UNIVERZA V LJUBLJANI
EKONOMSKA FAKULTETA

MAGISTRSKO DELO

SPLOŠNA UREDBA O VARSTVU PODATKOV IN STROŠKI NJENE IMPLEMENTACIJE V GOSPODARSKIH DRUŽBAH

Ljubljana, 30. maj 2018 MANCA SMOLEJ

IZJAVA O AVTORSTVU

Podpisana Manca Smolej, študentka Ekonomske fakultete Univerze v Ljubljani, avtorica predloženega dela z naslovom Splošna uredba o varstvu podatkov in stroški njene implementacije v gospodarskih družbah, pripravljenega v sodelovanju s svetovalcem doc. dr. Jakom Cepcem,

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 in pravico dajanja predloženega dela na voljo javnosti na svetovnem spletu prek 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 30. 5. 2018 Podpis študentke: _____

KAZALO

KAZALO SLIK

SEZNAM KRATIC

ang. – angleško

CIPL – Centre for Information Policy Leadership at Hunton Andrews Kurth LLP

DPIA – (ang. Data protection impact assessment); ocena učinka na varstvo podatkov

DPO – (ang. Data Protection Officer); pooblaščena osebo za varstvo osebnih podatkov

ENVP – Evropski nadzornik za varstvo osebnih podatkov

EU – (ang. European Union); Evropska unija

EUR – evro

GDPR – (ang. General Data Protection Regulation); splošna uredba o varstvu podatkov

IAPP – ang. International Association of Privacy Professionals

IP – informacijski pooblaščenec

IT – informacijska tehnologija

SES - (ang. Security Effectivness Score); ocena učinkovite varnosti

slov. – slovensko

ZInfP – Zakon o Informacijskem pooblaščencu

ZVOP – Zakon o varstvu osebnih podatkov

UVOD

Pravica do varstva osebnih podatkov je pomembna temeljna pravica vsakega posameznika. Do sedaj je zaščito posameznikov pri obdelavi osebnih podatkov urejala Direktiva Evropskega parlamenta in Sveta 95/46/ES z dne 24. oktobra 1995 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov Ur. l. EU št. 281/95 (v nadaljevanju Direktiva), ki je osrednji del zakonodaje o varstvu osebnih podatkov v Evropski uniji (v nadaljevanju EU). V njej je predstavljeno temeljno izhodišče, ki ureja pravice in svoboščine posameznika (Kramar, 2013, str. 11). V Sloveniji pravice, načela in ukrepe glede varstva podatkov ureja Zakon o varstvu osebnih podatkov (ZVOP-1), Ur. l. RS, št. 94/07.

Aprila 2016 pa je Evropski parlament potrdil Uredbo (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES (Splošna uredba o varstvu podatkov) Ur. l. EU št. 119/16 (ang. General Data Protection Regulation, v nadaljevanju GDPR). GDPR bo nasledil nacionalne zakone o varstvu osebnih podatkov vseh 28 članic Evropske unije. Določbe iz GDPR se bodo v vseh državah članicah uporabljale neposredno od 25. maja 2018 naprej.

GDPR predstavlja najbolj prelomno evropsko regulativo v zadnjem desetletju, ki bo postala svetovni standard na področju varovanja osebnih podatkov. Prinaša pomemben korak k izboljšani zasebnosti državljanov EU, k harmoniziranemu varstvu podatkov v vseh državah članicah Evropske unije ter promoviranju zasebnosti in varnosti kot osrednji vidik evropske industrije (Mikkelsen, Soller & Strandell-Jansson, 2017).

Določbe se bodo morale uporabljati v vseh državah članicah EU kot tudi v vseh gospodarskih družbah, ki bodo hranila (in obdelovale) podatke o državljanih EU, ne glede na to, kje so le-ta geografsko pozicionirana. Utemeljitev uvedbe nove regulative na področju varstva podatkov prinaša preskok moči in kontrole nad osebnimi podatki od upravljavcev do posameznikov. GDPR omogoča posameznikom večji nadzor nad podatki s pravico do pozabe in popravka, pravico do omejitve uporabe, pravico do prenosa podatkov in pravico do ugovora. Na drugi strani pa bo skladnost s predpisi začela postavljati pomemben del poslovne politike gospodarskih družb zaradi zelo visokih kazni, ki lahko znašajo tudi do 20 milijonov evrov (v nadaljevanju EUR). V izogib le-tem bodo gospodarske družbe morale posodobiti interna pravila o varovanju podatkov, pripraviti oceno tveganja in ukrepati v primeru kršitve ter sprejeti ukrepe za učinkovit nadzor, kar pomeni, da bo gospodarska družba morala imeti pooblaščeno osebo za varstvo osebnih podatkov (ang. Data Protection Officer, v nadaljevanju DPO) (Sobolewski & Palinski, 2017, str. 1). Gospodarske družbe se bodo ob uvedbi GDPR vsekakor soočale z dodatnimi, novimi stroški.

Namen magistrskega dela je s pregledom literature ponuditi celovit pregled nad novo zakonodajo o varovanju podatkov. Pri tem bodo predstavljene ključne nove določbe, ki predstavljajo spremembe tako za posameznike kot tudi gospodarske družbe, ki hranijo in upravljajo s podatki. Na podlagi strokovne literature ter dostopnih podatkov in znanih dejstev bodo v delu obravnavani tudi vsi stroški, s katerimi se soočajo gospodarske družbe ob implementaciji GDPR. Obvladovanje stroškov je bistvenega pomena za učinkovito in uspešno poslovanje gospodarske družbe. Šele ko gospodarska družba dobro pozna svoje stroške, jih lahko obvladuje in s tem postane konkurenčnejše trgu. Ključni izziv podjetij v današnjem času je vsekakor povezan z razumevanjem, obvladovanjem in zmanjševanjem stroškov poslovanja (Zabukovec, 2011, str. 1).

Cilj magistrskega dela je predstaviti ključne spremembe na področju varovanja osebnih podatkov in na tej podlagi oceniti stroške implementacije uredbe v gospodarski družbi. V magistrskem delu želim odgovoriti na raziskovalno vprašanje, s katerimi dodatnimi stroški se bodo gospodarske družbe soočale ob implementaciji GDPR. Za odgovor na zastavljeno vprašanje bo magistrsko delo skozi vsa poglavja vsebovalo teoretično-analitičen pregled strokovne, predvsem tuje literature, raziskav in znanstvenih razprav. Pri tem si bom pomagala z opisno metodo, ki jo bom nagradila z metodo kompilacije in tako teoretični del zaokrožila z oceno ter s tem odgovorila na zastavljeno raziskovalno vprašanje.

Na področju stroškov, ki pridejo z implementacijo GDPR, ni veliko relevantne literature, zato sem bila pri analizi in odgovarjanju na raziskovalno vprašanje zelo omejena. Slovenske literature na temo stroškov nisem zasledila. Nabor tuje literature je nekoliko večji, a vseeno nikjer nisem zasledila nobene zelo konkretne analize in študije, ki bi povzela vsa področja. Analizo sem zato nadgradila z lastnimi mnenji in znanjem, ki sem ga pridobila pri natančni proučitvi GDPR. Tematiko stroškov sem zasledila v naslednjih člankih in študijah, ki sem jih upoštevala in uporabila pri analizi: Ponemon Institute je decembra 2017 izdal študijo The True Cost of Compliance with Data Protection Regulations. Glavni fokus študije so celotni stroški, povezani s skladnostjo z GDPR, vključno s stroški neskladnosti z GDPR, z zakoni, predpisi in politikami. London Economics s poročilom Analysis of the potential economic impact of GDPR, izdan oktobra 2017, opisuje, kako bodo nove zahteve glede privolitve vplivale na profitabilnost poslovanja, na baze in vrednost podatkov itd. Chistensen, Cocliago, Etro in Rafert so leta 2013 napisali članek z naslovom The Impact of the Data Protection Regulation in the EU – analizo za srednja in mala podjetja s posebnim poudarkom na vplivu na delovna mesta in ustvarjanje poslovanja gospodarske družbe. Skladnost z novimi pravili bo po njihovem vsekakor povzročila dodatne stroške, vključno z zaposlitvijo dodatnih zaposlenih, nakupom nove IT-programske opreme in posvetovanjem z organi za varstvo osebnih podatkov v povezavi z načrtovanjem in ustvarjanjem novih projektov (Christensen, Colciago, Etro & Rafert, 2013, str. 1). Deloittova raziskava, prav tako izvedena leta 2013, z naslovom Economic impact assessment of the proposed Eurepean General Data Protection Regulation, analizira vpliv GDPR na direktni marketing, obnašanje potrošnikov

na spletu, storitve spletne analitike in kreditne informacije. Poročilo predstavlja učinke GDPR na vse omenjene sektorje in posledično na celotno gospodarstvo. Oba vira sta bila izdana leta 2013 in temeljita na paketu reforme varstva osebnih podatkov, ki je bil predstavljen januarja 2012, kjer je bil prvič predstavljen tudi GDPR. Kljub temu da sta vira relativno stara, še vedno predstavljata objektiven in primeren vir za analizo, saj sta bila narejena za lažjo in transparentnejšo obravnavo predloga GDPR.

Z izvajanjem obsežnega sistematičnega pregleda literature bom prispevala k raziskovalnemu področju varstva osebnih podatkov in stroškov, ki pridejo z novim zakonskim okvirom.

Magistrsko delo predstavlja celostni pregled novih pravil s področja varstva osebnih podatkov, napisanih v GDPR, in stroške, ki pridejo z implementacijo GDPR. Sestavljeno je iz štirih vsebinskih poglavij. V prvem poglavju predstavim zgodovino varovanja podatkov in razvoj skozi čas. V podpoglavju predstavim, kako je prišlo do pobude o novem zakonu. V osrednjem, drugem poglavju predstavim ključne nove določbe, ki bodo prišle v veljavo z GDPR. Podrobneje predstavim temeljne določbe GDPR, pravice posameznikov, ki prinašajo eno izmed ključnih sprememb na področju varovanja podatkov; obveznosti obdelovalcev in upravljavcev osebnih podatkov posameznikov ter spremembe in zahteve na področju pridobivanja privolitev. V pripadajočem poglavju opišem novo definirane posebne vrste osebnih podatkov in predstavim novosti v povezavi z neodvisnimi nadzornimi organi, ki jim nov koncept omogoča poenoteno in usklajeno ukrepanje. V tretjem poglavju predstavim in podrobno opišem normativni okvir varstva osebnih podatkov v Sloveniji. Opišem obveznosti in pravice, opredeljene v ZVOP-1, zakonu, ki je predhodnik GDPR. Na koncu pa osvetlim in predstavim stroške, s katerimi se bodo gospodarske družbe srečevale ob implementaciji GDPR. Stroške sem razdelila na pet skupin, jih opisala in podrobneje razdelila. Analizo zaključim z opisom dejavnikov vpliva.

1 ZGODOVINA VAROVANJA OSEBNIH PODATKOV

Pravico do zasebnosti posameznika v mednarodnih dokumentih zasledimo prvič v Splošni deklaraciji o človekovih pravicah Združenih narodov, sprejeto leta 1948 v Parizu. V 12. členu določa varstvo posameznikovega zasebnega življenja, v 8. členu pa določa učinkovito pravno varstvo proti dejanjem, ki kršijo temeljne pravice posameznika, priznane po ustavi ali zakonu. Splošna deklaracija je prva postavila pomembna merila uresničevanja človekovih pravic in vplivala na razvoj drugih aktov o človekovih pravicah v Evropi (Kranjc, 2004, str. 12).

Svet Evrope, ki spodbuja načela pravne države, demokracije, človekovih pravic in družbenega razvoja, je leta 1950 sprejel Evropsko konvencijo o človekovih pravicah. Pravica do varstva osebnih podatkov je varovana z 8. členom, s katerim je zagotovila pravico do spoštovanja zasebnega in družinskega življenja in svobode misli. V Strasbourgu

je bilo za zagotavljanje izpolnjevanja in spoštovanja obveznosti pogodbenic oz. držav, ki so podpisale Evropsko konvencijo o človekovih pravicah, ustanovljeno Evropsko sodišče za človekove pravice. Zaradi naraščanja pretoka osebnih podatkov čez državne meje, pojava informacijske tehnologije in želje po doseganju še večje enotnosti članic Sveta Evrope je bila leta 1981 sprejeta Konvencija o varstvu posameznikov glede na avtomatsko obdelavo osebnih podatkov oziroma Konvencija št. 108. Predstavlja prvi pravno zavezujoč mednarodni instrument na področju varstva osebnih podatkov, katerega so ratificirale vse države članice EU, nato pa je pogodbenica postala tudi EU. Pogodbenica, ki je podpisala Konvencijo št. 108, se je zavezala, da bo sprejela in prevzela vse ukrepe, ki so potrebni za uresničevanje temeljnih načel. Temeljna načela v povezavi z zbiranjem in obdelavo osebnih podatkov se nanašajo na pošteno in zakonito zbiranje ter predvsem na avtomatsko obdelavo osebnih podatkov. Konvencija št. 108 je naložila delne omejitve prostega pretoka osebnih podatkov med državami (12. člen Konvencije št. 108), posameznikom omogoča, da vedo, kateri podatki o njem se shranjujejo, in jim daje pravico zahtevati popravek (8. člen Konvencije št. 108). Hkrati pa je prepovedala obdelavo »občutljivih« podatkov o osebi (podatki o zdravju, rasi, spolnem življenju, verskem prepričanju, političnem prepričanju, kazenski evidenci). Leta 2001 so bile uvedene dodatne določbe in s tem je bil sprejet Dodatni protokol h Konvenciji (Agencija Evropske unije za temeljne pravice, Svet Evrope, 2014, str. 15–17).

Varovanje temeljnih pravic fizičnih oseb in njihovih pravic do varovanja osebnih podatkov je cilj vseh predpisov v EU s področja varovanja osebnih podatkov. Do 25. maja 2018 sta veljavni zakonodajni instrument Evropske unije na področju varovanja osebnih podatkov predstavljala Direktiva o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem gibanju takih podatkov 95/46/ES z dne 24. oktobra 1995 ter Okvirni sklep Sveta 2008/977/PN z dne 27. novembra 2008 o varstvu osebnih podatkov, ki se obdelujejo v okviru policijskega in pravosodnega sodelovanja v kazenskih zadevah.

Direktiva Evropskega parlamenta in Sveta Evropske unije predstavlja temeljno izhodišče in mejnik v zgodovini varstva osebnih podatkov v EU. Uporaba Direktive ne zajema le 28 držav članic EU, pač pa vključuje tudi države, ki so del Evropskega gospodarskega prostora, ki niso del EU (Islandijo, Lihtenštajn in Norveško). Cilj sprejetja Direktive je bil uskladiti in zagotoviti ustrezno raven varstva pravic in svoboščin v vseh državah članicah ter zagotoviti prost pretok osebnih podatkov med državami članicami, kar je v nasprotju s Konvencijo. Pomembna novost, ki jo je prinesel 28. člen Direktive, je uvedba nadzornega neodvisnega instrumenta v vsaki državi članici, ki spremlja uredbe predpisov, ki so jih sprejele države članice, kar se je izkazalo za pomemben prispevek k učinkoviti implementaciji in delovanju evropske zakonodaje o varstvu osebnih podatkov (Agencija Evropske unije za temeljne pravice, Svet Evrope, 2014, str. 17–19). Direktiva je bila razveljavljena 25. maja 2018, ko je začel veljati nov, celovit pravni okvir o varstvu osebnih podatkov z novo Uredbo (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila

2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES (Splošna uredba o varstvu podatkov).

Dodatni pravni instrumenti, zaradi stare stebrne strukture, povezani z varovanjem osebnih podatkov, so bili (Agencija Evropske unije za temeljne pravice, Svet Evrope, 2014, str. 19):

- Uredba št. 45/2001 Ur. l. EU št. 8/2001 – Uredba o varstvu osebnih podatkov v institucijah EU. Ta pravni instrument je potreben, ker Direktiva sama ni urejala varstva podatkov v institucijah in organih EU;
- Direktiva 2002/58/ES Ur. l. EU št. 201/2002 – Direktiva o zasebnosti in elektronskih komunikacijah. Potrebne so bile natančnejše določbe v zvezi z jasnostjo pri uravnoteženju drugih zakonitih interesov;
- Direktiva 2006/24/ES Ur. l. EU št. 105/2006 – Direktiva o hrambi podatkov, pridobljenih ali obdelanih v zvezi z zagotavljanjem javno dostopnih elektronskih komunikacijskih storitev ali javnih komunikacijskih omrežij.

Evropska komisija je zaradi GDPR pripravila in predstavila nov predlog: Uredba Evropskega parlamenta in Sveta o varstvu posameznikov pri obdelavi osebnih podatkov v institucijah, organih, uradih in agencijah Unije in o prostem pretoku takih podatkov ter o razveljavitvi Uredbe (ES) št. 45/2001 in Sklepa št. 1247/2002/ES, ki je še vedno v obravnavi. Prav tako je zaradi GDPR še vedno v obravnavi predlog Uredbe Evropskega parlamenta in Sveta o spoštovanju zasebnega življenja in varstvu osebnih podatkov na področju elektronskih komunikacij ter razveljavitvi Direktive 2002/58/ES. Direktiva 2006/24/ES je bila razveljavljena aprila 2014 zaradi resnega poseganja v zasebno življenje posameznika.

Tudi Listina o temeljnih pravicah (v nadaljevanju Listina) predstavlja pravno zavezujoč instrument, ki določa temeljne pravice posameznikov, ki jih morajo pri izvajanju zakonodaje upoštevati tako države članice kot tudi EU. Listino so slovesno razglasili leta 2000 v Nici, neposredno pravno zavezujoča pa je kot del Lizbonske pogodbe postala šele z njenim sprejetjem 1. decembra 2009. Vsebuje pomembne določbe o varstvu osebnih podatkov. Listina določa, da spoštovanje zapisanih pravil nadzira neodvisen organ – Varuh človekovih pravic, ki zagotavlja spoštovanje zasebnega in družinskega življenja. Z vidika varstva osebnih podatkov 8. člen Listine ureja temeljne pravice z vidika varstva osebnih podatkov, kjer je določeno, da ima vsakdo pravico do varstva podatkov, ki se nanaša nanj. Prav tako pravi, da mora imeti vsak posameznik, ki ima pravico do varstva podatkov, dostop do podatkov, ki se nanj navezujejo, in lahko zahteva, da se ti podatki popravijo. Obdelava le-teh mora biti poštena in imeti določen namen, prav tako pa mora posameznik privoliti oz. mora obstajati druga legitimna podlaga, določena z zakonom. Ta člen je bil izoblikovan več let po samem sprejetju Direktive, zato bi lahko rekli, da je izraz predhodno veljavne zakonodaje (Kranjc, 2004, str. 17).

Uredba št. 45/2001 skrbi, da institucije in organi EU izpolnjujejo obveznosti v povezavi z varstvom osebnih podatkov, za kar je bil leta 2004 ustanovljen Evropski nadzornik za varstvo osebnih podatkov (ang. European data protection supervisor, v nadaljevanju ENVP). Glavne naloge ENVP so: svetovanje, nadzor in posvetovanje predvsem z institucijami in organi EU. V skladu z 29. členom Direktive pa je bila leta 1996 ustanovljena Delovna skupina za varstvo posameznikov pri obdelavi osebnih podatkov (v nadaljevanju Delovna skupina). Predstavlja neodvisen svetovalni organ, sestavljen iz predstavnikov nadzornega organa vsake države članice, predstavnika Evropske komisije in ENVP. Formalna vloga skupine je podana v 1. odstavku 30. člena Direktive, ki pravi, da svetuje o vseh predlaganih spremembah Direktive, poda mnenje in proučuje vsa vprašanja v povezavi z obdelavo osebnih podatkov. Delovna skupina je izdala več smernic, ki temeljijo na GDPR, saj želi z njimi spodbuditi pravilno uporabo GDPR in z mnenji prispevati k enotni razlagi in uporabi predpisov iz EU (European Commission, 2016).

1.1 Predlog GDPR

Evropska komisija (2010, str. 2), ki predstavlja izvršilno oblast EU, je v sporočilu za javnost, ki ga je izdala leta 2010, zapisala, da se je 15 let po začetku veljave Direktive treba vprašati, ali se sedanja veljavna zakonodaja EU o varstvu osebnih podatkov uspešno in v celoti spopada z izzivi, kot sta hiter tehnološki razvoj in globalizacija (računalništvo v oblaku, spletna socialna omrežja …), ter z vse bolj izpopolnjenimi načini zbiranja osebnih podatkov, ki jih je vse težje odkriti (npr. avtomatsko zbiranje podatkov z elektronskih vozovnic, elektronsko cestninjenje). Sklenili so, da »mora EU oblikovati celovit in skladen pristop, ki bo zagotovil popolno spoštovanje temeljne pravice posameznikov do varstva podatkov v EU in zunaj nje« (Evropska komisija, 2010, str. 4). Cilji celovitega skladnega pristopa k popolnemu varstvu podatkov so:

- krepitev pravic posameznika,
- krepitev razsežnosti notranjega trga,
- spremembe predpisov o varstvu osebnih podatkov na področju policijskega in pravosodnega sodelovanja v kazenskih zadevah,
- globalna razsežnost varstva podatkov,
- trdnejša institucionalna ureditev za boljše izvrševanje predpisov o varstvu podatkov.

