeluje osebne podatke v imenu upravljavca, imenujemo obdelovalec (8. točka 4. člena GDPR). Torej je zbiranje osebnih podatkov upravljavčevo delo, obdelovalec pa podatke beleži, spreminja, shrani (Bouca, brez datuma).

3.1.1 Privolitev otrok

Otroci se ne zavedajo ravno vseh tveganj, zaščitnih ukrepov, posledic in pravic obdelave njihovih osebnih podatkov. Potrebujejo posebno varstvo osebnih podatkov, še posebej, ko se osebni podatki obdelujejo v trženjske namene, v namen ustvarjanja profilov in storitev, ki so otroku ponujene (8. člen GDPR).

8. člen GDPR omejuje sposobnost otroka, da privoli v obdelavo svojih osebnih podatkov brez soglasja, vednosti staršev oz. nosilca starševske odgovornosti. Otroci lahko samostojno privolijo v obdelovanje njihovih osebnih podatkov, ko dopolnijo starost 16 let.

Prvi osnutki GDPR so določevali zakonitost privolitve otroka, ko dopolni 13 let, da bi bili v skladu s starostjo privolitve v Združenih državah Amerike. (Article 29 Data Protection Working Party, 2016, str. 25)V končnem osnutku so nato določili starost 16 let z možnostjo, da lahko države članice uvedejo nižjo starost, vendar ne nižje od 13 let. (Informacijski pooblaščenec, 2017) Torej, če države članice starosti ne določijo v svojem zakonu drugače, mora upravljavec dobiti soglasje staršev ali zakonitih skrbnikov, da lahko obdeluje osebne podatke otroka, mlajšega od 16 let (INFO HIŠA, svetovanje in izobraževanje, d.o.o., brez datuma b, str. 4).

Upravljavec mora glede na razpoložljivo tehnologijo tudi preverjati (s kontaktiranjem), ali je zakoniti skrbnik otroka dal in odobril ustrezno privolitev, saj na ta način lahko prepreči privolitev osebe, mlajše od 16 let (2. odstavek 8. člena GDPR). Tretji odstavek 11. člena osnutka ZVOP-2 določa, da »*soglasje mladoletne osebe ne sme biti pogojevana s pretiranimi pogoji s strani upravljavca*«. To pomeni, da upravljavec ne sme dovoliti, da mladoletna oseba da več podatkov, kot je potrebno za sodelovanje v nagradnih igrah, vključitvi v družbeno omrežje…

Po mnenju DPO novice je starostna omejitev v Sloveniji 15 let, saj takrat glede na Družinski in Obligacijski zakonik otrok pridobi delno opravilno sposobnost. Družinski zakonik (Uradni list RS, št. 15/17.) v 146. členu namreč določa, da »*otrok, ki dopolni 15 let, lahko*

sam sklepa pravne posle, če zakon ne določa drugače« (INFO HIŠA, svetovanje in izobraževanje, d.o.o., brez datuma b, str. 4).

3.1.2 Posebne vrste podatkov

V GDPR 9. člen določa posebne vrste podatkov (občutljivi osebni podatki). To so osebni podatki, ki si zaslužijo posebno varstvo, saj so po svoji naravi občutljivi z vidika temeljnih pravic in svoboščin, kar lahko ogrozi njihovo obdelovanje. Posebne vrste podatkov so podatki o posamezniku, ki »*razkrivajo rasno ali etično poreklo, politično mnenje, versko ali filozofko prepričanje, članstvo v sindikatu, obdelava genetskih podatkov, biometričnih podatkov za namene edinstvene identifikacije posameznika (ID), podatkov v zvezi z zdravjem, posameznikovim spolnim življenjem, spolno usmerjenostjo*«.

Za obdelavo posebnih vrst podatkov GDPR (točka a drugega odstavka 9. člena) zahteva, da upravljavci pridobijo izrecno privolitev posameznikov. Standard za izrecno privolitev ostaja enak kot v ZVOP-1. Izrecno privolitev je Delovna skupina 29 (v skladu z Direktivo 95/46/ES) opredelila kot primer, ko je posamezniku predstavljena zahteva za njegovo strinjanje ali nestrinjanje z uporabo ali razkritjem njihovih osebnih podatkov, ter na to njihov pisni ali ustni odziv. Posameznikova izbira nastavitev v spletnem brskalniku ne bo dovolj za upravljavčevo obdelavo posebnih vrst osebnih podatkov (INFO HIŠA, svetovanje in izobraževanje, d.o.o., brez datuma b, str. 3).

