UNIVERZA V LJUBLJANI
EKONOMSKA FAKULTETA

MAGISTRSKO DELO

VPLIV SPLOŠNE UREDBE O VARSTVU OSEBNIH PODATKOV NA TRŽENJE

Ljubljana, oktober 2019

MATEVŽ KADAK

IZJAVA O AVTORSTVU

Podpisani Matevž Kadak, študent Ekonomske fakultete Univerze v Ljubljani, avtor predloženega dela z naslovom Vpliv splošne uredbe o varstvu osebnih podatkov na trženje, pripravljenega v sodelovanju s svetovalcem izr. prof. dr. Brankom Koržetom

IZJAVLJAM

1. da sem predloženo delo pripravil 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 poskrbel, 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 pridobil vsa potrebna dovoljenja za uporabo podatkov in avtorskih del v predloženem delu in jih v njem jasno označil;

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

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

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

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

V Ljubljani, dne _____ Podpis študenta:_____

KAZALO

KAZALO TABEL

KAZALO PRILOG

SEZNAM KRATIC

ang. – angleško

DPO – (ang. Data protection officer); Pooblaščena oseba za varstvo osebnih podatkov

EU – (ang. European Union); Evropska unija

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

lat. – latinsko

OP – osebni podatek

ZDA – Združene države Amerike

UVOD

Telekomunikacijska tehnologija in svetovni splet sta spremenila način življenja. Brezmejno širjenje podatkov pa poleg neizmernih prednosti in priložnosti prinaša tudi nove grožnje na področju varstva osebnih podatkov. Vedno več aktivnosti opravimo preko spleta, od komunikacije s prijatelji in znanci do spletnih nakupov. Pri izvajanju takšnih aktivnosti večkrat pustimo sled osebnih podatkov. Kljub temu da ne vemo, kdo je na drugi strani, z upravljavcem (največkrat je to neko podjetje[1]) brez razmišljanja delimo osebne podatke. Splošne pogoje, ki so večkrat skriti nekje »v kotu«, hitro potrdimo, da ne izgubljamo dragocenega časa. V večini primerov to pripelje zgolj do nadaljnje komunikacije z nami v obliki prejemanja nezaželene e-pošte (ang. spam) in prejemanja sporočil preko različnih medijev, lahko pa tudi do morebitnih zlorab.

Zaradi razvoja informacijskih tehnologij je prišlo do večjih sprememb v obsegu, intenzivnosti in načinu prenosa osebnih podatkov (razvoj računalništva v oblaku, porast uporabe družbenih omrežij in uporabe pametnih telefonov), kar je terjalo posodobitev zakonodaje na tem področju. Spremembo na področju varovanja osebnih podatkov je predlagala Evropska komisija v letu 2012, da bi posodobila in prenovila določbe iz Direktive o varstvu podatkov iz leta 1995, ki je bila napisana, ko se nihče še ni zavedal, kako zelo pomembna bodo postala družbena omrežja.

Glavne spremembe, ki jih je zakonodajalec želel uveljaviti oziroma dopolniti, se nanašajo na naslednja področja:

- pravice posameznika,
- obveznosti upravljavcev in obdelovalcev;
- pravice do pravnega sredstva in sankcije v primeru kršitev.

Pred sprejetjem novosti v pravni ureditvi je imela vsaka država članica Evropske unije (v nadaljevanju EU) svojo pravno ureditev, ki naj bi se s sprejetjem Splošne uredbe o varstvu osebnih podatkov (ang. General Data Protection Regulation, v nadaljevanju GDPR) poenotila. Tržni udeleženci sedaj lažje vstopajo oziroma delujejo na trgih drugih držav članic EU. Izvajanje GDPR-ja bo sčasoma pripeljalo do tega, da bodo osebni podatki dostopni v strukturirani obliki. To bo pripeljalo do dodatnih investicij, ki pa se bodo na dolgi rok povrnile. Delo s strukturiranimi podatki je za gospodarske subjekte namreč manj zahtevno.

Eden izmed ključnih argumentov, po mnenju Evropske komisije (2018), sprejetja nove uredbe je bil povrniti zaupanje potrošnika v gospodarske subjekte in institucije. Ratio legis GDPR-ja je omogočiti prebivalcem nadzor nad lastnimi osebnimi podatki in hkrati dvigniti zavedanje o pomenu varstva osebnih podatkov. Nova uredba prav tako vsem podjetjem, ki delujejo na območju EU, zagotavlja enake pogoje poslovanja na tem področju. Evropska komisija kot predlagatelj je z GDPR-jem želela doseči enake pogoje za vsa podjetja, kar bi se v gospodarstvu izrazilo pozitivno.

[1] Podjetje je generični pojem za skupek organiziranega premoženja, namenjenega za opravljanje gospodarske dejavnosti, ki mu pravni red neposredno ali posredno preko nosilca podjetništva priznava status pravne osebe, kot nosilcu določenih pravic in obveznosti (Korže, 2016, str. 69).

V maju leta 2014 so podjetja Google, Facebook in Amazon predstavljala več kot 50 % svetovne tržne kapitalizacije od 20 največjih podjetij, ki se ukvarjajo s spletnimi rešitvami – od tega je bilo 12 podjetij iz Združenih držav Amerike (v nadaljevanju ZDA), prav nobeno pa iz držav članic EU. Cilj sprejetja GDPR-ja je bil hkrati dati jasen signal velikim korporacijam o pomembnosti področja varstva osebnih podatkov znotraj EU.

V 6. členu GDPR (Uredba (EU) 2016/679) določa, da mora biti privolitev za zbiranje osebnih podatkov dana izrecno. Posameznik mora biti seznanjen z namenom obdelave osebnih podatkov in o svojih pravicah.

Če imajo tržniki dostop do osebnih podatkov stranke, lahko zaradi tega identificirajo potencialne stranke, ki bodo prej opravile nakup, jim pripravijo bolj primerne promocije, jih uvrstijo v primernejše programe zvestobe, personalizirajo oglaševanje in hkrati lažje ocenijo uspešnost ter stroškovno učinkovitost kampanj.

Na področju varovanja osebnih podatkov se soočamo z dvema nasprotujočima pravicama oz. dvema nasprotnima interesa. Prva stran si želi neomejenega dostopa do osebnih podatkov, druga pa si želi te podatke varovati. Zato je pomembno premisliti kateri interes prevlada.

V magistrskem delu sem raziskal smer, v katero se razvija trženje z vidika zaupanja potrošnikov. Preveril sem, ali nova evropska ureditev na področju varstva osebnih podatkov resnično pomeni prelomnico ali pa so podjetja že pred sprejetjem GDPR-ja sprejela ukrepe, ki so povečali pripravljenost potrošnikov, da jim svoje osebne podatke posredujejo.

Preveril sem tudi, kaj so podjetja naredila, da so potrošnike prepričala v to, da se strinjajo (podajo izrecno privolitev) z obdelavo osebnih podatkov. Raziskal sem tudi, kaj so podjetja naredila, da niso izgubila zaupanja potrošnikov.

V primeru da potrošnik podjetju ne zaupa, predvsem da ne zaupa v namen upravljanja z njegovimi osebnimi podatki, bo uveljavljal pravico do izbrisa. Pravico do izbrisa poznamo od maja 2014, ko je avstrijski odvetnik zaradi nezaupanja v podjetje Facebook želel vpogled v osebne podatke, ki jih je podjetje hranilo o njem. Po vpogledu je želel te podatke tudi za vedno izbrisati. Njegovi tožbi je pritrdilo Evropsko sodišče za človekove pravice. Pravica do izbrisa je sedaj opredeljena tudi v GDPR-ju. Po ureditvi v Republiki Sloveniji so sicer potrošniki imeli to pravico že prej.

Namen magistrskega dela je bil podrobno preučiti zakonodajo na področju varovanja osebnih podatkov ter vpliv zakonodaje na podjetja, natančneje na trženje podjetij v Sloveniji. Preveril sem, ali je učinek sprejetja GDPR-ja na gospodarske subjekte tako radikalen, kot so trdili nekateri akterji v mesecih, preden je GDPR stopil v veljavo.

Cilj magistrskega dela je bil ugotoviti, kako se podjetja soočajo z uvedbo GDPR-ja in kakšne posledice ima to za trženje v izbranih podjetij. Zanimalo me je, ali so bila podjetja na sprejetje zakonodaje pripravljena že pred 25. majem 2018. To sem naredil z analizo spletnih strani pred 25. majem 2018 in po 25. maju 2018. Hkrati pa sem z raziskavo med posamezniki ugotovil, do kakšne mere so pripravljeni deliti svoje osebne podatke z izbranimi podjetji.

Raziskovalno vprašanje se glasi:

Kako bo sprejeta Splošna uredba o varstvu osebnih podatkov vplivala na pripravljenost potrošnikov, da svoje osebne podatke posredujejo gospodarskim subjektom?

Metodološko sem magistrsko delo razdelil na dva dela: (1) kritično analizo in sintezo obstoječe literature ter (2) konkretno študijo s pomočjo metode anketiranja:

- s kritično analizo in sintezo obstoječe literature sem primerjal pravno ureditev področja varstva osebnih podatkov pred in po sprejetju GDPR-ja. Hkrati me je zanimalo, zakaj je prišlo do takšne različice GDPR-ja, kot jo poznamo danes, in kakšen vpliv je in bo imelo sprejetje.
- Konkretno študijo sem izpeljal zato, da sem izvedel, kako posledice sprejetja GDPR-ja čutijo potrošniki in kako to vpliva na gospodarske subjekte.

S pomočjo kvalitativne analize sem preveril aktivnosti v zvezi z varovanjem osebnih podatkov 10 slovenskih podjetij v digitalnem okolju. Preveril sem, ali so podjetja že pred 25. majem 2018 izvajala aktivnosti (ozaveščanje in uveljavljanje pravic), ki jasno kažejo na to, da so si izbrana podjetja želela potrošniku jasno predstaviti pravice na področju varovanja osebnih podatkov in so na tak način poskrbela za večje zaupanje. Preveril sem, ali so podjetja pred 25. majem 2018 omogočala uporabniku uveljavljanje pravic, ki jih predpisuje Zakon o varstvu podatkov (ZVOP-1), Ur. l. RS, št. 94/07. Te so pravica do vpogleda (seznanitev), spremembe in do izbrisa.

Preverjal sem tudi, kdaj in če sploh, so začela podjetja omogočati uveljavljanje novih pravic skladno z 18. členom GDPR-ja:

- omejevanje:
  - posameznik oporeka točnosti podatkov – obdobje, ki upravljavcu omogoča preveriti točnost;
  - obdelava je nezakonita – posameznik nasprotuje izbrisu in zahteva omejitev;
  - ni več namena pri upravljavcu – posameznik jih potrebuje za uveljavljanje, izvajanje ali obrambo pravnih zahtevkov;
  - posameznik je vložil ugovor – do presoje oziroma preverbe;
- pravica prejeti osebne podatke (prenosljivost), ki jih je upravljavcu posredoval v:
  - strukturirani,
  - splošno uporabni,
  - strojno berljivi,
  - interoperabilni obliki.

Da sem to dosegel, sem primerjal spletne strani podjetij na dan 1. januarja 2018 in spletne strani podjetij na dan 1. januarja 2019. Vpogled v arhiv spletnih strani je dostopen na www.archive.org. Ker nekatere strani niso bile arhivirane s strani www.archive.org, sem pogledal arhiv strani, ki je najbližji izbranem datumu.

1 PRAVNA UREDITEV VARSTVA OSEBNIH PODATKOV

1.1 Zgodovinski pregled

V Slovarju slovenskega knjižnega jezika je pridevnik oseben (1994, str. 464) opredeljen kot nekaj, kar se nanaša na neko osebo in kar je posamezniku lastno in se ne nanaša na družbeno skupnost. Pridevnik zaseben (1994, str. 756) pa kot nekaj, kar je last posameznika. Nasprotje zasebnega je javno. Kovačič (2003, str. 34) trdi, da je zasebnost temelj človeškega dostojanstva in drugih vrednot. Pravica do zasebnosti je sicer temeljna, ne pa absolutna. Čebulj (1992, str. 7) govori o treh sestavinah zasebnosti: zasebnost v prostoru, zasebnost osebnosti in informacijska zasebnost – to je možnost posameznika, da obdrži podatke in informacije o sebi, ker ne želi, da bi bili z njimi seznanjeni drugi.

Osebnostne pravice so se razvile kot pravice, ki naj varujejo določene človekove dobrine, človeka, njegovo osebnost (Finžgar, 1985, str. 13). Njihova zgodovina sega v leto 1215, ko je prišlo do zapisa Velike listine svoboščin (lat. Magna Carta Libertatum), in se nadaljuje s slednjimi pomembnejšimi dokumenti:

- Petition of Right iz leta 1628;
- Bill and Declaration of Rights and Liberties of the Subject iz leta 1689;
- Bill of Rights iz Virginije z dne 12. junij 1776;
- Francoska deklaracija pravic človeka in državljana z dne 26. avgust 1789;
- Splošna deklaracija človekovih pravic z dne 10. december 1948;
- Mednarodni akt o državljanskih in političnih pravicah z dne 16. december 1966;
- Mednarodni pakt o ekonomskih, socialnih in kulturnih pravicah z dne 16. december 1966.

Da bi razumeli pojem zasebnosti, moramo razumeti osebnostne pravice kot ene izmed temeljnih pravic in svoboščin. So posebna vrsta pravic, ki ščitijo pravico do nepredmetne dobrine človeka – njegovo čast, javno podobo, pravico do zasebnosti, ohranjenosti svoje intimne sfere ter v tem oziru odmaknjenosti in varovanja informacij o sebi. Pri tem gre za pravice, ki pripadajo posamezniku in tvorijo osebnost v odnosu do drugih. Temeljne osebnostne pravice in zasebnost so za razvoj posameznika pomembne osebne dobrine. Določenim osebnostnim pravicam se lahko odpovemo – npr. operacija (Finžgar, 1985, str. 14).

Dolenc (2018, str. 125) trdi, da je zasebnost nujen instrument za vzpostavitev javne podobe nekega posameznika. Vsak sam lahko izbira, katere informacije o sebi bo dovolil javnosti v vpogled in komu bo te informacije izdal. V primeru, da posameznik ne more samovoljno razpolagati s svojimi podatki, bo zelo težko prevzel podobo nedoločenega abstraktnega človeka, ki je nujno potreben za delovanje demokratične družbe. Informacijska tehnologija zmeraj bolj odstranjuje meje zasebnosti, s čimer je zasebnost postala nedotakljiva in prav tako pomembna pravica kot sta pravica do življenja in pravica do svobode. V svetu je splošno sprejet koncept pričakovane zasebnosti. Koncept govori o temu, da je potrebno pretehtati dva elementa tj. pričakovanje zasebnosti in upravičenost takšnega pričakovanje v družbi. Če posameznik na nekem področju izrazi pričakovanje oz. željo do zasebnosti in je to njegovo pričakovanje družbeno upravičeno, potem v takšnem primeru ne moremo in ne smemo oporekati njegovi zasebnosti.

Kovačič (2003, str. 35) trdi, da začetki zakonodaje na področju varstva osebnih podatkov segajo že v leto 1361, ko je britanski zakon o pravici do miru (ang. Justice of the Peace Act) predvidel kazni za osebe, ki so skrivaj opazovale druge posameznike in jim prisluškovale. Leta 1765 je britanski lord Camden protestiral, ker so preiskovalci želeli vstopiti v njegovo hišo in zaseči neke listine. Leta 1776 je švedski parlament sprejel zakon o dostopnosti javnih zapisov. Leta 1890 pa sta ameriška pravnika Samuel Warren in Louis Brandeis opredelila zasebnost kot pravico posameznika, da se ga pusti pri miru. Da bi razumeli koncept prava človekovih pravic v 21. stoletju, moramo razumeti njihov razvoj. Po množičnem kršenju človekovih pravic je v mednarodni skupnosti prišlo do ugotovitve, da je trebe vzpostaviti mehanizem mednarodnega prava. S tem namenom so bili v okviru Združenih narodov sprejeti:

- Splošna deklaracija o človekovih pravicah (1948);
- Mednarodni pakt o državljanskih in političnih pravicah (1966);
- Mednarodni pakt o ekonomskih, socialnih in kulturnih pravicah (1966).

To je le del dokumentov, ki opredeljujejo univerzalno mednarodno pravo.

Poleg univerzalnega mednarodnega prava moramo poznati tudi regionalno pravno ureditev. V državah članicah Evropske unije tako poznamo pravice s področja varstva osebnih podatkov predvsem v okviru Sveta Evrope in njegovega glavnega pravnega temelja prava človekovih pravic – Evropske konvencije o varstvu človekovih pravic in temeljnih svoboščin (RS 33/1994), Ur. l. RS, št. 7-41.

Prvi nacionalni zakon o varstvu osebnih podatkov na evropskem področju je sprejela Zvezna republika Nemčija leta 1970. Prve potrebe po varovanju osebnih podatkov so se sicer najprej pojavile v ZDA že v letih 1965 in 1966. Na osnovi tega so bili izdelani tudi prvi osnutki zakona o zaščiti in varstvu podatkov. Prvi uradni pravni dokument, ki je temeljil na teh razpravah, je bil sprejet v ZDA leta 1970 in je urejal posredovanje osebnih podatkov o posojilojemalcih. Istega leta je bil sprejet prvi zakon o zaščiti podatkov v nemški zvezni deželi Hessen v ZR Nemčiji. Prvi državni zakon na tem področju je sprejela Švedska leta 1973, leto kasneje ZDA, kmalu pa je sledilo še več evropskih držav. Povod za sprejetje teh zakonov je bilo poročilo, ki ga je 31. januarja 1974 pripravil Generalni sekretar OZN za Ekonomsko-socialni svet Združenih narodov: »Človekove pravice, znanstveni in tehnološki razvoj – uporaba elektronike, ki lahko vpliva na pravice oseb in omejitve, ki bi morale veljati pri taki uporabi v demokratičnih družbah« (Križaj, 1989, str. 79).

Ministrski Zbor Evropskega sveta je leta 1974 objavil posebno resolucijo o varovanju zasebnosti zaradi uporabe elektronske obdelave podatkov v javnem in zasebnem. S to resolucijo so bila vsem članicam Evropskega sveta dana priporočila za pravno varstvo osebnih podatkov in zasebnosti v smislu 8. člena Evropske konvencije o varstvu človekovih pravic in temeljnih svoboščin. Leta 1981 je bila kot posledica tega sprejeta Konvencija Evropskega sveta o zaščiti osebnih podatkov zaradi avtomatske obdelave osebnih podatkov. Konvencija je definirala pojme, kot so osebni podatek (od sedaj naprej OP), avtomatska obdelava, odgovorna oseba za datoteko. Prav tako je definirala merila za opredelitev kakovosti, npr. da morajo biti podatki obdelani pošteno in zakonito, shranjeni naj bodo za točno določen namen, zbrani naj bodo le nujno potrebni, naj bodo ažurni, naj bodo shranjeni le do takrat, ko je to nujno potrebno. Definirala je tudi posebne občutljive podatke (Križaj, 1989, str. 81).

1.2 Razvoj prava varstva osebnih podatkov

Varstvo osebnih podatkov se je razvilo iz varstva zasebnega življenja, ki ga opredeljuje 12. člen Splošne deklaracije človekovih pravic (A/RES/217A (III) 1948), ki govori o tem, da ima vsakdo pravico do pravnega varstva v primeru tujega vmešavanja v zasebno življenje, družino, dom ali dopisovanje ali v primeru žaljenja časti in dobrega imena.

Zaradi zavedanja o pomembnosti področja varstva osebnih podatkov je bila leta 1981 v Strasbourgu sprejeta Konvencija o varstvu posameznikov glede na avtomatsko obdelavo osebnih podatkov (v nadaljevanju KonVOP), ki je bila v Sloveniji ratificirana v začetku leta 1994 (Ur. l. RS, št. 11/1994). Temelj konvencije je na ozemlju vsake pogodbenice vsakemu posamezniku zagotoviti spoštovanje njegovih pravic in temeljnih svoboščin. Še posebej spoštovanje pravic do zasebnosti glede na avtomatsko obdelavo osebnih podatkov, ki se nanašajo na posameznika.