Skladno z naštetimi cilji je Evropska komisija 25. januarja 2012 v Bruslju podala in objavila »paket reforme varstva osebnih podatkov«, ki vsebuje:

- Predlog Splošne uredbe o varstvu podatkov (nadomesti Direktivo iz leta 1995) in
- Predlog Direktive 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 (nadomesti Okvirni sklep Sveta 2008/977/PNZ iz leta 2008).

Reformni predlog je prav tako v skladu z načrtom za oblikovanje enotnega digitalnega trga, ki ga je Evropska komisija objavila maja 2015. Predstavlja najpomembnejšo prednostno nalogo Evropske komisije in pomemben korak k okrepitvi pravic Evropejcev v digitalni dobi ter pomaga pri posploševanju regulatornih pravil za gospodarske družbe. Cilj enotnega digitalnega trga je namreč odprava regulatornih okvirov in 28 nacionalnih trgov ter vzpostavitev enega samega. Sloni na treh stebrih in določa 16 ključnih ukrepov za izvajanje strategije. Prvi steber predstavlja boljši dostop potrošnikov in podjetij do digitalnega blaga in storitev po vsej Evropi, drugi steber oblikovanje ustreznega okolja in enakih konkurenčnih pogojev za razcvet digitalnih omrežij in inovativnih storitev, tretji steber pa čim boljše izkoriščanje potenciala rasti digitalnega gospodarstva. Na podlagi ukrepa iz drugega stebra, ki poudarja »okrepitev zaupanja v digitalne storitve in njihovo varnost, zlasti v zvezi z obdelavo podatkov«, je Komisija konec aprila 2016 sprejela GDPR, ki bo nadomestil Direktivo (Evropska komisija, 2016).

Najbolj očitna razlika med GDPR in Direktivo je v poimenovanju, ki je posledica pravne narave, saj bo obstoječo direktivo nasledila uredba. Oba pravna akta predstavljata sekundarni pravni vir EU, ki je izveden iz primarnih pravnih virov. Direktiva predstavlja sredstvo harmonizacije, kjer so po navadi zapisani minimalni standardi, ki jih morajo države članice implementirati v svojo zakonodajo. Na kakšen način in kako strogo bodo države članice implementirale direktivo v nacionalni red, je odločitev posamezne države. Najbolj očitni in pomembni razliki med samo direktivo in uredbo sta, da direktiva ni nujno zavezujoča za vse države članice EU, ampak se lahko navezuje zgolj na nekaj držav, medtem ko je uredba neposredno uporabna v čisto vseh državah članicah EU, ter drugič, pri direktivi je pravno zavezujoč samo rezultat, ki ga je treba doseči. Obe vrsti pravnih aktov omogočata visoko raven harmonizacije, vendar pa uredba omogoča poenotenje posameznega pravnega področja in neposredno velja v vseh državah članicah, kjer ni potrebnih prenašanj v notranji pravni red (Cepec & Kovač, 2012, str. 67, 68). Neposredna uporabnost uredbe bo tako omogočila večjo pravno varnost ter pripomogla k izboljšanju varstva temeljnih pravic in boljšemu delovanju notranjega trga (European commission, 2012, str. 5).

2 NOVA SPLOŠNA UREDBA O VAROVANJU OSEBNIH PODATKOV

Nova splošna uredba o varovanju osebnih podatkov oziroma GDPR, ki nadomešča Direktivo, je stopila v veljavo 25. maja 2018 in prinaša pomembne novosti tako na strani gospodarskih družb kot tudi na strani posameznikov. GDPR je sestavljen iz 173 uvodnih določb, katerim sledi 11 poglavij z 99 členi. Poglavja si sledijo: splošne določbe; načela; pravice posameznika, na katerega se nanašajo osebni podatki; upravljavec in obdelovalec; prenos osebnih podatkov v tretje države ali mednarodne gospodarske družbe; neodvisni nadzorni organ; sodelovanje in skladnost; pravna sredstva, odgovornost in kazni; določbe o posebnih primerih obdelave; delegirani akti in izvedbeni akti; končne določbe. Pri pisanju

magistrskega dela sem se osredotočala zgolj na začetna poglavja, ki se tičejo splošnih določb in načel, pravic posameznikov in obveznosti obdelovalcev. Na koncu poglavja pa sem predstavila še pomembne spremembe na strani privolitev posameznika ter posebne vrste osebnih podatkov in neodvisnih nadzornih organov. Za gospodarsko družbo je tako ključno dobro poznavanje členov GDPR, saj bo tako vodilo do lažjega razumevanja sprememb in definiranja stroškov implementacije.

2.1 Temeljna načela

GDPR definira, določa sedem temeljnih načel, s katerimi uokviri osnovne cilje in namene uredbe. Z načeli nakazuje pot za pravilno uporabo GDPR in posledično omogoča zakonsko ustrezno obdelavo osebnih podatkov. Neupoštevanje načel pomeni grobo kršitev GDPR, kar lahko vodi v sankcije. Načela, ki so navedena v 5. in 6. členu GDPR ter so predstavljena v nadaljevanju poglavja, mora gospodarska družba upoštevati v celotnem procesu ravnanja z osebnimi podatki (Taylor Wessing, 2016a):

- **načelo zakonitosti, pravičnosti in preglednosti:** GDPR zahteva, da upravljavec podatkov posreduje posamezniku, na katerega se nanašajo osebni podatki, informacije o obdelavi osebnih podatkov na jedrnat, pregleden in razumljiv način, ki je lahko dostopen, z uporabo jasnega in preprostega jezika. Načelo preglednosti je doseženo z obveščanjem posameznika pred obdelavo podatkov. Treba je vedeti, da podatki niso vedno zbrani neposredno od posameznika, ampak jih je možno pridobiti iz drugih podatkovnih nizov. V GDPR je jasno navedeno, katere informacije morajo biti posredovane posameznikom, ko so osebni podatki zbrani neposredno ali posredno od njih. Način, kako je posameznikom posredovana informacija, je odvisen od komunikacije kot tudi od tipa posameznika. Skladno z načelom zakonitosti (1. odstavek 6. člen GDPR) mora imeti obdelovalec zakonsko podlago za obdelavo osebnih podatkov. Kot zakonito obdelavo se šteje:
  a. privolitev posameznika;
  b. obdelava je potrebna za izvajanje pogodbe;
  c. obdelava je potrebna za izpolnitev zakonske obveznosti upravljavca;
  d. obdelava je potrebna za zaščito življenjskih interesov posameznika;
  e. obdelava je potrebna za opravljanje nalog, ki so v javnem interesu;
  f. obdelava je potrebna zaradi zakonitih interesov upravljavca, ki ne prevladajo nad interesi ali temeljnimi pravicami posameznika.
- **načelo omejitve namena:** obdelava osebnih podatkov je dovoljena le, če je to skladno s prvotnim namenom, za katerega so bili osebni podatki zbrani. V kolikor želi obdelovalec uporabljati podatke za drugi namen, mora zahtevati dovoljenje, razen če je drugi namen združljiv s prvotnim namenom. Kadar so okoliščine, v katerih so bili zbrani osebni podatki ali narava osebnih podatkov ali možne posledice nameravane nadaljnje obdelave ali obstoj ustreznih zaščitnih ukrepov, združljive s prvotnim namenom, je torej potrebno ponovno dovoljenje.

- **načelo najmanjšega obsega podatkov:** upravljavci podatkov morajo zagotoviti, da se obdelujejo le podatki, ki so potrebni za namen obdelave (glede na količino zbranih osebnih podatkov, obseg obdelave, čas procesiranja in dostopnosti). V skladu z GDPR (5. člen) morajo biti podatki »ustrezni, relevantni in omejeni na tisto, kar je potrebno glede na namene, za katere se obdelujejo«. Le to je povezano z načelom omejitve namena. Upravljavci morajo poskrbeti, da zberejo dovolj podatkov, da dosežejo svoj namen, vendar ne več, kot je potrebno.
- **načelo omejitve shranjevanja:** ko upravljavec podatkov, ki jih hrani, ne potrebuje več za namen, za katerega so bili zbrani, jih mora izbrisati, razen če ima druge razloge za njegovo hranitev. Za zagotavljanje omejevanja shranjevanja mora obstajati reden postopek preverjanja obdelave podatkov s čiščenjem baze podatkov.
- **načelo točnosti:** osebni podatki, ki so obdelani, morajo biti točni in pravilni. Nepravilni ali stari podatki morajo biti izbrisani, spremenjeni ali popravljeni.
- **načelo celovitosti in zaupnosti:** v skladu z GDPR morajo biti osebni podatki zaščiteni pred nepooblaščenim dostopom z uporabo ustreznih organizacijskih in tehničnih ukrepov. Upravljavci in obdelovalci podatkov morajo oceniti tveganje in izvajati ustrezno varnost nad podatki. Prav tako obstajajo stroge določbe o poročanju v primeru kršitve varstva osebnih podatkov. Visoke kazni za kršitve lahko povzročijo precejšnje stroške in nevšečnosti za gospodarske družbe.

Poleg vseh zgoraj naštetih načel je v 2. odstavku 5. člena GDPR definirano **načelo odgovornosti**, ki pravi, da je upravljavec definiran kot fizična ali pravna oseba, ki zagotavlja skladnost z vsemi zgoraj naštetimi načeli. Lahko bi rekli, da predstavlja gonilo za učinkovito izvajanje načel varstva osebnih podatkov (Cerasaro, 2017, str. 225). Zahteva preventivno in proaktivno ravnanje tako obdelovalcev kot upravljavcev. Prav ocena učinkov v zvezi z varstvom osebnih podatkov (ang. Data protection impact assessment, v nadaljevanju DPIA) je tista, ki predstavlja ključni koncept v okviru tega načela. Za upravljavca ni dovolj, da spoštuje določbe uredbe, pač pa da se tega ves čas drži. Kompleksnost obdelave osebnih podatkov vpliva na obseg procesov in ukrepov, ki jih morajo gospodarske družbe vzpostaviti za dokazovanje skladnosti (Taylor Wessing, 2016a).

Temeljni mehanizmi v GDPR (Informacijski pooblaščenec, 2017b, str. 31) za zagotavljanje načela odgovornosti so:

- vgrajeno in privzeto varstvo podatkov (25. člen GDPR),
- evidenca dejavnosti obdelave osebnih podatkov (30. člen GDPR),
- varnostni ukrepi (šifriranje, psevdonimizacija, načelo najmanjšega obsega podatkov) (32. člen GDPR),
- obveščanje o varnostnih incidentih (33. člen GDPR),
- DPIA (35. člen GDPR),
- zahteva glede uporabe obdelovalcev,

– DPO (37. člen GDPR).

Po mnenju Cerasara (2017, str. 219, 220) načelo odgovornosti predstavlja višji standard kot sama skladnost z GDPR, ki nekaterim predstavlja zgolj upoštevanje pravil. Priznavanje odgovornosti kot načela predstavlja in vzbuja družbeno-kulturno razmišljanje, kar lahko vodi k paradigmatični spremembi načina varstva osebnih podatkov. Varovanje osebnih podatkov se tako od togega in statičnega pogleda giblje k dinamičnemu in prilagodljivemu konceptu, kjer so za varstvo osebnih podatkov odgovorni vsi udeleženi akterji. Odgovornost je paradigmatična sprememba v zvezi z varstvom podatkov. Predstavlja priložnost in orodje za izvajanje prilagojenih ukrepov, sprejetih glede na posebnosti vsake gospodarske družbe, in s tem omogoča učinkovitejšo zaščito podatkov.

2.2 Pravice posameznikov

Izhodišče GDPR predstavljajo človek, posameznik in njegove pravice. Nanaša se na vse posameznike, ki živijo na območju EU, ne glede na to, kje se izvršuje obdelava osebnih podatkov. Posameznikom zagotavlja, v svojih zmožnostih, vrsto specifičnih pravic, ki jih lahko uporabljajo pod posebnimi pogoji z nekaj izjemami. Spoštovanje GDPR za upravljavca pomeni uresničevanje v nadaljevanju naštetih pravic. Pravice posameznikov niso absolutne, obstajajo namreč določeni pogoji in izjeme. Ko govorimo o pravicah posameznikov, se moramo vprašati po kontekstu – poznati je treba pravice, obveznosti in okoliščine (i-SCOOP, 2017). V primerjavi s sedaj veljavnim zakonom, ki ga bom predstavila v 3. poglavju, GDPR omogoča boljše varstvo osebnih podatkov, saj prinaša nove in okrepljene pravice posameznikov. V nadaljevanju bom predstavila vse pravice posameznikov, ki so v GDPR opredeljene od 15. do 22. člena.

2.2.1 Pravica dostopa posameznika, na katerega se nanašajo osebni podatki, in pravica do obveščenosti (15. člen GDPR)

Posamezniki imajo pravico do dostopa do svojih osebnih podatkov in drugih dodatnih informacij, ki jih ima upravljavec ali obdelovalec. Pravica dostopa omogoča posameznikom, da se zavedajo in preverijo zakonitost obdelave podatkov (uvodna izjava 63 GDPR). Pravica do obveščenosti obsega obveznost upravljavca, da zagotavlja »poštene informacije o obdelavi«, običajno prek obvestila o zasebnosti.

15. člen GDPR podrobneje opisuje pravico dostopa posameznika do osebnih podatkov in naslednjih informacij:

– kopijo osebnih podatkov, ki se obdelujejo;
– namen obdelave osebnih podatkov (predvsem, ko gre za obstoj avtomatiziranega odločanja s profiliranjem ter razlago in posledice take obdelave);
– kategorijo osebnih podatkov, ki so obdelani (na primer: ime, naslov, vedenje na spletu);

- v kolikor so podatki posredovani v tretje države, ima posameznik pravico izvedeti, kakšni zaščitni ukrepi bodo sprejeti za zaščito podatkov;
- kadar osebni podatki niso zbrani pri posamezniku, na katerega se nanašajo vse informacije v zvezi z njihovim virom;
- predvideno obdobje hrambe osebnih podatkov;
- obstoj pravic do pritožbe nadzornemu organu, izbrisa, popravka, omejitve obdelave osebnih podatkov in ugovora obdelave.

Upravljavec mora v okviru pravice do obveščenosti podati posamezniku vse informacije, »povezane z obdelavo, v jedrnati, pregledni, razumljivi in lahko dostopni obliki ter jasnem in preprostem jeziku« (GDPR, 12. člen). Informacije se lahko v tem primeru posredujejo pisno ali v drugi obliki, ki pa morajo biti zagotovljene brez nepotrebnega odlašanja, v enem mesecu od prejema zahtevka. Zagotovljene informacije morajo biti po 5. odstavku 12. člena GDPR brezplačne, razen če so zahteve posameznika neutemeljene ali pretirane. V tem primeru lahko upravljavec zaračuna pristojbino ali zavrne ukrepanje (i-SCOOP, 2017).

Kadar upravljavec obdeluje osebne podatke za namen, ki ni namen, za katerega so bili osebni podatki posredovani, je dolžan pred nadaljnjo obdelavo zagotoviti informacije o drugem namenu (3. odstavek 13. člena GDPR).

2.2.2 Pravica do popravka in izbrisa (16. in 17. člen GDPR)

Posameznik ima na podlagi GDPR pravico do popravka in izbrisa. Na zahtevo posameznika mora upravljavec »brez nepotrebnega odlašanja« popraviti ali izbrisati vse netočne podatke v zvezi z njim. Upravljavec mora izbrisati podatke, kadar velja eden od naštetih razlogov:

- osebni podatki niso več potrebni za namene, za katere so bili zbrani;
- posameznik prekliče privolitev, za nadaljnjo obdelavo podatkov pa ne obstaja noben pravni interes;
- posameznik ugovarja obdelavi podatkov na podlagi pravice do ugovora;
- osebni podatki so obdelani nezakonito;
- osebne podatke je treba izbrisati za izpolnitev pravne obveznosti.

V praksi to pomeni, da so osebni podatki izbrisani iz upravljavčevega sistema, če pa je upravljavec posredoval podatke v javnost (npr. na internet), mora le-ta poskrbeti, da bodo izbrisane vse povezave do teh osebnih podatkov. Upravljavec mora na zahtevo o izbrisu reagirati »brez nepotrebnega odlašanja«, razen če je obdelava potrebna: za uresničevanje pravic do svobode izražanja; iz razlogov javnega interesa na področju javnega zdravja; za uveljavljanje, izvajanje ali obrambo pravnih zahtevkov; za namene arhiviranja v javnem interesu, v raziskovalne namene in bi izbris onemogočil ali resno oviral obdelavo; za

izpolnjevanje pravne obveznosti na podlagi prava EU ali države članice (Safari, 2017, str. 829).

Primer Google Spain vs Mario Costeja Gonzalez[1] je pomemben primer, ki je vplival na izoblikovanje posameznikove pravice do izbrisa. Pritožba je temeljila na tem, da s tem, ko internetni uporabnik vpiše v iskalnik Google Mario Costeja Gonzalez, najde povezave do dnevnika, kjer je bila objavljena informacija o nepremičninski dražbi zaradi izvršbe neplačila socialnih prispevkov Maria. Mario je vložil pritožbo proti družbi La Vanguardia Ediciones SL, ki izdaja dnevnik, ter družbama Google Spain in Google Inc. ter zahteval, da se navedena stran izbriše ali spremeni. V tem primeru je Google upravljavec, saj je obdeloval osebne podatke Maria. Sodišče Evropske unije je leta 2014 upravljavcu naložilo, naj sprejme ustrezni ukrep, da onemogoči dostop do osebnih podatkov Maria. Primer Google Spain je imel resne posledice za iskalnike in za vlogo internetnih posrednikov na splošno. Posameznikom je omogočilo uveljavljanje pravic, hkrati pa so globoko vplivale na razpoložljivost in pretok informacij na svetovnem spletu. Pravica do izbrisa je tako eden osrednjih in pomembnejših elementov GDPR. V primerjavi s sodbo v primeru Google Spain je pravica do izbrisa v GDPR nekoliko okrepljena. Le-ta vključuje obveznost upravljavca, ki je javno objavil osebne podatke, da drugim upravljavcem, ki obdelujejo takšne podatke ali kopije, sporoči, da morajo te podatke izbrisati in sprejeti določene ukrepe (Burri & Schär, 2016, str. 482–483).

2.2.3 Pravica do omejitve obdelave (18. člen GDPR)

Pravica do omejitve obdelave je predstavljena v 18. členu GDPR in je alternativa pravici do izbrisa. Posameznikom omogoča, da omejijo oz. »zamrznejo« obdelavo osebnih podatkov, ko:

- posameznik nasprotuje obdelavi (na podlagi zakonitih interesov), osebni podatki bodo omejeni za obdobje preverjanja zakonitih interesov;
- upravljavec nima več potrebe po podatkih, vendar posameznik zahteva, da osebni podatki uveljavljajo, izvajajo ali branijo pravne zahtevke;
- je obdelava nezakonita, vendar posameznik ne želi, da se podatki izbrišejo, in namesto tega zahteva omejitev;
- kadar posameznik izpodbija točnost podatkov, bodo osebni podatki omejeni za obdobje, ko je to preverjeno.

Če so osebni podatki »omejeni«, lahko upravljavec podatke samo shranjuje, obdelava in kakršna koli uporaba podatkov pa nista dovoljeni. Podatkov ne more naprej obdelovati, razen če: posameznik soglaša z obdelavo; je obdelava potrebna za vzpostavitev pravnih zahtevkov; za zaščito pravic druge fizične ali pravne osebe; zaradi pomembnega javnega

[1] Case 131/12 *Google Spain SL, Google Inc* v *Agencia Española de Protección de Datos and Mario Costeja González.*

interesa (2. odstavek 18. člena GDPR). Kadar želi upravljavec ponovno začeti obdelovati podatke oziroma prekiniti omejitev obdelave, mora pred tem o tem nujno obvestiti posameznika, na katerega se podatki nanašajo. Kadar se podatki obdelujejo samodejno, je treba opraviti omejitev s tehničnimi sredstvi in opozoriti informacijske sisteme upravljavca (i-SCOOP, 2017).

2.2.4 Pravica do prenosljivosti podatkov (20. člen GDPR)

Pravica do prenosljivosti osebnih podatkov, ki je definirana v 20. členu GDPR, predstavlja novost tako za posameznike kot tudi za upravljavce in obdelovalce. Posameznik namreč lahko v skladu s to pravico zahteva, da gospodarske družbe zagotovijo enostaven premik, kopiranje ali prenos osebnih podatkov iz enega okolja informacijske tehnologije (v nadaljevanju IT) v drugega (Diker Vanberg & Ünver, 2017, str. 2). Ali kot je napisano v 20. členu GDPR: »Posameznik, na katerega se nanašajo osebni podatki, ima pravico, da prejme osebne podatke v zvezi z njim, ki jih je posedoval upravljavcu, v strukturirani, splošno uporabljani in strojno berljivi obliki, in pravico, da te podatke posreduje drugemu upravljavcu, ne da bi ga upravljavec, ki so mu bili osebni podatki zagotovljeni, pri tem oviral.« Kot je razvidno iz zapisanega, lahko pravico do prenosljivosti razdelimo na pravico do prejema osebnih podatkov in pravico do prenosa osebnih podatkov od enega upravljavca podatkov k drugemu. Prenos osebnih podatkov od enega upravljavca k drugemu je lahko tudi neposreden, če je to tudi tehnično izvedljivo, kar je zapisano v 2. odstavku 20. člena GDPR. Neposreden prenos se vzpostavi, ko je med dvema sistemoma možna varna komunikacija in je sistem tehnično zmožen sprejeti podatke (Diker Vanberg & Ünver, 2017, str. 2).