Razlika med Zakonom o varstvu osebnih podatkov in GDPR je ta, da slednji razširja zbirko posebnih podatkov na biometrične podatke, genetske podatke in podatke o spolni usmerjenosti. Biometrični podatki so glede na GDPR 14. točko 4. člena »*rezultat posebne tehnične obdelave v zvezi z fizičnimi, fiziološkimi ali vedenjskimi značilnostmi posameznika, ki omogočajo ali potrjujejo edinstveno identifikacijo tega posameznika, kot so podobe obraza ali daktiloskopski podatki*«. V uvodni izjavi 51 je zapisano, da obdelane fotografije spadajo pod biometrične podatke v primeru, ko so obdelane s tehničnimi sredstvi, ki omogočajo edinstveno identifikacijo ali avtentikacijo posameznika. V 13. točki 4. člena GDPR so genetski podatki opisani kot »*osebni podatki v zvezi s podedovanimi ali pridobljenimi značilnostmi posameznika, ki dajejo edinstvene informacije o fiziologiji ali zdravju posameznika in rezultat analize biološkega vzorca zadevnega posameznika*.«.

3.2 Preglednost podatkov

3.2.1 Načelo preglednosti

Načelo preglednosti, opisano v 12. členu GDPR, določa, da mora upravljavec vse informacije, ki se obdelujejo v zvezi s posameznikom, posamezniku zagotoviti v jedrnati, pregledni, razumljivi in lahko dostopni obliki. Jezik mora biti jasen in preprost, še posebej v primeru, če so informacije in komunikacija namenjene otroku.

Posredovane informacije so lahko v pisni obliki ali elektronski obliki, kjer je to mogoče, na primer informacije na spletni strani, ki so namenjene javnosti. V uvodni izjavi 58 je zapisano, da zaradi tehnološke kompleksnosti posameznik »*težko ve in razume, ali se zbirajo njegovi osebni podatki, kdo jih zbira in v kakšen namen, kot je to v primeru spletnega oglaševanja*«.

Upravljavec olajša posamezniku, da uresniči svoje pravice do dostopa, ugovora, popravka in izbrisa (2. odstavek 12. člena GDPR). Posamezniku mora dati vse informacije o ukrepih v enem mesecu od prejema zahteve, brez odlašanja in brezplačno. Ob upoštevanju kompleksnosti in številu zahtev, se lahko rok ukrepanja upravljavca podaljša za dva meseca, vendar mora upravljavec o podaljševanju in razlogih zanj obvestiti posameznika (3. odstavek 12. člena GDPR). Če se osebni podatki obdelujejo z elektronskimi sredstvi, je po uvodni izjavi 59. upravljavec dolžan omogočiti posamezniku elektronsko vlaganje zahtev.

Če upravljavec na zahtevo posameznika ne ukrepa, mora po 4. odstavku 12. člena GDPR v enem mesecu od prejema zahteve obvestiti posameznika o razlogih, zakaj ni ukrepal, ter o možnosti vložitve pritožbe pri nadzornem organu in uveljavljanja pravnih sredstev. Upravljavec zahtevo posameznika lahko zavrne v primeru, da je neutemeljena, pretirana, ali ko ne more identificirati posameznika. Posameznik lahko zaradi tega tudi plača pristojbino, npr. upravni stroški posredovanja informacij in izvajanja ukrepa (5. odstavek 12. člena GDPR).

V Zakonu o varstvu osebnih podatkov je v 31. členu zapisano, da mora upravljavec istega dne ali najkasneje v 15 dneh od prejema zahteve omogočiti posamezniku vpogled v osebne podatke, prepis, kopiranje in potrdilo. Izpis, seznam, informacije ali pojasnila pa mora posamezniku posredovati v 30 dneh od dneva prejema zahteve.

Posameznik svojo zahtevo iz 30. člena ZVOP-1 predloži upravljavcu pisno ali ustno na zapisnik in sicer lahko le enkrat na tri mesece. Kar se tiče občutljivih podatkov in osebnih podatkov v zvezi z videonadzorom lahko posameznik vloži zahtevo enkrat na mesec. V skladu z 31. členom ZVOP-1 mora »*posameznik upravljavcu povrniti materialne stroške posredovanja zahtevanih informacij*«. Upravljavec se lahko tudi odloči ali bo zaračunal posamezniku ali pa mu bo podatke posredoval brezplačno (ustne informacije in potrdila so brezplačna).

Glede na ZVOP-1 ima GDPR prednost v tem, da je enomesečni rok enoten pri vseh državah članicah. Rok se lahko podaljša na dva meseca glede na kompleksnost in število zahtev. GDPR nikjer nima zapisano, kolikokrat lahko posameznik odda zahtevo in tudi vse informacije se mu zagotovijo brezplačno.