1.3 Temeljna načela

Konvencija o varstvu posameznikov glede na avtomatsko obdelavo osebnih podatkov je izredno pomembna za razumevanje varstva osebnih podatkov, saj v prvem poglavju definira izraze:

- osebni podatek,
- avtomatska zbirka osebnih podatkov,
- avtomatska obdelava,
- upravljavec zbirke podatkov.

V drugem poglavju pa so določena temeljna načela zaščite varstva osebnih podatkov. Državam pristopnicam narekuje tudi, da morajo z nacionalno zakonodajo prevzeti ukrepe, potrebne za uresničitev temeljnih načel; ta so:

- načelo kakovosti podatkov – osebni podatki morajo biti pridobljeni in obdelani pošteno in zakonito, smejo biti shranjeni le za določene namene in le za namene, za katere so bili shranjeni. Posebne vrste osebnih podatkov se ne smejo obdelovati avtomatsko;
- načelo zavarovanja podatkov;
- načelo odprtosti in sodelovanja – vsak posameznik, na katerega se osebni podatek nanaša, ima pravico, da ugotovi obstoj posamezne avtomatske zbirke, namene in sedež zbirke. Posameznik ima pravico do izpisa osebnih podatkov, ki se nanašajo nanj. Ima tudi pravico do popravka ali izbrisa podatkov, če so bili obdelovani v nasprotju s pravili.

Konvencija v tretjem poglavju določa področje prenosa čez državne meje. Prenos je mogoč, če zakonodaja druge oz. tretje države na področju varstva osebnih podatkov omogoča enakovredno zaščito. Na pomembnost načel kaže tudi dejstvo, da so bila ta povzeta tudi v Evropsko direktivo iz leta 1995. Gre za Direktivo o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku teh podatkov (DirVOP) (Čebulj & Žurej, 2005, str. 19).

Ustava Republike Slovenije (Ur. l. RS, št. 33/91-I, 42/97 – UZS68, 66/00 – UZ80, 24/03 – UZ3a, 47, 68, 69/04 – UZ14, 69/04 – UZ43, 69/04 – UZ50, 68/06 – UZ121, 140, 143, 47/13 – UZ148 in 47/13 – UZ90, 97, 99; v nadaljevanju Ustava) v 35. členu zagotavlja nedotakljivost človekovega telesa in zasebnosti vsem fizičnim osebam.

Informacijski pooblaščenec (2019) trdi, da je za normativno urejanje varstva osebnih podatkov pomemben predvsem drugi odstavek 38. člena Ustave, ki določa, da zbiranje, obdelovanje, namen uporabe, nadzor in varstvo tajnosti osebnih podatkov določa zakon (splošen, sistemski zakon in področni zakoni). Tukaj se govori o ti. obdelovalnem modelu z določenimi pravili za urejanje dopustne obdelave osebnih podatkov na zakonski ravni. Na podlagi tega modela je na področju varstva osebnih podatkov prepovedano vse, razen tistega, kar je z zakonom (na področju zasebnega sektorja tudi z osebno privolitvijo posameznika) izrecno dovoljeno. Vsaka obdelava osebnih podatkov torej pomeni poseg v ustavno varovano človekovo pravico. Tak poseg je dopusten le, če je v zakonu opredeljeno, kateri osebni podatki se smejo obdelovati, kaj je namen njihove obdelave, zagotovljeno pa mora biti ustrezno varstvo in zavarovanje osebnih podatkov. Namen obdelave osebnih podatkov mora biti tudi ustavno dopusten, obdelovati pa se smejo tisti osebni podatki, ki so primerni in nujno potrebni.

Iz besedila 38. člena tako razberemo štiri ključna načela:

- načelo zakonitosti,
- načelo namenskosti (namen mora biti določen prej),
- načelo seznanjenosti (o tem, da se zbirajo podatki o posamezniku),
- načelo sodnega varstva.

V Republiki Sloveniji (od sedaj naprej Slovenija) sicer področje varstva osebnih podatkov opisuje ZVOP-1. Razlog za sprejetje tega zakona je bil prenos vsebin določb Direktive 95/46/ES o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku podatkov. ZVOP-1 je na trenutke težko razumljiv in z vidika zaščite osebnih podatkov rigorozen zakon, vendar je v slovenski pravni red prinesel pomembne novosti glede zavedanja o teži in pomenu varstva osebnih podatkov. V Sloveniji je zagotovljeno varstvo osebnih podatkov, uporaba v nasprotju z namenom zbiranja pa je prepovedana. Že Ustava določa pravico posameznika do seznanitve z zbranimi osebnimi podatki (Pirc Musar, Prelesnik & Bien, 2006a, str. 361).

Za razumevanje področja varstva osebnih podatkov se je potrebno seznaniti s temeljnimi pojmi, ki jih v 6. členu določa ZVOP-1:

- osebni podatek je katerikoli podatek, ki se nanaša na posameznika, ne glede na obliko, v kateri je izražen;
- posameznik je določena ali določljiva fizična oseba, na katero se osebni podatek nanaša. Oseba je določljiva, če se jo lahko neposredno ali posredno identificira, predvsem s sklicevanjem na identifikacijsko številko (npr. EMŠO, davčna številka) ali na enega ali več dejavnikov, ki so značilni za njeno fizično, fiziološko, duševno, ekonomsko, kulturno ali družbeno identiteto, pri čemer način identifikacije ne povzroča velikih stroškov, nesorazmerno velikega napora ali velike porabe časa;
- obdelava osebnih podatkov pomeni kakršnokoli delovanje ali niz delovanj v zvezi z osebnimi podatki, ki so obdelani avtomatizirano, so pri ročni obdelavi del zbirke osebnih podatkov ali pa so namenjeni vključitvi v zbirko osebnih podatkov, zlasti pa za zbiranje, pridobivanje, vpis, urejanje, shranjevanje, prilagajanje ali spreminjanje, priklicanje, vpogled, uporabo, razkritje s prenosom, sporočanje, širjenje ali drugo dajanje na razpolago, razvrstitev ali povezovanje, blokiranje, anonimiziranje, izbris ali uničenje, pri čemer je prepovedana obdelava osebnih podatkov v nasprotju z namenom njihovega

zbiranja, ki mora biti predhodno, vnaprej določen. Obdelava je lahko ročna ali avtomatizirana s sredstvi informacijske tehnologije.

Vodila pri vsaki obdelavi osebnih podatkov so tri temeljna načela ZVOP-1:

- načelo zakonitosti in poštenosti, po katerem se morajo osebni podatki obdelovati zakonito in pošteno (2. člen ZVOP-1);
- načelo sorazmernosti določa, da morajo biti osebni podatki, ki se obdelujejo, ustrezni in po obsegu primerni glede na namene, za katere se zbirajo in nadalje obdelujejo (3. člen ZVOP-1);
- načelo prepovedi diskriminacije zagotavlja varstvo osebnih podatkov vsakemu posamezniku ne glede na narodnost, raso, barvo, veroizpoved, etično pripadnost, spol, jezik, politično ali drugo prepričanje, spolno usmerjenost, premoženjsko stanje, rojstvo, izobrazbo, družbeni položaj, državljanstvo, kraj oziroma vrsto prebivališča ali katerokoli drugo osebno okoliščino (4. člen ZVOP-1).

1.3.1 Občutljivi osebni podatki

Določba 19. točke 6. člena ZVOP-1 govori o posebej zaščiteni kategoriji osebnih podatkov. Ti so, zaradi svoje subtilnosti, občutljivi osebni podatki. To so podatki o rasnem, narodnem ali narodnostnem poreklu, političnem, verskem ali filozofskem prepričanju, članstvu v sindikatu, zdravstvenem stanju, spolnem življenju, vpisu ali izbrisu v kazensko ali prekrškovno evidenco ter biometrične značilnosti posameznika.

1.3.2 Iznos osebnih podatkov v druge države

ZVOP-1 dovoljuje iznos osebnih podatkov po Sloveniji in drugih državah članicah EU. Iznos v tretje države pa je dovoljen pod pogojem, da tretja država zagotavlja ustrezno raven varstva osebnih podatkov. To določi Informacijski pooblaščenec.

1.4 Naloge države pri varovanju pravic

Sodno varstvo ob zlorabi osebnih podatkov posamezniku zagotavlja že Ustava, kljub temu pa je v ZVOP-1 zapisanih več kavtel:

- točnost in ažurnost podatkov – obdelovani osebni podatki morajo biti točni in ažurni;
- obveščanje posameznika o obdelavi osebnih podatkov – posameznik ima ob vsaki obdelavi pravico, da se seznani o upravljavcu, kot z namenom obdelave;
- rok hrambe osebnih podatkov – osebni podatki se morajo brisati takoj, ko je namen obdelave dosežen, razen če so opredeljeni kot arhivsko gradivo oziroma če zakon določa drugače;
- posredovanje osebnih podatkov – upravljavec jih mora posredovati uporabnikom (praviloma za plačilo). Dolžnost upravljavca pa je zagotavljanje sledljivosti za vsako posredovanje;
- varstvo osebnih podatkov umrlih posameznikov;

- zavarovanje osebnih podatkov – namen teh določb je preprečevanje naključnega ali namernega nepooblaščenega uničevanja podatkov ter preprečevanje sprememb, izgube ali nepooblaščene obdelave.

Konec leta 2005 smo v Sloveniji združili Inšpektorat za varstvo osebnih podatkov in Pooblaščenca za dostop do informacij javnega značaja v samostojen in neodvisen državni organ Informacijskega pooblaščenca. Ta pod svojo streho združuje dostop do informacij javnega značaja in varstvo osebnih podatkov. Informacijski pooblaščenec se ukvarja z izjemno pomembnima človekovima pravicama, ki sta v Sloveniji zapisani kot ustavni kategoriji. V 2. odstavku 39. člena Ustave je zapisano, da ima vsakdo pravico dobiti informacijo javnega značaja, za katero ima v zakonu utemeljen pravni interes, razen v primerih, ki jih določa zakon. 38. člen Ustave pa določa, da je v Sloveniji zagotovljeno varstvo osebnih podatkov. Prepovedana je uporaba osebnih podatkov v nasprotju z namenom njihovega zbiranja. Zbiranje, obdelovanje, namen uporabe, nadzor in varstvo tajnosti osebnih podatkov določa zakon. Drugi odstavek 38. člena še določa, da ima vsakdo pravico seznaniti se z zbranimi osebnimi podatki, ki se nanašajo nanj in pravico do sodnega varstva ob njihovi zlorabi (Pirc Musar, Prelesnik & Bien, 2006a, str. 363).

Pristojnosti Informacijskega pooblaščenca na podlagi 2. člena Zakona o Informacijskem pooblaščencu (ZInfP), Ur. l. RS, št. 113/05 so:

- odloča o pritožbi zoper odločbo, s katero je organ zavrgel ali zavrnil zahtevo ali drugače kršil pravico do dostopa ali ponovne uporabe informacije javnega značaja;
- v okviru postopka na drugi stopnji je pristojen tudi za nadzor nad izvajanjem zakona, ki ureja dostop do informacij javnega značaja, in na njegovi podlagi izdanih predpisov;
- izvršuje inšpekcijski nadzor nad izvajanjem zakona in drugih predpisov, ki urejajo varstvo ali obdelavo osebnih podatkov oziroma iznos osebnih podatkov iz Slovenije;
- odloča o pritožbi posameznika, kadar upravljavec osebnih podatkov ne ugodi zahtevi posameznika glede njegove pravice do seznanitve z zahtevanimi podatki, do izpisov, seznamov, vpogledov, potrdil, informacij, pojasnil, prepisovanja ali kopiranja po določbah zakona, ki ureja področje varstva osebnih podatkov;
- kot prekrškovni organ nadzoruje izvajanje ZInfP, Zakona o dostopu do informacij javnega značaja v okviru pritožbenega postopka in Zakona o varstvu osebnih podatkov (2. čl. ZInfP).

1.5 Pravice posameznika

V zvezi z obdelovanjem osebnih podatkov ima posameznik znotraj ZVOP-1 (30. člen) nekaj pravic:

- vpogled v katalog zbirke osebnih podatkov (nabor, opis zbirke);
- potrditev, ali se osebni podatki obdelujejo;
- vpogled v osebne podatke;
- prepisovanje ali kopiranje osebnih podatkov;
- seznam uporabnikov njegovih osebnih podatkov;
- informacije o virih, metodi in namenu obdelave;
- pojasniti tehnične postopke odločanja, če se izvaja avtomatizirano odločanje;
- pravica do dopolnitve, popravka, blokiranja, izbrisa in ugovora.

Zahtevo je mogoče vložiti enkrat na tri mesece, za občutljive osebne podatke in za videonadzor pa enkrat na mesec. Upravljavec mora omogočiti seznanitev najkasneje 15 dni po prejemu zahteve.

2 PREUČITEV PRAVNIH PODLAG VARSTVA OSEBNIH PODATKOV PO POSAMEZNIH PODROČNIH PREDPISIH

2.1 Neposredno trženje in varstvo osebnih podatkov

Statista, Inc. (2016) je objavila raziskavo, v kateri je 39 % evropskih potrošnikov izjavilo, da ponudniki rešitev medomrežje stvari (ang. internet of things) ne izražajo dovolj jasno informacij o tem, katere osebne podatke obdelujejo, in to niža zaupanje potrošnikov v storitev.

Quin in Roggers (2015) sta v študiji ugotovila, da kar 75 % potrošnikov z veseljem deli svoje osebne podatke s podjetjem, ki mu zaupajo. Avtorji študije o pripravljenosti strank za deljenje osebnih podatkov (Phelps, Nowak & Ferrell, 2000) so v raziskavi ugotovili, da tri četrtine intervjuvanih lastnikov osebnih podatkov želi več informacij o tem, za kaj jih podjetja uporabljajo. Hkrati pa so ugotovili, da lastnike osebnih podatkov, ki menijo, da bo dajanje osebnih podatkov podjetju prineslo njim bolj zanimive vsebine in oglase preko elektronske pošte, varnost skrbi precej manj.

Goodwin (1991) je v svoji raziskavi ugotovila, da bi potrošnike razjezilo dejstvo, da bi bili zaradi nedeljenja osebnih podatkov prikrajšani v marketinških akcijah. Mednarodno podjetje Deloitte v izvedeni študiji (Pingitore, Rao, Cavallaro & Dwivedi, 2017) predlaga, naj podjetja potrošnikom jasno povedo, za kateri namen potrebujejo njihove osebne podatke, jim omogočijo, da kadarkoli prenehajo z deljenjem le-teh, ter jih seznanijo z njihovimi pravicami. Temu pritrjuje tudi podjetje Swirl Networks Inc. (2015), ki trdi, da bodo podjetja na tak način od potrošnikov pridobila več podatkov, ki jih bodo lahko analizirala.

Evropski nadzornik za varstvo podatkov (2019) trdi, da lahko znotraj GDPR-ja poiščemo razlike med trženjem končnim kupcem in trženjem podjetjem. Za trženje končnim kupcem velja 6 načel, na podlagi katerih lahko obdelujemo osebne podatke. 2 izmed teh načel pa govorita o legitimnem interesu. Legitimen interes lahko povežemo z trženjem podjetjem. Uporaba legitimnega interesa je dovoljena pod naslednjimi pogoji:

- obdelava osebnih podatkov je dovoljena, če obstaja legitimni interes podjetja v povezavi z legitimnim interesom podjetja kot stranke;
- obdelava je nujno potrebna, da se doseže legitimen interes podjetja.

Godec (2018, str. 110) trdi, da bodo podjetja morala zelo dobro pregledati svoje sisteme za obdelavo osebnih podatkov in preveriti kdo na njihovih listah potrebuje katero informacijo v katerem trenutku. V nasprotnem primeru pa podatke o tej osebi ali stranki izbrisati.

2.1.1 Zakon o varstvu osebnih podatkov

72. člen ZVOP-1 govori o neposrednem trženju kot ponujanju blaga, storitev, zaposlitev ali začasnega opravljanja del z uporabo poštnih storitev, telefonskih klicev, elektronske pošte ali drugih telekomunikacijskih storitev. ZVOP-1 določa, katere osebne podatke lahko upravljavec upravlja in pod kakšnimi pogoji. Določen je tudi postopek in način prenehanja, če posameznik to izrecno zahteva. Upravljavec lahko uporablja osebne podatke posameznikov, ki jih je zbral iz javno dostopnih virov ali v okviru zakonitega opravljanja dejavnosti, tudi za namene ponujanja blaga, storitev, zaposlitev ali začasnega opravljanja del z uporabo poštnih storitev, telefonskih klicev, elektronske pošte ali drugih telekomunikacijskih sredstev (tj. neposredno trženje). Uporablja lahko le naslednje podatke: osebno ime, naslov stalnega ali začasnega prebivališča, telefonsko številko, naslov elektronske pošte ter številko telefaksa. Na podlagi osebne privolitve posameznika pa lahko obdeluje tudi ostale, občutljive pa pod pogojem, da je privolitev izrecna. Upravljavec mora posameznika obvestiti o njegovih pravicah. Če želi upravljavec osebne podatke posredovati, mora pridobiti pisno privolitev posameznika (Pirc Musar, Bien, Bogataj, Prelesnik & Žaucer, 2006, str. 87).

Pirc Musar (v Pirc Musar, Prelesnik & Bien, 2006b, str. 366-367) opredeli neposredno trženje kot način tržnega komuniciranja ter hkrati prodajna metoda preko različnih prodajnih poti. Poznamo več vrst neposrednega trženja:

- osebna prodaja,
- neposredno trženje po pošti,
- neposredno trženje po katalogu,
- neposredno trženje s pomočjo klicnih avtomatov,
- neposredno trženje s pomočjo faksimilnih naprav,
- neposredno trženje po televiziji,
- neposredno trženje po radiu, revijah in časnikih,
- neposredno trženje s pomočjo kioskov (informacijskih terminalov),
- neposredno elektronsko trženje (videotekst, prodaja preko interneta).

Najbolj razširjena je prodaja po internetu. Najpogosteje uporabljena internetna storitev je elektronska pošta. Poznamo pa še prenašanje datotek med vozlišči (FTP), priključitev na oddaljene računalnike (Telnet), svetovni splet (www), krožke razprav (Newsgroup) (Pirc Musar, Prelesnik in Bien, 2006b, str. 367).

Eden izmed najbolj pogosto uporabljenih načinov za pridobivanje soglasij za neposredno trženje, ki se jih poslužujejo podjetja, so nagradne igre. Izvajalci v drobnem tisku (skladno z ZVOP-1) zapišejo, da bodo osebne podatke uporabljali za namene neposrednega trženja. Posameznik, po mnenju Nataše Pirc Musar (Pirc Musar, Prelesnik & Bien, 2006a, str. 372), z vstopom v igro tiho soglaša s tem, da bodo njegovi osebni podatki uporabljeni za namene neposrednega trženja.

2. odstavek 72. člena omeni izrecno privolitev, ki pa v 6. členu (Pomen izrazov) ni omenjena. Pirc Musar in sodelavci (Pirc Musar, Prelesnik & Bien, 2006a, str. 373) menijo, da je zakonodajalec s tem hotel preprečiti uporabo t. i. občutljivih osebnih podatkov že na podlagi različnih konkludentnih (tihih) dejanj.

Posledice kršitev določb so sledeče. V inšpekcijskem postopku se v primeru kršitev izreče opozorilo, v prekrškovnem pa opozorilo ali sankcija (opomin, globa).

Razpon glob:

- pravna oseba in samostojni podjetnik: 4.170 EUR;
- odgovorna oseba pravne osebe: 830 EUR;
- odgovorna oseba državnega organa: 830 EUR;
- posameznik: 200 EUR.

Za kršitve določb o neposrednem trženju, videonadzoru večstanovanjskih objektov, določb o evidenci vstopov in izstopov so globe za polovico nižje. Če se plačilo izvede v predpisanem roku, se lahko plača polovično globo.