Pravica do prenosljivosti se uporablja le, kadar »se obdelava izvaja z avtomatiziranimi sredstvi«, kar ne vključuje večine papirnatih in fizičnih datotek. Predmet prenosljivosti vključuje edino osebne podatke posameznika in podatke, ki jih je posameznik posredoval. Anonimni podatki in podatki, ki niso povezani s posameznikom, ne spadajo v to področje (Delovna skupina za varstvo podatkov iz člena 29, 2016, str. 4). V uvodni izjavi GDPR piše, da pravica do prenosljivosti podatkov ni omejena le na spletna mesta za socialno mreženje, temveč se uporablja tudi za računalništvo v oblaku, spletne storitve, pametne sisteme in druge sisteme za avtomatsko obdelavo podatkov. Pravica do prenosljivosti podatkov velja za številna področja, kot so socialni mediji, iskalniki, shranjevanje fotografij, e-pošte ali spletne trgovine. Enako velja za banke, farmacevtske družbe, ponudnike energije, letalske prevoznike (Diker Vanberg & Ünver, 2017, str. 2).

Naloga upravljavcev bo torej zagotoviti, da se podatki posredujejo »v strukturirani, splošno uporabljani in strojno berljivi obliki« (GDPR, 20. člen). Upravljavce bi bilo treba spodbuditi, da pri izpolnjevanju zahteve za prenosljivost podatkov zagotovijo interoperabilnost oblike podatkov. Prav tako pa se posamezniku omogoči, da lahko svoje osebne podatke sam enostavno in ponovno uporablja. Posameznik lahko s tem, ko zahteva

na primer seznam stikov iz aplikacije za spletno pošto, sam sestavi seznam povabljencev za na poroko. Podobno lahko posameznik zahteva zgodovino poslušanih skladb v storitvi predvajanja glasbe, da bo lahko preveril, katero glasbo želi poslušati na drugi platformi (Delovna skupina za varstvo podatkov iz člena 29, 2016, str. 7).

Posameznik ima pravico, da se njegovi osebni podatki posredujejo drugemu upravljavcu, »ne da bi ga upravljavec, ki so mu bili osebni podatki zagotovljeni, pri tem oviral« (GDPR, 20. člen). Za ovire se tu šteje kakršno koli pravno, tehnično ali finančno oviranje ali preprečevanje in upočasnjevanje dostopa do podatkov, kot na primer zaračunavanje pristojbin, pretirano zamudo, namerno zameglitev nabora podatkov, pomanjkanje dostopa do oblike podatkov, pretirane zahteve glede standardizacije ali akreditacije (Delovna skupina za varstvo podatkov iz člena 29, 2016, str. 18).

Nova pravica do prenosljivosti podatkov predstavlja pomembno orodje, ki bo spodbudilo konkurenco med upravljavci in pomembno prispevalo k prostemu pretoku osebnih podatkov v EU. V okviru strategije za enotni digitalni trg bo tako spodbudila razvoj novih storitev in olajšala zamenjavo ponudnika storitev na trgu. Čeprav bo pravica do prenosljivosti lahko okrepila konkurenčnost storitev (lažja menjava storitev), GDPR ne ureja konkurence, ampak osebne podatke. Prenosljivost podatkov bo tako priložnost za ponovno vzpostavitev ravnovesja med upravljavci podatkov in posamezniki, na katere se nanašajo podatki. S tem se bo krepil nadzor posameznikov nad njihovimi podatki in zagotovilo, da imajo posamezniki v podatkovnem ekosistemu dejavno vlogo (Delovna skupina za varstvo podatkov iz člena 29, 2016, str. 3).

2.2.5 Pravica do ugovora (21. člen GDPR)

Posameznik ima po 21. členu GDPR pravico do ugovora obdelave osebnih podatkov v treh primerih:

- kadar se osebni podatki obdelujejo za namene neposrednega trženja – posameznik ima možnost kadar koli in brezplačno ugovarjati obdelavi podatkov;
- kadar se podatki obdelujejo v znanstveno- ali zgodovinsko-raziskovalne ali statistične namene – posameznik mora imeti razloge, ki so povezani z njegovim posebnim položajem, da lahko ugovarja obdelavi podatkov, razen »če je obdelava potrebna za opravljanje naloge, ki se izvaja zaradi razlogov javnega interesa«;
- kadar je obdelava potrebna za izvajanje nalog v javnem interesu in je obdelava potrebna zaradi zakonitih interesov upravljavca.

2.2.6 Pravice v zvezi z avtomatizirano obdelavo in profiliranjem (22. člen GDPR)

Avtomatizirana obdelava in profiliranje se dandanes uporabljata v vse več sektorjih, tako javnih kot tudi zasebnih. Bančništvo, finance, zdravstvo, obdavčenje, zavarovanje, trženje

in oglaševanje je samo nekaj področij, kjer se profiliranje uporablja na dnevni ravni in vpliva na pomembne odločitve v gospodarski družbi. Profiliranje prinaša posameznikom in gospodarskim družbam, kot tudi gospodarstvu in družbi kot celoti, prednosti, kot sta povečana učinkovitost in prihranek virov. Prav tako pa na drugi strani predstavlja veliko tveganje za posameznikove pravice in varnost. GDPR tako uvaja nove določbe za obravnavo tveganj, ki izhajajo iz profiliranja in avtomatizirane obdelave, vendar pri tem ne omejuje zasebnosti posameznika (Article 29 data protection working party, 2017a, str. 5).

Profiliranje ali oblikovanje profilov »pomeni vsako obliko avtomatizirane obdelave osebnih podatkov, ki vključuje uporabo osebnih podatkov za ocenjevanje nekaterih osebnih vidikov v zvezi s posameznikom« (4. člen GDPR). To preprosto pomeni zbiranje informacij o posamezniku ali skupini posameznikov in analiziranje njihovih lastnosti ali vedenja, da bi jih lahko kategorizirali, naredili oceno ali napoved, npr. ocenjevanje ali razvrščanje posameznikov na podlagi značilnosti, kot so njihova starost, spol in višina. Avtomatizirano odločanje ima drugačno širino in se delno prekriva/usklajuje s profiliranjem. Samo avtomatizirano odločanje pomeni zmožnost odločanja s tehnološkimi sredstvi, brez pomoči človeka. Avtomatizirano odločanje lahko vključuje profiliranje ali pa tudi ne (Article 29 data protection working party, 2017a, str. 10).

Obstajajo torej trije načini uporabe profiliranja:

- profiliranje,
- avtomatizirano odločanje na podlagi profiliranja (vključen človeški faktor),
- avtomatizirano odločanje na podlagi profiliranja (ni vključen človeški faktor).

Če povzamemo 22. člen GDPR, obstaja torej prepoved popolnega avtomatiziranega individualnega odločanja, vključno s profiliranjem, ki ima pravni ali podoben učinek, za katero obstajajo izjeme (ko je to potrebno za sklenitev ali izvedbo pogodbe, ko ima upravljavec izrecno privolitev posameznika in ko je to dovoljeno z zakonodajo EU ali državo članico). Za popolno avtomatizirano odločanje morajo obstajati legitimen interes in ukrepi za zaščito pravic in svoboščin posameznikov, na katere se podatki nanašajo.

Ko upravljavec izvaja avtomatizirano odločanje s profiliranjem, je le-ta na podlagi pravice o informiranosti in seznanitvi posamezniku dolžan sporočiti in zagotoviti informacije o uporabljeni logiki ter pojasniti in sporočiti namen in posledice predvidene obdelave. Vse te informacije morajo biti podane posamezniku pred obdelavo osebnih podatkov (Article 29 data protection working party, 2017a, str. 13), kar pomeni, da mora upravljavec izrecno in jasno navesti, da bo osebne podatke avtomatizirano profiliral.

2.3 Obveznosti obdelovalcev in upravljavcev

GDPR prinaša velike spremembe na področju obveznosti posrednikov – torej upravljavcev in obdelovalcev podatkov. V Direktivi je bil upravljavec podatkov opredeljen kot oseba ali

subjekt, ki določi namene ali sredstva obdelave osebnih podatkov, obdelovalec pa je opredeljen kot oseba ali subjekt, ki zgolj izvršuje obdelavo podatkov v imenu upravljavca podatkov. Le upravljavec je tako nosil obveznosti in odgovornost za kršitve. Ta razmejitev v odgovornosti je bila v preteklih letih močno problematična, še posebej pri vedno bolj zapletenih odnosih obdelave podatkov, saj ni bilo vedno jasno, kdo določi, če in kako se podatki obdelujejo, nekateri akterji pa so se lahko izognili odgovornosti za svoja dejanja z uporabo zakonskih vrzeli (Burri & Schär, 2016, str. 493).

GDPR tako pomembno razlikuje med upravljavcem in obdelovalcem ter uvaja obveznosti obeh. Razlikovanje uporablja pragmatično, saj GDPR dopušča skupne, večkratne in soupravljavce. Upravljavci so na splošno izpostavljeni večjemu bremenu, saj so odgovorni za zagotavljanje, da je obdelava podatkov v skladu z določbami uredbe in ima obveznost dokazovanja skladnosti. Glavna razlika med upravljavcem in obdelovalcem je navedena v 4. členu GDPR. Upravljavec pomeni fizično ali pravno osebo, javni organ, agencijo ali drugo telo, ki določa namene in sredstva obdelave, medtem ko obdelovalec samo obdeluje osebne podatke v imenu in po navodilih upravljavca.

Upravljavec mora biti po 1. odstavku 24. člena GDPR venomer zmožen dokazati, da obdelava osebnih podatkov poteka v skladu z GDPR, ob tem pa mora upoštevati okoliščine, namene, obseg in naravo obdelave ter tveganja za pravice in svoboščine posameznika. Dokazovanje izpolnjevanja obveznosti lahko upravljavec dokaže z zavezanostjo k odobrenim kodeksom ravnanja (40. člen GDPR) ali s potrjevanjem (42. člen GDPR). Spoštovanje kodeksov ravnanja in certifikacijskih shem gospodarskim družbam prinaša številne koristi, ki dokazujejo, da so skladne z GDPR. Preden upravljavec odda v obdelavo osebne podatke obdelovalcu, bo morda želel proučiti, ali ima pridobljen certifikat in ali je zavezan k določenemu kodeksu ravnanja. Certificiranje in kodeksi ne zmanjšujejo odgovornosti za varstvo osebnih podatkov upravljavcev ali obdelovalcev (Information Commissioner's Office United Kingdom, brez datuma).

Kodeksi ravnanja (40. člen GDPR) prispevajo k pravilni uporabi GDPR, ob upoštevanju specifik sektorja in posebnih potreb različno velikih podjetij. S strani držav članic in nadzornih organov je spodbudno pripravljati kodekse ravnanja z namenom podrobne obrazložitve uporabe GDPR. Le-ti lahko vključujejo obrazložitve poštene in pregledne obdelave, zakonitih interesov, za katere si prizadevajo upravljavci v posebnih okoliščinah, psevdonimizacijo osebnih podatkov, odgovornosti upravljavcev, uradno obveščanje nadzornih organov itd. Ko bodo združenja pripravila kodekse, se bodo gospodarske družbe, predvsem mikro, mala in srednja, zavezala k njihovi uporabi in s tem omogočila izvajanje obveznega sprotnega spremljanja skladnosti. Spoštovanje kodeksov ravnanja lahko služi kot olajševalna okoliščina, v kolikor nadzorni organ obravnava izvršilne ukrepe z upravno globo (Information Commissioner's Office United Kingdom, brez datuma).

Poleg kodeksov ravnanja so tu tudi certifikati (42. člen GDPR), ki igrajo pomembno vlogo pri omogočanju doseganja in dokazovanja odgovornosti ter, natančneje, skladnosti z

GDPR za nekatere ali vse njihove storitve, dejavnosti ali izdelke. Posamezniki bodo tako lažje in hitreje ocenili raven varstva podatkov za določen izdelek ali storitev. Predstavljajo resnične koristi za vse zainteresirane strani, še posebej za posameznike. Certifikate je treba obravnavati kot eno od številnih orodij za gospodarske družbe, ki pomaga gospodarskim družbam pri zagotavljanju učinkovitega varstva za posameznike. Vsak certifikat bo lahko veljal največ tri leta in se bo pod enakimi pogoji tudi podaljšal (7. odstavek 42. člena GDPR). Gospodarska družba ga lahko prekliče, če ne izpolnjuje več zahtev, in o tem obvesti nadzorni organ, vendar pa v tem primeru tvega naložitev glob. Certifikat lahko izdajo nadzorni organi za potrjevanje iz 43. člena GDPR ali strokoven in neodvisen organ za potrjevanje, ki ima pooblastilo s strani nacionalnega nadzornega organa (Centre for Information Policy Leadership at Hunton Andrews Kurth LLP – v nadaljevanju CIPL, 2017a, str. 3, 4).

V GDPR je na novo razširjena ozemeljska veljavnost uredbe in posledično obdelave osebnih podatkov upravljavcev in obdelovalcev. GDPR svojo pozornost preusmerja na posameznika. Direktiva je omejila varstvo osebnih podatkov na ozemlje vsake države članice posebej, GDPR pa v 3. členu določa ozemeljsko uporabnost za upravljavce in obdelovalce, ne glede na to, ali obdelava poteka v EU. Torej, če obdelovalec ali upravljavec nima sedeža v EU in je dejavnost obdelave povezana z nudenjem blaga ali storitev posamezniku, ki se nahaja v EU, ali s spremljanjem vedenja posameznika, ki poteka v EU, kot je zapisano v 2. odstavku 3. člena GDPR, sta skladnost in upoštevanje GDPR nujna. Kadar pa dejavnost obdelave poteka zunaj področja uporabe prava EU, ta uredba ni aplikativna (Voigt & Bussche, 2017, str. 9–12).

Po 1. odstavku 28. člena GDPR lahko upravljavec najame obdelovalca, »ki zagotovi zadostna jamstva za izvedbo ustreznih tehničnih in organizacijskih ukrepov na tak način, da obdelava izpolnjuje zahteve iz te uredbe in zagotavlja varstvo pravic posameznika«. Obdelavo mora po 3. odstavku 28. člena GDPR s strani obdelovalca urejati pogodba oziroma sporazum o obdelavi podatkov, v kateri so navedene obveznosti obdelovalca do upravljavca z vsebino, trajanjem, naravo in namenom obdelave, vrsto osebnih podatkov, kategorijo posameznikov ter obveznosti in pravice upravljavca. Obdelovalci morajo obdelovati osebne podatke v skladu z navodili upravljavca. Le-ta pa je dolžan povedati upravljavcu, če meni, da je navodilo za obdelavo osebnih podatkov v nasprotju z GDPR ali katero koli drugo zakonodajo EU.

Tako obdelovalci kot tudi upravljavci morajo izvajati ustrezne varnostne ukrepe. Varnostni ukrepi se razlikujejo glede na občutljivost osebnih podatkov, ki jih obdelujejo, tveganje za posameznike, ki je povezano s kakršno koli kršitvijo varnosti, najsodobnejšimi tehnologijami, naravo obdelave in stroški izvajanja. Ukrepi lahko vključujejo ali psevdonimizacijo ali šifriranje. Prav tako je pomembno redno spremljanje in preverjanje učinkovitosti varnostnih ukrepov. Takoj ko obdelovalec ugotovi, da je prišlo do kršitve varstva osebnih podatkov, morajo brez nepotrebnega odlašanja obvestiti upravljavca (Taylor Wessing, 2016c).

Poleg pogodbenih obveznosti do upravljavca ima obdelovalec v skladu z GDPR naslednje neposredne odgovornosti (Inside Privacy, 2017):

- ne sme imenovati soobdelovalca brez predhodnega pisnega pooblastila upravljavca;
- sodelovati mora z nadzornim organom;
- brez nepotrebnega odlašanja obvestiti upravljavca o kršitvi osebnih podatkov;
- zagotavljati varno obdelavo osebnih podatkov;
- voditi evidenco dejavnosti obdelave;
- zaposliti DPO (v kolikor ustreza kriterijem).

Če ne izpolnjuje navedenih obveznosti, posebej določenih za obdelovalce, določenih v pogodbi med upravljavcem in obdelovalcem, ali pa je deloval zunaj ali v nasprotju z zakonitimi navodili upravljavca, je obdelovalec lahko v sodnem postopku in plača kazen. Če so posamezniki, na katere se podatki nanašajo, utrpeli materialno ali nematerialno škodo, lahko zaradi kršitve GDPR ukrepajo in zahtevajo odškodnino od obdelovalca (Inside Privacy, 2017).

Obdelovalec lahko zaposli drugega obdelovalca s pisnim dovoljenjem upravljavca, vendar pa zanj veljajo enake obveznosti varstva podatkov, kot so določene v pogodbi s prvim obdelovalcem. Drugi obdelovalec je lahko ponudnik gostovanja, računovodski servis, klicni center, oblačne in druge IT-storitve. Kadar drugi obdelovalec ne izpolnjuje obveznosti iz pogodbe, prvi obdelovalec v celoti prevzame obveznosti drugega obdelovalca (Taylor Wessing, 2016c).

Upravljavci, obdelovalci in drugi posredniki morajo po 30. členu GDPR voditi evidenco dejavnosti obdelave oz. kataloge. DPO ni tista, ki je odgovorna za vodenje evidence, lahko pa ji upravljavec dodeli nalogo vodenja evidence v okviru odgovornosti upravljavca. Vodena mora biti v pisni ali elektronski obliki. Nadzorni organ lahko kadar koli zahteva dostop do evidence. Evidenca dejavnosti mora vsebovati: kontaktne podatke upravljavca, namen obdelave, opis kategorij in vrsto osebnih podatkov, možne predvidene roke za izbris podatkov, možen splošni opis varnostnih ukrepov. Izjema obstaja za gospodarske družbe, ki imajo manj kot 250 zaposlenih, razen če obstaja veliko tveganje za pravice in svoboščine posameznika ali ko obdelava vključuje posebne vrste osebnih podatkov (Taylor Wessing, 2016c). Po mnenju Delovne skupine za varstvo podatkov iz člena 29 (2017b, str. 21) bi morale evidence predstavljati eno od ključnih orodij k spremljanju skladnosti z GDPR ter obveščanju in svetovanju upravljavcu ali obdelovalcu.

2.3.1 Ocena učinka na varstvo osebnih podatkov

Ključni del zagotavljanja skladnosti z GDPR, kadar se obdelujejo podatki z velikim tveganjem, predstavlja DPIA, saj predstavlja najpomembnejši instrument zagotavljanja in doseganja načela odgovornosti. Z oceno učinka upravljavci zagotavljajo, da se sistematično in zavestno ocenjevanje tveganja obdelave osebnih podatkov posameznika

uporablja pri zbiranju, uporabi in razkrivanju osebnih podatkov. DPIA pomaga gospodarskim družbam prepoznavati tveganja, predvidevati probleme in predlagati rešitve (Cerasaro, 2017, str. 222, 223).

Delovna skupina za varstvo podatkov iz člena 29 (2017a, str. 10–12) je na podlagi 35. člena sestavila niz devetih meril, za katere se po njihovem mnenju zahteva DPIA zaradi velikega tveganja:

- evalvacija in razvrščanje posameznikov (vključno s profiliranjem in napovedovanjem);
- avtomatizirano odločanje, ki ima pravne ali podobno pomembne učinke;
- sistematični nadzor;
- občutljivi ali zelo osebni podatki;
- podatki, ki jih obdelujejo v velikem obsegu;
- usklajeni ali združeni nabori podatkov;
- podatki o ranljivih posameznikih, na katere se nanašajo osebni podatki;
- inovativna uporaba ali uporaba novih tehnoloških ali organizacijskih rešitev;
- kadar sama obdelava posameznikom preprečuje uresničevanje pravice ali uporabo storitve ali pogodbe.

Več meril kot obdelava izpolnjuje, večja bo verjetnost, da obdelava pomeni veliko tveganje, zato je zanj potrebna DPIA. V večini primerov je priporočljiva izvedba ocene učinka, če obdelava izpolnjuje dve prej napisani merili. V primerih, ko se upravljavec odloči, da kljub izpolnjevanju naštetih dejanj obdelave ne bo opravil ocene učinka, utemelji in dokumentira razloge za neizvedbo ocene ter priloži stališče DPO. Med zelo veliko tveganje lahko štejemo nezakonit dostop do podatkov, zaradi katerega je posameznik v finančnih težavah ali odpuščen (posameznika doletijo nepopravljive posledice, ki jih ne more odpraviti), ali kadar ni mogoče zmanjšati števila oseb, ki imajo dostop do podatkov, zaradi njihove izmenjave, razširjanja ali uporabe (ko je očitno, da se navedeno tveganje uresniči). V GDPR ni napisano, kakšne postopke je treba izvesti za oceno učinka, pač pa le-te lahko določijo upravljavci sami ali pa uporabijo že obstoječe okvire (okviri EU, ki se nanašajo na posamezne panoge, ali generični okviri EU) (Delovna skupina za varstvo podatkov iz člena 29, 2017a, str. 12, 22, 24).