3.3 Informacije in dostop do osebnih podatkov

3.3.1 Zagotavljanje informacij

Kadar upravljavec pridobi osebne podatke od posameznika, na katerega se ti podatki tudi nanašajo, mu upravljavec po 13. členu GDPR zagotovi določene informacije:

- obvesti ga o obdelavi njegovih osebnih podatkov in za kašen namen/-e se bodo obdelovali (skupaj z njihovo pravno podlago za obdelovanje),
- preda kontaktne podatke upravljavca in njegovega predstavnika,
- kontaktne podatke pooblaščene osebe za varstvo podatkov (če ta obstaja),
- pravico do vložitve pritožbe pri nadzornem organu, Informacijskem pooblaščencu,
- pravico do dostopa, popravka, izbrisa, omejitve obdelave posameznika,
- rok hrambe osebnih podatkov, ki je zakonsko določen,
- o uporabnikih posameznikovih osebnih podatkov, tudi iz tretjih držav in pojasnila za njihovo uporabo,
- ali je zagotovitev osebnih podatkov zakonska, pogodbena obveznost ali obveznost za sklenitev pogodbe, ter kakšne posledice ima posameznik, če zagotovi informacije,
- o možnosti avtomatiziranega sprejemanja odločitev, oblikovanja profilov in njihovih razlogih, pomenu in predvidenih posledicah obdelave posameznikovih osebnih podatkov na tak način.

Upravljavec lahko osebne podatke posameznika pridobi tudi od tretje osebe. Takrat mora posameznika čim prej obvestiti o prejemu in obdelovanju njegovih osebnih podatkov. V uvodni izjavi 62 je zapisano, da obveznost zagotavljanja informacij ni nujna, ko ima posameznik že informacije, ko je razkritje in shranjevanje informacij v skladu z zakonom ali v primeru, da je zagotavljanje informacij nemogoče, saj vključuje nesorazmeren napor (4. odstavek 13. člena GDPR).

3.3.2 Pravica dostopa posameznika

Ustava Republike Slovenije (Uradni list RS, št. 33/91-I z dne 28. 12. 1991) v 38. členu določa, da ima *»vsakdo pravico seznaniti se z zbranimi osebnimi podatki, ki se nanašajo nanj in pravico do sodnega varstva ob njihovi zlorabi.«* Vsak posameznik se lahko seznani z obdelavo njegovih osebnih podatkov in preverja zakonitost obdelave. (Informacijski pooblaščenec, brez datuma)

Pravica do seznanitve je v 15. členu GDPR opisana kot pravica do dostopa in omogoča posamezniku, da ga upravljavec seznani z obdelavo njegovih osebnih podatkov. Upravljavec mora posamezniku zagotoviti tudi kopijo o obdelavi osebnih podatkov. Posameznik lahko (z zahtevo) dostopa do svojih osebnih podatkov in pridobi naslednje informacij o njih:

- namen obdelave,
- vrsta osebnih podatkov (ime, spletno brskanje, naslov …),
- tretji uporabniki, ki so ali jim bodo razkriti njegovi osebni podatki (posebno o uporabnikih v tretjih državah, saj mora biti posameznik tudi po 3. odstavku 15. člena GDPR obveščen o zaščitnih ukrepih v zvezi s prenosom podatkov),
- predvidena hramba osebnih podatkov, ali če to ni določeno, kako se bo določilo obdobje hrambe,
- pravice do popravka, izbrisa ali ugovora obdelave osebnih podatkov,
- vložitev pritožbe pri Informacijskem pooblaščencu oz. nadzornem organu,
- če so osebni podatki posameznika zbrani pri tretji osebi in ne pri posamezniku, mora posameznik pridobiti informacije o tretjem viru,
- obstoj avtomatiziranega odločanja in oblikovanja profilov, ter informacije o pomenu, razlogih in posledicah take obdelave podatkov.

V četrti točki 30. člena ZVOP-1 se pravica seznanitve nekoliko razlikuje od GDPR. Upravljavec mora posamezniku ne le posredovati seznam uporabnikov, ki jim bodo njegovi osebni podatki razkriti, kot navaja GDPR, ampak po ZVOP-1 tudi kdaj jim bodo razkriti, na kakšni podlagi in za kakšen namen. GDPR je v tem primeru znižal dosežen standard v naši državi glede posameznikovega dostopa do informacij o uporabnikih njegovih osebnih podatkov. Seveda pa imajo države članice možnost spreminjanja določenih podrobnosti.

Uvodna izjava 63 pravi, da mora upravljavec zagotoviti dostop na daljavo do varnostnega sistema, kjer je posamezniku omogočen direkten dostop do njegovih osebnih podatkov, ko je to le mogoče. Pravica do dostopa ne sme negativno vplivati na svoboščine ali pravice drugih (avtorske pravice, poslovne skrivnosti, intelektualna lastnina). Če upravljavec obdeluje veliko količino osebnih podatkov posameznika, ima možnost zahtevati od posameznika, da mu podrobno pove, do katerih informacij in dejavnosti želi dostopati.