2.1.2 Zakon o elektronskih komunikacijah

157. člen Zakona o elektronski komunikacijah (ZEKom-1) Ur. l. RS, št. 109/12, 110/13, 40/14 – ZIN-B, 54/14 – odl. US, 81/15 in 40/17, je podlaga za regulacijo piškotkov. Ta od upravljavcev spletnih strani zahteva, da na spletno stran namestijo obvestilo o piškotkih in seznam piškotkov. Pred nameščanjem piškotkov mora biti predstavljena privolitev, bodisi domnevna ali izrecna. Temu pritrjuje tudi Informacijski pooblaščenec (2007), ki trdi, da je za uporabo piškotkov potrebna privolitev, razen če spletna stran uporablja t. i. nujne piškotke, ki so potrebni za nemoteno delovanje spletne strani.

Državni inšpektor Drev (2016) trdi, da če uporabljate lastno analitiko ali osnovno Google analitiko, zadošča le domnevna privolitev. To velja tudi za piškotke valutnih raziskav. Domnevna privolitev v tem primeru pomeni, da se piškotek namesti avtomatsko, vendar ima uporabnik možnost piškotke odstraniti, če jih ne želi. Če upravljavec uporablja kakršnekoli druge piškotke tretjih strani (napredna analitika, Facebook in Twitter vtičniki, oglasne piškotke), potrebuje izrecno privolitev posameznika. Prav tako to velja za oglaševalske piškotke, lastne ali tuje. Z izrecno privolitvijo se piškotek pred potrditvijo (npr. gumb »v redu« ali »strinjam se«) ne sme namestiti.

158. člen ZEKom z naslovom Nezaželene komunikacije omogoča nadzor naročnika nad uporabo osebnih podatkov za namene izvajanja neposrednega trženja, pri čemer je naročnik (20. točka 3. člena) vsaka fizična ali pravna oseba, ki z izvajalcem sklene pogodbo za uporabo storitev. Uporaba samodejnih klicnih sistemov je dovoljena samo, če naročnik predhodno soglaša s tem. Kljub temu pa lahko kadarkoli pridobi elektronski naslov posameznika in ga uporablja za namene neposrednega trženja svojih podobnih izdelkov ali storitev, vendar mora kupcu dati možnost, da kadarkoli na brezplačen in enostaven način zavrne takšno uporabo svojega elektronskega naslova. Uporaba drugačnih sredstev s pomočjo elektronskih komunikacij je dovoljena le s soglasjem naročnika. Uporaba trženja s skrito oz. prikrito identiteto ali brez veljavnega naslova, preko katerega odjava ni mogoča, ni dovoljena (Pirc Musar, Prelesnik & Bien, 2006b, str. 368).

ZEKom v nasprotju z ZVOP-1 ne dovoljuje uporabe osebnih podatkov iz javnih virov. Gre za tako imenovano načelo *opt-in* (upoštevanje privolitve), ki pomeni, da pošiljatelj ne sme pošiljati sporočil brez vnaprejšnjega soglasja posameznika. Nasprotje temu je načelo *opt-*

out (upoštevanje zavrnitve), ki velja v ZVOP-1 in ki predvideva, da mora prejemnik sam izraziti zahtevo za prekinitev prejemanja trženjskih oz. reklamnih sporočil. Načelo *opt-out* v ZEKom velja v primeru trženja svojih podobnih izdelkov ali storitev preko elektronske pošte. ZEKom specialno ureja zgolj vidike elektronske komunikacije, vse druge oblike neposrednega trženja pa so v celoti podrejene ureditvi, ki jo določa ZVOP-1 (Pirc Musar, Prelesnik & Bien, 2006a, str. 370).

2.1.3 Zakon o varstvu potrošnikov

45a. člen Zakona o varstvu potrošnikov (ZVPot) Ur. l. RS, št. 98/04 – uradno prečiščeno besedilo, 114/06 – ZUE, 126/07, 86/09, 78/11, 38/14, 19/15, 55/17 – ZKolT in 31/18, govori o neposrednem trženju, ki pa je delno v nasprotju s 158. členom ZEKom. Ker pa je ZEKom novejši izmed obeh zakonov in je uzakonil novejšo ureditev, ki izhaja iz Direktive 2002/58/ES Evropskega parlamenta in Sveta, ZEKom po načelu *lex posterior derogat legi priori* prevlada nad ZVPot (Pirc Musar, Prelesnik & Bien, 2006b, str. 369).

2.1.4 Zakon o poštnih storitvah

38. člen Zakona o poštnih storitvah (ZPSto-2) Ur. l. RS, št. 51/09, 77/10, 40/14 – ZIN-B in 81/15 ureja neposredno trženje v zvezi s prepovedjo vročanja nenaslovljenih pošiljk v poštni predalčnik. V primeru da posameznik na poštni predalčnik nalepi ustrezno nalepko, ki jo izda Agencija za telekomunikacije, radiodifuzijo in pošto Republike Slovenije, s tem prepove vročanje nenaslovljenih oglaševalskih, marketinških in drugih reklamnih sporočil.

2.1.5 Zakon o elektronskem poslovanju na trgu

Zakon o elektronskem poslovanju na trgu (ZEPT) Ur. l. RS, št. 96/09 definira komercialno sporočilo kot vsako oblika sporočila, namenjeno neposredni ali posredni promociji blaga, storitev ali podobe podjetja, organizacije ali osebe, ki opravlja trgovsko, industrijsko ali obrtno dejavnost ali reguliran poklic, pri čemer podatki, ki omogočajo neposreden dostop do dejavnosti podjetja, organizacije ali osebe, predvsem ime domene ali elektronski naslov in sporočila v zvezi z blagom, storitvami ali podobo podjetja, organizacije ali osebe, ki se zagotavljajo neodvisno in brez finančnega nadomestila, sami po sebi še niso komercialno sporočilo (Pirc Musar, Prelesnik & Bien, 2006a, str. 380).

Ponudnik storitev po mnenju Pirc Musarjeve (Pirc Musar, Prelesnik & Bien, 2006a, str. 381) tako lahko pošilja komercialna sporočila, ki so del storitev informacijske družbe, če:

- prejemnik storitve vnaprej soglaša s pošiljanjem;
- je komercialno sporočilo kot tako jasno razpoznavno;
- je nedvoumno navedena fizična ali pravna oseba, v imenu katere je komercialno sporočilo poslano;
- so jasno in nedvoumno navedeni pogoji za sprejem posebnih ponudb, ki so povezane s popusti, premijami in darili, ki morajo biti kot taki nedvoumno označeni;
- so jasno in nedvoumno ter lahko dostopno navedeni pogoji za sodelovanje v nagradnih tekmovanjih ali igrah na srečo, ki morajo biti kot taki jasno razpoznavni.

Prav tako je potrebno upoštevati pravila o soglasju prejemnika skladno z ZVOP-1. Nekoliko drugače je z elektronskimi naslovi, če ga pravna oseba javno objavi kot svoj kontaktni elektronski naslov. V tem primeru je pošiljanje dovoljeno, saj se šteje kot kontakt poslovnega subjekta (Pirc Musar, Prelesnik & Bien, 2006a, str. 370).

2.2 Smernice Informacijskega pooblaščenca

Informacijski pooblaščenec (2019) trdi, da so bistvene novosti, ki jih prinaša GDPR predvsem nove in okrepljene pravice posameznika, poleg obstoječih predvsem pravica do prenosljivosti podatkov. Opozarja, da je večji poudarek na transparentnosti obdelave, torej glede zagotavljanja preglednih in lahko dostopnih informacij posameznikom o obdelavi njihovih podatkov. GDPR določa tudi nove obveznosti upravljavcev in obdelovalcev podatkov, kot so obveznost izvajanja ustreznih varnostnih ukrepov in obveznost uradnega obveščanja o kršitvah varstva osebnih podatkov, imenovanje pooblaščenih oseb za varstvo podatkov, izvajanje ocen učinka. Upravljavci sedaj niso več dolžni prijavljati zbirk osebnih podatkov v register zbirk osebnih podatkov, ostajajo pa dolžnosti sprejema popisa zbirk (t. i. evidence dejavnosti obdelave), ki se krepijo in uvajajo tudi za (pogodbene) obdelovalce. GDPR daje večji poudarek načelu odgovornosti in preventivnim ukrepom, poleg omenjenih mehanizmov zagotavljanja skladnosti pa uvaja tudi možnost potrjevanja sektorskih kodeksov ravnanja in certifikacije.

Informacijski pooblaščenec (2018a) opozarja na načine, ki jih podjetja uporabljajo, da bi prišla do več informacij o svojih potrošnikih. Primer takih je izpolnjevanje vprašalnika, pri katerem za nagrado sodeluješ v nagradni igri. Pri tem se je potrebno zavedati, da podjetja to delajo, da bi bolje spoznala svoje potencialne in obstoječe stranke. Temu pritrjuje tudi Kotler (1996, str. 21), ki trdi, da lahko podjetja te podatke nato uporabijo, za namen izboljšanja trženja. Predvsem za razdeljevanje strank v podskupine glede na starost, nakupne navade, hobije itd. Vsaki stranki nato pošiljajo sporočila v zvezi s tematiko, ki bi jih najbolj znala zanimati. Če ima nekdo rad pse, mu pošiljajo oglase o psih. Potrebno se je zavedati, da so to posameznikovi podatki in je odločitev na potrošniku, hkrati pa je podjetje dolžno obvestiti potrošnika o tem, da s tem, ko nekdo reši anketo dovoljuje obdelavo osebnih podatkov. To mora storiti zelo jasno. Podjetje lahko sprašuje po posebnih vrstah osebnih podatkov (zdravstveno stanje, politična pripadnost, itd.). Če namerava podjetje te podatke uporabiti, mora potrošnika o tem tudi prehodno obvestiti.

Informacijski pooblaščenec (2018a) posebno pozornost namenja tudi karticam ugodnosti, ki jih uporablja že praktično vsaka trgovina. Z včlanitvijo v tak klub stranka pridobi možnost popustov in raznih ugodnosti, sodelovanja v nagradni igri itd. Podjetja pa tako pridobljene osebne podatke uporabljajo tudi za namene trženja. Člani kluba oziroma imetniki kartice tako prejemajo komercialna obvestila ipd. Pravila obdelave osebnih podatkov potrošnika so v tem primeru enaka. Podjetje je dolžno pojasniti kdo bo te podatke obdeloval, kakšen je namen in katere podatke se bo obdelovalo. Informacijski pooblaščenec opozarja na dejstvo, da se zbirajo podatki o tem kdo kupuje, kje, kaj, kdaj. Na podlagi takšnih informacij lahko podjetje trženjsko popolnoma personalizira. To pomeni, da ima v praksi popolno sliko nekega posameznika.

Informacijski pooblaščenec (2018a) posebno pozornost namenja nagradnim igram. V pravilih nagradne igre mora biti določena obdelava osebnih podatkov. Večkrat se na spletu pojavijo imena nagrajencev. To se lahko naredi le, če je v pravilih igre izrecno pisalo, da

bodo nagrajenci objavljeni in so se sodelujoči s temi pogoji strinjali. Torej, da so podali izrecno privolitev. Za prav vsak namen posebej je potrebno podati ločeno privolitev. Npr. za EMŠO, davčno številko.

Klemenčič trdi (Klemenčič, Makarovič, Klobučar, Bogataj Jančič & Pahor, 2003, str. 46.), da mora podjetje mora takoj po prenehanju namena obdelave podatkov podatke uničiti. Torej, ko je nagradna igra zaključena, je treba zbrane osebne podatke uničiti ali ireverzibilno šifrirati – spraviti v brezosebno obliko.

Informacijski pooblaščenec (2018b) govori tudi o virusnem marketingu, kot o eni izmed oblik marketinga, ki temelji na širjenju sporočila od »ust do ust«. Npr. Mojca obišče njej zanimivo spletno stran, kjer oglašujejo nagradno igro. Glavna nagrada je najnovejši iPhone. Za sodelovanje v nagradni igri se mora Mojca zgolj prijaviti in vpisati e-mail naslove svojih prijateljev, ki jim nato avtomatsko pošlje vabilo za sodelovanje v nagradni igri. S tem Mojca sodeluje v žrebanju za obljubljeno nagrado. Pravzaprav gre tukaj za to, da se z obljubo nagrade dregne potrošnike, da svojim prijateljem sami pošljejo oglase v imenu podjetja. Podjetje s tem ne krši zakonodaje o neposrednem trženju (ti. spam). Podjetja trdijo tudi, da v tem procesu oni niso v vlogi nekoga, ki zbira in obdeluje osebne podatke (e-mail naslove) brez privolitve lastnikov, temveč le v vlogi ponudnika storitve posredovanja elektronske pošte.

Kot eno od vrst virusnega marketinga Informacijskih pooblaščenec (2018b) opozarja tudi na sistem priporočanja povezav. Gre za spletne strani z gumbom »Priporočite to stran znancu«. S klikom na povezavo se odpre posebno okno, ki vsebuje prazna polja, kamor je potrebno vnesti (vsaj) elektronski naslov prijatelja, ki mu želi obiskovalec priporočiti spletno stran oziroma njeno vsebino. Naslovniku se s tem posreduje prijazno sporočilo, kjer med drugim piše, da mu njegov prijatelj priporoča ogled strani.

Informacijski pooblaščenec (2018b) odgovornost za pošiljanje teh vrst elektronskih sporočil prelaga na stran potrošnika. Podjetje tukaj deluje le kot ponudnik infrastrukture, ki to storitev omogoča, in ne more prevzemati odgovornosti za dejanja uporabnikov svojih storitev, če so izpolnjeni naslednji pogoji:

- posameznik je tisti, ki vnese elektronske naslove prijateljev in odloči, komu bo sporočilo poslano;
- oglasno sporočilo, poslano potrošniku preko njegovega prijatelja, mora zelo jasno navajati, kdo je pobudnik pošiljanja sporočila;
- potrošnik mora imeti možnost prebrati celotno oglasno sporočilo, ki ga pošlje svojemu prijatelju, še preden se za to odloči. Le tako namreč lahko potrošnik prevzame odgovornost za vsebino sporočila. Podjetje pod nobenim pogojem ne sme spreminjati vsebine sporočila;
- podjetje ne sme shranjevati ali kakorkoli obdelovati elektronskih naslovov in drugih podatkov potrošnikov, ki jih vnesejo njihovi prijatelji.

Informacijski pooblaščenec (2008) poudarja, da moramo obdelavo osebnih podatkov razumeti precej široko. Obdelava osebnih podatkov je namreč kakršnokoli ravnanje z njimi. Med drugim o obdelavi osebnih podatkov govorimo tudi ob vpogledu, urejanju, brisanju, uničevanju, vnašanju, hrambi. O obdelavi govorimo tudi, če obdelovalec sploh ne ve, da za nekega upravljalca hrani določene vrste osebnih podatkov. Upravljalec je dolžan, da je

obdelovalec seznanjen z obdelavo osebnih podatkov, tudi v primerih, ko govorimo le o hrambi ali uničenju. Temu pritrjuje tudi Možina (2000, str. 24). Namreč, če obdelovalec ne ve, da je prejel v hrambo osebne podatke, potem ne more poskrbeti za ustrezno varovanje le teh. Izpostavlja še, da me pogodbeno obdelavo sodi:

- najem storitev podjetja, ki za podjetje izvaja videonadzor vhoda v poslovne objekte,
- najem storitev kontaktnega centra,
- najem storitev arhiviranja in hrambe OP,
- najem računovodskega podjetja,
- najem storitev arhiviranja in hrambe OP,
- najem podatkovnega centra za namen hrambe OP,
- vzdrževanje spletne strani s strani zunanjega ponudnika,
- prevoz OP na uničenje, vendar ne samo uničenje.

Informacijski pooblaščenec trdi (2009), da se vse večkrat zgodi, da v primeru uporabe sodobnih informacijskih rešitev ni jasno, kdo je odgovoren za kaj. Ne ve se namreč kdo je upravljalec in kdo obdelovalec. Kot primer navaja ponudnike gostovanja. Te namreč za svoje stranke večkrat hranijo tudi njihove zbirke OP in so tako tudi pogodbeni obdelovalci. Hramba namreč spada med obdelavo osebnih podatkov. Naročnik mora v teh primerih z njimi skleniti ustrezno pogodbo za obdelavo OP, kot upravljalec. Če pogodbe ni, je upravljalec tisti, ki nosi odgovornost, ker je on OP predal v hrambo brez ustrezne pravne podlage. Zapisano velja tudi v primerih, ko so osebni podatki šifrirani. Namen primerne ureditve pogodbene obdelave osebnih podatkov je:

- jasnost odnosa med izvajalcem in naročnikom,
- zagotovitev primerne varnosti pri obdelavi OP,
- točna razmejitev odgovornosti med obema stranema.

Ključno je, da ima upravljalec ves čas nadzor nad OP in, da ves čas skrbi za ustrezno varstvo teh podatkov (Praprotnik, 2006, str. 33). Primerna ureditev pogodbene obdelave pa mora biti v interesu upravljalca, saj je njegova dolžnost, da so te osebni podatki primerno varovani. V primeru nepravilnosti pa on nosi odgovornost za kršitve, ki jih je naredil obdelovalec ali pa v nekaterih primerih zunanji izvajalci. Če se postavimo v čevlje posameznika, nam hitro postane jasno, da je posamezniku vseeno kdo ima v določenem trenutku njegove osebne podatke. Važno je predvsem to, da so osebni podatki ustrezno varovani. Vloga upravljalca je ta, da obdeluje podatke le za točno določen namen in za točno določene cilje. Ključno pa je, da določi tudi, kdaj bodo te podatki izbrisani ali pa nepovratno šifrirani, ter kdo ima dostop do teh podatkov.

Informacijski pooblaščenec (2019) nadaljuje, da kadar se o namenih, ciljih in načinih obdelave odloča več entitet govorimo o skupnem upravljalcu. Obdelovalec pa lahko, za razliko od upravljalca, osebne podatke obdeluje le v okviru v naprej določenih pooblastil. Po opravljenem delu oziroma po dosegu določenega cilja v pogodbi, mora osebne podatke vrniti upravljalcu ali pa jih izbrisati. Le v določenih primerih podatke obdrži in takrat še vedno nosi odgovornost upravljalec. Pri razmejitvi vlog in določanju kdo je obdelovalec in kdo upravljalec, pa je pomembna vloga subjekta pri zajemu osebnih podatkov, določanju namenov in sredstev obdelave. V primerih, ko ima neko podjetje dostop do podatkov in določa namere ter sredstva obdelave, takrat ima to podjetje odgovornost upravljalca. Večkrat

se pojavljajo vprašanja ali je podjetje, ki ponuja neke nujno potrebne storitve, tudi obdelovalec. Takšna podjetja in organizacije so:

- prevajalci,
- pošta,
- telefonski operaterji,
- revizorji,
- sodni izvedenci,
- odvetniki,
- ponudniki storitev čiščenja,
- ponudniki spletnega gostovanja,
- ponudniki fizične hrambe (sefi).

Ko ugotavljamo ali je tako podjetje oz. organizacija obdelovalec, moramo pogledati naslednje kriterije:

- ali lahko sami določajo namen in sredstva obdelave OP,
- ali je obdelavo prenesel na nekoga drugega, čeprav bi obdelavo lahko opravil sam,
- kakšna je intenzivnost obdelovanja osebnih podatkov,
- ali ima pravno podlago, ki določa da je upravljalec,
- ali je prvotni namen najema storitev obdelava osebnih podatkov ali je to zgolj posledica.

Zgornje kriterije je vsakič potrebno presojati skupaj. Obdelovalec je tako tista fizična ali pravna oseba, ki bo obdelavo OP izvajala:

- samo za potrebe upravljalca,
- bo imela podlago za obdelavo OP kot upravljalec.

Upravljalec lahko da podatke obdelovalcu, ki poda zagotovila, da bo izvajal ustrezne tehnične in organizacijske ukrepe. Med elementi, ki jih je potrebno ob tem pogledati pa so:

- reference pogodbenega obdelovalca,
- zaupanje na trgu,
- zagotavljanje zadostnih pogojev storitve.