Izvedba učinka na varstvo osebnih podatkov ni obvezna pred vsakim dejanjem obdelave, pač pa le, kadar je verjetno, da bo vrsta obdelave povzročila veliko tveganje za pravice in svoboščine posameznikov, kar v praksi pomeni, da mora za vsako obdelavo podatkov najprej opredeliti kontekst obdelave, kjer navede: namene obdelave, nabor podatkov, način pridobivanja podatkov, rok hrambe itd. Na podlagi konteksta družba oceni tveganje, kar je treba določiti za čisto vsako obdelavo podatkov. Na tej točki je nato za vsa visoka tveganja potreben tudi ukrep za obvladovanje tveganja. S tem, ko gospodarska družba uspešno izvede oceno, pravočasno identificira, odpravi, zmanjša ali sprejme tveganja in se izogne kršitvam zakonodaje, ki lahko vodijo v stroške, ki pridejo z neskladnostjo (izrek glob, uvedba inšpekcijskih postopkov), ter posredno tudi negativnemu medijskemu poročanju in

izgubi ugleda in zaupanja s strani posameznikov in javnosti (Informacijski pooblaščenec, 2017b, str. 21–25, 32–34).

DPIA je stalen proces in ne enkratno dejanje, kar je razvidno tudi s slike 1. GDPR določa minimalne značilnosti ocene učinka v 7. odstavku 35. člena GDPR. Vključuje naj opis predvidenih dejanj in namenov obdelave, oceno potrebnosti in sorazmernosti dejanj obdelave, oceno tveganj za pravice in svoboščine posameznikov ter ukrepe tako za obvladovanje tveganj kot za dokazovanje skladnosti z GDPR (Delovna skupina za varstvo podatkov iz člena 29, 2017a, str. 19).

Slika 1: Generični prikaz izvajanja ocene učinka

Vir: Delovna skupina za varstvo podatkov iz člena 29 (2017a).

Oceno učinka v zvezi z varstvom podatkov mora zagotoviti upravljavec. Pri tem mora za mnenje zaprositi tudi DPO, ki pa je med drugim zadolžena za nadziranje izvajanja ocene učinka. Kadar je imenovan obdelovalec, mora le-ta pomagati upravljavcu pri izvedbi ocene in zagotoviti vse potrebne informacije. V posebnih primerih lahko upravljavec za mnenje zaprosi posameznika, na katerega se osebni podatki nanašajo. Skladno z načeloma vgrajenega in privzetega varstva mora biti DPIA izvedena pred obdelavo podatkov (Delovna skupina za varstvo podatkov iz člena 29, 2017a, str. 16, 17).

S tem, ko upravljavec analizira tveganje, pripravi ukrepe za zmanjšanje tveganja, dokaže skladnost z GDPR. Možni ukrepi za zmanjšanje tveganja so: psevdonimizacija, šifriranje, uporaba načela najmanjšega obsega podatkov in nekateri mehanizmi nadzora (Delovna skupina za varstvo podatkov iz člena 29, 2017a, str. 4).

Psevdonimizacija omogoča obdelavo podatkov, ki niso anonimni ali neposredno identificirani. S tem postopkom ločimo podatke od neposrednih identifikatorjev, tako da povezava z identiteto ni mogoča brez dodatnih informacij, ki se hranijo ločeno. Psevdonimizacija nam lahko olajša obdelavo osebnih podatkov po izvirnih zbirkah, je pomemben zaščitni ukrep za obdelavo osebnih podatkov v znanstvene, zgodovinske in statistične namene. Predstavlja osrednjo značilnost vgrajenega varstva osebnih podatkov. GDPR spodbuja upravljavce k sprejetju kodeksov ravnanja, ki spodbujajo psevdonimizacijo. Pomembno razlikovanje med psevdonimizacijo in anonimizacija je v tem, ali so podatki lahko ponovno identificirani. Pri anonimiziranih podatkih le-to ni več mogoče, medtem ko so podatki pri psevdonimizaciji lahko ponovno prepoznavni, če jih povežemo. GDPR uvaja nov koncept, kjer psevdonimizacija predstavlja sredstvo za zaščito pravic posameznikov in obenem omogoča upravljavcem, da izkoristijo in uporabijo podatke. Šifriranje predstavlja proces kodiranja informacij ali sporočil, kjer lahko do njega dostopajo le tisti, ki imajo dodeljen dostop. Navedeni ukrepi niso nujno ustrezni ukrepi, vendar je odvisno od primera do primera, predvsem pa od okoliščin in tveganj, ki so značilne za posamezno dejanje obdelave (International Association of Privacy Professionals – v nadaljevanju IAPP, 2016).

2.3.2 Vgrajeno in privzeto varstvo osebnih podatkov

25. člen GDPR pravi, da mora upravljavec ob upoštevanju vseh stroškov, narave, obsega in namena obdelave, tveganj, ki so povezani s pravicami, ter tehnološkega razvoja izvajati ustrezne tehnične in organizacijske ukrepe ter v obdelavo vključiti primerne varovalke, da zagotovi in je zmožen dokazati, da obdelava osebnih podatkov poteka v skladu z GDPR. Le-to pa doseže z vgrajenim in privzetim varstvom podatkov. Z implementacijo vgrajenega in privzetega varstva osebnih podatkov gospodarska družba omogoča: zbiranje osebnih podatkov samo za določen namen, podatke, ki so zbrani samo za določen namen, je nato mogoče obdelati, podatke, ki jih upravljavec ne potrebuje več, je treba izbrisati ter fizičnim osebam je omogočeno, da zavrnejo zbiranje, shranjevanje, obdelavo ali brisanje svojih podatkov (Imperva Inc., 2017).

Gospodarske družbe morajo pri privzetem varstvu podatkov zagotoviti najvišjo raven varstva osebnih podatkov že v samem začetku, pri privzetih, začetnih nastavitvah. Obveznost privzetega varstva velja tako za količino zbranih osebnih podatkov posameznika kot tudi za obseg in obdobje njihovega shranjevanja in dostopnosti. Takšni ukrepi morajo biti zagotovljeni zlasti zaradi tega, da ne bodo samodejno dostopni nedoločenemu številu posameznikov. Temeljna načela, ki podpirajo privzeto varstvo podatkov, so omejitev namena, omejitev shranjevanja, najmanjši obseg podatkov. Primer privzetega varstva podatkov predstavlja platforma socialnih medijev, ki nastavi nastavitve uporabnika v najbolj zaščitenem okolju. Tako na primer družbeno omrežje Instagram že od začetka uporabe omejuje dostopnost profila uporabnika, kar pomeni, da ima uporabnik, ko

se registrira v omrežje, profil zaprt. Profil si lahko uporabnik odklene šele sam (Taylor Wessing, 2016b).

Vgrajeno varstvo podatkov je večplasten koncept, ki je v pravnih dokumentih na eni strani opisan kot načelo, na drugi strani pa ga računalniški znanstveniki in inženirji pogosto enačijo z uporabo posebnih tehnologij za izboljšanje zasebnosti (npr. šifriranj, protokolov za anonimne komunikacije, zasebnega iskanja baz podatkov, poverilnic, ki temeljijo na datumu). Z uporabo teh tehnologij se tveganje za informacijsko zasebnost posameznikov zmanjša, upravljavci pa lažje izpolnjujejo obveznosti varovanja podatkov. Vendar pa zasebnost ni zbirka načel v pravnem dokumentu niti tehnologija za izboljševanje zasebnosti, pač pa gre za proces, ki vključuje tehnološke in organizacijske komponente, ki izvajajo načela zasebnosti in varstva osebnih podatkov (Taylor Wessing, 2016b). Vgrajeno varstvo podatkov mora biti vključeno v zasnovo in arhitekturo IT-sistemov in poslovnih praks. S tem zasebnost postane bistveni element funkcionalnosti gospodarske družbe. Zasebnost je tako vključena v tehnologije, operacije in informacijsko arhitekturo na celovit, integrativen in ustvarjalen način:

- celovit način, ker je treba razmisliti o dodatnih, širših kontekstih;
- integrativen način, ker se je treba posvetovati z vsemi deležniki, zainteresiranimi stranmi in interesi;
- ustvarjalen način, ker vključevanje zasebnosti v procese včasih pomeni ponovno izumljanje obstoječih izbir, ker so nekatere alternative nesprejemljive.

Primer vgrajenega varstva osebnih podatkov predstavljata psevdonimizacija, ko upravljavec nadomešča osebno prepoznavni material z umetnimi identifikatorji, in šifriranje, ko upravljavec kodira sporočila, tako da jih lahko preberejo le pooblaščeni posamezniki (Cavoukian, 2009).

2.3.3 Pooblaščena oseba za varstvo osebnih podatkov

DPO predstavlja eno izmed ključnih novosti v GDPR. Informacijski pooblaščenec (v nadaljevanju IP) ocenjuje DPO kot pomemben element novega temeljnega načela odgovornosti, saj pripomore k odgovornemu ravnanju z osebnimi podatki s ciljem izogibanja kršitvam in k proaktivnemu varovanju osebnih podatkov (Informacijski pooblaščenec, 2017a). Praksa DPOjev se je z leti že razvila, predvsem v večjih gospodarskih družbah, ki se zavedajo pomembnosti varstva osebnih podatkov.

DPO predstavlja osebo, ki izvaja svetovalne in nadzorne naloge na področju varstva osebnih podatkov v gospodarski družbi. Ta oseba mora dosegati določeno strokovno znanje in spretnosti. Imeti mora poklicne odlike, znanje s področja prava o varstvu osebnih podatkov, poznati mora zadevne prakse in imeti zmožnost izpolnjevanja doseljenih nalog (Delovna skupina za varstvo podatkov iz člena 29, 2017b, str. 13). Po mnenju IP vodje finančnih, kadrovskih, pravnih, trženjskih ali IT-oddelkov niso primerne osebe za DPO, saj

so velikokrat vključene in vpete v procesne obdelave in opredeljujejo namene ali storitve obdelave osebnih podatkov. Primerni DPO so njihovi strokovni sodelavci, če le ne določajo in opredeljujejo namena obdelave osebnih podatkov. V kolikor je DPO imenovana znotraj gospodarske družbe, mora delovati neodvisno, prav tako pa ne sme prihajati do konflikta interesov. DPO je lahko neodvisen posameznik ali neodvisen kolegijski organ (sestavljen iz več posameznikov). Le-ta predstavlja razpršeno vlogo DPO, kjer je pomembno, da se imenuje glavnega, vodjo DPO, se določi njegove naloge in naloge ostalih, pri tem pa je pomembno, da se poskrbi, da v izvajanje nalog ni vpet zgolj en posameznik. V kolikor gospodarska družba ne najde primernega kandidata za DPO med zaposlenimi, lahko funkcijo izvaja nekdo zunanji na podlagi storitvene pogodbe (Informacijski pooblaščenec, 2017a).

Imenovanje enega DPO za več gospodarskih družb je po 2. odstavku 35. člena GDPR dovoljeno, v kolikor je oseba »dostopna iz vsake enote«. To je mišljeno predvsem za javne organe ali zavode, pri čemer je treba upoštevati organizacijsko strukturo in velikost gospodarske družbe.

Imenovanje DPO je potrebno tako za upravljavca kot tudi obdelovalca glede na to, kdo izpolnjuje merila iz 1. odstavka 37. člena GDPR. V nekaterih primerih bo potrebno imenovanje DPO obema ali samo enemu. Če upravljavec imenuje DPO, ga ni nujno treba imenovati tudi njenemu obdelovalcu (Delovna skupina za varstvo podatkov iz člena 29, 2017b, str. 11). V skladu s 1. odstavkom 37. člena GDPR je treba imenovati DPO vedno:

- kadar obdelavo opravlja javni organ ali telo, razen sodišč (to so šole, javni zavodi, javna uprava …);
- kadar temeljne dejavnosti upravljavca ali obdelovalca zajemajo dejanja obdelave osebnih podatkov;
- kadar temeljne dejavnosti upravljavca ali obdelovalca zajemajo obsežno obdelavo posebnih vrst podatkov ali osebnih podatkov v zvezi s kazenskimi obsodbami in prekrški (zdravstveni sektor, finančni sektor, policija).

Treba je opozoriti, da lahko naloge v javnem interesu opravljajo fizične ali pravne osebe tako javnega kot zasebnega prava, kot so na primer storitve javnega prevoza, cestna infrastruktura, oskrba z vodo in energijo. V tem primeru je tako obvezno imenovanje DPO (Delovna skupina za varstvo podatkov iz člena 29, 2017b, str. 7).

Delovna skupina za varstvo podatkov iz člena 29 (2017b, str. 8) opozarja na termin »temeljne dejavnosti«, saj le-ta ne sme izključevati dejavnosti, pri katerih je obdelava osebnih podatkov neločljiv del dejavnosti upravljavca. Kot primer navaja zasebno varnostno službo, ki varuje zasebna nakupovalna središča in katere temeljna dejavnost je nadzor. Nadzor pa je neločljivo povezan s samo obdelavo osebnih podatkov, zato mora zasebna varnostna služba imenovati DPO. Podobno navaja zdravstvene domove, saj je

njihova temeljna dejavnost zagotavljanja zdravstvenega varstva neločljivo povezana z obdelavo zdravstvene dokumentacije bolnikov.

Glavne naloge DPO, opredeljene v 1. odstavku 39. člena GDPR, so (Delovna skupina za varstvo podatkov iz člena 29, 2017b, str. 5, 20, 27):

- **obveščanje upravljavca, obdelovalca in zaposlenih, ki izvajajo obdelavo, ter svetovanje o obveznostih glede GDPR**;
- **spremljanje skladnosti z GDPR:** DPO ni osebno odgovorna za zagotavljanje skladnosti z določbami iz GDPR, kar je tudi jasno napisano v 1. odstavku 24. člena GDPR. Ključna naloga upravljavca in obdelovalca je torej omogočanje učinkovitega opravljanja nalog DPO in zagotovitev zadostne neodvisnosti in sredstev za učinkovito izvajanje nalog. Zagotavljanje skladnosti je torej naloga upravljavca, naloga DPO pa je pomoč pri spremljanju notranje skladnosti z GDPR. DPO tako zbirajo informacije za opredelitev dejavnosti obdelave, analizirajo in preverjajo skladnost ter obveščajo upravljavca ali obdelovalca, mu svetujejo in pripravljajo priporočila. Za lažje spremljanje skladnosti oblikuje popise in vodi register dejanj obdelave na podlagi informacij, ki so jih pridobile od gospodarskih družb;
- **vloga pri DPIA:** DPIA je naloga upravljavca. Koristno in pomembno vlogo pa ima pri tem tudi DPO, saj mora v okviru nalog zagotavljati pomoč ali podati mnenje, v kolikor zanj zaprosi upravljavec. DPO tako poda mnenje upravljavcu, ali naj izvede oceno učinka, katero metodologijo naj uporabi pri ocenjevanju, kateri zaščitni ukrepi bodo potrebni in ali je bila DPIA pravilna ter kakšne so ugotovitve;
- **sodelovanje z nadzornim organom in delovanje kot kontaktna točka za nadzorni organ:** s tem, ko DPO deluje kot kontaktna točka, nadzornemu organu olajša dostop do dokumentov in informacij za izvajanje nalog iz 57. člena GDPR ter izvaja preiskovalna in popravljalna pooblastila in pooblastila v zvezi z dovoljenji in svetovalnimi pristojnostmi iz 58. člena GDPR.

Pri izvajanju nalog mora upoštevati tveganje. »Od DPO v bistvu zahteva, da prednostno razvrstijo svoje dejavnosti in svoja prizadevanja usmerijo v vprašanja, ki povzročajo večja tveganja v zvezi z varstvom podatkov. To ne pomeni, da bi morale zanemariti spremljanje skladnosti dejanj obdelave podatkov, ki so povezana s primerljivo nižjo ravnjo tveganja, temveč, da bi se morale osredotočiti predvsem na področja z večjim tveganjem« (Delovna skupina za varstvo podatkov iz člena 29, 2017b, str. 21).

DPO lahko po 5. odstavku 38. člena GDPR »opravlja druge naloge in dolžnosti«, vendar pri tem »zaradi vsakršnih takih nalog in dolžnosti ne pride do nasprotja interesov«. To namreč pomeni, da oseba ne sme zavzemati položaja v gospodarski družbi, ki lahko določa sredstva in namen obdelave osebnih podatkov (Delovna skupina za varstvo podatkov iz člena 29, 2017b, str. 18).

2.3.4 Kršitev varstva osebnih podatkov

GDPR v 4. členu definira kršitev varstva osebnih podatkov kot naključno ali nezakonito uničenje, izgubo, spremembo, nepooblaščeno razkritje ali dostop do osebnih podatkov, ki se prenašajo, shranjujejo ali kako drugače obdelujejo. Ključno pri tem je, da je upravljavec sposoben prepoznati in preprečiti kršitve ter ko je to potrebno, reagirati v doglednem času (CIPL, 2017b, str. 4).

Delovna skupina za varstvo podatkov iz člena 29 (2017b, str. 6) je pojasnila, da lahko kršitev varstva podatkov kategoriziramo v skladu z naslednjimi načeli:

- kršitev zaupnosti – nepooblaščeno in naključno razkritje ali dostop do osebnih podatkov;
- kršitev celovitosti – nedovoljeno ali naključno spreminjanje osebnih podatkov;
- kršitev razpoložljivosti – nedovoljena ali naključna izguba dostopa do osebnih podatkov ali njihovo uničenje.

Pri tem je treba opozoriti, da je lahko posamezna kršitev, na primer kršitev zaupnosti in celovitosti, kombinacija vseh treh načel ali pa samo enega. Prav tako gre za kršitev razpoložljivosti osebnih podatkov, ko gre samo za začasno izgubo podatkov ali nedostopnost le-teh. Takšne kršitve ni treba prijaviti nadzornemu organu, razen ko bo v danih okoliščinah to pomenilo veliko tveganje za pravico posameznika (Article 29 data protection working party, 2017b, str. 6).

Smernice delovne skupine ločijo med incidenti in kršitvami varovanja osebnih podatkov. Kršitev varovanja osebnih podatkov bo vedno varnostni incident, vendar vsi incidenti ne bodo kršili varovanja osebnih podatkov. GDPR zahteva, da upravljavci vodijo evidenco o kakršnih koli kršitvah osebnih podatkov, ne glede na to, ali je bilo treba kršitev priglasiti ali ne. Zapisi morajo vsebovati podrobnosti o kršitvah, njenih učinkih in posledicah ter morebitnih ukrepih. Delovna skupina predlaga, da se dokumentirajo tudi razlogi za primer, ko se kršitev ne sporoči nadzornemu organu ali posamezniku (Article 29 data protection working party, 2017b, str. 19–22).

2.3.4.1 Obvestilo o kršitvi varstva osebnih podatkov

V 1. odstavku 33. člena GDPR je zapisano, da mora upravljavec obvestiti pristojni nadzorni organ o kršitvi, ko gre za ogrožene pravice in svoboščine posameznikov. Obvestilo mora biti podano v roku 72 ur od seznanitve s kršitvijo. Delovna skupina za varstvo podatkov iz člena 29 (2017b, str. 9) definira »seznanitev« kot razumno stopnjo gotovosti, da se je zgodila kršitev, ki bo privedla do ogrožanja pravic. V nekaterih primerih bo že od samega začetka jasno, da je prišlo do kršitve, v drugih pa lahko traja nekaj časa, da se ugotovi, ali so bili podatki ogroženi. Obvestilo o kršitvi mora vsebovati opis narave kršitve, vključno s številom prizadetih posameznikov in vrsto kršitve, kontaktne podatke

DPOja, verjetne posledice in ukrepe, ki jih je sprejel upravljavec. Kadar upravljavec sam pri sebi zazna kršitev, mora samoprijaviti kršitev nadzornemu organu. Kadar upravljavec dodeli obdelovalca, mora le-ta, ko zazna kršitev varstva osebnih podatkov, brez nepotrebnega odlašanja obsvetiti upravljavca (Information Commissioner's Office United Kingdom, 2017a).

Upravljavec mora imeti vzpostavljene dobre notranje procese, s katerimi lahko odkrije in obravnava kršitev. Na primer za ugotavljanje nepravilnosti pri obdelavi podatkov lahko upravljavec ali obdelovalec uporabi nekatere tehnične ukrepe, kot je analiza toka podatkov ali analiza vnosov, iz katerih je mogoče določiti dogodke in opozorila, ki so povezana z vsemi podatki. Pomembno je, da se ob odkritju kršitve poroča nadrejenim po managerski lestvici in ustreznemu nadzornemu organu in/ali prizadetemu posamezniku. Kadar kršitev vpliva na posameznike v več kot eni državi članici, mora upravljavec obvestiti svoj vodilni nadzorni organ. Lahko poroča tudi nadzornemu organu v državi članici, v kateri so bili prizadeti posamezniki. V okoliščinah, v katerih je jasno, da je prišlo do kršitve, vendar upravljavec ni zbral vseh zahtevanih informacij, da bi lahko v ustreznih okoliščinah podal obvestilo nadzornemu organu, je dovoljeno uradno obvestilo podati kasneje ali v fazah (Article 29 data protection working party, 2017b, str. 19).