3.4 Popravek in izbris podatkov

3.4.1 Pravica do popravka

Vsak posameznik ima po 16. členu Splošne uredbe pravico izboljšati in popraviti vse netočnosti v zvezi s svojimi osebnimi podatki. Pravica do popravka govori o tem, da upravljavec na zahtevo posameznika (brez odlašanja) popravi osebne podatke posameznika, ki niso točni. Posameznik lahko tudi dopolni svoje nepopolne osebne podatke.

3.4.2 Pravica do pozabe (izbrisa)

Vsak posameznik ima s prvim odstavkom 17. člena GDPR pravico do pozabe oz. izbrisa njegovih osebnih podatkov. Vendar pa pravica do pozabe velja le v določenih okoliščinah.

Razlogi posameznika za izbris podatkov so lahko različni. Na primer, kadar podatki niso več potrebni za namen, za katerega so bili zbrani, ko posameznik ugovarja obdelavi podatkov ali jo prekliče, ali če obdelava osebnih podatkov posameznika ni v skladu s GDPR. V uvodni izjavi 65 je zapisano, da je pravica do pozabe pomembna v primeru, ko posameznik želi izbrisati svoje osebne podatke, za katere je dal privolitev kot otrok (nespametne objave podatkov na družbenih omrežjih), saj se takrat ni popolnoma zavedal tveganj obdelave osebnih podatkov.

Obdelovalec, ki je objavil osebne podatke posameznika, je dolžen zaradi pravice do pozabe obvestiti druge upravljavce, ki obdelujejo osebne podatke tega posameznika, da izbrišejo vse povezave do podatkov ali njihovih kopij (2. odstavek 17. člena GDPR).

3. odstavek 17. člena GDPR pravi, da je »*hranjenje osebnih podatkov zakonito v primeru:*

- *udejanjenja pravice do svobode izražanja in obveščanja,*
- *izpolnjevanja pravne obveznosti obdelave v javnem interesu ali izvajanju javne oblasti (dodeljeno upravljavcu),*
- *znanstvene, zgodovinsko raziskovalne, statistične namene, namen arhiviranja v javnem interesu,*
- *uveljavljanje, izvajanje ali obrambo pravnih zahtevkov,*
- *obdelava podatkov je potrebna zaradi javnega interesa in na področju javnega zdravja (npr. zagotavljanje visokih standardov kakovosti in varstva zdravljenja*«.

Pravica do izbrisa v 32. členu ZVOP-1 je skoraj enaka kakor pravica do pozabe. V ZVOP-1 pravica do izbrisa velja v primeru, ko »*posameznik dokaže, da so njegovi osebni podatki nepopolni, netočni, neažurni in bili zbrani ali obdelani v nasprotju z zakonom*«. V nasprotju je pravica do pozabe določena širše. Z njo ima posameznik možnost dejanskega izbrisa vseh svojih osebnih podatkov.

3.4.3 Pravica do omejitve uporabe (obdelave)

18. člen GDPR določa pravico do omejitve obdelave. S to pravico ima posameznik možnost doseči, da upravljavec omeji obdelavo njegovih osebnih podatkov. Ta pravica je alternativa izbrisu osebnih podatkov. V večini primerov zahteva omejitve obdelave ne velja za nedoločen čas, ampak se mora določiti določen čas omejitve. Pravica velja v primeru, ko:

- posameznik trdi, da njegovi osebni podatki niso točni,
- obdelava osebnih podatkov ni zakonita, vendar namesto izbrisa podatkov posameznik zahteva omejitev uporabe,
- posameznik potrebuje osebne podatke za uveljavljanje, izvajanje ali obrambo pravnih zahtevkov (vendar upravljavec teh podatkov ne potrebuje več za obdelavo),
- posameznik vloži ugovor o obdelavi podatkov v skladu s pravico do ugovora, dokler ni preverjeno, ali prevladajo zakoniti razlogi upravljavca.

V primeru, da posameznik doseže omejitev obdelave njegovih osebnih podatkov, jih upravljavec lahko shranjuje, vendar ne sme obdelovati, razen v primeru, da ima za obdelovanje soglasje posameznika: ko gre za vzpostavitev, uveljavljanje ali obrambo pravnih zahtevkov, varstvo pravic drugih oseb ali zaradi javnega interesa Evropske unije ali države članice (3. odstavek 18. člena GDPR).

Omejitev obdelave lahko upravljavec doseže z začasnim premikanjem osebnih podatkov v drug procesni sistem, preprečitvijo dostopa uporabnikom do osebnih podatkov ali z odstranitvijo osebnih podatkov iz spletnih strani. Posebno pri avtomatiziranih sistemih morajo uporabiti tehnične ukrepe, da se osebni podatki ne obdelujejo več in jih ni mogoče spreminjati (Information Commissionar's Office, brez datuma).