Upravljalec je dolžan ohraniti kontrolo nad subjekti, ki dostopajo do OP iz zbirk upravljalca. Ključno je torej, da upravljalec določa s kom bo sodeloval in s kom ne. GDPR določa, da more obdelovalec pridobiti pisno soglasje upravljalca, da lahko pogodbeni izvajalec obdeluje njegove osebne podatke. Upravljalec pa lahko obdelovalcu izda tudi splošno soglasje. To naredi v primerih, ko obdelovalcu tako zaupa, da bo on izbiral zgolj in samo najbolj primerne pogodbene obdelovalce. Mora pa v teh primerih obveščati upravljalca o vseh spremembah pogodbenih partnerjev. Pravice in obveznosti morata obe strani urediti pisno, to je s pogodbo. Obličnost sicer ni določena, vendar GDPR pravi, da mora biti znotraj dokumenta določena:

- vsebina in trajanje,
- narava in namen,
- vrste OP,
- kategorije lastnikov osebnih podatkov,

- obveznosti in pravice upravljalca.

Informacijski pooblaščenec (2019) priporoča, da so v vseh pogodbah tudi podatki pooblaščene osebe za varstvo osebnih podatkov, če so jo podjetja imenovala. Ta predlog ni obvezen, je pa smiseln, saj doseže to, da se nesoglasja hitreje razrešijo kot bi se sicer. Obstoječe pogodbe je zaradi sprejetja GDPR-ja potrebno dopolniti. Najbolj smiselno jih je skleniti na novo. Tako se zagotovi največja preglednost. V primeru, da pride do spora med obema akterjema, mora pogodbeni obdelovalec nemudoma vrniti vse osebne podatke in uničiti vse kopije, ki bi lahko obstajale.

V precej primerih se porajajo vprašanja, o dolžnostih upravljalca, kadar obdelovalec po naročilu obdeluje osebne podatke posameznika, o tem kdo mora obvestiti posameznika o obdelavi in o izvajanju pravic. Informacije morajo biti zelo jasne, saj se posameznik lahko odloči o obdelavi le takrat, ko bo imel na voljo vse informacije. V nekaterih primerih, pa ga je potrebno o tem le seznaniti. Tak primer je ob zaposlitvi. Tukaj je razvidno, da ima dolžnost, da posameznika obvesti, upravljalec. Upravljalec se lahko odloči sam katere pogodbene obdelovalce bo izbral za izvedbo obdelave osebnih podatkov in ne potrebuje privolitve posameznika. Informacijski pooblaščenec (2019) v nadaljevanju navede najbolj pogoste napake in te so:

- upravljalec ni sklenil pogodbe s pogodbenim obdelovalcem,
- pogodba ne vsebuje zahtevanih določb iz GDPR-ja,
- pogodba ni dovolj konkretna,
- upravljalec nima pregleda nad tem kaj obdelovalec uporablja za dosego cilja,
- upravljalec narobe oceni pogodbenega obdelovalca,
- upravljalec nima kontrole in ne nadzira pogodbenega obdelovalca,
- upravljalec prenaša OP v tretje države in pozablja na določila povezana z iznosom v tretje države,
- obdelovalci obdelujejo podatke na drugačen način brez odobritve upravljalca,
- delavci obdelovalca ne poznajo GDPR-ja.

Preden upravljalec zaupa svojemu pogodbenemu izvajalcu podatke v obdelavo, mora vedeti s kakšnim namenom bo te osebne podatke posredoval. Hkrati pa mora zagotoviti da bo pogodbeni obdelovalec opravljal naloge tako kot je v naprej dogovorjeno in zapisano. Ključno pri temu je, da je pred obdelavo osebnih podatkov podpisana pogodba, kjer so natančno določeni varnostni postopki in ukrepi kako bodo osebni podatki varovani, kako bodo osebni podatki izbrisani in kako bo poskrbljeno za sled obdelave in dostopa do osebnih podatkov. Upravljalec je ne glede na vse odgovoren za zakonitost obdelave. Tudi, ko jih posreduje podizvajalcu. Zato je pomembno, da opredeli kako bo nadzoroval pogodbenega izvajalca, ki bo izvajal obdelavo osebnih podatkov. Po izvedbi obdelave osebnih podatkov, pa mora partner podatke vrniti oziroma jih izbrisati.

Informacijski pooblaščenec (2019) trdi, da je potrebno moramo v začetnih fazah projekta obdelave osebnih podatkov določiti tisti minimalni nabor podatkov, s katerimi lahko dosežemo namen obdelave:

- če določenih OP ne potrebujemo, potem jih ne zbirajmo,
- če je zbiranje potrebno, potem upoštevajmo načelo sorazmernosti.

Če ugotovimo, da je potrebno zbiranje in obdelovanje osebnih podatkov, potem upoštevamo naslednje:

- uporabimo manj občutljive osebne podatke,
- ne zbirajmo enoličnih identifikatorjev, če to ni potrebno,
- raje uporabimo psevdonime,
- na sorazmernost pazimo ves čas. Tako na primer pri:
  - oblikovanju iskalnikov,
  - uporabniških pravicah.

Marsikateri cilj je mogoče doseči na način, da se osebni podatki hranijo pri posamezniku in prenosa ni potrebnega. Če obdelava na strani posameznika ne ponuja vse možnosti in ni smiselna, potem uporabniku vedno lahko omogočimo možnost elektronskega vpogleda v osebne podatke. To lahko naredimo tudi z izvozom osebnih podatkov. Večkrat pozabljamo, da je posameznik upravičen do vpogleda v lastne podatke, nima pa pravice do vpogleda v to kdo je vpogledal v njegove osebne podatke. To lahko preveri le Informacijski pooblaščenec, kot državni nadzorni organ.

Informacijski pooblaščenec (2019) dodaja, da je koncept odločanja o dajanju privolitve brezpredmeten v več primerih. Navaja politike zasebnosti na spletnih straneh, ki so prevečkrat zapisana v popolnoma nejasni in neberljivi obliki za potrošnika. Nujno potrebne podatke, se da predstaviti na jedrnat in pregleden način. Posebno pozornost daje na zavarovanje podatkov v informacijskih sistemih. Temu pritrjuje tudi Hughes (1994, str. 116), ki trdi, da se da večino podatkov zavarovati z uporabo kriptografskih metod, ki omogočajo veliko večjo varnost. Omogočajo varno hrambo in varen prenos zaradi neberljivosti. Predvsem pa morajo razvijalci informacijskih rešitev ves čas iskati morebitne napake ali šibke točke. Pri izvajanju tega je smiselno uvesti način, da sistem sam zaznava morebiten nastanek napak v prihodnosti. Te morajo biti jasne in skladne. Predvsem pa se mora z njimi ažurno upravljati in morajo biti hierarhične in dokumentirani.

Informacijski pooblaščenec (2019) v nadaljevanju govori o beleženju dostopov do podatkov. Ker sta obdelava osebnih podatkov in osebni podatek široka pojma, to posledično pomeni, da se sledljivost ugotavlja v več primerih. Pod črto to pomeni, da je potrebno za vsako podatek, ki se bo obdeloval, potrebno zagotoviti popolno revizijsko sled. To vsebuje beleženje vsakega dostopa do kateregakoli osebnega podatka. Sledenje mora biti tako, da omogoča kasnejše preverjanje. Predvsem je pomembno, da se ve:

- kdo je dostopal,
- kdaj je dostopal,
- do katerih osebnih podatkov je dostopal.

Identifikacija oseb, ki so do osebnih podatkov dostopale, pa mora biti zelo jasna in enolična. To pomeni, da se naša na konkretno osebo. Na konkretnega posameznika. Nadzornik vedno preverja pooblastila administratorjev. Torej tistih oseb, ki imajo najvišje pravice. Informacijski sistemi morajo delovati tako, da se sledljivosti ne da prav nikoli izklopiti. Prav nihče ne sme dostopati do osebnih podatkov brez sledljivosti. Zahteve nadzornika so načeloma manjše, če se obdelovalec drži načela sorazmernosti in obdeluje le tiste podatke, ki so nujno potrebni za dosego cilja.

Največje napake s področja zavarovanja osebnih podatkov, ki jih je opredelil Informacijski pooblaščenec (2019) so:

- pravice uporabnikov niso jasno opredeljene,
- pravice ne ustrezajo potrebam dela,
- obstajajo pravice, ki niso vezane na posameznika,
- sredstva za avtentikacijo se izmenjujejo med zaposlenimi,
- ni sledljivosti,
- sledljivost je, ni pa beleženja izvoza podatkov,
- administratorji lahko prikrijejo sledljivost,
- uporabniki ne zaklepajo računalnikov,
- občutljivi osebni podatki se pošiljajo preko elektronske pošte,
- ni ločevanja testnega okolja in produkcijskega okolja,
- ni izobraževanj za uporabnike.

Informacijski pooblaščenec (2019) opredeli največje napake s področja neupoštevanja načel minimizacije in sorazmernosti. Takšne prakse se večkrat pojavljajo v informacijskih sistemih. Določene podatke rabimo, sicer sistem ne bo deloval kot bi moral. Napake pa so slednje:

- zbirajo se osebni podatki, katerih sistem ne potrebuje za delovanje,
- osebni podatki se zbirajo ponovno, čeprav so še vedno v sistemu,
- osebne podatke se zbira na zalogo,
- zahteva se več identifikatorjev kot je to potrebno.

Informacijski pooblaščenec (2019) trdi, da zagovorniki vidijo koncept vgrajen zasebnosti kot nujno orodje za ohranjanje zasebnega. Težava pa je, ker se pogledi na koncept razlikujejo med različnimi akterji. Te so vodstvo, regulatorji in oblikovalci rešitev. Vgrajena zasebnost je za regulatorja nekaj normalnega, vodstva podjetij in organizacij pa se prevečkrat vprašajo ali se njim to splača. Vprašanje je koliko se jim bo to poznalo, če se tega ne bodo držali. Oblikovalce rešitev je predvsem strah, saj koncept vgrajene zasebnosti, po njihovem mnenju vpliva na oblikovanj inovativnih pristopov in nove storitve.

3 NOVOSTI PO SPLOŠNI UREDBI O VARSTVU OSEBNIH PODATKOV

Leta 2010 je Evropska komisija predstavila idejo o tem, kako poenotiti varstvo osebnih podatkov v Evropski uniji. Kot posledica tega je bil leta 2012 predstavljen predlog o reformi varstva osebnih podatkov. Že istega leta je bil pripravljen predlog Splošne uredbe o varstvu osebnih podatkov in predložen Svetu Evropske unije. Evropski parlament je v začetku leta 2014 v prvi obravnavi sprejel stališče. Začela so se tudi pogajanja med Svetom Evropske unije in Evropskim parlamentom, ki so trajala do zaključka leta 2015 (Centa, 2018). GDPR je bil sprejet 14. aprila 2016 in je stopil v veljavo 25. maja 2018.

Uredba (EU) 2016/679 Evropskega parlamenta in Sveta opredeli varstvo posameznika pri obdelavi osebnih podatkov kot temeljno pravico vsakega posameznika. Namen uredbe, kot je zapisano v uvodnih pojasnilih Uredbe, je poenotenje zakonodaje na področju varstva osebnih podatkov in posledično prispevanje k oblikovanju enotnega območja svobode,

varnosti in pravice ter ekonomske unije, kar bi posledično privedlo do gospodarskega in socialnega napredka.

Razlog za pripravo nove zakonodaje je v vse večjem vplivu osebnih podatkov. Uredba GDPR je naslednica Direktive 95/46/ES in velja na področju Evropske unije in Evropske ekonomske unije.

Podjetje Accenture (2018) trdi, da so ponudniki spletnih storitev, družbenih omrežij in komunikacijskih platform kot to Facebook, Google in Instagram so zaradi uvedbe GDPR-ja pod velikim pritiskom glede svojega načina delovanja v zvezi z obdelovanjem osebnih podatkov. Njihov poslovni model v večini primerov sloni na storitvi, ki je na prvi pogled za uporabnika brezplačna, a prinaša denar preko personaliziranega in ciljanega oglaševanja, ki deluje na modelu pridobivanja in obdelovanja velike količine osebnih podatkov. Z podatki upravlja umetna inteligenca, ki predvideva zanimanja, želje in potrebe posameznikov, ter jim prikazuje njim zanimive oglase. Te načini delovanja so potrošniku nevidne in se jih ne zaveda, hkrati pa je potrošnik pomanjkljivo obveščen. Vse to ima lahko precej negativen vpliv na njegove pravice povezane z varstvom osebnih podatkov. Vse to lahko vodi v diskriminacijo in družbeno razslojevanje. Problem personalizacije oglasov je postal še posebej pereč ob izbruhu politične afere v času trajanja volilne kampanje v Franciji, ZDA in Veliki Britaniji. GDPR je nadzornim organom držav članic Evropske unije dal že težko pričakovanja in prepotrebna orodja za nadzor nad največjimi tehnološkimi podjetji. Ena izmed ključnih novosti je širši domet GDPR-ja, ki jo morajo upoštevati podjetja, ki sicer niso ustanovljena v Evropski unija, vendar ponujajo svoje storitve državljanom članic EU.

Farmer trdi (Farmer, Rogers & Smart, 2017), da večjo kontrolo pravic posameznikov zagotavljajo tudi precej stroge določbe glede obveščanja, profiliranja posameznikov in izvajanja pravic posameznikov, ter mnogo večje odgovornosti podjetji, ki morajo sama presojati kakšne učinke ima lahko obdelava osebnih podatkov na potrošnika. GDPR pa je nenazadnje prinesel pomembno novost in to je povečanje možnosti operativnega sodelovanja vseh nadzornih organov za varstvo osebnih podatkov držav članic EU pri nadzoru zgoraj omenjenih primerov. Sodelovanje sedaj temelji na načelu, da je vse na enem mestu. V primeru čezmejnih kršitev postopek vodi vodilni organ, vendar v sodelovanju z preostalimi organi za varovanje osebnih podatkov držav članic EU. Z enotnim pristopom lahko države članice EU vplivajo na aktivnosti tehnoloških velikanov.

Tankard (2016) trdi, da je eden izmed glavnih razlogov za sprejetje nove uredbe oz. spreminjanje Direktive 95/46/ES v tem, da je bila slednja sprejeta v času, ko je splet uporabljal zgolj 1 % svetovnega prebivalstva. Že samo dejstvo, da je naslednica direktive uredba, kaže na pomembnost področja varstva osebnih podatkov na področju EU.

Poleg osnovnih pojmov, ki so bili že določeni v ZVOP-1, so v podobni obliki prisotni v GDPR-ju, ta pa uporablja še nekatere druge izraze: omejitev obdelave, oblikovanje profilov, psevdonimizacija, kršitev varstva osebnih podatkov, genetski podatki, biometrični podatki, podatki o zdravstvenem stanju, glavni sedež, predstavnik, povezana družba, zavezujoča poslovna pravila. Dopolnjena je tudi definicija osebnega podatka, ki sedaj vključuje tudi podatke o lokaciji in spletne označevalce (IP, MAC ...).

2. člen GDPR-ja pravi, da se GDPR uporablja za obdelavo osebnih podatkov, ki se obdelujejo z avtomatiziranimi sredstvi ali drugače, in ki so del zbirk ali pa so namenjeni

oblikovanju dela zbirke.
GDPR se ne uporablja, če:

- gre za področje obdelave podatkov zunaj EU
- če fizične osebe obdelujejo podatke za lastno ali domačo uporabo
- ko pristojni organi izvajajo naloge preprečevanja, preiskovanja in sankcioniranja kaznivih dejanj.

Kljub temu se GDPR uporablja, če upravljavec ali pogodbeni obdelovalec nista v EU, vendar prebivalcem EU nudita storitve ali izdelke (npr. spletna trgovina) oz. spremljata njihovo vedenje, kolikor to poteka v EU (npr. spletni piškotki).

Poleg osnovnih pojmov, ki so že določeni v ZVOP-1 in so prisotni v podobni obliki v GDPR-ju, ta uporablja še nekatere druge izraze:

- omejitev obdelave,
- oblikovanje profilov,
- psevdonimizacija,
- kršitev varstva osebnih podatkov,
- genetski podatki, biometrični podatki, podatki o zdravstvenem stanju,
- glavni sedež,
- predstavnik,
- povezana družba,
- zavezujoča poslovna pravila.

Osnovna načela za obdelavo osebnih podatkov, ki jih vsebuje GDPR, so zelo podobna osnovnim načelom ZVOP-1.

6. člen GDPR-ja opredeli več pogojev, pod katerimi je obdelava osebnih podatkov zakonita. Na prvo mesto pa postavlja osebno privolitev. Ta mora biti izrecna in ne domnevna oz. privzeta. To je ena izmed ključnih razlik, v primerjavi z ZVOP-1.

12. člen govori o pravici do seznanitve z lastnimi osebnimi podatki. Informacije upravljavec posreduje upravičenemu posamezniku čim prej, najkasneje pa v roku enega meseca od prejema zahteve (v izjemnih primerih se rok lahko podaljša za dodatna dva meseca). ZVOP-1 določa 15-dnevni rok. Tukaj bo zakonodajalec moral s spremembo zakonodaje doseči soglasje o časovnem obdobju. Upravljavec je dolžan zagotoviti posamezniku vse ustrezne informacije v zvezi z obdelavo njegovih osebnih podatkov v jedrnati, pregledni, razumljivi in lahko dostopni obliki. To še posebej velja, če so informacije namenjene otroku. Informacije upravljavec posreduje upravičenemu posamezniku čim prej, najkasneje pa v roku enega meseca od prejema zahteve (v izjemnih primerih se rok za lahko podaljša za dodatna dva meseca). Če posameznik v roku ne prejme od upravljavca odgovora oz. zahtevanih informacij, ima pravico pri nadzornem organu vložiti pritožbo.
13. člen GDPR-ja govori o tem, da kadar se osebni podatki pridobijo na podlagi privolitve, mora upravljalec posamezniku takrat, ko pridobi osebne podatke, zagotoviti vse naslednje informacije:

- identiteto in kontaktne podatke upravljavca in njegovega predstavnika, kadar ta obstaja;
- kontaktne podatke pooblaščene osebe za varstvo podatkov, kadar ta obstaja;

- namene, za katere se osebni podatki obdelujejo, kakor tudi pravno podlago za njihovo obdelavo;
- zakonite interese upravljavca, če obdelava temelji na njih;
- uporabnike ali kategorije uporabnikov osebnih podatkov, če obstajajo;
- obdobje hrambe osebnih podatkov;
- pravico, da zahtevajo popravek ali izbris podatkov oz. omejitev obdelave teh podatkov;
- pravico do preklica obdelave;
- pravico do pritožbe pri nadzornem organu;
- obstoj avtomatiziranega sprejemanja odločitev.

15. člen GDPRja pa pravi, da ima posameznik pravico od upravljalca, ki obdeluje njegove osebne podatke, pridobiti naslednje informacije:

- namen obdelave;
- vrste osebnih podatkov, ki se obdelujejo;
- uporabnike, ki so jim bili ali jim bodo razkriti osebni podatki;
- predvideno obdobje hrambe osebnih podatkov;
- pravico do popravka, omejitve ali izbrisa osebnih podatkov;
- pravico do pritožbe pri nadzornem organu;
- kadar osebni podatki niso bili zbrani pri posamezniku, vse razpoložljive informacije v zvezi z virom podatkov;
- obstoj avtomatiziranega sprejemanja odločitev, vključno z oblikovanjem profilov ter v takih primerih smiselne informacije o razlogih zanj, kot tudi pomen in predvidene posledice take obdelave.

GDPR govori o petih večjih skupinah pravic posameznikov v zvezi z njihovimi osebnimi podatki:

- seznanitev,
- sprememba,
- izbris,
- omejevanje,
- prenosljivost.

Novosti v GDPR-ju so pravica do omejevanja in prenosljivosti. V nadaljevanju bom opisal novosti in razlike med prejšnjo zakonodajo in GDPR-jem.