2.3.4.2 Sporočilo upravljavca posamezniku

V nekaterih primerih je treba poleg obvestila nadzornemu organu kršitev sporočiti tudi prizadetemu posamezniku. 1. odstavek 34. člena GDPR pravi: »Kadar je verjetno, da kršitev varstva osebnih podatkov povzroči veliko tveganje za pravice in svoboščine posameznikov, upravljavec brez nepotrebnega odlašanja sporoči posamezniku, na katerega se nanašajo osebni podatki, da je prišlo do kršitve varstva osebnih podatkov.«

Veliko tveganje za pravice in svoboščine posameznikov pomeni, da lahko kršitev povzroči fizično, materialno ali nepremoženjsko škodo za posameznike, kot so:

- diskriminacija,
- kraja identitete ali goljufija,
- finančna izguba,
- škoda na ugledu.

Posameznik mora biti tako obveščen o kršitvi čim prej, sporočilo pa mora vsebovati korake, ki jih posameznik mora sprejeti, da se zaščiti (npr. spremeniti geslo). Sporočilo mora biti napisano v jasnem in preprostem jeziku, vsebovati pa mora opis narave kršitve, kontaktne podatke DPO, verjetne posledice in ukrepe, ki jih je sprejel ali predlagal upravljavec (Article 29 data protection working party, 2017b, str. 17). 1. odstavek 82. člena GDPR pravi: »Vsak posameznik, ki je utrpel premoženjsko ali nepremoženjsko škodo kot posledico kršitve te uredbe, ima pravico, da od upravljavca ali obdelovalca dobi odškodnino za nastalo škodo.«

Obstajajo izjeme, ko upravljavcu ni treba obvestiti prizadetega posameznika, in sicer ko (Information Commissioner's Office United Kingdom, 2017a):

- upravljavec uporabi ustrezne tehnične in organizacijske ukrepe za zaščito podatkov pred kršitvijo (npr. šifriranje prenosnika ali USB-ključka);
- takoj po kršitvi upravljavec sprejme ukrepe, ki bodo zagotovili, da se večje tveganje za posameznike ne bo več uresničilo (npr. upravljavec odpusti zaposlenega, ki je povzročil izgubo osebnih podatkov);
- kadar je za sporočilo posamezniku potreben zelo velik napor, na primer, ko so bili podatki posameznika izgubljeni zaradi kršitve. V tem primeru je treba kršitev sporočiti javno.

2.3.4.3 Naložitev glob

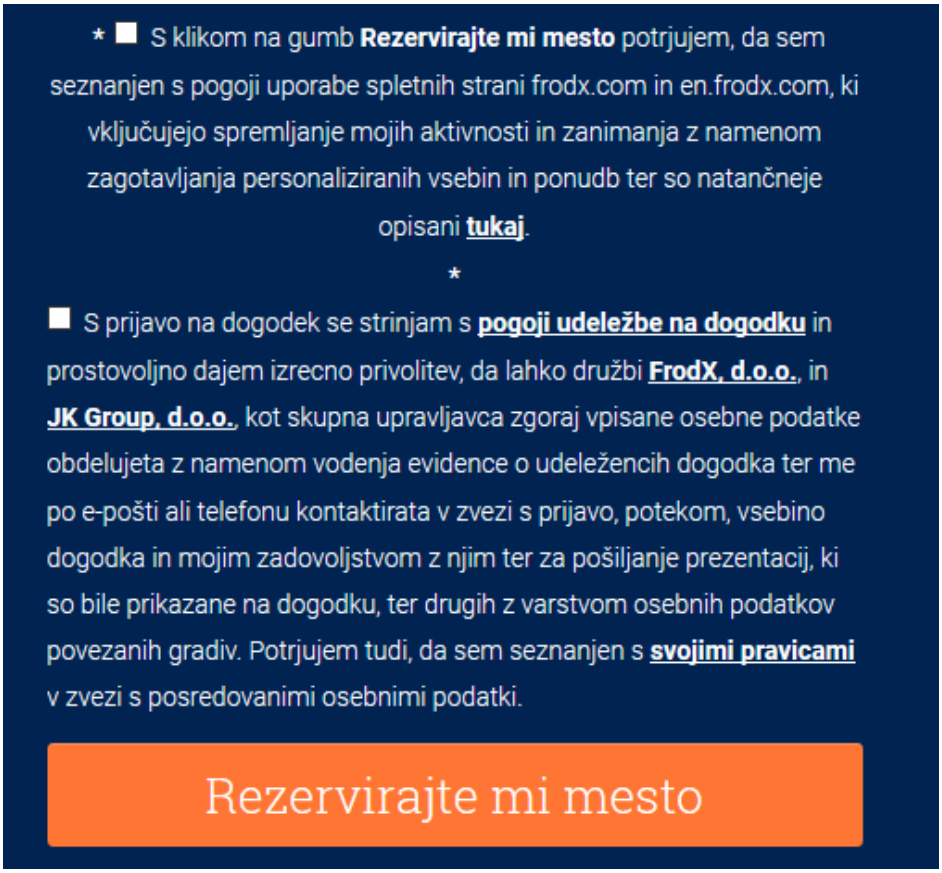
83. člen GDPR nalaga in predstavlja splošne pogoje za naložitev upravnih glob. Na naložitev in višino upravne globe vplivajo: narava, teža in trajanje kršitve; ali je kršitev naklepna ali posledica malomarnosti; vrsta osebnih podatkov, ki jih zadeva kršitev; stopnja odgovornosti upravljavca ali obdelovalca; stopnja sodelovanja z nadzornim organom; ukrepi, ki jih je sprejel upravljavec, da bi omilil škodo … Pristojni nadzorni organ lahko gospodarski družbi najprej izreče opomin. Manjše denarne kazni znašajo do 10 milijonov EUR ali za gospodarske družbe do 2 % skupnega letnega prometa na svetovni ravni za preteklo proračunsko leto, odvisno od tega, kateri znesek je višji. Resnejše kršitve pa znašajo do 20 milijonov EUR ali v primeru gospodarske družbe do 4 % skupnega svetovnega prometa v preteklem proračunskem letu (Gemserv Ltd., 2017, str. 4). Za izvajanje in določanje glob za kršitve zakona je pristojen nadzorni organ v državi članici, v Sloveniji je to Urad informacijskega pooblaščenca.

2.4 Privolitev posameznika

Privolitev predstavlja enega od šestih pravnih podlag za zakonito obdelavo osebnih podatkov po GDPR. Je bistvena sprememba, ki pomembno vpliva tako na poslovanje gospodarske družbe kot tudi na zasebnost posameznika v družbi. Poznavanje definicije privolitve je ključno za gospodarsko družbo. V 1. odstavku 6. člena GDPR je navedeno, da v kolikor je upravljavec zmožen dokazati, da je posameznik podal privolitev, le ta zakonito obdeluje osebne podatke. GDPR v 4. členu definira privolitev kot »vsako prostovoljno, izrecno, informirano in nedvoumno izjavo volje posameznika, na katerega se nanašajo osebni podatki, s katero z izjavo ali jasnim pritrdilnim dejanjem izrazi privolitev z obdelavo osebnih podatkov, ki se nanašajo nanj«. Upravljavec mora biti kadar koli zmožen dokazati, da je bila privolitev pridobljena od posameznika. To pomeni, da morajo upravljavci imeti dovolj podatkov, da dokažejo pridobitev privolitve, vendar ne smejo zbirati več informacij, kot je potrebno. Z arhiviranjem prejetih izjav upravljavec dokaže, kako in kdaj je bilo pridobljeno privolitev in katere informacije so bile na izjavi, ter s tem

dokaže, da je privolitev, pridobljena od posameznika, veljavna (Article 29 data protection working party, 2017c, str. 20).

Slika 2: Primer privolitve, ki je v skladu z novimi pravili GDPR. Gospodarski družbi FrodX in JK Group sta načela GDPR že implementirali



Vir: FrodX (brez datuma).

Privolitev na sliki 2 izpolnjuje merilo prostovoljno, specifično, informirano in nedvoumno. Privolitev bo izpolnjevala merilo »prostovoljno«, če ima posameznik resnično in svobodno izbiro in možnost zavrnitve ali umika privolitve brez škode. Posamezniki morajo biti obveščeni o pravici do odstopa od privolitve, ki mora biti tako enostavna kot privolitev k obdelavi podatkov. Pomembno je, da privolitev ni izsiljena, torej pogojevana ali skrita. Glede na uvodno določbo 43 GDPR privolitev ni prostovoljna, ko ne dovoljuje ločenih privolitev za različna dejanja obdelave osebnih podatkov ali kadar je izvajanje pogodbe pogojeno s privolitvijo, čeprav za samo izvedbo pogodbe privolitev ni nujna.

Privolitev bo izpolnjevala merilo »specifično in informirano«, ko je posameznik seznanjen z identiteto upravljavca, nameni obdelave podatkov, vrsto podatkov, ki bo obdelana, pravicami, ki jih ima kot posameznik, informacijo o avtomatiziranem odločanju ter vključno z morebitnim obdelovalcem ali tretjimi osebami. Kadar je obdelava večnamenska, mora biti privolitev dana jasno za vse namene obdelave (Bohan, McGirr, Carney & Woods, 2017). GDPR ne prepisuje oblike privolitve ali vnaprej pripravljenega

obrazca, da bi izpolnili zahtevo za informirano privolitev. Veljavna privolitev je lahko pridobljena na različne načine (pisno, ustno, avdio, video sporočilo), upravljavci pa morajo biti le-to zmožni vedno dokazati.

»Nedvoumnost« je ključen element privolitve v okviru GDPR, ki pravi, da ne sme obstajati dvom, ali se je posameznik res strinjal z obdelavo osebnih podatkov. Za aktivno, jasno, dano privolitev šteje dejanje, če posameznik sam označi okence ob obisku spletne strani, da se strinja s pogoji obdelave podatkov; kadar posameznik sam zaprosi za informacije in vnese osebne podatke ali ko vpiše svoje osebne podatke in elektronski naslov ter nato še dodatno s klikom na povezavo v elektronskem sporočilu potrdi, da se prijavlja na določene novice in dovoljuje uporabo osebnih podatkov. V zvezi s tem GDPR jasno navaja, da molk, vnaprej označena polja in nedejavnost (ang. opt-out) ne pomenijo privolitve. Upravljavec mora vedeti, da privolitve ni mogoče pridobiti istočasno, ko se posameznik strinja s pogodbo ali sprejema splošne pogoje poslovanja/storitve (Article 29 data protection working party, 2017c, str. 20).

2.5 Posebna vrsta osebnih podatkov in njihova zakonita obdelava

GDPR namenja posebno pozornost posebnim vrstam podatkov in otrokom.

Obdelava posebnih vrst podatkov je prepovedana, razen če posameznik, na katerega se osebni podatki nanašajo, poda izrecno privolitev. Med posebne vrste podatkov spadajo rasni in etični izvor, politično mnenje, versko in filozofsko prepričanje, članstvo v sindikatu, podatki o zdravju, spolno življenje in usmeritev ter biometrični in genetski podatki. Najbolj očitni način, da se zagotovi izrecna privolitev, je s pomočjo pisne izjave, ki je na koncu podpisana. V poštev pa pride tudi elektronski podpis, izpolnjevanje zahtevane izjave v elektronski obliki, pošiljanje elektronske pošte ali nalaganje skeniranega dokumenta s podpisom posameznika. Dvostopenjska verifikacija/preverjanje privolitve je prav tako ustrezen način izrecne privolitve (Article 29 data protection working party, 2017c, str. 18–19).

Zelo pomemben del GDPR je namenjen zaščiti otrok in mladih na spletu (uvodna izjava 38 GDPR), saj vsebuje številne določbe, kot so pravica do pozabe, navedba jasnih in nedvoumnih informacij o obdelavi podatkov, ki so za otroke razumljive. Pomemben 8. člen GDPR, ki se navezuje na otroke, pravi, da morajo upravljavci in/ali obdelovalci zahtevati privolitev staršev za obdelavo osebnih podatkov otroka, ki je mlajši od 16 let. GDPR dovoljuje državam članicam, da znižajo starostno mejo za pridobitev privolitve na najmanj 13 let. Upravljavci bodo morali uporabiti razpoložljivo tehnologijo in dobro mero razuma, da bodo presodili, ali je bila privolitev staršev res podano. Digitalne storitve morajo namenjati posebno pozornost dostopnosti in jasnosti informacij, ki so posredovane otrokom in mladim v povezavi z obdelavo njihovih podatkov (Information Commissioner's Office United Kingdom, 2017b).

GDPR ustvarja dodatne obveznosti za upravljavce glede profiliranja, ko obdeluje osebne podatke otrok. 22. člen GDPR, ki obravnava avtomatizirano obdelavo s profiliranjem, ne zajema direktno otrok, vendar pa v uvodni izjavi 71 GDPR navaja, da avtomatizirano odločanje, vključno s profiliranjem, ki ima pravne ali podobne posledice, ne bi smelo veljati za otroke. Ker otroci predstavljajo najbolj ranljivo skupino družbe, se jih na splošno ne bi smelo profilirati v tržne namene. Še posebej so dovzetni za spletno okolje in hitreje in lažje vplivamo na njihovo vedenje. Tako bi lahko na primer pri spletnem igranju igric uporaba profiliranja določila, kateri igralci bodo bolj verjetno porabili denar v igri in tako za njih uporabili prilagojene spletne oglase (Article 29 data protection working party, 2017a, str. 26, 27).

2.6 Neodvisni nadzorni organi

Nacionalni organi za varstvo osebnih podatkov oziroma nadzorni organ je v 4. členu GDPR definiran kot neodvisen javni organ, ki ga ustanovi vsaka država članica. V Sloveniji kot glavni in edini državni nadzorni organ deluje IP, njegovo delovanje pa se deli na področje varstva osebnih podatkov in področje dostopa do informacij javnega značaja. V večjih državah članicah je dovoljen več kot en nadzorni organ, kar je zapisano v 51. členu GDPR.

Ko gre za obdelavo podatkov v več državah članicah, je GDPR naredil pomemben korak. Gre namreč za koncept (definiran v uvodni izjavi 127 in 128 GDPR), ko gospodarske družbe, ki delujejo v več državah članicah, niso več odgovorne vsakemu nadzornemu organu v vsaki državi članici posebej. Z mehanizmom usklajenosti tako nadzorni organi v državah članicah sodelujejo med seboj in Komisijo, kar zagotavlja poenoteno in usklajeno ukrepanje v vseh državah članicah. Načelo »vse na enem mestu« (ang. one-stop-shop) tako zagotavlja zmanjšanje administrativnih stroškov ter zakonito obdelavo in dosledno uporabo. Pri čezmejni obdelavi osebnih podatkov je treba uporabiti mehanizem sodelovanja med vodilnim nadzornim organom in zadevnim nadzornim organom (Barnard-Wills, Pauner Chulvi & de Hert, 2016, str. 589).

Nadzorni organi morajo delovati popolnoma neodvisno, vendar so še vedno predmet finančnega in sodnega nadzora. Države članice morajo svojim nadzornim organom zagotoviti človeške, finančne, tehnične in druge vire, ki so potrebni za nemoteno opravljanje nalog in učinkovito izvajanje njihovih pristojnosti. Obravnavajo pritožbe, vložene pri njih, in kršitve, če se vsebina nanaša zgolj na upravljavca v tej državi članici. Opravljanje nalog nadzornega organa je za posameznika brezplačno, razen če so zahteve neutemeljene – takrat lahko nadzorni organ zaračuna stroške. Vsak nadzorni organ ima preiskovalna in popravljalna pooblastila, pooblastila v zvezi z dovoljenji in svetovalnimi pristojnostmi ter dodatna pooblastila, ki jih določi vsaka država članica posebej. Popravljalna pooblastila vključujejo: izreko opomina ali opozorila obdelovalcu ali upravljavcu, začasno ali dokončno omejitev obdelave podatkov, popravek ali izbris

osebnih podatkov … Določbe o ustanovitvi nadzornega organa niso nič presenetljivo novega, saj so bile definirane že v Direktivi (Article 29 data protection working party, 2016, str. 4).

Vodje nadzornega organa vsake članice, ENVP in predstavnik Komisije, ki nima glasovalne pravice, sestavljajo Evropski odbor za varstvo podatkov (ang. European Data Protection Board), definiran v 68. členu GDPR, ki bo nadomestil Delovno skupino. Evropski odbor za varstvo podatkov predstavlja neodvisni organ, ki spodbuja k dosledni uporabi GDPR v EU in svetuje Komisiji, predvsem ko gre za čezmejno obdelavo osebnih podatkov.

3 NORMATIVNI OKVIR VARSTVA OSEBNIH PODATKOV V REPUBLIKI SLOVENIJI

V večini držav članic je varstvo podatkov zajamčeno z ustavo. Tudi v Sloveniji je v 38. členu Ustave Republike Slovenije Ur. l. RS, št. 3/91-I zapisano, da mora zakonodajalec z zakonom urediti zbiranje, obdelovanje, namen uporabe, varstvo tajnosti in nadzor osebnih podatkov. Poleg sistemske ureditve pa je treba s področnimi zakoni jasno določiti podrobnosti. Tako je Republika Slovenija leta 1990 sprejela prvi Zakon o varstvu osebnih podatkov (ZVOP) Ur. l. RS, št. 59/1999, ki predstavlja vseobsežni pristop varstva podatkov (Pirc Musar, Bien, Bogataj, Prelesnik & Žaucer, 2006, str. 20). Po vstopu v Evropsko unijo 1. 5. 2004 je morala Republika Slovenija zakonodajo prilagoditi pravnemu redu EU ter zaradi določb iz Direktive sprejeti nov ZVOP-1, ki ga bom predstavila v nadaljevanju.

3.1 Zakon o varstvu osebnih podatkov – ZVOP-1

ZVOP-1 s svojimi 117 členi predstavlja trenutno veljaven zakon na področju varovanja osebnih podatkov, ki je bil sprejet 5. 8. 2004 in stopil v veljavo 1. 1. 2005. ZVOP-1 predstavlja veliko bolj obsežnejši in kompleksnejši zakon, kot je bil prejšnji ZVOP, saj predstavlja tako sistemski kot področni zakon. V svojem zadnjem, četrtem delu določa tudi neposredno zakonsko podlago za neposredno trženje, biometrijo, videonadzor, evidentiranje vstopov in izstopov ter strokovni nadzor, kar v ZVOP ni bilo urejeno. Temeljna načela, ki jih je treba upoštevati pri ravnanju z osebnimi podatki in so definirana v ZVOP-1, so: načelo zakonitosti in poštenosti, načelo sorazmernosti, načelo prepovedi in diskirminacije (Kramar, 2013, str. 13–16).

Obveznosti upravljavcev, opredeljene v ZVOP-1, so (Informacijski pooblaščenec, brez datuma):

- zagotavljanje točnosti in ažurnosti podatkov (18. člen);
- pred obdelavo pridobiti osebno privolitev posameznika ali zakonito obdelovati podatke;

- priskrbeti informacije o obdelavi osebnih podatkov (19. člen);
- odgovoriti na zahtevo do seznanitve z lastnimi osebnimi podatki (30. člen);
- sprejeti ukrepe za zavarovanje osebnih podatkov (24. in 25. člen);
- izbrisati, uničiti, blokirati ali anonimizirati osebne podatke, v kolikor je to zahtevano, ter s tem zagotoviti pravico do popravka, blokiranja, izbrisa, ugovora in dopolnitve (32. člen);
- zagotoviti sledljivost obdelave osebnih podatkov (kdaj, komu in kateri osebni podatki so bili posredovani);
- zavarovanje zbirk osebnih podatkov (sprejeti notranje akte, sestaviti postopke in ukrepe);
- popisati kataloge osebnih zbirk (vsebuje 13 določenih podatkov oz. dejstev) in jih posredovati v register zbirk osebnih podatkov ter določiti seznam oseb, ki so odgovorne za posamezne zbirke (26. člen);
- prijava biometrijskih ukrepov (pridobiti dovoljenje Informacijskega pooblaščenca) (80. člen);
- vzpostavitev videonadzora (sprejeti pisni sklep, objaviti, pisno seznaniti zaposlene) (74. člen);
- povezava zbirk osebnih podatkov (upravljavci iz javnega sektorja obvestiti nadzorni organ o povezovanju dveh ali več zbirk) (84. člen).

V 25. členu ZVOP-1 določa, da mora imeti vsak upravljavec izdelan pravilnik in operacijski predpis o varstvu osebnih podatkov, skladno z 11. členom ZVOP-1 pa podpisano pogodbo, ki ureja medsebojne pravice upravljavca in pogodbenega obdelovalca osebnih podatkov. Prav tako mora upravljavec voditi katalog zbirk, skladno s 26. členom ZVOP-1, ki ga mora prijaviti državnemu nadzornemu organu za varstvo osebnih podatkov.

Na podlagi 28. člena Direktive, kjer je zapisano, da mora vsaka država članica določiti enega ali več nadzornih organov, in ZVOP-1 je bil sprejet tudi Zakon o Informacijskem pooblaščencu (ZInfP) Ur. l. RS, št. 113/05. Samostojen nadzorni organ za varstvo osebnih podatkov je bil imenovan IP, kot prekrškovni in inšpekcijski organ.

Pravice posameznika, opredeljene v tretjem delu zakona, so naslednje:

- pravica posameznika do seznanitve (30. člen),
- pravica posameznika do dopolnitve, popravka, blokiranja, izbrisa in ugovora (32. člen) na zahtevo posameznika ali iniciativo upravljavca.

Globe v primeru nespoštovanja določb iz ZVOP-1 znašajo med 200 in 12.510 EUR in so določene v kazenskih določbah zakona.