3.4.4 Pravica do prenosljivosti podatkov

Pravica do prenosljivosti podatkov je nova pravica, določena v 20. členu GDPR posameznikom, na katere se nanašajo osebni podatki, omogoča dve stvari.

- Posamezniki prejmejo svoje osebne podatke, ki so jih posredovali upravljavcu. Torej prejmejo nek podsklop osebnih podatkov, ki jih je upravljavec obdeloval in jih shranijo za nadaljnjo rabo (na zasebni napravi ali zasebnem oblaku). Podatke morajo posamezniki prejeti *»v strukturirani, splošno uporabljeni in strojno berljivi obliki*«, da jim je omogočeno enostavno upravljanje in ponovna uporaba podatkov (1. odstavek 20. člena GDPR). Posredovani podatki posameznika so vsi podatki, ki jih je posameznik zavestno in dejavno posredoval (uporabniško ime, starost, elektronski naslov …) in podatki, ki jih je posameznik posredoval z uporabo naprave ali storitev (podatki o lokaciji, zgodovina iskanja, srčni utrip …).
- Posamezniki pridobijo pravico do prenosa osebnih podatkov od enega upravljavca k drugemu upravljavcu podatkov, s tem, da upravljavec, kateremu so bili osebni podatki zaupani, prenosa ne ovira. Prenos podatkov je lahko namenjen za enako ali drugo dejavnost. Posameznik lahko zahteva neposreden prenos podatkov od enega upravljavca k drugemu, če je to tehnično možno izvesti (2. odstavek 20. člena GDPR). Pravica do prenosljivosti podatkov preprečuje vezanost na enega ponudnika storitev, pravzaprav še spodbuja k izmenjavi osebnih podatkov med upravljavci pod posameznikovim nadzorom. Izkušnje uporabnikov in storitve so lahko še bolj obogatene z izmenjavo osebnih podatkov.

Prvi odstavek 20. člena GDPR velja kadar:

a) je obdelava temelječa na podlagi privolitve v obdelavo osebnih podatkov za enega ali več namenov, izrecne privolitve v obdelavo ali na pogodbi, kjer je obdelava potrebna za izvajanje pogodbe,
b) je obdelava izvedena z avtomatiziranimi sredstvi.

GDPR v tretjem odstavku 20. člena in v uvodni izjavi 68 določa, da upravljavci niso zavezani k zagotovitvi prenosljivosti osebnih podatkov, če je obdelava potrebna za opravljanje naloge v javnem interesu, izvajanju javne oblasti, ali ko upravljavec izpolnjuje svojo pravno obveznost.

Četrti odstavek 20. člena določa tudi, da izpolnjevanje pravice o prenosljivosti podatkov ne sme vplivati na pravice in svoboščine drugih oz. tretjih oseb v negativnem smislu. Na primer, da upravljavec pridobi podatke drugih posameznikov, ki so v telefonskem imeniku stikov posameznika, na katerega se nanašajo osebni podatki in jih uporabi v namen trženja. (Delovna skupina za varstvo osebnih podatkov iz člena 29, 2016, str. 13)

Pravica do prenosljivosti podatkov je nekoliko povezana z pravico do dostopa , kjer mora upravljavec posamezniku omogočiti vpogled v njegove osebne podatke. Na podlagi Direktive 95/46/ES in ZVOP-1 je pravica do dostopa omejena na obliko, ki jo izbere upravljavec podatkov pri zagotavljanju zahtevane informacije. Nova pravica do prenosljivosti podatkov pa omogoča posameznikom premik, kopiranje in prenos njihovih osebnih podatkov iz enega informacijsko tehnološkega okolja v drugega, na primer v sistem novih upravljavcev podatkov, sistem tretjih oseb, ki so vredni zaupanja ali pa kar v lasten sistem (Delovna skupina za varstvo osebnih podatkov iz člena 29, 2016, str. 4). Namen pravice do prenosljivosti podatkov je zagotoviti večji nadzor posameznika nad njegovimi osebnimi podatki.

3.4.5 Obveznost obveščanja v zvezi s popravkom ali izbrisom

Upravljavec mora glede na 19. člen GDPR sporočiti vse popravke, izbrise, omejitve obdelave osebnih podatkov posameznika vsakemu uporabniku, ki so mu bili ti osebni podatki razkriti. Posameznik, na katerega se osebni podatki nanašajo, je na svojo zahtevo lahko obveščen tudi o vseh uporabnikih, ki uporabljajo njegove osebne podatke.