6. člen GDPR-ja pravi, da je obdelava zakonita, če je izpolnjen vsaj eden od naslednjih pogojev:

- podana je osebna privolitev (mora biti izrecna, ne domnevna oz. privzeta);
- obdelava je potrebna za izvajanje pogodbe, kjer je pogodbena stranka zadevni posameznik, ali za izvajanje ukrepov na zahtevo takega posameznika pred sklenitvijo pogodbe.;
- obdelava je potrebna za izpolnitev zakonske obveznosti, ki velja za upravljavca;
- obdelava je potrebna za zaščito življenjskih interesov posameznika.;
- obdelava je potrebna za opravljanje naloge v javnem interesu ali pri izvajanju javne oblasti, dodeljene upravljavcu;
- obdelava je potrebna zaradi zakonitih interesov upravljavca, razen kadar nad temi interesi prevladajo interesi ali temeljne pravice in svoboščine posameznika.

9. člen GDPR govori o tem, da je obdelava posebnih vrst osebnih podatkov prepovedana, razen če:

- je posameznik podal izrecno privolitev;
- je obdelava potrebna za namene izpolnjevanja obveznosti in izvajanja posebnih pravic upravljavca ali posameznika na področju delovnega prava ter prava socialne varnosti in socialnega varstva;
- je obdelava potrebna za zaščito življenjskih interesov posameznika;
- obdelavo v okviru svojih zakonitih dejavnosti z ustreznimi zaščitnimi ukrepi izvaja ustanova, združenje ali neprofitno telo s političnim, filozofskim, verskim ali sindikalnim ciljem in pod pogojem, da se obdelava nanaša samo na člane ali nekdanje člane ali na osebe, ki so v rednem stiku z njim v zvezi z njegovimi nameni, ter da se osebni podatki ne posredujejo zunaj tega telesa brez privolitve posameznikov, na katere se nanašajo osebni podatki;
- osebne podatke objavi sam posameznik.

Obdelava posebnih vrst osebnih podatkov je prepovedana, razen če:

- je obdelava potrebna za uveljavljanje, izvajanje ali obrambo pravnih zahtevkov ali kadar koli sodišča izvajajo svojo sodno pristojnost;
- je obdelava potrebna iz razlogov bistvenega javnega interesa na podlagi prava EU ali prava države članice;
- je obdelava potrebna za namene preventivne medicine ali medicine dela, oceno delovne sposobnosti zaposlenega, zdravstveno diagnozo, zagotovitev zdravstvene ali socialne oskrbe ali zdravljenja ali upravljanje sistemov in storitev zdravstvenega ali socialnega varstva;
- je obdelava potrebna iz razlogov javnega interesa na področju javnega zdravja;
- je obdelava potrebna za namene arhiviranja v javnem interesu, za znanstveno ali zgodovinsko-raziskovalne namene ali statistične namene, ki je sorazmerno z zastavljenim ciljem, spoštuje bistvo pravice do varstva podatkov ter zagotavlja ustrezne in posebne ukrepe za zaščito temeljnih pravic in interesov posameznika.

3.1 Pravica do omejitve obdelave

5. odstavek 32. člena ZVOP-1 govori o tem, da državni nadzorni organ za varstvo osebnih podatkov odloči o zahtevi iz prejšnjega odstavka v dveh mesecih od prejema zahteve. Vložena zahteva zadrži obdelavo osebnih podatkov posameznika, glede katerih je vložil zahtevo.

18. člen GDPR-ja govori o pravici od upravljavca doseči, da omeji obdelavo OP, če:

- posameznik oporeka točnosti podatkov – obdobje, ki upravljavcu omogoča preveriti točnost,
- je obdelava nezakonita – posameznik nasprotuje izbrisu in zahteva omejitev,
- ni več namena pri upravljavcu – posameznik jih potrebuje za uveljavljanje, izvajanje ali obrambo pravnih zahtevkov,
- je posameznik vložil ugovor – do presoje oziroma preverbe.

3.2 Pravica do prenosljivosti podatkov

20. člen GDPR-ja govori o pravici prejeti osebni podatek, ki jih je upravljavcu posredoval v :

- strukturirani,
- splošno uporabni,
- strojno berljivi,
- interoperabilni obliki.

Pravica je tudi te osebne podatke posredovati drugemu upravljavcu brez oviranja kadar obdelava temelji na privolitvi ali pogodbi in se izvaja z avtomatiziranimi sredstvi. Pravica, da se te osebni podatki neposredno prenesejo od enega upravljavca k drugemu kadar je to tehnično izvedljivo. Uresničevanje te pravice nikakor ne posega v pravico do izbrisa.

GDPR ukinja register zbirk osebnih podatkov. Še vedno bo moral upravljavec voditi evidenco dejavnosti obdelave osebnih podatkov, ki naj vključuje:

- naziv ali ime in kontaktne podatke upravljavca;
- kadar obstajajo: skupnega upravljavca, predstavnika upravljavca in pooblaščene osebe za varstvo podatkov;
- namene obdelave;
- opis kategorij posameznikov, na katere se nanašajo osebni podatki, in vrst osebnih podatkov;
- kategorije uporabnikov, ki so jim bili ali jim bodo razkriti osebni podatki, vključno z uporabniki v tretjih državah ali mednarodnih organizacijah;
- kadar je ustrezno, informacije o prenosih osebnih podatkov v tretjo državo ali mednarodno organizacijo, vključno z identifikacijo te tretje države ali mednarodne organizacije, pa tudi dokumentacijo o ustreznih zaščitnih ukrepih;
- kadar je mogoče, predvidene roke za izbris različnih vrst podatkov;
- kadar je mogoče, splošni opis tehničnih in organizacijskih varnostnih ukrepov.

Ob upoštevanju najnovejšega tehnološkega razvoja in stroškov izvajanja ter narave, obsega, okoliščin in namenov obdelave pa tudi tveganj za pravice in svoboščine posameznikov upravljavec in obdelovalec z izvajanjem ustreznih tehničnih in organizacijskih ukrepov zagotovita ustrezno raven varnosti glede na tveganje. Ustrezni ukrepi so tako tehnologija (ki je na voljo), viri (denar, ljudje, znanje), narava obdelave osebnih podatkov in tveganje za posameznike. Število dejavnikov je namenoma veliko, kar pomeni, da bo ocena o ne/ustreznosti ravni varnosti obdelave odvisna od primera do primera.

Ustrezne ukrepe lahko razdelimo v štiri skupine: šifriranje in psevdonimizacija; redno testiranje, ocenjevanje in vrednotenje varnostnih ukrepov; razpoložljivost in dostop do osebnih podatkov v primeru incidenta; zaupnost, celovitost, dostop in odpornost sistemov in storitev za obdelavo osebnih podatkov (Drev, 2018).

3.3 Sprememba ostalih pravic

3.3.1 Pravica do popravka

1. odstavek 32. člena ZVOP-1 določa, da mora upravljavec na zahtevo posameznika dopolniti, popraviti, blokirati ali izbrisati osebne podatke, za katere posameznik dokaže, da so nepopolni, netočni ali neažurni ali da so bili zbrani ali obdelani v nasprotju z zakonom.

16. člen GDPR-ja govori o:

- pravici od upravljavca doseči popravo netočnih osebnih podatkov brez odlašanja;
- pravica do dopolnitve nepopolnih osebnih podatkov
  - ob upoštevanju namenov obdelave,
  - vključno s predložitvijo dopolnilne izjave.

3.3.2 Pravica do izbrisa oz. pravica do pozabe

1. odstavek 32. člena ZVOP-1 govori o tem, da mora upravljavec na zahtevo posameznika dopolniti, popraviti, blokirati ali izbrisati osebni podatek za katere posameznik dokaže, da so nepopolni, netočni ali neažurni ali da so bili zbrani ali obdelani v nasprotju z zakonom.

17. člen GDPR-ja govori o pravici od upravljavca doseči izbris osebnih podatkov in obveznosti upravljalca, da osebne podatke izbriše, ko:

- preneha namen obdelave;
- umik privolitve (in ni druge pravne podlage);
- utemeljen ugovor posameznika po 21. členu GDPR-ja;
- osebni podatki so obdelani nezakonito;
- izbris potreben za izpolnitev pravne obveznosti upravljavca.

Volokh (2000) trdi, da pravica do pozabe omejuje pravico do svobodo govora. Veliko držav na svetu ima namreč pomembne zakone na tem področju, ki bi lahko kontrirali pravici do pozabe. Sam sicer govori o Združenih državah Amerike. Trdi, da bi morali upravljalci vložiti mnogo več dela kot je potrebno, da bi odkrili in izbrisali vse osebne podatke, ki se nanašajo na neko osebo. Govori celo o cenzuriranju tehnoloških velikanov, ki bi v želji, da zadostijo zakonodajalcu, raje brisali vse podatke, kot jih zagovarjali. GDPR po njegovem mnenju omogoča, da posameznik zbriše tiste podatke, ki njemu niso všeč. Brisanje teh podatkov ima lahko velik vpliv na izvajanje nalog podjetja kot je na primer osnovna analitika. Predvsem bi onemogočalo podjetjem, da spoznajo svoje stranke in jim ponudijo najbolj primerne storitve ali produkte. Govori tudi o tem, da bodo tehnološki velikani ponujali prilagojene in ne najboljše oziroma resnične rezultate. Kot pozitivno pa vidi, da GDPR ne posega na področje novinarskega dela. Tukaj pa se ponovno poraja vprašanje. Kako je s tem v državah, kjer ima vladajoča elita velik vpliv na medije.

3.3.3 Avtomatizirana obdelava osebnih podatkov

15. člen ZVOP-1 govori o avtomatizirani obdelavi osebnih podatkov, pri kateri se o posamezniku lahko sprejme odločitev, ki ima za posledico pravne učinke v zvezi z njim ali na njega znatno vpliva in ki temelji zgolj na avtomatizirani obdelavi podatkov, ki je namenjena ovrednotenju nekaterih osebnih vidikov v zvezi z njim, kakršni so zlasti njegova uspešnost pri delu, kreditna sposobnost, zanesljivost, ravnanje ali izpolnjevanje zahtevanih pogojev. Dovoljena je le, če je odločitev:

- sprejeta med sklepanjem ali izvajanjem pogodbe, pod pogojem, da je pobuda za sklenitev ali izvajanje pogodbe, ki jo je vložil posameznik, na katerega se osebni podatki nanašajo, izpolnjena ali da obstajajo primerni ukrepi za varstvo njegovih zakonitih interesov, kakršni so zlasti dogovori, ki mu omogočajo ugovarjati takšni odločitvi ali izraziti njegovo stališče;
- določena z zakonom, ki določa tudi ukrepe za varstvo zakonitih interesov posameznika, na katerega se nanašajo osebni podatki, zlasti možnost pravnega sredstva zoper takšno odločitev.

22. člen GDPR-ja pa govori o pravici posameznika, da zanj ne velja odločitev, ki:

- temelji zgolj na avtomatizirani obdelavi vključno z oblikovanjem profilov, na podlagi katerih se ocenjujejo osebni vidiki v zvezi s posameznikom, zlasti za analizo ali predvidevanje uspešnosti pri delu, ekonomskega položaja, zdravja, osebnega okusa ali interesov, zanesljivosti ali vedenja, lokacije ali gibanja;
- ima pravne učinke v zvezi z njim ali na podoben način nanj znatno vpliva (npr. avtomatska zavrnitev spletne prošnje za posojilo ali prakse zaposlovanja prek spleta brez človekovega posredovanja).

Razen, če je odločitev:

- nujna za sklenitev ali izvajanje pogodbe z upravljavcem,
- dovoljena v pravu EU ali državi članici, ki velja za upravljavca in določa tudi ukrepe za zaščito pravic in svoboščin ter zakonitih interesov posameznika (tudi za namene spremljanja in preprečevanja zlorab in davčnih utaj;
- utemeljena z izrecno privolitvijo posameznika.

3.3.4 Zahteve po večji varnosti obdelave osebnih podatkov

14. člen ZVOP-1 pravi, da morajo biti občutljivi osebni podatki med prenosom po telekomunikacijskem omrežju šifrani in elektronsko podpisani. 24. člen ZVOP-1 pa govori, da zavarovanje osebnih podatkov obsega organizacijske, tehnične in logično-tehnične postopke in ukrepe s katerimi se varujejo osebni podatki, preprečuje slučajno ali namerno nepooblaščeno uničevanje podatkov, njihovo spremembo ali izgubo ter nepooblaščeno obdelavo teh podatkov.

25. člen ZVOP-1 pravi, da morajo podatke zavarovati tako upravljavci kot pogodbeni obdelovalci. Predpisati morajo postopke in ukrepe za zavarovanje osebnih

podatkov, določiti odgovorne osebe za posamezne zbirke osebnih podatkov in določiti osebe, ki so pooblaščene za obdelavo osebnih podatkov.

2. odst. 32. člena GDPR-ja pravi, da se pri določanju ustrezne ravni varnosti upoštevajo zlasti tveganja, ki jih pomeni obdelava, zlasti zaradi nenamernega ali nezakonitega uničenja izgube, spremembe, nepooblaščenega razkritja ali dostopa do osebnih podatkov, ki so poslani, shranjeni ali kako drugače obdelani.

3. odst. 32. člena GDPR-ja pa govori o zavezanosti k odobrenemu kodeksu ravnanja iz člena 40 ali izvajanju odobrenega mehanizma potrjevanja iz člena 42, da se ta lahko uporabi za dokazovanje izpolnjevanja zahtev iz 1. odstavka tega člena.

4. odst. 32. člena GDPR-ja govori o tem, da upravljalec in obdelovalec zagotovita, da katerakoli fizična oseba, ki ukrepa pod vodstvom upravljalca ali obdelovalca, ki ima dostop do osebnih podatkov, slednjih ne sme obdelati brez navodil upravljalca, razen če to od nje zahteva pravo EU ali pravo države članice.

Nova pravila niso radikalno drugačna, prinašajo pa nekaj pomembnih nadgradenj:

- eksteritorialna aplikativnost – GDPR se uporablja tudi, če upravljavec ali pogodbeni obdelovalec nista v EU, vendar prebivalcem EU nudita storitve ali izdelke (npr. spletna trgovina) oz. spremljata njihovo vedenje, v kolikor to poteka v EU (npr. spletni piškotki);
- kazni – institucije lahko prejmejo kazen v višini do 4 % letnega prihodka ali 20 milijonov EUR, karkoli predstavlja višji znesek. Maksimalna zagrožena globa se izda v primeru, da institucija obdeluje osebne podatke brez privolitve posameznika. To pomeni kršitev t. i. principa *privacy by design.* Globe se izrekajo v stopnjah. Če so zbirke osebnih podatkov neurejene, se npr. izreče globa v višini 2 % letnega prihodka.

Treba se je zavedati, da skladno z Zakonom o inšpekcijskem nadzoru in z Zakonom o prekrških nadzorni organ v okviru nadzornih in prekrškovnih postopkov še vedno lahko izreče opozorilo in/ali opomin (Drev, 2018).

83. in 84. člen GDPR-ja govorita o tem, da morajo biti globe učinkovite, sorazmerne in odvračilne. V vsakem primeru pa se tehta ključne okoliščine: narava, teža in trajanje kršitve, malomarnost, ukrepi, ki so bili sprejeti za zmanjšanje škode, morebitne predhodne kršitve, sodelovanje z nadzornim organom, vrste in obseg osebnih podatkov, zavezanost kodeksom ravnanja ali odobrenim mehanizmom potrjevanja.

3.3.5 Upoštevanje koncepta vgrajene zasebnosti

To pravico poznamo že nekaj let, razlika pa je v tem, da je z GDPR-jem postala zakonska obveznost. Upravljavec je tako dolžan vzpostaviti primerne tehnične in organizacijske ukrepe, da bi zavaroval osebne podatke, ki jih upravlja. 23. člen govori o tem, da mora upravljavec upravljati zgolj s podatki, ki so nujno potrebni za dosego cilja**.**

3.3.6 Pooblaščena oseba za varstvo osebnih podatkov

Upravljavec in obdelovalec imenujeta pooblaščeno osebo za varstvo osebnih podatkov (v nadaljevanju DPO), če obdelavo izvaja javni organ, predstavlja obdelava osebnih podatkov temeljno dejavnost oz. je zaradi narave dela potrebno redno in sistematično spremljati obdelavo, se obdelujejo posebne vrste osebnih podatkov (občutljivi osebni podatki). Če gre za povezano družbo ali organ z več enotami, se lahko imenuje ena oseba za varstvo osebnih podatkov, ki zastopa (pod)družbe oz. enote organa. Pooblaščena oseba je lahko zaposlena pri upravljavcu in obdelovalcu, lahko pa gre za najeto zunanjo osebo.

Glavne naloge pooblaščene osebe za varstvo osebnih podatkov znotraj podjetja, opredeljene v 1. odstavku 39. člena GDPR, so (Falque-Pierrotin, 2017, str. 5-27):

- obveščanje upravljavca, obdelovalca in zaposlenih v podjetju, ki izvajajo obdelavo, ter svetovanje o obveznostih skladno z GDPR;
- spremljanje skladnosti z GDPR: DPO ni odgovoren za zagotavljanje skladnosti z določbami iz GDPR, kar je zelo jasno zapisano v 1. odstavku 24. člena GDPR. Njegova naloga je, da omogoča učinkovito opravljanja nalog in zagotovitev zadostne neodvisnosti in sredstev za učinkovito izvajanje nalog. Za zagotavljanje skladnosti je odgovoren upravljalec, naloga DPO pa je pomoč upravljalcu pri spremljanju notranje skladnosti z GDPR. DPO zbira 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 jih je pridobil od gospodarskih družb;
- sodelovanje z nadzornim organom in delovanje kot kontaktna točka za nadzorni organ: s tem, ko DPO deluje kot kontaktna točka, nadzornemu organu, v Sloveniji je to Informacijski pooblaščenec, 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. DPO je v primeru kršitev prvi kontakt z Informacijskim pooblaščencem.

3.3.7 Priprava ocene učinka

Kadar je verjetno, da bi lahko obdelava osebnih podatkov predstavljala veliko tveganje za pravice in svoboščine posameznikov, upravljavec pred obdelavo opravi oceno učinka predvidenih dejanj obdelave. Ocena učinka se opravi predvsem:

- če gre za sistematično in obsežno obdelavo osebnih podatkov z avtomatiziranimi sredstvi;
- gre za obdelavo posebnih vrst osebnih podatkov;
- gre za obsežno sistematično spremljanje javno dostopnega območja.

Če je iz ocene učinka razvidno, da bi obdelava osebnih podatkov predstavljala veliko tveganje, če ne bi bili sprejeti ukrepi za ublažitev tveganja, se upravljavec predhodno posvetuje z nadzornim organom.

Pri posvetovanju mora upravljavec nadzornemu organu predložiti:

- dolžnosti upravljavca, skupnih upravljavcev in obdelovalcev;
- namene in sredstva predvidene obdelave;
- ukrepe in zaščitne ukrepe za zaščito pravic in svoboščin posameznikov, na katere se nanašajo osebni podatki;
- kontaktne podatke pooblaščene osebe za varstvo podatkov;
- oceno učinka v zvezi z varstvom podatkov;
- vsakršne druge informacije, ki jih zahteva nadzorni organ.

Nadzorni organ praviloma v roku do 8 tednov od prejema zahteve za posvetovanje pisno svetuje upravljavcu oz. obdelovalcu.
Ocena naj zajema vsaj naslednje:

- sistematičen opis predvidenih dejanj obdelave in namenov obdelave, kadar je ustrezno pa tudi zakonitih interesov, za katere si prizadeva upravljavec;
- oceno potrebnosti in sorazmernosti dejanj obdelave glede na njihov namen;
- oceno tveganj za pravice in svoboščine posameznikov, na katere se nanašajo osebni podatki;
- ukrepe za obravnavanje tveganj;
- zaščitne ukrepe;
- varnostne ukrepe ter mehanizme za zagotavljanje varstva osebnih podatkov in za dokazovanje skladnosti z GDPR-jem.

Upravljavec se pri pripravi ocene učinka (»ocene tveganja«) posvetuje z osebo, ki je pooblaščena za varstvo podatkov (če je ta imenovana) (Drev, 2018).