Za lažjo oceno stroškov implementacije GDPR v gospodarsko družbo je treba dobro poznati tako ZVOP-1 kot GDPR. ZVOP-1 predstavlja začetno, današnje stanje, skladnost z GDPR pa končno stanje, ki ga želi gospodarska družba doseči. Razlike, koraki med

končnim in začetnim stanjem, predstavljajo in povzročajo stroške implementacije za gospodarsko družbo.

Razlike med ZVOP-1 in GDPR lahko razdelimo v štiri kategorije: pojme, pravice posameznikov, obveznosti upravljavcev in obdelovalcev ter sankcije in nadzor. V GDPR so na novo definirani pojmi: osebni podatek (širši okvir definicije), oblikovanje profilov, psevdonimizacija, občutljivi osebni podatki (namesto posebne vrste osebnih podatkov) in genetski podatki.

Obveznosti upravljavcev in obdelovalcev so se z GDPR okrepile. Dodatna obveznost upravljavcev je preveritev veljavnosti obstoječih privolitev, gospodarske družbe pa se bodo morale pripraviti na izvajanje načela odgovornosti (vključuje izvajanje ocene učinka, imenovanje odgovorne osebe za varovanje osebnih podatkov ter v obdelavo podatkov vključiti načelo vgrajenega in privzetega varstva podatkov).

Pravice posameznikov se bodo z uveljavitvijo GDPR okrepile, saj posameznikom namenjajo veliko večjo pozornost kot v ZVOP-1. Novosti v GDPR so torej: pravica do pozabe, pravica do omejitve obdelave osebnih podatkov in pravica do prenosljivosti podatkov. Sankcije in nadzor nad kršitvami osebnih podatkov so strožji v GDPR. Po ZVOP-1 se sankcije gibljejo do 12.510 EUR, odvisno od velikosti kršitve, v GDPR pa do 20 milijonov EUR ali do 4 % skupnega svetovnega prometa gospodarske družbe v preteklem proračunskem letu, naloge nadzornih organov pa okrepljene.

Iz predstavljenih razlik je razvidno, da GDPR vsekakor prinaša kar nekaj novosti na področju varovanja osebnih podatkov, vendar pa ZVOP-1 s svojimi 117 členi vsekakor ni nezahteven in slabo napisan zakon. Treba je poudariti, da ZVOP-1 ureja veliko stvari, ki jih nato prihajajoč GDPR samo še bolj podrobno definira in postavi v strožji zakonodajni okvir.

4 ANALIZA STROŠKOV VPELJAVE UREDBE NA RAVNI GOSPODARSKE DRUŽBE

Čisto vsaka gospodarska družba si želi maksimalno obvladovati in poznati stroške svojega delovanja kot tudi procesa uvajanja določenih sprememb – v našem primeru implementacije GDPR v gospodarsko družbo.

Za poslovanje v močno konkurenčnem okolju je potreben učinkovit sistem spremljanja in načrtovanja stroškov gospodarske družbe. Zato je zelo pomembno, na kakšen način se gospodarska družba loti implementacije GDPR ter da dobro načrtuje in pozna stroške, s katerimi se bo soočalo pri implementaciji. Šele dobro poznavanje in razumevanje vseh stroškov nam omogočata, da jih lahko, v kolikor se le da, tudi znižamo. Dobro poznavanje stroškov, ki jih bo povzročila implementacija GDPR v gospodarsko družbo, nam bo omogočalo širši pogled na situacijo, lažjo implementacijo novega zakona, predvsem pa v

dani situaciji povečati učinkovitost poslovanja in pri tem posledično optimizirati stroške. Dejstvo namreč je, da so stroški v povezavi z implementacijo GDPR za vsako gospodarsko družbo neizogibni.

V raziskovalnem centru Ponemon Institute so se analize stroškov skladnosti GDPR lotili tako, da so definirali šest aktivnosti (politiko skladnosti podatkov, komunikacijo, upravljanje in vodenje skladnosti, varnost podatkov, spremljanje skladnosti in izvrševanje), na katere so nato vezali direktne in indirektne stroške ter tako pojasnili ekonomski vpliv stroškov skladnosti z GDPR. Stroške vpeljave GDPR so razdelili na: (1) direktne, (2) indirektne in (3) oportunitetne. Po njihovem mnenju največji strošek (40 % vseh stroškov implementacije) predstavljajo indirektni stroški v povezavi z administracijo, oportunitetni stroški (30 % vseh stroškov implementacije), ki predstavljajo nezmožnost izvajanja marketinških kampanj v takem obsegu kot pred GDPR zaradi nove politike privolitve, ter direktni stroški, kot so plačila pravnikom in zunanjim izvajalcem, revizorjem in ostalim ekspertom na tem področju, pa 27 % vseh stroškov implementacije (Ponemon Institute, 2017, str. 7, 24).

Na podlagi analize 53 multinacionalk iz Združenih držav Amerike in 237 intervjujev z zaposlenimi v teh gospodarskih družbah, ki so na višjih položajih in so vpleteni v implementacijo GDPR, so ocenili direktne in indirektne stroške skladnosti z GDPR ter direktne, indirektne in oportunitetne stroške neskladnosti z GDPR v obdobju enega leta. Tako so določili ključne trende in skupne značilnosti med stroški neskladnosti in skladnosti. Njihova ocena je, da so stroški neskladnosti **2,71-krat** večji od stroškov skladnosti z GDPR. Stroški neskladnosti so večji kot stroški implementacije GDPR. Prav tako ugotavljajo, da gospodarske družbe premalo denarja namenjajo temeljnim dejavnostim skladnosti, kot so notranja revizija, vpeljava pravilne tehnologije, usposabljanje zaposlenih (Ponemon institute, 2017, str. 5, 6).

Christensen, Colciago, Etro in Rafert (2013, str. 2) predpostavljajo, da bo imela povprečna srednja in mala gospodarska družba v EU letno stroškov s skladnostjo z GDPR približno med 3.000 in 7.200 EUR, odvisno, v kateri industriji posluje, kar predstavlja med 16 in 40 % trenutnih letnih stroškov za IT.

Analiz in člankov na temo stroškov, ki pridejo z implementacijo GDPR, nisem našla veliko, zato sem v nadaljevanju stroške razdelila v pet skupin: stroški v povezavi s pregledom obstoječega stanja, stroški v povezavi s privolitvami, stroški v povezavi s pravicami posameznikom, stroški v povezavi z DPO in dodatni stroški. Vse stroške sem na kratko predstavila, jih podrobneje razdelila in opisala, kar v dani situaciji, z danimi viri in literaturo predstavlja analizo stroškov implementacije. Pri oceni stroškov sem upoštevala, da so vse gospodarske družbe že popolnoma skladne z ZVOP-1. Analizo sem zaključila s predstavitvijo dejavnikov vpliva na stroške.

4.1 Stroški v povezavi s pregledom obstoječega stanja

4.1.1 Pravni pregled skladnosti poslovanja gospodarske družbe z GDPR

Interni akti oziroma pravilniki omogočajo gospodarski družbi učinkovito organizacijo in poslovanje. »Pravilnik o varovanju osebnih podatkov« predstavlja pravilnik, kjer so določeni postopki in ukrepi za varovanje osebnih podatkov ter postopki za varnost. V skladu s sprejetjem GDPR bodo morale gospodarske družbe posodobiti in pravilno urediti ta pravilnik in vse pravilnike, ki se navezujejo na varovanje in obdelavo osebnih podatkov. Preveriti je treba, ali se zapisane določbe res izvajajo v praksi, jih popraviti, predvsem pa zapisati, kako so osebni podatki zaščiteni pred izgubo, zlorabami in nepooblaščenimi dostopi. S tem, ko bo gospodarska družba posodobila in uredila pravilnike in posodobila varnostne politike, bo zadostila potrebam zakonodajalca in dodatno optimizirala poslovanje družbe. Oddelek pravne službe bo tako v skladu projekta skladnosti dobil dodatno zadolžitev.

V GDPR so na novo in podrobneje definirane tudi podrobnosti o razmerju obdelovalec – upravljavec. Pogodba (dogovor o nivoju storitve, ang. Service level agreement) mora vsebovati določbe o nalogah in obveznostih obdelovalca. Te določbe vključujejo, kako in kdaj bodo podatki po obdelavi vrnjeni ali izbrisani ter vse podrobnosti obdelave, kot so: vrsta podatkov, namen, predmet, trajanje in kategorija oseb, na katere se podatki nanašajo (Taylor Wessing, 2016c). To vse prinaša direktne stroške za upravljavca, saj je treba posodobiti že obstoječe pogodbe ali sestaviti nove. Treba se je dogovoriti, na kakšen način se bo komuniciralo, predvsem pa je pomembno, da obdelovalec redno spremlja obdelavo podatkov in pravočasno sporoči upravljavcu o zaznani kršitvi. Obdelovalec mora imeti vzpostavljen učinkovit nadzor nad obdelavo, kar pomeni, da morajo vedeti, kdaj so imeli vdor. Stroški, ki jih ima obdelovalec s samo uvedbo in implementacijo GDPR v svojo gospodarsko družbo, predstavljajo indirektne stroške za upravljavca. Predvsem gre tu za indirektne stroške za nadzor nad obdelavo podatkov, zagotavljanje dovolj velike varnosti in poročanje o morebitnih kršitvah.

Ker med pregledom literature nisem našla ocene teh stroškov niti, kako obsežno in zahtevno delo prinaša pravni pregled gospodarske družbe, predstavljam stroške, ki lahko nastanejo ob pravnem pregledu gospodarske družbe. Potencialni stroški pravnega pregleda so:

- stroški pregleda pravnih aktov gospodarske družbe:
  - delo zaposlenega, ki bo pregledal vse pravilnike in interne akte gospodarske družbe, ki se nanašajo na GDPR, in pripravil popravke in novosti;
  - najem morebitne pravne pomoči/gospodarske družbe za nasvet in/ali usmeritev;
- stroški, ki nastanejo na strani upravljavcev zaradi obveznosti do obdelovalcev:

- delo zaposlenega, ki bo pregledal pogodbe, definiral nove člene in zagotovil, da se pogodba, ki je v skladu z GDPR, ponovno podpiše.

Strošek dela predstavlja pomembno postavko odhodka gospodarske družbe in vključuje stroške bruto plače, dodatkov (prevoz na delo, prehrana), regres, prispevke, ki jih mesečno plača delavec, prispevke, ki jih plača gospodarska družba, izobraževanja, usposabljanja in amortizacijo. Republika Slovenija se uvršča v skupino s srednje visoko povprečnimi stroški dela na zaposlenega in ne zaostaja za povprečjem držav članic EU (Data d.o.o., 2014). Način, kako se bo gospodarska družba lotila implementacije, vpliva tudi na to, kakšne dodatne stroške dela bodo imeli. Nekateri bodo verjetno zaposlovali dodatne ljudi ali pa jih trajno preusmerili, predpostavljam pa, da bo v večini potekala alokacija delovne sile in nadobremenitev. Stroški v povezavi z delovno silo torej so:

- stroški dela alokacije ljudi, ki bi sicer delali nekaj drugega;
- alokacija stroškov na/za zaposlene, ki zaradi GDPR več delajo in imajo začasno povečan obseg dela, vendar ne dobijo denarnega nadomestila;
- strošek zaposlovanja novih ljudi.

4.1.2 Pregled zbranih osebnih podatkov posameznikov

Gospodarska družba mora popisati vse osebne podatke, ki jih hrani o posameznikih. Pomembno je, da se zaveda, kako podatki pridejo v gospodarsko družbo, kaj, na kakšen način so podatki obdelani, kdo od zaposlenih ali drugih podjetij (obdelovalcev) ima dostop do njih, kako se podatke lahko uniči in kje so zapisani oziroma shranjeni. Pregledati je treba podatke v strukturiranih in nestrukturiranih virih ter tiskanih dokumentih. Pogledati je treba v različne evidence, zbirke, kadrovske mape zaposlenih, računovodske podatke, Excelove tabele, v same posnetke videonadzora, elektronske pošte in pri pogodbenih partnerjih – obdelovalcih. Namreč, če želimo podatke ustrezno varovati, moramo vedeti, kje in katere podatke imamo. Podroben pregled in popis življenjskega cikla osebnih podatkov zahteva čas zaposlenih. Za hitrejše odkrivanje podatkov IT-gospodarske družbe ponujajo programsko rešitev, ki omogoča hitrejše in učinkovitejše odkrivanje lokacij osebnih podatkov po strukturiranih in nestrukturiranih virih.

Tudi tu nisem našla virov in analiz na temo pregleda zbranih osebnih podatkov, zato ocenjujem, da bodo stroški, ki nastanejo ob popisu osebnih podatkov, naslednji:

- strošek dela zaposlenega, ki pregleduje baze osebnih podatkov, privolitve itd.;
- če se gospodarska družba tako odloči in če obdeluje zelo veliko osebnih podatkov, lahko nastanejo tudi stroški nakupa programske opreme, ki prepozna in omogoča hitrejše in učinkovitejše pregledovanje baz osebnih podatkov.

4.1.3 Vodja projekta implementacije

Pomembno je, da gospodarska družba določi vodjo projekta implementacije GDPR, ki ima pregled in nadzor nad izvajanjem skladnosti z GDPR, kar pomeni, da izvaja in bdi nad oceno učinkov, ima nadzor nad delovanjem in izvajanem obdelav osebnih podatkov, spremlja in sprejema nova podatke, ureja dostope in spremlja varnostno stanje. Dogovoriti se je treba, kdo bo poročal v primeru varnostnega incidenta, torej če pride do izgube ali nepooblaščenega dostopa. V začetni fazi, ko se gospodarska družba pripravlja na implementacijo, vodenje skladnosti zahteva kar nekaj časa in energije zaposlenega, zato vodja projekta predstavlja ključen člen implementacije. Ker med viri nisem nikjer zasledila, koliko ur dela zahteva vodenje projekta implementacije, ocenjujem, da z vodenjem implementacije nastanejo naslednji stroški:

- strošek dela zaposlenega, ki dobi novo zadolžitev: vodja projekta implementacije GDPR;
- širši obseg dela lahko pripelje do višjega mesečnega plačila, bonusov, dodatkov.

4.2 Stroški v povezavi s privolitvami

Potreben bo temeljit pregled vseh obstoječih obrazcev za pridobitev privolitev, sklenjenih pogodb, splošnih pogojev storitev in spletnih obrazcev, s katerimi gospodarska družba pridobi privolitev za obdelavo osebnih podatkov. Več kot ima upravljavec ali obdelovalec opravka z osebnimi podatki, več privolitev bo posledično treba pregledati in ugotoviti, ali so v skladu z GDPR.

V primeru email marketinga, kjer ima gospodarska družba veliko obstoječih uporabnikov na adremi, bo treba vse elektronske naslove osvežiti oziroma pridobiti nove privolitve. V kolikor to ne bo urejeno, bo pošiljanje elektronske pošte prepovedano oziroma ne bo v skladu z GDPR. Za pridobljene privolitve bo treba imeti ustrezno revizijsko sled in jih ustrezno arhivirati (Pomagalnik – strokovnjak za digitalne medije, 2017). V mislih je potrebno imeti tudi pozitiven stranski učinek GDPR in pošiljanj ponovnih privolitev, saj se bodo mailing liste, ki so se v preteklosti brez kakršnegakoli nadzora polnile, prečistile. Ostali bodo le tisti posamezniki, ki jih bo poslana vsebina zanimala (Škerl Kramberger, 2018).

Ker je marketing preko elektronske pošte v veliko gospodarskih družbah zelo pomemben kanal komuniciranja s strankami in publiko, bo imelo kar nekaj družb s tem velik problem. V dneh pred 25. 5. 2018 so gospodarske družbe pošiljale veliko prošenj za ponovno privolitev, vendar je bil odziv v Sloveniji po poročanju zelo majhen. V Dnevniku so zapisali, da je pošiljateljem v povprečju odgovorilo okrog 5% naslovnikov. Tiste gospodarske družbe, ki so do sedaj že imele zgrajen dober in kvaliteten odnos s strankami in so izvajale kvalitetne marketinške kampanije ter vanje vključevale relevantno vsebino, bodo imele odstotek podanih privolitev večji (Škerl Kramberger, 2018). Večina poslovnih

modelov, ki so jih gospodarske družbe uporabljale do sedaj, ni skladna z GDPR. Na tej točki je zato potrebno prilagoditi poslovanje in marketinške aktivnosti GDPR ter sestaviti in posodobiti obstoječe poslovne modele.

V več virih so omenjene le ocenjene vrednosti izgube prodaje zaradi nepodanih privolitev. Rezultati Deloittove raziskave potrošnikov so pokazali, da bo samo polovica posameznikov ponovno podala privolitev za obdelavo osebnih podatkov. Dodatno, samo polovica vseh, ki se strinjajo z obdelavo osebnih podatkov, bi dovolila uporabo in posredovanje podatkov obdelovalcu oziroma drugi gospodarski družbi. Rezultati predpostavljajo, da GDPR vodi v veliko zmanjšanje moči targetiranja posameznikov s strani podjetnikov in gospodarskih družb v direktnem marketingu, kar bo zmanjšalo izdatke v tem sektorju za 34 % oziroma 18 bilijonov EUR. V praksi pa bo to vodilo do povečane uporabe drugih marketinških kanalov, kot so televizija, radio, časopisi, in s tem prerazporedilo izdatke. Prav zaradi prerazporeditve sredstev v druge marketinške kanale je izračun 62 bilijonov EUR izgube prodaje na območju EU oziroma 15,1 bilijona EUR za Veliko Britanijo (Deloitte LLP, 2013, str. 11).

Direktna izguba prodaje (po tem, ko se bo zgodila prerazporeditev sredstev za marketinške kampanje) vpliva na prizadete gospodarske družbe in s tem zmanjšuje BDP za 28 milijard EUR. To posledično vpliva na dobavitelje in obdelovalce prizadetih podjetij, ki zmanjšajo njihov BDP za 33 milijard EUR. Vse to se kaže v tem, da bodo zaposleni prizadetih gospodarskih družb in dobaviteljev izgubili službe in prihodek, kar bo vodilo do zmanjšanja osebne potrošnje in s tem vplivalo na BDP ter ga zmanjšalo za dodatnih 24 milijard EUR. Skupen vpliv na BDP zaradi izgube prodaje znaša 85 milijard EUR (Deloitte LLP, 2013, str. 12).

Na podlagi raziskave, ki so jo izvedli v gospodarski družbi London Economics, je očitno, da se bo ob opt-in privolitvi/privolitev, ki je v skladu z GDPR, zmanjšalo število posameznikov, ki bodo podali privolitev za obdelavo podatkov, kar pomeni, da se bodo baze podatkov zmanjšale in tako bodo imele gospodarske družbe, ki se aktivno ukvarjajo z obdelavo podatkov, nekaj težav. Po drugi strani pa bodo baze podatkov, pridobljenih z opt-in, več vredne, vendar pa čisto vse gospodarske družbe ne bodo občutile te dodane vrednosti (odvisno od narave poslovanja in velikosti družbe) (London Economics, 2017, str. 15, 16). Tisti posamezniki, ki bodo privolitev za obdelavo podatkov podali, bodo

Na to temo sem našla zgolj en relevanten članek, ki je predstavljen v nadaljevanju, nikjer pa nisem zasledila, kakšna je ocena stroškov obnovitve privolitev in kakšna je ocena stroškov izgube podatkov v bazi, ker privolitev ne bo podana. Predpostavljam, da bodo zaradi ostrejših pogojev v povezavi s privolitvijo nastali naslednji stroški:

– stroški popravljanja, prilagajanja in oblikovanja novih privolitev, ki so skladne z GDPR:

- stroški pravnikov/zunanjih izvajalcev, ki pomagajo pri skladnem oblikovanju privolitev;
- v kolikor so gospodarske družbe pridobivale privolitve na internetu, so tu tudi stroški programerja/skrbnika spletne strani, ki bo prilagodil in popravil stvari na spletni strani;
- ker je potrebna tudi revizijska sled privolitve (upravljavec mora točno vedeti, kdaj je prejel privolitev, in jo hraniti), je potrebna tudi »nadgradnja« obstoječega sistema spletne strani;

– stroški pošiljanja novih privolitev (tako po elektronski pošti kot tudi fizično);
– stroški izgube velikosti baze: izguba mailing list oziroma strank, ker družbe ne bodo pridobile privolitev.

V članku The Impact of the Data Protection Regulation in the E.U. predpostavljajo, da bo treba v večini podjetij pridobiti nove privolitve, ki temeljijo na zakoniti podlagi. Predpostavljajo, da bo načelo zakonitosti povzročilo približno 633 EUR letno stroškov, povezanih z dodatnim pisarniškim delom in pravnim vrednotenjem. Podobno bo s stroški, ki bodo nastali pri pridobivanju ponovnih privolitev od otrok, kjer bodo stroški zaradi manjšega števila privolitev nekoliko manjši (Christensen, Colciago, Etro & Rafert, 2013, str. 18, 19).

Ocena učinka Evropske komisije GDPR (v Christensen, Colciago, Etro & Rafert, 2013, str. 20) predpostavlja in ocenjuje stroške v povezavi z 12. členom GDPR (preglednost in načini nad pravicami posameznikov) v vrednosti 100 EUR (dve uri dela na vsaki dve leti), vendar se ocena zdi zelo nizka, saj je treba popraviti in razviti novo politiko varovanja osebnih podatkov, ki verjetno potrebuje pravno pomoč in posodobitev spletne strani z novimi pravili.