Če obveščanje vseh uporabnikov vključuje nesorazmeren napor ali se obveščanje izkaže za nemogoče, upravljavcu te obveznosti ni potrebno izpolniti.

V 2. odstavku 32. člena ZVOP-1 je zapisano, da mora upravljavec le na zahtevo posameznika pred kakršnim koli ukrepom (dopolnitvijo, popravkom, blokiranjem, izbrisom) obvestiti vse uporabnike in pogodbene obdelovalce, katerim je posredoval osebne podatke posameznika. Obveznost obveščanja upravljavca v zvezi s popravkom ali izbrisom (ukrepi) je po Zakonu o varstvu osebnih podatkov nujna v primeru, ko posameznik sam to zahteva.

3.5 Ugovor in avtomatizirano sprejemanje odločitev

3.5.1 Pravica do ugovora

S 21. členom GDPR ima posameznik pravico ugovarjati obdelavi njegovih osebnih podatkov, kadar:

- obdelava osebnih podatkov temelji na podlagi opravljanja naloge v javnem interesu ali izvajanju javne oblasti in obdelavi, ki je potrebna zaradi zakonitih interesov upravljavca ali tretje osebe (vključeno z oblikovanjem profilov),
- direktnim trženjem, vključno s profiliranjem. Posameznik lahko kadarkoli in brezplačno ugovarja vsakemu prvotnemu ali nadaljnjemu obdelovanju svojih osebnih podatkov v primeru direktnega trženja in profiliranju, ko je oblikovanje profilov povezano z neposrednim trženjem. V primeru ugovora (zaradi neposrednega trženja) se posameznikovi osebni podatki ne smejo obdelovati več (2. odstavek 21. člena GDPR),
- obdelavo v znanstveno- ali zgodovinsko raziskovalne ali statistične namene. Če za opravljeno nalogo, izvedeno zaradi javnega interesa, potrebujejo obdelavo osebnih podatkov, takrat posameznik ne more več ugovarjati (6. odstavek 21. člena GDPR).

Kadar zakoniti razlogi za obdelavo ne prevladujejo nad pravicami in svoboščinami posameznika ali so namenjeni za vzpostavitev, izvajanje ali obrambo pravnih zahtevkov, upravljavec takoj neha obdelovati posameznikove osebne podatke. (1. odstavek 21. člena GDPR)

Obveznost upravljavca je obveščanje posameznikov o njihovi pravici do ugovora. Obvestilo mora biti predstavljeno izrecno in ločeno od katere druge informacije (4. odstavek 21. člena GDPR).

3.5.2 Avtomatizirano sprejemanje posameznih odločitev

22. člen GDPR ima določbe o:

1. Avtomatiziranem individualnem odločanju. Pri avtomatiziranem odločanju se sprejemajo odločitve izključno z avtomatiziranimi sredstvi, brez vpletenosti človeka.
2. Oblikovanju profilov. Profiliranje je, glede na 4. Točko 5. člena GDPR, »*avtomatsko obdelovanje posameznikovih osebnih podatkov, s katerimi se ocenjujejo osebni vidiki posameznika.«* Pomeni, da s pomočjo danih osebnih podatkov podjetja lahko predvidijo kakšen je posameznik, ga ocenijo in analizirajo. Ugotovijo lahko, kakšen je njegov ekonomski položaj, osebni okus, interesi, zdravje, kje se giba (lokacija) itd. Oblikovanje profilov je lahko del procesa avtomatiziranega odločanja.

22. člen GDPR prinaša dodatna pravila, ki še bolj zaščitijo posameznikove osebne podatke v primeru, da odločitve temeljijo na avtomatiziranem odločanju, ki imajo pomemben vpliv pravnih ali podobnih učinkov na posameznika.

Odločitev o avtomatiziranem odločanju lahko podjetja uporabijo le, ko (2. odstavek 22. člena GDPR) »:

- *je pomembno za sklenitev, izvajanje pogodbe med posameznikom in upravljavcem,*
- *je odobreno s strani zakonodaje Evropske unije ali države članice, ki velja za upravljavca (za namen spremljanja in preprečevanja zlorab in davčnih utaj…),*
- *posameznik izrecno privoli.«*

V vsakem primeru morajo glede na uvodno izjavo 71 za avtomatizirano odločanje in oblikovanje profilov veljati zaščitni ukrepi, ki posameznikom zagotovijo informacije o obdelavi njihovih podatkov. Posamezniki imajo pravico do posredovanja, izražanje svojega vidika in izpodbijanja take vrste odločitev. Upravljavci morajo redno preverjati, ali sistemi za avtomatizirano odločanje delujejo po načrtih, saj tako zmanjšajo tveganje napak in zavarujejo osebne podatke. S tem preprečijo nevarnosti, povezane s pravicami in interesi posameznika ter diskriminacijo.