3.3.8 Sporočilo o kršitvi varstva osebnih podatkov

V primeru kršitve varstva osebnih podatkov upravljavec brez nepotrebnega odlašanja uradno obvesti pristojni nadzorni organ, razen če ni verjetno, da bi bile s kršitvijo ogrožene pravice in svoboščine posameznikov. 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.

Drev (2018) trdi, da so prednosti takega sistema prijav:

- odgovornost poročanja na strani upravljalcev in obdelovalcev;
- nadzorni organ bo dobil več informacij o kršitvah;
- postopek poročanja o kršitvah bo do neke mere standardiziran.

Slabosti samodejnega sistema prijav so:

- več bo dela za nadzorne organe;
- šele praksa bo pokazala v kakšni meri in na kakšen bo način poročanja zares zaživel.

Pot obveščanja sedaj zgleda tako, da se zgodi incident pri pogodbenemu obdelovalcu, ki obvesti upravljalca, ki obvesti nadzorni organ.

Obvestilo mora vsebovati:

- opis vrste kršitve, kategorije in približno število posameznikov, na katere se nanašajo osebni podatki, vrste in približno število evidenc osebnih podatkov;
- kontaktne podatke pooblaščene osebe za varstvo podatkov;
- opis verjetnih posledic kršitve varstva osebnih podatkov;
- opis ukrepov, ki jih upravljavec sprejme, pa tudi ukrepov za ublažitev morebitnih škodljivih učinkov kršitve.

3. odstavek 34. člena GDPR-ja govori o tem, da sporočilo posamezniku, ni potrebno, če je izpolnjen kateri koli izmed naslednjih pogojev:

- upravljavec je izvedel ustrezne tehnične in organizacijske zaščitne ukrepe in so bili ti ukrepi uporabljeni za osebne podatke, v zvezi s katerimi je bila storjena kršitev varstva, zlasti ukrepe, na podlagi katerih postanejo osebni podatki nerazumljivi vsem, ki niso pooblaščeni za dostop do njih, kot je šifriranje;
- upravljavec je sprejel naknadne ukrepe za zagotovitev, da se veliko tveganje za pravice in svoboščine posameznikov, na katere se nanašajo osebni podatki, verjetno ne bo več udejanjilo;
- to bi zahtevalo nesorazmeren napor. V takšnem primeru se namesto tega objavi javno sporočilo ali izvede podoben ukrep, s katerim so posamezniki, na katere se nanašajo osebni podatki, enako učinkovito obveščeni.

4. odst. 34. člena GDPR-ja pa pravi, da v primeru, da upravljalec posameznika, na katerega se nanašajo osebni podatki, še ni obvestil o kršitvi varstva osebnih podatkov, lahko nadzorni organ od njega to zahteva po preučitvi verjetnosti, da bi kršitev varstva osebnih podatkov povzročila veliko tveganje.

3.3.9 Kodeksi ravnanja

Združenja ali organi, ki predstavljajo upravljavce in obdelovalce, lahko pripravijo posebne kodekse ravnanja, ki urejajo:

- pošteno in pregledno obdelavo osebnih podatkov;
- zakonite interese upravljavcev;
- zbiranje osebnih podatkov;
- psevdonimizacijo osebnih podatkov;
- obveščanje javnosti in posameznikov, na katere se nanašajo osebni podatki;
- uresničevanje pravic posameznikov, na katere se nanašajo osebni podatki;
- obveščanje in zaščito otrok, če gre za obdelavo osebnih podatkov otrok;
- ukrepe za zavarovanje osebnih podatkov;
- uradno obveščanje nadzornih organov o kršitvah varstva osebnih podatkov in obveščanje posameznikov, če in kadar je to potrebno;
- prenos osebnih podatkov v tretje države;
- postopke za reševanje sporov.

Združenja ali organi, ki pripravijo, spremenijo ali dopolnijo kodeks, osnutek najprej predložijo nadzornemu organu. Ta oceni, ali je kodeks skladen z zahtevami GDPR-ja in ga šele nato potrdi (ali ne).

Potrjen osnutek kodeksa nadzorni organ registrira in objavi. Če se kodeks nanaša na obdelavo osebnih podatkov v več državah, nadzorni organ osnutek posreduje odboru, ki poda svoje mnenje. Če ta izda pritrdilno mnenje, se osnutek kodeksa pošlje še Komisiji, ki lahko kodeks sprejme. Odobreni kodeksi so objavljeni v posebnem registru.

41. člen GDPR-ja govori o spremljanju odobrenih kodeksov ravnanja. Organ, ki želi biti pooblaščen (s strani nadzornega organa) za spremljanje odobrenih kodeksov ravnanja, mora:

- izkazati ustrezno raven strokovnega znanja;
- dokazati, da v okviru izvajanja nadzora ne bo prihajalo do konflikta interesov;
- vzpostaviti postopke, ki omogočajo ugotavljanje ali so upravljavci in obdelovalci upravičeni do uporabe kodeksa;
- vzpostaviti postopke, ki omogočajo spremljanje skladnosti z določbami kodeksa;
- redno pregledovati delovanje upravljavcev in obdelovalcev;
- vzpostaviti postopke za izvajanje pritožb zaradi kršitve kodeksa.

Nadzorni organ lahko pooblastilo za spremljanje odobrenih kodeksov prekliče, če niso (več) izpolnjeni našteti pogoji.

3.3.10 Mehanizmi potrjevanja

Mehanizmi potrjevanja za varstvo osebnih podatkov, pečati in označbe za varstvo podatkov se lahko uporabijo za dokazovanje, da obdelava osebnih podatkov poteka skladno z zahtevami GDPR-ja (predvsem koristno za dokazovanje izvedenih zaščitnih ukrepov, tudi v kontekstu iznosa v tretje države). To še ne pomeni, da je obstoj takšnih mehanizmov potrjevanja zadosten pogoj za zagotavljanje skladnosti oz. da nadzorni organ v primeru zaznane kršitve ne bo sankcioniral upravljavca ali obdelovalca. Potrdila niso obvezna. Izdajo jih organi za potrjevanje ali pristojen nadzorni organ. Izdajo se za obdobje največ treh let, lahko se podaljšajo (Drev, 2018).

3.3.11 Iznos osebnih podatkov v tretje države

Iznos osebnih podatkov v tretjo državo je dopusten, če je zagotovljena ustrezna varnost pri obdelavi osebnih podatkov. To konkretno pomeni:

- da je dopusten, če gre za državo članico EU.;
- iznos osebnih podatkov iz EU v ZDA je dopusten na podlagi sporazuma Ščit zasebnosti (ang. Privacy Shield). Organizacija, ki ji želimo posredovati osebne podatke, mora pristopiti k omenjenemu sporazumu.
- iznos osebnih podatkov v tretjo državo je dopusten, če je Informacijski pooblaščenec izdal odločbo, da je konkretna tretja država varna.
- iznos osebnih podatkov v tretjo državo je dopusten na podlagi izjem, ki jih določa 70. člen ZVOP-1.

Informacijski pooblaščenec (2018a) v Smernicah o iznosu osebnih podatkov v tretje države navaja, da se iznos na podlagi 7. točke 1. odstavka 70. člena ZVOP-1, lahko opravi:

- na podlagi tipskih pogodb, ki jih je pripravila Evropska komisija oziroma t.i. standardnih pogodbenih klavzul;
- na podlagi (2) zavezujočih poslovnih pravil (ang. Binding Corporate Rules), ki omogočajo iznos podatkov znotraj iste (mednarodne) korporacije;
- na podlagi (3) drugih pogodb ali pogojev poslovanja, ki zadovoljijo pogoje ustreznega varstva osebnih podatkov.

45. člen GDPR-ja pravi, da lahko Evropska komisija odloči, da tretja država, ozemlje, sektor ali mednarodna organizacija v tretji državi zagotavlja ustrezno raven varstva podatkov in je iznos dopusten brez posebnega dovoljenja. Seznam držav, ozemlja, sektorjev in organizacij, ki zagotavljajo ustrezno raven varstva osebnih podatkov oz. te ne zagotavljajo več, redno objavlja v Uradnem listu EU in na svoji spletni strani.

46. člen GDPR-ja pravi, da je prenos podatkov v tretjo državo mogoč tudi, tudi če Evropska komisija ni izdala sklepa o ustreznosti glede varstva osebnih podatkov v tej državi. Vendar pa je tak iznos dopusten le, če je upravljavec ali obdelovalec predvidel ustrezne zaščitne ukrepe in če imajo posamezniki, na katere se nanašajo osebni podatki, na voljo izvršljive pravice in učinkovita pravna sredstva.

Ustrezni zaščitni ukrepi se lahko zagotovijo s:

- pravno zavezujočim instrumentom, ki ga sprejmejo javni organi ali telesa;
- zavezujočimi poslovnimi pravili;
- standardnimi določili o varstvu podatkov, ki jih sprejme Evropska komisija;
- standardnimi določili o varstvu podatkov, ki jih sprejme nadzorni organ in odobri Evropska komisija;
- odobrenim kodeksom ravnanja, skupaj z zavezujočimi in izvršljivimi zavezami upravljavca ali obdelovalca v tretji državi, da bo uporabljal ustrezne zaščitne ukrepe, tudi glede pravic posameznikov, na katere se nanašajo osebni podatki.
- odobrenim mehanizmom potrjevanja, skupaj z zavezujočimi in izvršljivimi zavezami upravljavca ali obdelovalca v tretji državi, da bo uporabljal ustrezne zaščitne ukrepe, tudi glede pravic posameznikov, na katere se nanašajo osebni podatki.

3.3.12 Poseg GDPR-ja v področno zakonodajo ZVOP-1

ZVOP-1 je v posebnih poglavjih urejal posamezne področne ureditve, kot so:

- videonadzor (vhodov v delovne prostore, delovnih prostorov, večstanovanjskih zgradb);
- neposredno trženje;
- evidenca dostopov;
- uporaba biometričnih podatkov;
- javne knjige.

Ni pa izrecno urejal nekaterih ostalih področji:

- video analitike;
- nadzora s pomočjo GPS tehnologije;
- nadzor elektronske pošte;
- nadzora interneta;
- pametnih števcev;
- interneta stvari;
- brezpilotnih letalnikov.

GDPR (neposredno) ne ureja nobene od naštetih področnih področnih ureditev. Določa pa, da lahko posamezne države v svoji nacionalni zakonodaji (pod pogojem, da je skladna z GDPR-jem) bolj natančno uredijo posamezne vidike obdelave in varstva osebnih podatkov.

Jamnik (2018) vidi ključne izzive GDPR-ja na področju trženja v tem, da morajo podjetja popolnoma spremeniti način razmišljanja o varstvu osebnih podatkov. Podjetja morajo začeti pridobivati veljavna soglasja za obdelavo osebnih podatkov, ugotoviti/določiti namene obdelave in posledice: zakonita podlaga, čas hrambe, obdelava za nov namen. Vpeljati morajo mehanizem za zaznavanje in poročanje o varnostnih incidentih. Ključni izziv GDPR-ja pa vidi v tem, kako bodo imela podjetja v vsakem trenutku popoln pregled nad tokom osebnih podatkov (kje, od koga, kdo, kaj, zakaj, koliko časa) in kako bodo podjetja zagotovila izpis, izbris, prenos osebnih podatkov na zahtevo.

3.4 Povzetek sprememb

Ključno je, da v vsakem trenutku vemo, katere osebne podatke sploh imamo, kje in kdo ima do njih dostop. Prav tako je pomembno, da zagotavljamo varnost osebnih podatkov:

- da preprečujemo slučajno ali namerno nepooblaščeno uničevanje podatkov;
- nepooblaščeno spremembo;
- seznanitev nepooblaščenih oseb s podatki;
- izgubo podatkov.

Pomembno je tudi, da varnost podatkov zagotavljamo s kombinacijo tehničnih ukrepov, kot so:

- zaklepanje prostorov, omar, predalov;
- učinkovitim uničevanjem podatkov na papirnih in elektronskih nosilcih;
- uporabo protivirusnih programov, požarnega zidu, rednega nameščanja varnostnih popravkov strojne in programske opreme ter organizacijskih ukrepov, kot so:
  - pravilno izbrana gesla;
  - redna izobraževanja zaposlenih;
  - interni akti, ki določajo, kaj se sme delati z osebnimi podatki, kdo je odgovoren za posamezne zbirke osebnih podatkov ter katere osebe lahko zaradi narave svojega dela obdelujejo določene osebne podatke.

Predvsem pa je pomembno, da se zavedamo, da varnost podatkov še ne pomeni varstva osebnih podatkov. Podatki so lahko odlično zaklenjeni, težava pa nastane, ker to še ne pomeni, da imamo pravno podlago, da podatke sploh lahko imamo ali pa jih uporabljamo za namene za katere niso bili zbrani (Žagar & Blažič, 2017, str. 6).

83. in 84 člen GDPR-ja govori, da morajo biti globe učinkovite, sorazmerne in odvračilne.

V vsakem primeru se tehta ključne okoliščine:

- narava, teža in trajanje kršitve, malomarnost,
- ukrepi ki so bili sprejeti za zmanjšanje škode,
- morebitne predhodne kršitve,
- sodelovanje z nadzornim organom,
- vrste in obseg osebnih podatkov,
- zavezanost kodeksom ravnanja ali odobrenim mehanizmom potrjevanja.

Višina glob skladno s členom 84. znaša do 20.000.00 EUR ali do 4% skupnega svetovnega letnega prometa v preteklem proračunskem letu. Odvisno od tega, kateri znesek je višji.

GDPR po mnenju Informacijskega pooblaščenca (2018b) prinaša nove in okrepljene pravice posameznika, poleg obstoječe pravice do dostopa do osebnih podatkov ter pravice do popravka ureja še pravico do pozabe, izbrisa, omejitve obdelave, ugovora in prenosljivosti podatkov. Večji poudarek daje a transparentnosti obdelave glede na zagotavljanja preglednih in lahko dostopnih informacij posameznikom o obdelavi njihovih podatkov. GDPR določa tudi nove obveznosti upravljavcev in obdelovalcev podatkov, kot so obveznost izvajanja ustreznih varnostnih ukrepov in obveznost uradnega obveščanja o kršitvah varstva osebnih podatkov, imenovanje pooblaščenih oseb za varstvo podatkov, izvajanje ocen učinka. Upravljavci sedaj niso več dolžni prijavljati zbirk osebnih podatkov v register zbirk osebnih podatkov, ostajajo pa dolžnosti sprejema popisa zbirk (t. i. evidence dejavnosti obdelave); te dolžnosti se krepijo in uvajajo tudi za (pogodbene) obdelovalce. GDPR bistveno bolj poudarja načelo odgovornosti in preventivne ukrepe, poleg omenjenih mehanizmov zagotavljanja skladnosti uvaja tudi možnost potrjevanja sektorskih kodeksov ravnanja in certifikacije.

Informacijski pooblaščenec (2019) v letnem poročilu za leto 2018 pravi, da je v letu 2018 prejel veliko število prijav posameznikov. Število prijav se je povečalo za kar dvakrat po sprejetju GDPR-ja. Torej po 25. maju 2018. Trdi, da je do tega prišlo zaradi večjega zavedanja posameznikov o pomenu področja varstva osebnih podatkov in pravic, ki jih prinaša GDPR. Razlog za to daje predvsem velikem pomenu medijev, ki so ozaveščali o tej tematiki. Zavedanje je večje tudi na strani obdelovalcev, kjer je prišlo do veliko večjega zaprosila za pisna in ustna mnenja. Po pregledu prijav je Informacijski pooblaščenec ugotovil, da je v kar večini primerov prišlo do prijave zaradi nerazumevanja določb GDPR-ja. To velja predvsem v primerih, ko je prišlo do prijave na podlagi privolitve posameznika. GDPR sicer zelo strogo določa, kateri vsi pogoji morajo biti doseženi, da se privolitev šteje za skladno, potrebno pa omeniti, da je izrecna privolitev le ena izmed šestih pravnih podlag, ki jih določa 6. člen GDPR, da je obdelava osebnih podatkov zakonita. Upravljalci osebnih podatkov so predvsem zaradi nerazumevanja GDPR-ja pridobivali izrecne privolitve potrošnikov za vsako ceno. Tudi takrat, ko to, zaradi drugih zakonskih določil, ni bilo potrebno. Večkrat je bila obdelava osebnih podatkov nujno potrebna za izvajanje medsebojne pogodbe ali pa je bil izpolnjen kakšen izmed drugih pogojev iz 6. člena GPRR-ja. To pomeni, da zaprosilo za izrecno privolitev ni bilo potrebno. Večkrat se je pokazalo, da je prišlo do prejetja prijav zato, ker so upravljalci potrošnikom predložili nepopolne in neustrezne informacije o obdelavi osebnih podatkov. Temu pritrjuje tudi Evropska komisija (2018), ki trdi, da so upravljalci osebnih podatkov dolžni sprejemati takšne ukrepe, da posamezniku pridobi informacije na način, da jih razume. Torej v pregledni, razumljivi, jedrnati in dostopni obliki ter v jasnem in nezapletenem jeziku. Vrste teh informacij, ki jih

morajo upravljalci osebnih podatkov predložiti posamezniku, so navedene v 13. in 14. členu GDPR-ja. Banke zbirajo določene osebne podatke o prenosu sredstev zaradi druge za njih zavezujoče zakonodaje, vendar tega svojim strankam niso omenili. Stranke so tako menile, da banke zbirajo njihove osebne podatke brez ustrezne pravne podlage in so tako vložile veliko število prijav na Informacijskega pooblaščenca. V takšnih primerih so inšpektorji odrejali odpravo nepravilnosti.

Zanimivo je tudi dejstvo, ki ga omenja Informacijski pooblaščenec (2019) ta trdi, da je v času od sprejetja GDPR-ja prejel večje število prijav s strani upravljalcev osebnih podatkov. Vlaganje »samoprijav« je v GDPR-ju novost. V večini primerov je do takšnih prijav prišlo zaradi neupravičenega razkritja. To vključuje posredovanje osebnih podatkov napačnim ali nepooblaščenim osebam. Ali pa je prišlo do prijav zaradi nepooblaščenega dostopa do osebnih podatkov. Največkrat do tega pride zaradi programskih napah ali pa zaradi zlorabe določenih pooblastil s strani zaposlenih. Vse večkrat pa prihaja do tega zaradi neprimerne varnosti in posledičnega vdora v informacijski sistem upravljalca. Lahko pa zaradi izgube nosilca osebnih podatkov. Tukaj govorimo o kraji računalnikov in mobilnih telefonov na katerih so spravljeni podatki. Največ preventivnih inšpekcijskih nadzorov je Informacijski pooblaščenec namenjal ravno temu področju. Inšpektorji so preverjali področja, pri katerih je obstajalo največje tveganje zaradi opravljene ocene tveganja. To so področja zagotavljanja informacijske varnosti, pri kateri je cilj preprečiti nepooblaščeno obdelavo osebnih podatkov ali izgube osebnih podatkov. Zanimivo je, da je največ nezakonitih vpogledov v osebne podatke zaradi radovednosti zaposlenih oziroma zaradi pridobivanja informacij o določeni osebi za lastne namene. Inšpektorji so največ takih vpogledov odkrili na področju notranjih zadev, zdravstvenih institucij in centralnem registru psov. Večina teh registrov omogoča kasnejši vpogled v analitiko brskanja. Ob odkritju kršitev so zaposleni največkrat trdili, da je prišlo do napake zaradi zlorabe njihovih gesel ali pa uporabniških imen. Ta izgovor pa ne zadošča. Vsak zaposleni je namreč dolžan, da svoje osebne podatke varuje in predvsem, da se po vsaki seji odjavi iz sistema. Informacijski pooblaščenec je veliko namenil tudi preventivnem ozaveščanju malih podjetij. Predvsem na področju neposrednega trženja.

GDPR je po mnenju Edwardsa (2018) prinesel zelo pomembne spremembe glede sodelovanja nadzornih organov na področju varstva osebnih podatkov pri čezmejnih incidentih. GDPR je namreč omogočil in predvsem formaliziral postopek sodelovanja. To možnost je v letu 2018 večkrat izkoristil. Predvsem v prijavah zoper tehnološke velikane. Mednaroden način delovanja je edini način, da bodo nadzorni organi lahko vplivali na takšna podjetja. Predvsem zaradi kadrovskih resursov.