4.3 Stroški v povezavi s pravicami posameznikov

GDPR temelji in daje veliko pravic posameznikom, kot so pravica do popravka in izbrisa, pravica do prenosljivosti podatkov, pravica do informiranosti in seznanitve z osebnimi podatki. Vse te zahteve s strani posameznikov predstavljajo dodaten izziv gospodarski družbi. Treba je pregledati vse postopke za zagotavljanje pravic posameznika.

V kolikor je gospodarska družba manjša in ne obdeluje ter poseduje veliko osebnih podatkov, je teh zahtev malo, kar pomeni, da se bo izpolnjevanje/izvrševanje zahtev lahko izvajalo ročno. V tem primeru bo tako en zaposleni v gospodarski družbi zadolžen za urejanje, komunikacijo in izvrševanje zahtev, kar pomeni, da bo to predstavljalo le še dodatno delovno nalogo zaposlenemu. V kolikor gospodarska družba upravlja z več osebnih podatkov in je narava poslovanja družbe taka, da je zahtev v skladu s prenosljivostjo, izbrisom in izpisom podatkov več, pomeni dodatne stroške in spremembe za gospodarsko družbo. V takem primeru bo treba vzpostaviti nov proces, ga v pravilnik

pravilno zabeležiti in opredeliti ter določiti odgovorne osebe, odvisno od velikosti gospodarske družbe. Za lažje izvajanje in nadzor nad procesom lahko gospodarska družba kupi programsko rešitev.

Stroški, ki jih ima lahko gospodarska družba:

- nakup programske rešitve:
  - gospodarska družba lahko kupi programske rešitve informacijskih družb;
  - rešitev ni potrebna, saj gospodarska družba program Excel ali Access že ima. Je pa v tem primeru priporočljivo narediti analizo stroškov in koristi in se vprašati, ali se mogoče splača kupiti programsko rešitev in si olajšati delo ter prihraniti čas zaposlenega.

V članku The Impact of the Data Protection Regulation in the E.U. pravijo, da bodo stroški, povezani s pravicami posameznika, v veliki meri rezultat izgube prihodka zaradi nezmožnosti ciljnega oglaševanja in drugih dejavnosti neposrednega trženja, ki vključujejo profiliranje. Ti stroški so odvisni od količine ciljnega oglaševanja gospodarske družbe in jih lahko klasificiramo kot variabilne stroške (Christensen, Colciago, Etro & Rafert, 2013, str. 15).

Ocena učinka Evropske komisije GDPR (v Christensen, Colciago, Etro & Rafert, 2013, str. 19, 20) predpostavlja izhodiščne stroške v povezavi s pravico do prenosa podatkov in pravico do pozabe v vrednosti 67 EUR na leto za dodatno administrativno delo. Glede na to, da predpostavljajo, da večina malih in srednjih podjetij (do 250 zaposlenih) nima vzpostavljenih ustreznih programskih rešitev za izvajanje teh pravic, to pomeni dodatnih 2.000 EUR za vzpostavitev rešitve in dodatni manjši strošek (med 10 in 50 EUR) za obdelavo posamezne zahteve posameznika. V Veliki Britaniji predpostavljajo, da gospodarska družba letno prejme med 50 in 5.000 zahtevkov (odvisno od velikosti gospodarske družbe).

4.4 Stroški v povezavi z DPO

Gospodarske družbe morajo ugotoviti, ali ustrezajo kriterijem iz 37. člena GDPR o obveznem imenovanju DPO. DPO je lahko eksterni zunanji ali interni notranji zaposleni. Če imenovanje DPO za družbo ni obvezno, ga GDPR in IP priporočata kot dobro prakso in dokazovanje skladnosti. Če bo gospodarska družba najela zunanjega izvajalca na podlagi pogodbe o storitvi, bo to vsekakor dodaten strošek za gospodarsko družbo v primerjavi s stroškom, ki ga ima gospodarska družba, če najde nekoga interno, ki ima vsa znanja in kompetence za izvajanje te naloge. Notranji izvajalci pa imajo svoje prednosti, saj zaposleni bolje razumejo poslovanje družbe in imajo boljše odnose z ostalimi zaposlenimi v gospodarski družbi. Prvi korak pri uspešni implementaciji GDPR v gospodarsko družbo je imenovanje DPO, saj predstavlja pomemben člen pri uvajanju členov GDPR že pred začetkom veljavnosti uredbe.

Če gospodarska družba najame zunanje izvajalce so stroški: strošek nadzora nad opravljenim delom DPO ter strošek zunanjega izvajalca, ki izvaja DPO (načeloma lahko gospodarska družba izbere različne pakete DPO, ki vključujejo različen obseg aktivnosti). Po navadi se strošek paketa oblikuje glede na nivo tveganja obdelave osebnih podatkov z vidika GDPR in število zaposlenih v gospodarski družbi. Stroški eksternega DPO predstavlja fiksne stroške, saj načeloma ne naraščajo z velikostjo gospodarske družbe ali številom osebnih podatkov, ki jih hrani.

V članku The Impact of the Data Protection Regulation in the E.U. ocenjujejo časovno zahtevnost opravljanja nalog DPO:

- izobraževanje zaposlenih o GDPR (tako novih zaposlenih kot tudi že obstoječih zaposlenih), čas priprave na izobraževanje in izdelave materiala za izobraževanje obsega delo enega tedna;
- pregledati operacije obdelave osebnih podatkov in zagotoviti skladnost z obstoječimi predpisi o varstvu osebnih podatkov obsega delo enega ali več tednov;
- preiskava kršitve varstva osebnih podatkov in delovanje kot kontaktna točka za zaposlene obsega delo dva do tri tedne;
- prijava na varnostne protokole in sporočanje morebitnih težav višjemu vodstvu kot del ocene učinka zahteva najmanj en teden.

Upoštevajoč podane naloge, ocenjujejo, da potrebujemo DPO za minimalno 100 ur dela na leto in neprimerljivo več za gospodarske družbe, ki intenzivno obdelujejo osebne podatke. Predlagajo, da se DPO najema na uro, saj naloge DPO ne obsegajo toliko dela, da bi se izplačalo zaposliti novo osebo (Christensen, Colciago, Etro & Rafert, 2013, str. 12).

Christensen, Colciago, Etro in Rafert (2013, str. 27) predpostavljajo znaten negativen vpliv GDPR na ustvarjanje novih poslovnih priložnosti in zaposlovanja. To se bo najbolj kazalo v gospodarskih družbah, ki bodo morala zaposliti DPO, saj DPO predstavlja visoke fiksne stroške poslovanja družbe. Na podlagi njihovega modela se bo število zaposlenih zmanjšalo v rangu od 100.000 na kratki rok in vse do 300.000 na dolgi rok.

Stroška v povezavi z internim DPO sta samo dva: ure, ki jih bo zaposleni porabil za opravljanje nalog DPO namesto za »običajno« delo ter širši obseg dela, ki lahko pripelje do višjega mesečnega plačila, bonusov ali dodatkov.

4.5 Dodatni stroški

V nadaljevanju bom predstavila stroške, ki niso obvezni za uspešno implementacijo GDPR, so pa priporočljivi, saj omogočajo lažje poslovanje in sledenje skladnosti.

4.5.1 Strošek izobraževanja

Vse več inovativnih aplikacij, naprav in hitrejši informacijski napredek pomembno vplivajo na informacijsko varnost in posledično varstvo osebnih podatkov posameznika. Zato je ključno, da vsaka gospodarska družba ozavešča in izobražuje zaposlene o varstvu osebnih podatkov, kot tudi o novostih, ki pridejo v veljavo z GDPR. Smernice Informacijskega pooblaščenca in ostalih organov za varstvo osebnih podatkov poudarjajo, kako pomembno je, da se osebje seznani z GDPR in da gospodarske družbe vključijo izobraževanja v svoj projekt skladnosti z GDPR, čeprav le-ta niso predpisana. Brez učinkovitega programa ozaveščanja zaposlenih o novostih in zahtevah v GDPR gospodarska družba tvega kršitev. Zaposlenim je treba predstaviti, kaj sploh so osebni podatki, kako je treba ravnati z njimi in katera dejanja z njimi so nedopustna, saj je poznavanje te problematike po navadi na zelo nizkem nivoju. Pri samem varstvu podatkov ne smemo pozabiti tudi na napotke glede varne in ustrezne izbire in rednega menjavanja gesel ter pomena politike čiste mize. Samo s tehničnimi, programskimi ukrepi je nemogoče preprečiti nepooblaščeno obdelavo, zato so tu ključna izobraževanja, ki ozaveščajo in izobražujejo zaposlene (Informacijski pooblaščenec, 2015, str. 10).

Izobraževanja so priporočljiva za vse zaposlene, predvsem pa za IT-oddelek, vodje kadrovskih in pravnih služb, lastnike podatkov ter za vse zaposlene, ki delajo in imajo dostop do osebnih podatkov (npr. zaposlenemu, ki uporablja program za upravljanje odnosov s strankami (ang. custom relationship management)), je treba razložiti, da ima dostop do velikega obsega podatkov in mora biti pri tem previden).

Gospodarska družba se lahko odloči za ozaveščanje zaposlenih s pomočjo e-izobraževanj, individualnih treningov, seminarjev ali konferenc. Izobraževanja lahko izvedejo interno ali eksterno, kar bo prav tako vplivalo na stroške, povezane z implementacijo GDPR.

Stroški, povezani z izobraževanji, so:

- stroški organizacije internega izobraževanja z internimi ali eksternimi predavatelji:
  - v primeru internega predavatelja bodo stroški naslednji: stroški dela, ki jih bo zaposleni predavatelj namenil pripravam in izvedbi izobraževanja namesto delu;
  - v primeru eksternega predavatelja bodo stroški naslednji: najem eksternega strokovnjaka na področju GDPR;
  - v obeh primerih se bo izobraževanje izvajalo za zaposlene, ki bodo ure namesto za delo namenili za izobraževanje (v nekaterih gospodarskih družbah je to urejeno s kolektivno pogodbo);
- stroški udeležbe na eksternem izobraževanju za DPO, vodje IT-oddelkov, pravnike, vodje marketinškega oddelka:
  - gospodarska družba Mladi podjetnik je v sodelovanju s parterji pripravila konferenco Uredba GDPR – Pasti in nevarnosti, kjer je kotizacija 100 EUR brez DDV;

- seminar Kaj prinaša uredba o varstvu podatkov (GDPR)? Pod okriljem OPENIT Poslovna izobraževanja znaša 176 EUR brez DDV;
- seminar Kako do 25. maja 2018 zagotoviti skladnost z GDPR s kotizacijo 190 EUR brez DDV;
- tridnevna konferenca GDPR (ZVOP-2) – v sklopu konference INFOSEK 2017 900 EUR brez DDV;
- kar nekaj izobraževanj pa je tudi brezplačnih.

Delavci imajo lahko s kolektivno pogodbo določeno letno kvoto ur za izobraževanje, ki se bo nekaj let porabljala za GDPR.

4.5.2 Strošek certifikacije

Certifikacija varstva osebnih podatkov izkazuje proaktivno skladnost z GDPR. 42. člen GDPR določa, da je certifikacija prostovoljna, a plačljiva. Če se gospodarska družba odloči za certificiranje, izvajalec presoja skladnost poslovanja z zahtevami tehničnega standarda, vključno s samo učinkovitostjo procesov gospodarske družbe. S tem bo gospodarska družba vzpostavila zaupanje z zainteresiranimi stranmi in strankami, saj bo dokazala najvišjo zaščito njihovih osebnih podatkov in dokazala, da za podatke ustrezno skrbi. Uradno certificiranje bo omogočal IP, pogoji, cene in zahteve pa bodo znani po začetku veljavnosti GDPR. Stroški v povezavi s certifikati bodo nastali šele kasneje, najprej eno leto po implementaciji GDPR. Gospodarska družba se mora na tej točki vprašati, ali se gospodarski družbi izplača certificirati in imeti dodatne stroške v povezavi z GDPR, kar ji omogoča izvedba analize stroškov in koristi. Glede na razmere na trgu se certifikacije po navadi lotijo večje gospodarske družbe, ki imajo denar in jim ta dodatni strošek ne predstavlja prevelikega bremena, ampak v certificiranju vidijo poslovno priložnost tako za poslovanje kot za uporabnike. Certifikacije so po navadi drage, s tem pa lahko gospodarsko družbo postavijo v konkurenčno prednost, saj si s tem poveča ugled družbe, se izogne morebitnim stroškom glob in tveganju izgube ugleda. Ker cena certificiranja še ni znana, predpostavljam, da bodo ob certifikaciji nastali naslednji stroški:

- stroški certificiranja,
- stroški dela vodje projekta certificiranja.

4.6 Dejavniki vpliva

Na podlagi prej navedenih in opisanih stroškov lahko pridemo do sklepa, kateri dejavniki bodo vplivali na stroške implementacije.

- **sektor poslovanja gospodarske družbe:** s kako velikimi stroški se bo gospodarska družba soočala med samim procesom implementacije, je odvisno, v katerem sektorju/panogi je dejavna. GDPR najbolj vključuje in vpliva na naslednje panoge:

- zdravstvo – zdravstveni podatki;
- finančni sektor – finančni podatki o plačah, kreditih;
- javni sektor – podatki o prebivalstvu;
- informacijsko komunikacijski sektor (IT-ponudniki in oddelki, telekomunikacija) – kot obdelovalec podatkov;
- prodaja in marketing:
    - spletne trgovine – sledijo uporabnikom, kaj so kupili, katere izdelke so si ogledovali na spletnih straneh;
    - družbe s karticami, klubi zvestobe in ugodnosti (veliki trgovci);

– **intenzivnost obdelave osebnih podatkov:** intenzivneje kot gospodarska družba obdeluje osebne podatke, več časa in stroškov bo namenila implementaciji. Na intenzivnost obdelave osebnih podatkov vpliva, ali gospodarska družba hrani in obdeluje posebne vrste osebnih podatkov in koliko osebnih podatkov hrani gospodarska družba;

– **stopnja zrelosti gospodarske družbe:** pri stopnji zrelosti gospodarske družbe ne mislim na model razvoja vsake gospodarske družbe, temveč na tiste, ki imajo zrel in odgovoren pristop do varstva osebnih podatkov. Zrela gospodarska družba ima vzpostavljene politike varovanja gesel, izobražuje zaposlene o varovanju osebnih podatkov, ima dobro podprte procese in jim varstvo osebnih podatkov predstavlja pomembno vlogo pri poslovanju in razvijanju produktov. Bolj kot je gospodarska družba zrela, manjše stroške implementacije bo imela. Stopnjo zrelosti sem razdelila na naslednje dejavnike: zaposleni, procesi obdelave osebnih podatkov in uporabljena tehnologija ter pridobljeni certifikati;

- **zaposleni:** zaposleni predstavljajo ključen in enega izmed najpomembnejših notranjih resursov gospodarske družbe. Notranji resursi namreč predstavljajo notranje udeležence, torej lastnike, upravljavce, management družbe ter strokovnjake in druge zaposlene. Z notranjimi resursi je povezana tudi velikost gospodarske družbe. Večja kot je gospodarska družba, več ima notranjih resursov – zaposlenih, z različnimi znanji in kompetencami. Veliko večjih gospodarski družb bo implementacijo GDPR izvedlo samo, saj imajo dovolj zaposlenih in denarja, da si to lahko privoščijo. Poleg pa lahko najamejo zunanjo, neodvisno, družbo, ki bo naredila notranjo revizijo in s tem preverila, ali so pravilno implementirali spremembe GDPR. Stroški implementacije GDPR na zaposlenega bodo večji v manjših gospodarskih družbah v primerjavi z večjimi. Ta rezultat je mogoče povezati z ekonomijami obsega, saj velja, da imajo večje gospodarske družbe dostop do vodilnih tehnologij in zelo visoko usposobljeno osebje, ki ima izkušnje s področja varovanja osebnih podatkov in predpisov (Ponemon Institute, 2017, str. 11). Manjše gospodarske družbe se morajo tako zanašati na druge zunanje, dražje resurse, kot so svetovalci in odvetniki, da bi izpolnili zahtevam iz GDPR. Če je gospodarska družba do sedaj že vlagala v izobraževanja zaposlenih na področju varovanja osebnih podatkov, če so imeli izoblikovane politike varovanja osebnih podatkov, politiko menjavanja gesel, politiko prazne mize, bo imela manj stroškov

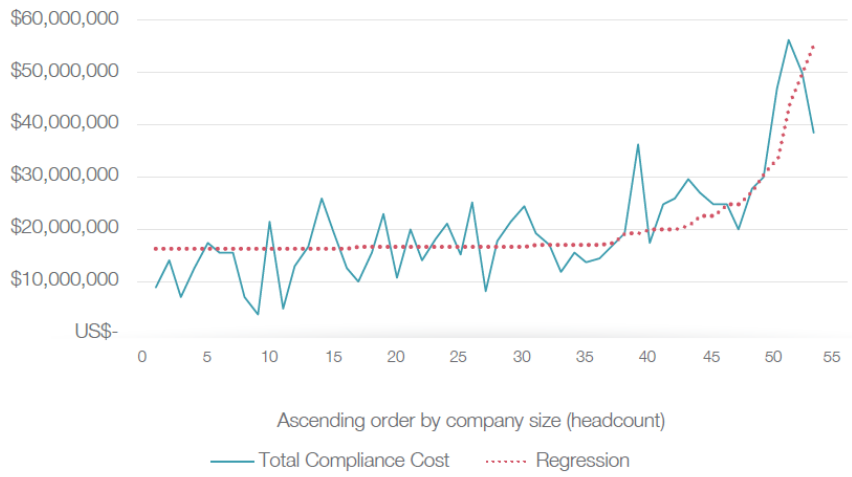
in bolj ozaveščene zaposlene, s katerimi bo treba manj delati, možnost kršitve varstva podatkov bo manjša;

- **procesi obdelave osebnih podatkov in uporabljena tehnologija:** pomembno je, kakšni procesi obdelave osebnih podatkov so v gospodarski družbi, ali so to ročni, razpršeni, IT-podprti, nepregledni – dobesedno razmetani. Če ima gospodarska družba pod nadzorom z IT podprte procese, je večja verjetnost, da bo imela manj stroškov, saj ji ne bo bilo treba kupovati novih programskih rešitev, prav tako pa bo z IT podprtimi procesi lažje identificirala in popisala osebne podatke. Če gospodarska družba pri poslovanju uporablja posodobljeno, primerno in novejšo tehnologijo, s samo implementacijo ne bo imelo veliko stroškov;
- **pridobljeni certifikati:** gospodarske družbe, ki že imajo vzpostavljene službe za tveganje in redno izvajajo notranje, tekoče, revizije skladnosti, bodo dosegale visoko stopnjo zrelosti gospodarske družbe. Gospodarske družbe, ki so v letu 2017 izvedle pet ali več notranjih revizij skladnosti, imajo manjše stroške implementacije (Ponemon Institute, 2017, str. 16). S pridobljenim standardom ISO/IEC 27001 Sistem vodenja varovanja informacij, katerega glavni namen je zavarovanje informacij in preprečitev izgube ali zlorabe informacij, gospodarska družba izkazuje visoko stopnjo varovanja osebnih podatkov posameznika. Gospodarska družba mora, da pridobi ta certifikat, oceniti tveganje in uvesti ustrezne nadzorne mehanizme, ki ohranjajo razpoložljivost, zaupnost in popolnost informacij (Bureau veritas Slovenija, brez datuma). Standard je mestoma še zahtevnejši od GDPR, vendar bodo s strani gospodarske družbe potrebne dopolnitve. Če ima gospodarska družba ta standard že pridobljen, pomeni, da so nekoč že popisali vse osebne podatke, zato bo identificiranje le-teh za preveritev skladnosti z GDPR veliko lažje in hitrejše. Skladnost bodo najhitreje in najlažje dosegle gospodarske družbe, ki imajo že pridobljen standard ISO 27001. Tiste gospodarske družbe, ki so do sedaj že odgovorno ravnale z osebnimi podatki, ne bodo imele večjih težav in stroškov implementacije. Svojega delovanja ne bodo drastično spremenile, pač pa bo verjetno potrebna le kakšna nadgradnja. Poleg ISO 27001 je moč iskati vzporednice s standardom ISO/IEC 31000 Obvladovanje tveganj – Načela in smernice za obvladovanje tveganja ter samo oceno učinka. V kolikor ima gospodarska družba že pridobljen standard, bo lažje in učinkoviteje izpeljala oceno. Če je gospodarska družba v preteklosti že opravila oceno učinka, bo to pomenilo stroškovno drugačen »rezultat«, kot če se s tem sooča prvikrat;

– **kompleksnost obdelave osebnih podatkov:** pomembno je, ali gospodarska družba samo hrani osebne podatke ali pa jih tudi na veliko in kompleksno obdeluje.