3.6 Omejitve

Obseg pravic posameznikov in njihovih dolžnosti, ki so omenjene v tretjem poglavju o spremembah pravic posameznikov drugem delu zaključne naloge, so lahko omejene. Omejitve morajo spoštovati človekove pravice in temeljne svoboščine. Ukrep je sprejet s strani upravljavca ali obdelovalca, ki upošteva pravo Evropske unije ali pravo države članice. 23. člen GDPR navaja, da so »*pravice posameznika omejene, če je v demokratični družbi potreben sorazmeren ukrep za zagotavljanje:*

- *državne varnosti,*
- *obrambe,*
- *javne varnosti (zaščita človeškega življenja pri odzivu na naravne nesreče ali nesreče povzročene zaradi človeškega ravnanja),*
- *preprečevanja, preiskovanja, odkrivanja, pregona kaznivih dejanj ali izvrševanja kazenskih sankcij (preprečevanje in varovanje pred grožnjami javni varnosti) in kršitev etike v zakonsko urejenih poklicih,*
- *drugih ciljev v splošnem javnem interesu Evropske unije ali države članice (gospodarski, finančni interes, denarne, proračunske, davčne zadeve, javno zdravje in socialna varnost),*
- *varstva neodvisnosti sodstva in sodnega postopka,*
- *uveljavljanja civilnopravnih zahtevkov,*
- *varstva posameznika, pravic in svoboščin drugih.*«

Zakon o varstvu osebnih podatkov v Sloveniji opredeljuje tudi omejitve pravic posameznikov iz enakih razlogov. »*Omejitve se lahko določijo samo v omejenem obsegu, to je v obsegu, ki je nujen za dosego namena*.« (Pirc Musar, 2006, str. 40)

SKLEP

Digitalizacija in globalizacija sta prinesli vse večje prizadevanje članov Evropske unije za boljše varstvo osebnih podatkov. S tem namenom so vse države članice sprejele Splošno uredbo Evropske unije (GDPR) o varstvu osebnih podatkov, ki je še bolj okrepila varstvo podatkov.

Marsikateri posameznik se ne zaveda, da je v osebne podatke izvedenih vedno več posegov in kakšne posledice ti posegi prinašajo, zato sta nadzor in regulacija osebnih podatkov izredno pomembna. Kot primer lahko omenim avtomatsko obdelavo, saj le ta zelo pripomore k lažji obdelavi osebnih podatkov, vendar je po drugi strani večja možnost, da te podatke nekdo zlorabi. Da je možnost zlorabe čim manjša, upravljavci pri obdelavi osebnih podatkov upoštevajo načela obdelave podatkov GDPR: zakonitosti, poštenosti, transparentnosti, zbiranja, minimizacije, točnosti, hranjenja podatkov, celovitosti in zaupnosti. Novo je načelo odgovornosti, kjer morajo upravljavci ali organizacije dokazati posameznikom skladno delovanje z ostalimi načeli. Posameznikovo dovoljenje za obdelavo podatkov mora biti prostovoljno in kazati na jasno potrditveno dejanje. Otrok, ki je mlajši od 16 let lahko privoli v ponujene, največkrat spletne storitve, samo s soglasjem staršev. Splošna uredba je zaostrila privolitev otrok, vendar lahko države članice same postavijo starost privolitve, ki pa ne sme biti manjša od 13 let.

Pravice posameznika so se s GDPR spremenile večinoma na bolje. Zakon o varstvu osebnih podatkov (ZVOP-1) pozna pravico do seznanitve, pravico do dopolnitve, popravka, blokiranja, izbrisa in ugovora, GDPR pa te pravice okrepi in doda še nekatere nove (pravica do pozabe, prenosljivosti in omejitve podatkov).

Informacije o posamezniku morajo biti jedrnate, lahko dostopne, razumljive, pregledne in brezplačno dostopne. Posameznik ima pravico, da ga upravljavec seznani z obdelovanjem osebnih podatkov, pojasni katere vrste osebnih podatkov obdeluje, za kakšen namen, kako dolgo je obdobje hrambe in komu so osebni podatki razkriti. GDPR kot prednosti pred Zakonom RS o varstvu osebnih podatkov posamezniku omogoča ne le vpogled, komu vse (tretji osebi) so njegovi osebni podatki razkriti, ampak tudi na kakšni podlagi in s kakšnim namenom. V primeru netočnih podatkov, posameznik lahko uveljavi pravico do popravka ali pravico do pozabe podatkov. V GDPR je pravica do pozabe še bolj okrepljena kot v ZVOP-1, saj posameznik lahko doseže čisti izbris osebnih podatkov (npr. iz vseh spletnih strani), posebno, če je zanje dal privolitev kot otrok. Posameznik ima po novem tudi pravico omejiti obdelavo svojih osebnih podatkov. Upravljavec mora na zahtevo posameznika o popravku, izbrisu ali omejitvi obdelave podatkov sedaj odgovoriti v roku enega meseca ali

v primeru kompleksnejše zahteve v dveh mesecih. Rok odgovora na zahtevo je enoten v vsej Evropski uniji, zato se roki ne bodo več veljali po slovenskem ZVOP-1, katerega rok je 30 dni. Nova pravica posameznika po GDPR je pravica do prenosljivosti. Z njo lahko posameznik prenese svoje podatke od enega upravljavca k drugemu.