Drev (2018) trdi, da je zakonodaja na tem področju pomembna, ni pa nova. Podjetja so imela 2 leti časa, da se seznanijo z novo zakonodajo in se nanjo pripravijo. Podjetja so naredila veliko v želji, da bi se pripravile na spremembo, vendar ob tem storila veliko napak. Ena izmed takšnih je, da so podjetja 25. maja 2018 poslala mail vsem svojim strankam v katerih so jih prosile za izrecno privolitev za obdelavo osebnih podatkov. To pa so storile v večini preko elektronskih naslovov, ki so jih prejela pred 25. majem 2018. To je seveda pravno neustrezno. Veliko število programskih rešitev je neprimerno pripravljeno oziroma neskladno z GDPR-jem. Neprimerno je ocenil delo nekaterih spletnih strani, ki nimajo sedeža v eni izmed držav članic Evropske unije. Več tujih časopisov in novinarskih hiš je raje blokiralo dostop državljanom držav članic Evropske unije, kot pa da bi se ustrezno pripravili na spremembo zakonodaje. Opaziti je bilo mogoče tudi precejšen upad personaliziranega oglaševanja. Prišlo je do več tožb zoper tehnološke velikane. Tehnološki

velikani pa so prejeli večje število denarnih in drugačnih kazni zaradi kršenja določb GDPR-ja.

4 ANALIZA

4.1 Raziskava med potrošniki

S pomočjo spletnega orodja 1ka sem oblikoval spletni vprašalnik, s katerim sem preučeval, kakšen vpliv ima Splošna uredba o varstvu osebnih podatkov na trženje. Anketni vprašalnik je bil sestavljen iz 12 vprašanj – 6 vprašanj, ki so se navezovala na vpliv GDPR-ja na trženje in šest demografskih vprašanj. Vsa vprašanja so bila zaprtega tipa, izpolnjevanje ankete pa je v povprečju trajalo pet minut.

4.1.1 Opis vzorca

Anketni vprašalnik je v celoti izpolnilo 153 anketirancev. To predstavlja priložnostni vzorec. 54 % anketirancev je bilo ženskega spola, 46 % anketirancev pa je bilo moškega spola. Več kot polovica anketirancev je bila stara od 21 do 40 let (54 %), 31 % anketirancev je bilo starih od 41 do 60 let, 8 % anketirancev je bilo starih 61 let ali več, najmanjši odstotek anketirancev pa so predstavljali mlajši od 21 let (6 %).

Največ anketirancev (27 %) ima zaključeno visoko univerzitetno izobrazbo, 20 % anketirancev ima zaključeno visoko strokovno izobrazbo, 12 % anketirancev ima zaključeno bodisi srednje strokovno izobraževanje bodisi višje strokovno izobraževanje oz. višješolsko izobraževanje. Specialistično povisokošolsko izobrazbo, magisterij ali doktorat ima 11 % anketirancev, najmanj anketirancev pa ima zaključeno bodisi nižjo ali srednjo poklicno izobrazbo (4 %) ali nižje.

Največ anketirancev prihaja iz osrednjeslovenske regije (35 %), 11 % anketirancev prihaja iz gorenjske regije, 8 % anketirancev pa prihaja bodisi iz savinjske bodisi iz notranjsko-kraške regije. Iz ostalih regij (pomurska, podravska, koroška, posavska, jugozahodna Slovenija, goriška in obalno-kraška) pa prihaja najmanjši odstotek anketirancev. Porazdelitev anketirancev po regijah je bila razdeljena dokaj sorazmerno. Izstopa zgolj osrednjeslovenska regija.

Skoraj polovica anketirancev (47 %) je zaposlena v podjetju, 21 % anketirancev je zaposlenih v javnem sektorju, 17 % anketirancev je samozaposlenih, 9 % anketirancev pa je študentov. Najmanjši delež anketirancev je brezposelnih, dijakov, osnovnošolcev ali pa so kot odgovor označili drugo. 31 % anketirancev ima od 901 do vključno 1300 € neto mesečnega dohodka, 24 % anketirancev ima mesečno od 1301 do vključno 1700 € neto dohodka, 18 % anketirancev ima od 501 do 900 € neto mesečnega dohodka, po 11 % anketirancev ima do 500 € neto mesečnega dohodka ter od 1701 do 2100 € neto mesečnega dohodka. Najmanjši delež anketirancev (5 %) pa ima nad 2101 € neto mesečnega dohodka.

4.1.2 Opis ankete

Tabela 1: Najpogostejše srečanje z vprašanjem ali s privolitvijo v obdelavo osebnih podatkov

Kje se največkrat srečujete z vprašanjem ali privolitvijo v obdelavo osebnih podatkov?		
	Frekvence	%
Na delovnem mestu.	29	14 %
Pri izpolnjevanju fizičnih dokumentacij.	26	13 %
Ko brskam po spletu.	87	43 %
Ko kupujem v fizičnih trgovinah.	19	9 %
Ko kupujem preko spleta.	43	21 %
SKUPAJ	204	100 %

Vir: lastno delo.

V tabeli 1 sem prikazal, kje se anketiranci najpogosteje srečajo z vprašanjem ali s privolitvijo v obdelavo osebnih podatkov.

Največji odstotek anketirancev se s tem vprašanjem ali s privolitvijo sreča, ko brskajo po spletu (43 %), 21 % anketirancev se s tem sreča, ko kupujejo preko spleta, 14 % anketirancev se s tem sreča na delovnem mestu, 13 % anketirancev se s tem sreča pri izpolnjevanju fizičnih dokumentacij in 9 % anketirancev se s tem sreča, ko kupujejo v fizičnih trgovinah.

Tabela 2: Strinjanje anketirancev s trditvami, ki se navezujejo na pravice posameznika s področja varstva osebnih podatkov

V kolikšni meri se strinjate s spodaj navedenimi trditvami, ki se navezujejo na pravice posameznika s področja varstva osebnih podatkov? Če se s trditvijo ne strinjate, izberite 1 – Sploh se ne strinjam. Bolj ko se s trditvijo strinjate, bolj proti desni boste našli odgovor, ki vam ustreza. Če se s trditvijo zelo strinjate, izberite 5 – Popolnoma se strinjam.								
	1 – Sploh se ne strinjam	2 – Se ne strinjam	3 – Se niti ne strinjam niti strinjam	4 – Se strinjam	5 – Popolnoma se strinjam	Skupaj	Povprečje	Std. od.
Zelo dobro poznam Splošno uredbo o varovanju osebnih podatkov.	13 8 %	40 26 %	24 16 %	71 46 %	5 3 %	153 100 %	3,1	1,09

se nadaljuje

Tabela 2: Strinjanje anketirancev s trditvami, ki se navezujejo na pravice posameznika s področja varstva osebnih podatkov (nad.)

V kolikšni meri se strinjate s spodaj navedenimi trditvami, ki se navezujejo na pravice posameznika s področja varstva osebnih podatkov? Če se s trditvijo ne strinjate, izberite 1 – Sploh se ne strinjam. Bolj ko se s trditvijo strinjate, bolj proti desni boste našli odgovor, ki vam ustreza. Če se s trditvijo zelo strinjate, izberite 5 – Popolnoma se strinjam.								
	1 – Sploh se ne strinjam	2 – Se ne strinjam	3 – Se niti ne strinjam niti strinjam	4 – Se strinjam	5 – Popolnoma se strinjam	Skup.	Povp.	Std. od.
Poznam pravice, ki mi jih nudi zakonodaja na področju varstva osebnih podatkov.	9	37	33	70	3	152	3,1	1
	6 %	24 %	22 %	46 %	2 %	100 %		
Če mi podjetje omogoči uveljavljanje pravic posameznika, se lažje odločim za nakup.	10	32	35	64	11	152	3,2	1,07
	7 %	21 %	23 %	42 %	7 %	100 %		
Podjetja, ki imajo urejeno področje varstva osebnih podatkov, so zaupanja vredna podjetja.	4	33	24	81	11	153	3,4	0,99
	3 %	22 %	16 %	53 %	7 %	100 %		
Podjetja načeloma jasno zapišejo pravice, ki mi jih omogočajo na področju varstva osebnih podatkov.	5	41	33	62	12	153	3,2	1,04
	3 %	27 %	22 %	41 %	8 %	100 %		

Vir: lastno delo.

V tabeli 2 sem prikazal povprečne vrednosti za trditve, ki se navezujejo na pravice posameznika s področja varstva osebnih podatkov. Strinjanje sem meril na petstopenjski Likertovi lestvici, kjer 1 pomeni sploh se ne strinjam, 5 pa popolnoma se strinjam. Vidimo lahko, da se anketiranci najbolj strinjajo s trditvami: »Podjetja, ki imajo urejeno področje varstva osebnih podatkov, so zaupanja vredna podjetja.« (μ=3,4), »Če mi podjetje omogoči uveljavljanje pravic posameznika, se lažje odločim za nakup.« (μ=3,2) in »Podjetja načeloma jasno zapišejo pravice, ki mi jih omogočajo na področju varstva osebnih podatkov.« (μ=3,2). Najmanj pa se anketiranci strinjajo s trditvama: »Zelo dobro poznam Splošno uredbo o varovanju osebnih podatkov.« (μ=3,1) in »Poznam pravice, ki mi jih nudi zakonodaja na področju varstva osebnih podatkov.« (μ=3,1).

Tabela 3: Strinjanje anketirancev s trditvami, ki se navezujejo na personalizacijo vsebine

V kolikšni meri se strinjate s spodaj navedenimi trditvami, ki se navezujejo na personalizacijo vsebine? Če se s trditvijo ne strinjate, izberite 1 – Sploh se ne strinjam. Bolj ko se s trditvijo strinjate, bolj proti desni boste našli odgovor, ki vam ustreza. Če se s trditvijo zelo strinjate, izberite 5 – Popolnoma se strinjam.								
	1 – Sploh se ne strinjam	2 – Se ne strinjam	3 – Se niti ne strinjam, niti strinjam	4 – Se strinjam	5 – Popolnoma se strinjam	Skup.	Povp.	Std. odk
Brez težav pustim OP, če podjetje to zahteva.	13	48	22	62	8	153	3	1,13
	8 %	31 %	14 %	41 %	5 %	100 %		
Brez težav delim lastne OP, če sem seznanjen s svojimi pravicami.	10	31	34	67	11	153	3,2	1,07
	7 %	20 %	22 %	44 %	7 %	100 %		
Brez težav delim lastne osebne podatke, če zaradi tega dobim personal. vsebino.	11	31	33	63	15	153	3,3	1,11
	7 %	20 %	22 %	41 %	10 %	100 %		
Brez težav delim lastne osebne podatke, če v zameno dobim brezplačne storitve.	15	36	30	56	15	152	3,1	1,18
	10 %	24 %	20 %	37 %	10 %	100%		

Vir: lastno delo.

V tabeli 3 sem prikazal povprečne vrednosti za trditve, ki se navezujejo na personalizacijo vsebine.

Strinjanje sem meril na petstopenjski Likertovi lestvici, kjer 1 pomeni sploh se ne strinjam, 5 pa popolnoma se strinjam.

Vidimo lahko, da se anketiranci najbolj strinjajo s trditvama: »Brez težav delim lastne osebne podatke, če zaradi tega dobim personalizirano vsebino/ponudbo.« (μ=3,3) in »Brez težav delim lastne osebne podatke, če sem seznanjen s svojimi pravicami.« (μ=3,2). Najmanj pa se anketiranci strinjajo s trditvama: »Brez težav delim lastne osebne podatke, če v zameno dobim brezplačne storitve.« (μ=3,1) in »Brez težav pustim osebne podatke, če podjetje to zahteva.« (μ=3,0).

Tabela 4: Ocenjevanje anketirancev, koliko nadzora imajo nad uveljavljanjem naštetih pravic v zvezi z obdelavo osebnih podatkov

Na lestvici od 1 do 5 ocenite, koliko nadzora menite, da imate nad uveljavljanjem naštetih pravic v zvezi z obdelavo osebnih podatkov. Če menite, da nad uveljavljanjem pravic nimate nobenega nadzora, izberite 1 – Nimam nobenega nadzora. Več nadzora ko imate, bolj proti desni boste našli odgovor, ki vam ustreza. Če imate popoln nadzor, izberite 5 – Imam popoln nadzor.						
	1 – Nimam nobenega nadzora	2 – Nimam nadzora	3 – Niti nimam niti imam nadzor	4 – Imam nadzor	5 – Imam popoln nadzor	Skupaj
Pravica do izbrisa	8	33	25	75	11	152
	5 %	22 %	16 %	49 %	7 %	100 %
Pravica do popravka	5	32	27	75	11	150
	3 %	21 %	18 %	50 %	7 %	100 %
Pravica do prenosljivosti	10	35	37	63	6	151
	7 %	23 %	25 %	42 %	4 %	100 %
Pravica do pozabe	10	41	31	53	17	152
	7 %	27 %	20 %	35 %	11 %	100 %
Pravica do omejitve obdelave	14	37	30	59	12	152
	9 %	24 %	20 %	39 %	8 %	100 %
Pravica do vpogleda	13	35	19	71	14	152
	9 %	23 %	13 %	47 %	9 %	100 %

Vir: lastno delo.

V tabeli 4 sem prikazal ocene anketirancev o tem, koliko nadzora imajo nad uveljavljanjem naštetih pravic v zvezi z obdelavo osebnih podatkov.

Največ anketirancev meni, da imajo nadzor oziroma, da imajo popoln nadzor nad pravico do popravka (57 %). Le eno odstotno točko manj anketirancev meni, da imajo pravico do izbrisa (56 %) in prav tako menijo za pravico do vpogleda (56 %).

Najmanj anketirancev pa je izrazilo mnenje, da imajo nadzor oziroma, da imajo popoln nadzor nad pravico do omejitve obdelave (37 %). Nekaj več odstotkov anketirancev meni,

da imajo pravico do prenosljivosti (46 %). Prav tako enako število anketirancev meni, da lahko uveljavljajo pravico do pozabe (46 %).

Tabela 5: Zaskrbljenost anketirancev glede zbiranja informacij podjetij o svojih kupcih in njihovih aktivnostih

Podjetja zbirajo veliko informacij o svojih kupcih in o njihovih aktivnostih. Kako zelo ste oziroma niste zaskrbljeni zaradi tega? Če sploh niste zaskrbljeni, izberite 1 – Sploh nisem zaskrbljen. Bolj ko se s trditvijo strinjate, bolj proti desni boste našli odgovor, ki vam ustreza. Če ste zelo zaskrbljeni, izberite 5 – Sem zelo zaskrbljen/a.						
	1 – Sploh nisem zaskrbljen/a	2 – Nisem zaskrbljen/a	3 – Nisem niti zaskrbljen/a niti nezaskrbljen/a	4 – Sem zaskrbljen/a	5 – Sem zelo zaskrbljen/a	Skup.
Zbiranje OP na javnem mestu (na cesti, vlaku, avtobusu, prireditvah itn.)	11	52	24	57	9	153
	7 %	34 %	16 %	37 %	6 %	100 %
Zbiranje OP prek mobilnega telefona ali z uporabo aplikacij na mobilnih telefonih (poslušanje klicev, uporaba geolokacije itn.)	8	39	29	49	28	153
	5 %	25 %	19 %	32 %	18 %	100 %
Zbiranje OP preko t. i. kartic zvestobe (personalizacija ponudbe, oglaševanje, analiza nakupnih vzorcev itn.)	14	50	23	51	15	153
	9 %	33 %	15 %	33 %	10 %	100 %
Zbiranje informacij preko plačilnih kartic	16	35	22	59	21	153
	10%	23 %	14 %	39 %	14 %	100 %

se nadaljuje

Tabela 5: Zaskrbljenost anketirancev glede zbiranjanja informacij podjetij o svojih kupcih in njihovih aktivnostih (nad.)

Podjetja zbirajo veliko informacij o svojih kupcih in o njihovih aktivnostih. Kako zelo ste oziroma niste zaskrbljeni zaradi tega? Če sploh niste zaskrbljeni, izberite 1 – Sploh nisem zaskrbljen. Bolj ko se s trditvijo strinjate, bolj proti desni boste našli odgovor, ki vam ustreza. Če ste zelo zaskrbljeni, izberite 5 – Sem zelo zaskrbljen/a.						
	1 – Sploh nisem zaskrbljen/a	2 – Nisem zaskrbljen/a	3 – Nisem niti zaskrbljen/a niti nezaskrbljen/a	4 – Sem zaskrbljen/a	5 – Sem zelo zaskrbljen/a	Skup.
Zbiranje osebnih podatkov preko spleta (zgodovina, prenos datotek, dostop do vsebin na spletnih straneh itn.)	13	24	20	65	29	151
	9 %	16 %	13 %	43 %	19 %	100 %

Vir: lastno delo.

V tabeli 5 sem prikazal zaskrbljenost anketirancev zaradi tega, ker podjetja zbirajo informacije o svojih kupcih in njihovih aktivnostih.

Iz raziskave je mogoče razbrati, da so anketiranci najbolj zaskrbljeni nad dejstvom, da podjetja zbirajo informacije o svojih kupcih in njihovih aktivnostih preko plačilnih kartic (82 %). Anketiranci so tudi bodisi zaskrbljeni bodisi zelo zaskrbljeni, da podjetja zbirajo informacije o svojih kupcih preko mobilnega telefona ali z uporabo aplikacij na mobilnih telefonih (poslušanje klicev, uporaba geolokacije) (39%).

Anketirance pa najmanj skrbi dejstvo, da podjetja zbirajo osebne podatke preko spleta (zgodovina, prenos datotek, dostop do vsebin na spletih straneh) (33 %). Dejstvo, da podjetja zbirajo informacije preko t. i. kartic zvestobe (personalizacija ponudbe, oglaševanje, analiza nakupnih vzorcev), skrbi le 27 % anketirancev, prav tako je le 19 % anketirancev zaskrbljenih oz. zelo zaskrbljenih, da podjetja zbirajo osebne podatke na javnem mestu (na cesti, vlaku, avtobusu, prireditvah).

Tabela 6: Strinjanje anketirancev s trditvami, ki se navezujejo na varstvo osebnih podatkov

V kolikšni meri se strinjate s spodaj navedenimi trditvami? Ocenite na lestvici od 1 do 5. Če se s trditvijo ne strinjate, izberite 1 – Sploh se ne strinjam. Bolj ko se s trditvijo strinjate, bolj proti desni boste našli odgovor, ki vam ustreza. Če se s trditvijo zelo strinjate, izberite 5 – Popolnoma se strinjam.								
	1 – Sploh se ne strinjam	2 – Se ne strinjam	3 – Se niti ne strinjam niti strinjam	4 – Se strinjam	5 – Popolnoma se strinjam	Skup.	Povp.	Std. odkl.
Podjetja bi morala bolje poskrbeti za varstvo osebnih podatkov.	2	13	16	82	40	153	3,9	0,91
	1 %	8 %	10 %	54 %	26 %	100 %		
Zavedam se, da podjetja upravljajo z mojimi osebnimi podatki.	0	9	20	78	45	152	4	0,82
	0 %	6 %	13 %	51 %	30 %	100 %		
Bolj zaupam podjetjem, ki jasno komunicirajo, kako skrbijo za varstvo osebnih podatkov.	0	10	29	75	38	152	3,9	0,84
	0 %	7 %	19 %	49 %	25 %	100 %		
Podjetjem, ki jasno predstavijo moje pravice, lažje dovolim uporabo svojih osebnih podatkov.	1	12	25	75	40	153	3,9	0,89
	1 %	8 %	16 %	49 %	26 %	100 %		

Vir: lastno delo.

V tabeli 6 sem prikazal strinjanje anketirancev s trditvami, ki se navezujejo na varstvo osebnih podatkov. Strinjanje sem meril na petstopenjski Likertovi lestvici, kjer 1 pomeni sploh se ne strinjam, 5 pa popolnoma se strinjam.