– Zatorej bo velika razlika med gospodarsko družbo, ki je na primer operater in izvaja veliko, kompleksno obdelavo osebnih podatkov, pri kateri izve in pridobi veliko informacij o posamezniku, ali pa če obdelavo izvaja mala informacijska družba. Menim, da je zmožnost kompleksne obdelave osebnih podatkov močno povezana z velikostjo gospodarske družbe. Ponemon Institute je na 53 gospodarskih družbah dokazal, da obstaja linearna korelacija med velikostjo gospodarske družbe in stroški implementacije/skladnosti. Večja kot je gospodarska družba, večji so tudi stroški v povezavi z GDPR. S slike 3 je razvidno, da stroški implementacije nihajo, vendar linearno rastejo z velikostjo gospodarske družbe, stroški pa začnejo strmo naraščati pri gospodarski družbi, ki šteje 40 zaposlenih in več (Ponemon Institute, 2017, str. 9);

Slika 3: Skupni stroški implementacije GDPR glede na velikost gospodarske družbe



Vir: Ponemon Institute (2017).

– **drugi dejavniki:** drugi dejavniki, ki vplivajo na velikost stroškov implementacije GDPR v gospodarski družbi, so:
  - če gospodarska družba iznaša osebne podatke v tretje države (posebne zahteve in določbe, definirane v petem poglavju GDPR oziroma od 44. do 50. člena GDPR);
  - če ima gospodarska družba veliko pogodbenih obdelovalcev (število pogodbenih obdelovalcev kot tudi različnih vrst), bo imela večje stroške implementacije. Treba bo preveriti podpisane pogodbe, uskladiti obveznosti in zahteve ipd;
– **skladnost z ZVOP-1:** s pravnega vidika zahteve in določbe v GDPR niso nobena velika sprememba. Temeljna načela varstva osebnih podatkov ostajajo enaka, bodo pa učinki GDPR tisti, ki bodo prinesli nekaj novosti. Če je bila gospodarska družba skladna po ZVOP-1, ne bo potrebno veliko truda, stroškov in vpeljave večjih novosti za skladnost z GDPR. V tem primeru bo treba aktivno pregledati vse privolitve in poslovne procese, potrebno bo minimalno prilagajanje, nekaj sestankov in izobraževanj. Za tiste, ki niso bili skladni z ZVOP-1 in se z varstvom osebnih podatkov niso veliko ukvarjali, pa GDPR predstavlja veliko priložnost za prevetritev osebnih

podatkov, procesov in delovanja na področju ter tudi nekaj več dodatnih stroškov. Zatorej, če se na tej točki vprašamo, ali GDPR predstavlja revolucijo ali evolucijo na področju varovanja osebnih, je odgovor jasen – evolucijo.

Treba je poudariti, da se dejavniki vpliva med seboj povezujejo. Veliko dejavnikov je prepletenih, predvsem sektor poslovanja gospodarske družbe, intenzivnost obdelave osebnih podatkov, kompleksnost obdelave osebnih podatkov in stopnja zrelosti gospodarske družbe. Če gospodarska družba na primer deluje v živilski industriji, se ne sooča s posebnimi vrstami osebnih podatkov in posledično njegova obdelava ni kompleksna in intenzivna.

Na zmanjšanje stroškov implementacije vplivajo kodeksi ravnanja (40. in 41. člen GDPR). Združenja lahko skupaj pripravijo kodekse ravnanja – predloge za enotne privolitve, skupna pravila za obdelavo osebnih podatkov itd., manjše gospodarske družbe in člani združenja (npr. obrtniki) pa bodo te kodekse samo vzeli, podpisali in implementirali v gospodarsko družbo. Namesto, da bodo sami študirali člene in določbe GDPR, bo nekdo drug za njih pripravil vse potrebno za implementacijo. Ocena učinka Evropske komisije GDPR ocenjuje, da bodo imeli kodeksi ravnanja in potrjevanja (40.–44. člen GDPR) pozitiven vpliv na tiste gospodarske družbe, ki poslujejo s tretjimi državami in državami izven EU, ter povečali konkurenčnost podjetij, ki upravljajo z osebnimi podatki izven EU. Navaja, da bodo prihranki, povezani s kodeksi in potrjevanjem, 50.000 EUR za upravljavca, ki pa bo imel dodatnih 5.000 EUR stroškov zaradi pravice do prenosljivosti (v Christensen, Colciago, Etro & Rafert, 2013, str. 21, 22). GDPR s tem pomembno prispeva k spodbujanju varnega prenosa osebnih podatkov med državami.

Poleg kodeksov ravnanja pa bo načelo »vse-na-enem-mestu« delno zmanjšalo stroške obdelovalcev in upravljavcev, ki delujejo v več državah članicah, saj bodo v tem primeru sodelovali in komunicirali samo z vodilnim nadzornim organom (Christensen, Colciago, Etro & Rafert, 2013, str. 4).

Dobre prakse, ki jih poudarjajo v raziskovalnem centru Ponemon Institute (2017, str. 17) in pravijo, da bodo znižale stroške implementacije, so (napisane od najbolj do najmanj pomembne): uporaba centraliziranega programa upravljanja podatkov, izvajanje notranjih revizij skladnosti, korporativna izobraževanja na temo varovanja osebnih podatkov, posebni pravni oddelki, ki poznajo področje varovanja osebnih podatkov, funkcija varnosti in zasebnosti, integrirana v poslovanje gospodarske družbe, izoblikovan postopek odziva na incidente, imenovanje izvršnega direktorja in poročanje na ravni upravnega odbora, regulatorni nadzor, pridobljeni certifikati na področju varovanja podatkov.

Ponemon Institute, najpomembnejši raziskovalni center, posvečen zasebnosti, varstvu podatkov in politiki varovanja informacij, iz Michigana je razvil sistem ocenjevanja varnosti gospodarskih družb, imenovan SES (ang. Security Effectivness Score; slov. ocena učinkovite varnosti), da bi ocenil varnostno zmogljivost gospodarske družbe. SES je v

rangu od –2 (najmanj točk) do +2 (največ točk). V nedavni raziskavi, ki vključuje 53 gospodarskih družb iz različnih industrij, so ugotovili, da večji kot je SES, bolj je gospodarska družba učinkovita v varovanju informacijskih sredstev in osebnih podatkov. V centru Ponemon Instutute so ugotovili, da so stroški skladnosti inverzno povezani s SES, večji so stroški implementacije, nižji je SES, kar pomeni, da se bodo gospodarske družbe, ki niso varnostno učinkovite, soočale z večjimi stroški skladnosti (Ponemon Institute, 2017, str. 18).

SKLEP

Varstvo in pomen osebnih podatkov iz leta v leto pridobivata na pomembnosti tako v svetovnem rangu kot tudi pri nas. Premoženje gospodarske družbe so tudi osebni podatki, saj spreminjajo svetovno gospodarstvo, analize podatkov pa predstavljajo pomembno vrednost pri ustvarjanju gospodarske vrednosti družbe kot tudi sveta (Deloitte LLP, 2013, str. 2).

V magistrskem delu sem predstavila GDPR, ki predstavlja zahteve po večji varnosti obdelave osebnih podatkov. Gospodarska družba bo to dosegla z ustreznimi ukrepi, ki so sestavljeni iz tehnologije, ki je na voljo, virov, ki predstavljajo ljudi, denar in znanje, narave obdelave osebnih podatkov in tveganja, ki ga posamezna obdelava za posameznika predstavlja.

Pomanjkanje literature in virov je oteževalo analizo stroškov vpeljave GDPR na ravni gospodarske družbe. Težko je namreč *ex ante* oceniti in določiti ceno implementacije. Poglavitni stroški, ki sem jih na podlagi opravljene analize zaznala, so: (1) fiksni strošek DPO, če gospodarska družba ustreza kriterijem o imenovanju DPO, (2) strošek dela vseh zaposlenih, ki bodo delali na »projektu« implementacije GDPR, (3) strošek izgube velikosti baze za oglaševanje in prodajo izdelkov. Ravno zaposleni na različnih položajih so tisti, ki bodo še dodatno obremenjeni z dodatnimi zadolžitvami, verjetno naredili kakšno naduro, gospodarske družbe pa bi posledično morale to tudi izplačati.

Vsekakor so stroški odvisni od veliko dejavnikov, najpomembnejši je skladnost s prejšnjo zakonodajo, torej ZVOP-1. Tistim gospodarskim družbam, ki so že bile skladne z ZVOP-1, implementacija novih pravil po GDPR ne bi smela predstavljati pretiranih dodatnih stroškov, temveč samo nekaj dodatnih prilagoditev na področju privolitev, prilagoditve pravnih vsebin in internih aktov.

S kakšnimi stroški so se gospodarske družbe soočale ob implementaciji GDPR, bo bolj jasno po začetku uporabe GDPR ali kakšno leto kasneje. Takrat bo namreč slika jasnejša in stroške bo verjetno lažje opredeliti in definirati. Za natančnejšo in konkretnejšo analizo bi lahko magistrsko delo nadgradila tako, da bi po enem letu od začetka uporabe GDPR v določenih gospodarskih družbah naredila strukturirane intervjuje in tako pridobila podatke

o stroških in času delovnih ur, ki so jih zaposleni porabili za implementacijo zakona, ter dobila sliko o stroškovni obremenjenosti.

Prepričana sem, da bodo dolgoročne koristi prevladale nad stroški, predvsem v družbah, ki so bile ob implementaciji premišljene v svojih pristopih. Pomembno je, da gospodarske družbe v GDPR ne vidijo le regulatornih prizadevanj, pač pa naj se osredotočijo na številne priložnosti, ki jih ponuja dobro oblikovan notranji okvir za varstvo osebnih podatkov. Strošek, ki bo prišel z implementacijo, res predstavlja finančno breme za vsako gospodarsko družbo, vendar pa se bo na dolgi rok povrnil v boljšem poslovanju gospodarske družbe, nadzoru poslovnih procesov, učinkovitejšem delu družbe in zmanjševanju tveganja. Lahko bi tudi rekli, da bo vsak strošek v povezavi z implementacijo GDPR nekoč predstavljal dodano vrednost gospodarski družbi. Družbe, ki razmišljajo pametno, bodo razumele skladnost z GDPR kot glavno vprašanje upravljanja družbe, ne le vprašanje pravne izpolnitve. GDPR se zato splača izkoristiti za izboljšanje odnosa do kupcev in ponudbo za njih in s tem postati konkurenčnejši.

Skladnost z GDPR ni projekt, ki se bo zaključil z začetkom uporabe zakona, pač pa predstavlja dolgoročen in zahteven proces, ki je spremenil rabo osebnih podatkov posameznikov in tako pomembno vplival na gospodarske družbe.

LITERATURA IN VIRI

1. Agencija Evropske unije za temeljne pravice, Svet Evrope. (2014). *Priročnik o evropskem pravu varstva osebnih podatkov*. Luxemburg: Urad za publikacije Evropske unije.
2. Article 29 data protection working party. (2016). *Guidelines for identifying a controller or processor's lead supervisory authority.* Bruselj: Evropska komisija.
3. Article 29 data protection working party. (2017a). *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679.* Bruselj: Evropska komisija.
4. Article 29 data protection working party. (2017b). *Guidelines on Personal data breach notification under Regulation 2016/679.* Bruselj: Evropska komisija.
5. Article 29 data protection working party. (2017c). *Guidelines on Consent under Regulation 2016/679.* Bruselj: Evropska komisija.
6. Barnard-Wills, D., Pauner Chulvi, C. & de Hert, P. (2016). Data protection authority perspectives on the impact of data protection reform on cooperation in the EU. *Computer Law & Security Review*, *32*(4), 587–598.
7. Bohan, A., McGirr, D., Carney A. & Woods C. (2017, 26. Maj). GDPR in Context: Consent. *Lexology*. Pridobljeno iz https://www.lexology.com/library/detail.aspx?g=69025020-7a32-4e47-ba05-1f1bcf14d407
8. Bureau veritas Slovenija. (brez datuma). *ISO 27001*. Pridobljeno 15. januarja 2018 iz http://www.bureauveritas.si/services+sheet/iso27001

9. Burri, M. & Schär, R. (2016). The Reform of the EU Data Protection Framework: Outlining Key Changes and Assessing Their Fitness for a Data-Driven Economy. *Journal of Information Policy*, *6*, 479–511.
10. Cavoukian, A. (2009, avgust). *Privacy by Design. The 7 Foundational Principles.* Pridobljeno 20. novembra 2017 iz https://iab.org/wp-content/IAB-uploads/2011/03/fred_carter.pdf
11. Cepec, J. & Kovač, M. (2012). *Poslovno pravo*. Ljubljana: GV Založba.
12. Cerasaro, E. F. (2017). Accountability principle under the GDPR: is data protection law moving from theory to practice? *LUISS Law Review, 2017*(2), 214–226.
13. CIPL - Centre for Information Policy Leadership at Hunton Andrews Kurth LLP. (2017a, 12. april). *Certifications, Seals and Marks under the GDPR and Their Roles as Accountability Tools and Cross-Border Data Transfer Mechanisms.* Discussion Paper. Bruselj: CIPL.
14. CIPL - Centre for Information Policy Leadership at Hunton Andrews Kurth LLP. (2017b, december). *Comments by the Centre for Infromation Policy Leadership On the article 29 Working Party's "Guidelines on personal data breach notification under Regulation 2016/679".* Pridobljeno 22. februarja 2018 iz https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_comments_to_wp29_guidelines_on_breach_notification.pdf
15. Christensen, L., Colciago, A., Etro, F. & Rafert, G. (2013, 13. februar). *The impact of the Data Protection Regulation in the E.U.* Intertic Policy Paper 13(1).
16. Data d.o.o. (2014, 15. januar). *Stroški dela v Sloveniji.* Pridobljeno 16. marca 2018 iz https://data.si/blog/2014/01/15/stroski-dela-v-sloveniji/
17. Deloitte LLP. (2013, 16. december) *Economic impact assessment of the proposed European General Data Protection Regulation.* Final report. London: Delloite LLP.
18. Delovna skupina za varstvo podatkov iz člena 29. (2016). *Smernice o pravici do prenosljivosti podatkov.* Bruselj: Evropska komisija.
19. Delovna skupina za varstvo podatkov iz člena 29. (2017a). *Smernice glede ocene učinka v zvezi z varstvom podatkov in opredelitve, ali je „verjetno, da bi [obdelava] povzročila veliko tveganje", za namene Uredbe (EU) 2016/679.* Bruselj: Evropska komisija.
20. Delovna skupina za varstvo podatkov iz člena 29. (2017b). *Smernice o pooblaščenih osebah za varstvo podatkov.* Bruselj: Evropska komisija.
21. Diker Vanberg, A. & Ünver, MB. (2017). The right to data portability in the GDPR and EU competition law: odd couple or dynamic duo? *European Journal of Law and Technology*, *8*(1), 1-22.
22. European Commission. (2012, 25. januar). *Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation).* Bruselj: Evropska komisija.
23. European Commission. (2016). *Article 29 Working Party*. Pridobljeno 20. februarja 2018 iz http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083

24. Evropska komisija. (2010). *Sporočilo Komisije Evropskemu parlamentu, Svetu, evropskemu ekonomsko-socialnemu odboru in odboru regij. „Celovit pristop k varstvu osebnih podatkov v Evropski uniji“.* Evropska komisija: Bruselj.
25. Evropska komisija. (2016, 6. maj). *Sporočilo za medije – Enotni digitalni trg za Evropo: 16 pobud Komisije za njegovo uresničitev*. Pridobljeno 15. novembra 2017 iz http://europa.eu/rapid/press-release_IP-15-4919_sl.htm
26. FrodX. (brez datuma). *GDPR +100 dni.* Pridobljeno 20. januarja 2018 iz http://frodx.com/uredba-gdpr/
27. Gemserv Ltd. (2017). *A Guide to GDPR Fines.* Pridobljeno 22. februarja 2018 iz https://www.gemserv.com/wp-content/uploads/GDPR-Fines-Guide.pdf
28. IAPP - International Association of Privacy Professionals. (2016, 12. februar). *Top 10 operational impacts of the GDPR: Part 8 – Pseudonymization.* Pridobljeno 3. februarja 2018 iz https://iapp.org/news/a/top-10-operational-impacts-of-the-gdpr-part-8-pseudonymization/
29. Imperva Inc. (2017). *GDPR Article 25.* Pridobljeno 2. februarja 2018 iz https://www.imperva.com/data-security/regulation-glossary/gdpr/gdpr-article-25/
30. Informacijski pooblaščenec. (2015, 22. september). *Zavarovanje osebnih podatkov. Smernice Informacijskega pooblaščenca.* Ljubljana: Informacijski pooblaščenec.
31. Informacijski pooblaščenec. (2017a, julij). *Iskalnik po odločbah in mnenjih VOP – imenovanje pooblaščenih oseb za varstvo osebnih podatkov.* Pridobljeno 22. februarja 2018 iz https://www.ip-rs.si/vop/imenovanje-pooblascenih-oseb-za-varstvo-osebnih-podatkov-2949/
32. Informacijski pooblaščenec. (2017b, 23. november). *Ocene učinkov na varstvo osebnih podatkov. Smernice Informacijskega pooblaščenca.* Ljubljana: Informacijski pooblaščenec.
33. Informacijski pooblaščenec. (brez datuma). *Obveznosti upravljavcev.* Pridobljeno 8. februarja 2018 iz https://www.ip-rs.si/varstvo-osebnih-podatkov/obveznosti-upravljavcev/
34. Information Commissioner's Office United Kingdom. (2017a). *Personal data breaches.* Pridobljeno 22. februarja 2018 iz https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/
35. Information Commissioner's Office United Kingdom. (2017b). *Children.* Pridobljeno 1. februarja 2018 iz https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/applications/children/
36. Information Commissioner's Office United Kingdom. (brez datuma). *Codes of conduct and certification.* Pridobljeno 2. februarja 2018 iz https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/codes-of-conduct-and-certification/
37. Inside Privacy. (2017, 18. september). *GDPR Contracts and Liabilities Between Controllers and Processors.* Pridobljeno 6. februarja 2018 iz https://www.insideprivacy.com/international/united-kingdom/gdpr-contracts-and-liabilities-between-controllers-and-processors/

38. i-SCOOP. (2017). *Data subject rights and personal information: data subject rights under the GDPR.* Pridobljeno 26. februarja 2018 iz https://www.i-scoop.eu/gdpr/data-subject-rights-gdpr/
39. Kramar, B. (2013). *Varstvo osebnih podatkov v Sloveniji* (diplomsko delo). Ljubljana: Ekonomska fakulteta.
40. Kranjc, A. (2004). *Varstvo osebnih podatkov v obdobju tranzicije in vstopanju Slovenije v Evropsko unijo* (diplomsko delo). Ljubljana: Fakulteta za družbene vede.
41. London Economics. (2017, oktober). *Analaysis of the potential economic impact of GDPR – Implication of the ICO's Draft Guide on consent.* Velika Britanija: London Economics.
42. Mikkelsen, D., Soller, H. & Strandell-Jansson, M. (2017, januar). *The EU data-protection regulation—compliance burden or foundation for digitization?* Pridobljeno 5. novembra 2017 iz https://www.mckinsey.com/business-functions/risk/our-insights/the-eu-data-protection-regulation-compliance-burden-or-foundation-for-digitization#
43. Pirc Musar, N., Bien, S., Bogataj, J., Prelesnik, M. & Žaucer, A. (2006). *Zakon o varstvu osebnih podatkov s komentarjem*. Ljubljana: GV Založba.
44. Pomagalnik – strokovnjak za digitalne medije. (2017, 12. maj). *GDPR: Nova Evropska pravila za E-mail marketing.* Pridobljeno 11. januarja 2018 iz https://www.pomagalnik.com/marketing/gdpr-nova-evropska-pravila-za-e-mail-marketing/
45. Ponemon Institute. (2017, december). *The true cost of compliance with data protection regulations.* Michigan: Ponemon Institute LLC.
46. Safari, B.A. (2017). Intangible privacy rights: how europe's GDPR will set a new global standard for personal data protection. *Seton hall law review, 47*(3), 809–848.
47. Sobolewski, M. & Palinski, M. (2017). *How much consumers value on-line privacy? Welfare assessment of new data protection regulation (GDPR)* (Working paper No.17/2017 (246)). Warsaw: Faculty of Economic Sciences.
48. Škerl Kramberger, U. (2018, 25.maj). Evropska uredba, zaradi katere lahko propadejo poslovni modeli. *Dnevnik.* Pridobljeno 25. maja 2018 iz https://www.dnevnik.si/1042823286/slovenija/evropska-uredba-zaradi-katere-lahko-propadejo-poslovni-modeli
49. Taylor Wessing. (2016a, november). *The data protection principles under the General Data Protection Regulation.* Pridobljeno 28. novembra 2017 iz https://united-kingdom.taylorwessing.com/globaldatahub/article-the-data-protection-principles-under-the-gdpr.html
50. Taylor Wessing. (2016b, november). *Privacy by design and default.* Pridobljeno 29. novembra 2017 iz https://united-kingdom.taylorwessing.com/globaldatahub/article-privacy-by-design-and-default.html
51. Taylor Wessing. (2016c, junij). *Obligations on data processors under the GDPR.* Pridobljeno 3. februarja 2018 iz https://united-kingdom.taylorwessing.com/globaldatahub/article-obligations-on-data-processors-under-gdpr.html

52. Voigt, P. & Bussche, A. (2017). *The EU General Data Protection Regulation (GDPR): A Practical Guide.* Berlin: Springer International Publishing.
53. Zabukovec, P. (2011). *Obvladovanje stroškov v podjetju Val marketing: Ocena stanja in možne izboljšave* (magistrsko delo). Ljubljana: Ekonomska fakulteta.