Zgornje spremembe pravic posameznikov med Zakonom o varstvu osebnih podatkov in Splošno uredbo o varstvu podatkov brez dvoma kažejo na zaostritev. ZVOP-1 postavlja pravico varstva osebnih podatkov na visok nivo v primerjavi z zakoni katerih drugih članic Evropske unije. Glede na to upam, da bo zakonodaja v naši državi še bolj zaostrila nekatere pravice posameznikov, saj GDPR dovoli državam članicam natančnejšo ureditev določb (nujno je upoštevanje načel). Sama sem mnenja, da so zaostritve varstva osebnih podatkov nekaj pozitivnega, saj se že v Sloveniji prepogosto pojavljajo zlorabe osebnih podatkov.

LITERATURA IN VIRI

1. Article 29 data protection working party. (2016). *Article 29 Working Party Guideliness on consent under Regulation 2016/679*. Brussels: European Comission.
2. Bouca, C. (brez datuma). *EU GDPR Controller vs. Processor – What are the differences?* [objava na blogu]. Pridobljeno 14. februarja 2018 iz https://advisera.com/eugdpracademy/knowledgebase/eu-gdpr-controller-vs-processor-what-are-the-differences/
3. Cepec, J. & Kovač, M. (2012). *Poslovno pravo*. GV založba: Ljubljana.
4. Delovna skupina za varstvo osebnih podatkov iz člena 29. (2016). *Smernice o pravici do prenosljivosti podatkov*. Bruselj: Evropska komisija.
5. INFO HIŠA, svetovanje in izobraževanje, d.o.o. (brez datuma a). *Smernice Delovne skupine 29 o privolitvi*. Pridobljeno 4. aprila 2018 iz https://www.dataprotection-officer.com/index.php?route=blog/article&blog_post=153&create_pdf=true
6. INFO HIŠA, svetovanje in izobraževanje, d.o.o. (brez datuma b). *GDPR obveznosti glede privolitve*. Pridobljeno 4. aprila 2018 iz https://www.dataprotection-officer.com/index.php?route=blog/article&blog_post=52&create_pdf=true
7. Information Commissioner's Office. (brez datuma). *Lawful basis for processing: Consent*. Pridobljeno 4. aprila 2018 iz https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/consent/
8. Informacijski pooblaščenec. (2017, 25. maj). *Kaj prinaša nova Splošna uredba (EU) o varstvu podatkov*. Pridobljeno 8. januarja 2018 iz https://www.ip-rs.si/fileadmin/user_upload/Pdf/GDPR/Splosna_uredba_o_varstvu_podatkov-letak_maj2017_v2.pdf
9. Informacijski pooblaščenec. (brez datuma). *Pravice posameznika: Seznanitev z lastnimi osebnimi podatki*. Pridobljeno 11. maja 2018 iz https://www.ip-rs.si/varstvo-osebnih-podatkov/pravice-posameznika/seznanitev-z-lastnimi-osebnimi-podatki/

10. IT Governance Privacy Team. (2017). *EU general data protection regulation (GDPR): an implementation and compliance guide*. Ely (Cambridgeshire): IT Governance Publishing.
11. Jamšek, B. (2018, 14. februar). GDPR: Uredba o varstvu podatkov. Pridobljeno 15. februarja 2018 iz https://mladipodjetnik.si/novice-in-dogodki/novice/gdpr-uredba-o-varstvu-podatkov
12. MacDonald, S. (2018, 20. junij). *GDPR for Marketing: The Definitive Guide for 2018* [objava na blogu]. Pridobljeno 22. junija 2018 iz https://www.superoffice.com/blog/gdpr-marketing/
13. Opt-in. (brez datuma). V *Business Dictionary*. Pridobljeno 15. junija 2018 na http://www.businessdictionary.com/definition/opt-in.html
14. Pirc Musar, N. (2006). Zakon o varstvu osebnih podatkov (ZVOP-1). Ljubljana: GV založba.
15. Trobentar, B. (2017, september). *Posodobitev varstva osebnih podatkov v EU* (magistrsko delo). Univerza v Mariboru: Pravna fakulteta.