Vidimo lahko, da se anketiranci v večini strinjajo z vsemi trditvami. Najbolj se strinjajo s trditvijo: »Zavedam se, da podjetja upravljajo z mojimi osebnimi podatki.« (μ=4), potem pa sledijo trditve: »Podjetja bi morala bolje poskrbeti za varstvo osebnih podatkov.« (μ=3,9), »Bolj zaupam podjetjem, ki jasno komunicirajo, kako skrbijo za varstvo osebnih podatkov.« (μ=3,9) in »Podjetjem, ki jasno predstavijo moje pravice, lažje dovolim uporabo svojih osebnih podatkov.« (μ=3,9).

4.2 Rezultati analize spletnih mest

Za potrebe magistrskega dela sem analiziral 10 spletnih strani podjetij in primerjal spletne strani podjetij na dan 1. januar 2018 ter spletne strani podjetij na dan 1. januar 2019. Vpogled v arhiv spletnih strani je dostopen na www.archive.org. Ker nekatere strani niso bile pregledane s strani www.archive.org, sem vpogledal v arhiv strani na dan, ki je najbližji izbranem datumu.

Pri ogledu sem bil pozoren na vsebino t. i. pravnih obvestil in pravnih obvestil v zvezi s piškotki. Preveril sem, ali so bili na dan 1. januarja 2018 skladni zgolj z ZVOP-1, predvsem omogočanje pravic seznanitev, sprememba, izbris, ali pa so bili skladni tudi z GDPR-jem. Tukaj je bila pozornost na pravici do omejevanja in prenosljivosti. Preverjal sem informiranje v zvezi z uporabo piškotkov. Torej ali podjetje preko spletne strani obvešča o uporabi piškotkov. Kakšen je način privolitve? So pred privolitvijo dovoljeni le lastni, analitični piškotki?

Preverjal sem, kako uporabnik izvede prijavo na spletne novice in prenos priročnika, kjer to ni bilo mogoče, pa kontakt s podjetjem. Kot primer dobre prakse sem si ogledal smernice Informacijskega pooblaščenca (2018), ki navajajo primer jasnega besedila:

Kaj: Pri naročanju na spletne novice zbiramo vaš naslov elektronske pošte (e-naslov), ki ga vpišete v spletni obrazec.

Zakaj: Te podatke obdelujemo izključno za namene obveščanja o novostih za področje, ki ga izberete.

Koliko časa: Podatki o vaši elektronski pošti se shranjujejo, dokler se od storitve obveščanja po e-pošti ne odjavite. Od prejemanja e-novic se lahko odjavite kadarkoli, in sicer tako, da v prejetem elektronskem sporočilu kliknete na označeno povezavo ali pa tako, da se od e-novic odjavite na naši spletni strani, in sicer tukaj. Ali bodo moji podatki posredovani tretjim osebam?

Upošteval sem tudi opozorila Informacijskega pooblaščenca (2018b), ki se je že v preteklosti srečal s številnimi primeri izjav o varstvu osebnih podatkov, ki so neprimerne in neustrezne zaradi različnih razlogov:

- izjave so kompleksne, predolge in navadnemu uporabniku nerazumljive zaradi uporabe ti. pravniškega jezika;
- uporabljajo se vnaprej pripravljeni vzorci izjav, ki niso prilagojeni dejanskemu stanju in konkretnemu spletnemu naslovu;
- izjave o varstvu osebnih podatkov so pripravljene ob vzpostavitvi spletnega mesta in se ne ažurirajo;
- oblikovanje izjave ni pregledno in zato uporabnike odvrača od branja.

Pri analizi sem se nanašal na 8 točk, ki jih morajo po mnenju Informacijskega pooblaščenca (2018b), ki jih morajo podjetja upoštevati, ko obiskovalce opozarjajo na obdelavo osebnih podatkov:

- kdo obdeluje podatke? Navesti morajo podatke o upravljavcu osebnih podatkov in morebitnem predstavniku, če gre za upravljavca izven EU; (osebno ime, če gre za fizično osebo, naziv oziroma firma in naslov oziroma sedež); podatki o pooblačeni osebi, če je ta imenovana.
- katere podatke podjetje obdeluje? Poleg podatkov, ki jih uporabnik zaupa ob morebitni registraciji, in uporabi spletnega mesta, podjetje ne sme pozabiti na podatke, ki jih zbira v zvezi s samim obiskov spletne strani. Podatki kot so npr. datum in ura obiska, IP naslov itd.
- zakaj podjetje obdeluje osebne podatke? Čim natančneje je potrebno opredeliti za kakšen namen oziroma kakšne namene in na kakšni pravni podlagi podjetje obdeluje osebne podatke; kadar obdelava poteka na podlagi zakonitih interesov (člen 6 (1f)), pa tudi o zakonitih interesih, ki se z obdelavo zasledujejo; če mora posameznik posredovati svoje osebne podatke (npr. zaradi pogodbe), tudi kakšne bodo posledice, če posameznik podatkov ne posreduje.
- komu podjetje posreduje podatke? Posameznike je potrebno obvestiti o morebitnih uporabnikih ali kategorijah teh uporabnikov (uporabniki so lahko npr. zunanji vzdrževalci spletnega mesta, trženjska podjetja) pri tem pa je treba posameznike obvestiti tudi, če bo prišlo do prenosa njihovih podatkov v tretje države z navedbo informacij o zagotavljanju varovanja podatkov po prenosu.
- koliko časa bo podjetje podatke hranilo? Potrebno je opredeliti čas hrambe osebnih podatkov oziroma, kjer to ni mogoče, vsaj kriterije po katerih se določi čas hrambe.
- podjetje mora opredeliti katere pravice imajo posamezniki:
  - pravica do seznanitve,
  - popravka,
  - izbrisa,
  - omejitve obdelave,
  - kjer je ustrezno pa tudi pravica do preklica privolitve,
  - ugovora,
  - pravica do prenosljivosti.
  - pravica do pritožbe pri nadzornem organu v primeru kršitve GDPR-ja.
- profiliranje, avtomatizirano odločanje: Če podjetje na podlagi podatkov o posamezniku zakonito izvaja profiliranje oz. sprejema avtomatizirane odločitve s pravnim ali podobnim učinkom, mora podjetje navesti tudi, kateri so razlogi za profiliranje ali avtomatizirano odločanje, kot tudi pomen in predvidene posledice, ki jih obdelava prinaša posamezniku.
- obdelava za drug namen: Kadar nameravata podjetje osebne podatke še obdelovati za namen, ki ni namen, za katerega so bili osebni podatki zbrani, je potrebno posamezniku sporočiti ta drugi namen že ob zbiranju (npr. neposredno trženje z uporabo podatkov zbranih v zvezi s spletnim nakupom izdelka).

22. člen GDPR-ja pravi, da ima posameznik pravico, da zanj ne velja odločitev, ki

- temelji zgolj na avtomatiziarni obdelavi vključno z oblikovanjem profilov, na podlagi katerih se ocenjujejo osebni vidiki v zvezi s posameznikom, zlasti za analizo ali predvidevanje uspešnosti pri delu, ekonomskega položaja, zdravja, osebnega okusa ali interesov, zanesljivosti ali vedenja, lokacije ali gibanja;
- ima pravne učinke v zvezi z njim ali na podoben način nanj znatno vpliva (npr. avtomatska zavrnitev spletne prošnje za posojilo ali prakse zaposlovanja prek spleta brez človekovega posredovanja).

Razen, če je odločitev:

- nujna za sklenitev ali izvajanje pogodbe z upravljavcem,;
- dovoljena v pravu Unije ali države članice, ki velja za upravljavca in določa tudi ukrepe za zaščito pravic in svoboščin ter zakonitih interesov posameznika (tudi za namene spremljanja in preprečevanja zlorab in davčnih utaj;
- utemeljena z izrecno privolitvijo posameznika.

Analiziral sem tudi pravna obvestila spletne strani. Zanimalo me je, ali obiskovalca spletne strani seznanijo s tem. kdo je upravljavec osebnih podatkov, katere osebne podatke se zbira, kaj so nameni obdelave, kakšen je čas hrambe, kako skrbijo za varnost, kakšne so pravice posameznika in kako jih lahko posameznik uveljavlja.

Analiziral sem:

- dve mikro podjetji,
- dve mali podjetji,
- tri srednje velika podjetja,
- tri velika podjetja.

Velikosti podjetji so skladne s poimenovanjem v 55. členu Zakona o gospodarskih družbah (ZGD-1) Ur. l. RS, št. 42/06, ki podjetja po velikosti razvrsti glede na povprečno število delavcev v poslovnem letu, čiste prihodke od prodaje in vrednost aktive.

4.2.1 Uporaba piškotkov

Večina podjetij, 6 od 10, je obvestilo o uporabi piškotkov zaradi GDPR-ja nekoliko spremenila. Strinjanje s piškotki je na večini spletnih strani prvi stik obiskovalca.

Sprememba tega kaže na to, da se podjetja zavedajo pomembnosti in želijo na nek način opozoriti posameznika, da jim je varnost osebnih podatkov pomembna. Dejstvo pa je, da je sprememba te pasice najbolj enostaven korak, s katerim podjetje pokaže, da jim je mar za varstvo osebnih podatkov.

Pri 4 od 10 analiziranih spletnih strani je bilo opaziti, da so obiskovalcem sedaj omogočili razširjeno definicijo in ponudili, da si sami izberejo, katere piškotke želijo, da podjetje uporablja. Podjetja se sedaj poslužujejo t. i. opt-out uporabe načina.

4.2.2 Prijava na spletne novice ali kontakt s podjetjem

Le 4 izmed 10 spletnih strani so bile v tej točki posodobljene v luči približevanja GDPR-ju. Na teh straneh je jasno izraženo, katere podatke potrebujejo za kateri namen in kakšne so pravice posameznika. Večina spletni strani (6) je začela uporabljati besedno zvezo izrecna privolitev, kar nakazuje na to, da se želijo približati skladnosti z GDPR-jem. Opaziti je tudi, da se podjetja ne zavedajo v katerih primerih lahko zahtevajo katere podatke, vseeno pa so

opozorili razširila, v želji, da bi obiskovalci spletnih strani vedeli katere osebne podatke dovoljujejo v uporabo in s katerim namenom.

4.2.3 Pravno obvestilo

7 izmed 10 spletnih strani podjetij je dopolnilo pravno obvestilo. Večje ko je bilo podjetje, do večjih sprememb je prišlo. Ta podjetja sedaj jasno definirajo pravno obvestilo oz. t. i. politiko varstva osebnih podatkov. Jasno je zapisano, kdo je upravljavec, DPO, katere osebne podatke se zbira, čas hrambe, skrb za varnost, pravice posameznika, postopek uveljavljanja pravic in pravica do vložitve pritožbe.

4.3 Analiza raziskovalnega vprašanja

Zanimalo me je, kako bo sprejeta Splošna uredba o varstvu osebnih podatkov vplivala na pripravljenost potrošnikov, da svoje osebne podatke posredujejo gospodarskim subjektom.

RV: Kako bo sprejeta Splošna uredba o varstvu osebnih podatkov vplivala na pripravljenost potrošnikov, da svoje osebne podatke posredujejo gospodarskim subjektom?

Na podlagi zgornjih rezultatov menim, da sprejeta Splošna uredba o varstvu osebnih podatkov ne bo vplivala na pripravljenost potrošnikov, da svoje osebne podatke posredujejo gospodarskim subjektom.

Potrošniki sicer lažje posredujejo osebne podatke podjetjem, ki jim jasno sporočajo, za kateri namen te osebne podatke potrebujejo, in jim omogočajo, da se lahko kot potrošniki kadarkoli odločijo za odstop. Kljub temu pa potrošniki svoje osebne podatke brez težav delijo tudi z ostalimi podjetji. Da bi razumeli točne razloge, zakaj je temu tako, so potrebne nadaljnje raziskave. Dejstvo, ki sem ga zaznal z analizo spletnih mest, pa je, da podjetja vlagajo velike napore v to, da bi bila skladna z obstoječo zakonodajo.

5 RAZPRAVA O UGOTOVITVAH

Večina anketirancev se največkrat sreča z dilemo, ali pustiti svoje osebne podatke v zameno za dostop do neke vsebine preko spleta. Vprašanje, ki se tukaj poraja, je, ali je temu res tako ali so anketiranci preprosto bolj pozorni na te vsebine. Dejstvo je, da je do večjega zavedanja o pomenu varstva osebnih podatkov prišlo prav v času porasta družbenih omrežij v digitalnih okoljih. Prav tako količina podatkov, ki jih podjetja tukaj lahko zberejo, ponuja veliko možnosti za obdelovanje (Klemenčič, Makarovič, Klobučar, Bogataj Jančič & Pahor, 2003, str. 112).

Večina anketirancev GDPR-ja ne pozna dovolj dobro. Kljub temu pa obstaja zavedanje o pomembnosti tega področja. Večina jih trdi, da so pripravljeni pustiti osebne podatke podjetjem, ki jim jasno predstavijo, za kaj se določen osebni podatek potrebuje in kako se bo z njim ravnalo. Še lažje pa jim dajo privolitev, ko jim podjetje jasno izrazi pravice, ki jih omogoča zakonodaja.

Na vprašanje o uveljavljanju pravic glede varstva osebnih podatkov je večina odgovorila, da so jim omogočene pravice, ki smo jih poznali že pred sprejetjem GDPR-ja. Težko je reči ali je temu res tako ali pa je to zgolj zaradi zavedanja o tej tematiki.

Večina anketirancev je zelo zaskrbljena nad zbiranjem informacij preko plačilnih kartic. Količina informacij, ki jih banke dobijo na tak način, je velika in zelo osebna. Razumljivo je, da ljudi to skrbi. Zanimivo pa je, da jih ne skrbi pridobivanje osebnih podatkov na javnih mestih.

Velika večina anketirancev se zaveda, da podjetja upravljajo z njihovimi osebnimi podatki, in se strinjajo, da bi podjetja morala bolj skrbeti za njihove osebne podatke. Podjetjem, ki dobro upravljajo z osebnimi podatki in to jasno komunicirajo, anketiranci bolj zaupajo.

Ugotovitve kažejo na to, da so podjetja vzela sprejetje GDPR-ja zelo resno, potrošniki pa malo manj. Skrb vzbujajoče je dejstvo, da večina anketirancev brez težav deli osebne podatke, če zaradi tega dobijo personalizirano vsebino oz. ponudbo. Prav to je razlog, da prihaja do večjih afer. Potrošniki v želji po tem, da čim prej prejmejo storitev oz. produkt, oddajo privolitev in spregledajo, kaj vse podjetje zahteva v zameno.

Na tem mestu se poraja vprašanje kako daleč so pripravljeni potrošniki iti, da bo zadovoljili svoje potrebe. Predvsem pa bi bilo potrebno ugotoviti s kakšnimi sporočili bi bilo potrošnike potrebno opozarjati, da bi preprečili brezglavo deljenje osebnih podatkov.

Ključna posledica GDPR-ja je zavedanje potrošnikov o tej tematiki. Po podatkih informacijskega pooblaščenca (2019) lahko to tezo še bolj pritrdim. Od 25. maja 2018 do 31. decembra 2018 je Informacijski pooblaščenec prejel 598 prijav zaradi kršitve varstva osebnih podatkov, medtem ko jih je v enakem obdobju leta 2017 prejel 290. Po mnenju informacijskega pooblaščenca (2019) lahko občutno povečanje števila prijav nedvomno pripišemo večji ozaveščenosti posameznikov v zvezi z obdelavo njihovih osebnih podatkov in pravicami, ki jim jih daje GDPR, saj se je o tematiki v obravnavanem obdobju v medijih veliko govorilo in pisalo.

Iz analize spletnih mest je jasno razbrati, da so podjetja naredila veliko v želji, da bi se čim bolj približala skladnosti z GDPR-jem. Večje ko je podjetje, večji korak je naredilo. Večja podjetja imajo veliko več sredstev, ki jih lahko namenijo temu področju. Prav tako pa se zavedajo, da jih potrošniki in inšpektorat ves čas spremljajo. Možnosti za napake tako ni. Izpostavil bi še dejstvo, da manjša podjetja kopirajo primere dobrih praks večjih podjetij. Razlogov za to je lahko več. Izpostavil bi dva. Prvi je ta, da je to cenovno najbolj ugodno. Drugi pa je ta, da imajo velika podjetja več znanja in virov na tem področju.

Večina podjetij je poskrbela za skladnost že pred 25. majem 2018. Tukaj je potrebno upoštevati dejstvo, da je bila področna zakonodaja na tem področju, že pred sprejetjem GDPR-ja precej rigorozna. Prav tako se je o ključnih novostih govorilo že v času sprejemanja GDPR-ja in v prehodnem obdobju.

To je razbrati tudi z letnega poročila Informacijskega pooblaščenca za leto 2018 (2019). Informacijski pooblaščenec namreč na podlagi člena 57 GDPR-ja in 49. člena ZVOP-1 izdaja neobvezna mnenja, pojasnila in stališča o vprašanjih s področja varstva osebnih podatkov, s katerimi prispeva k ozaveščenosti upravljavcev in obdelovalcev ter širše javnosti.

Leta 2018 je tako izdal 2192 pisnih mnenj in napotitev na mnenja, kar je 70-odstotkov več napram letu 2017, ko je bilo izdanih 1.289 pisnih mnenj in napotitev.

Zakonodaja na tem področju je sicer precej jasna in rigorozna, hkrati pa se je zakonodajalec zavedal širine in težavnosti tega področja. Ob sprejetju GDPR-ja se je zakonodajalec zavedal, da popolne skladnosti ne bo, vendar pa mora biti poglaviten cilj prav vsakega podjetja ves čas težiti k čim večji skladnosti z GDPR-jem. Podjetja morajo tako ves čas delati, da bodo osebne podatke potrošnikov obdelovala v najboljši veri. To je jasno razvidno tudi iz analize spletnih strani.

Podjetja se zavedajo, da upravljanje s podatki prinaša prednost. Večja podjetja imajo več denarja, ki ga lahko namenijo za investicije na tem področju. Takšna podjetja skrbijo, da bodo baze podatkov, ki jih obdelujejo, ves čas urejene tako, da bodo iz njih lahko pridobili informacije, ki jim bodo omogočale prednost na trgu. Takšnih podjetij sprejetje GDPR-ja ni presenetilo. Če pa jih je, so svojo strategijo prilagodila v dve leti trajajočem prehodnem obdobju in so bila 25. maja 2018 že dobro pripravljena.

Na podlagi analize lahko trdim, da je zavedanje podjetij o pomembnosti tega področja ključno za to, da ne bo prišlo do kršitev. Vsaka kršitev pripelje do nezaupanje potrošnikov. Nezaupanje potrošnikov v podjetje pa pripelje do izgube dobička. Cilj podjetij je torej slediti zakonodaji in volji potrošnikov.

Tej trditvi pritrjujejo tudi podatki Informacijskega pooblaščenca (2019) za obdobje med 25. majem 2018 in 31. decembrom 2018, ko je Informacijski pooblaščenec prejel 68 uradnih obvestil o kršitvi varnosti osebnih podatkov, ki so jih poslali upravljavci osebnih podatkov. Podjetja so v tem primeru sama opozarjala, da je prišlo do kršitev. Podjetja tako precej vestno prijavljajo varnostne incidente. Upravljavci osebnih podatkov so uradna obvestila o kršitvi varnosti osebnih podatkov najpogosteje pošiljali zaradi neupravičenega razkritja osebnih podatkov (posredovanja osebnih podatkov nepooblaščenim ali napačnim osebam), nepooblaščenega dostopanja do osebnih podatkov (zaradi programske napake ali zlorabe pooblastil s strani zaposlenih), vdora v informacijski sistem ter izgube ali kraje nosilcev osebnih podatkov (npr. osebnih računalnikov in službenih mobilnih telefonov).

Dejstvo, ki ga je na tem mestu treba izpostaviti, je, da so bila skoraj vsa podjetja skladna s prej veljavno zakonodajo, ki se v veliki meri ne razlikuje od GDPR-ja. Večina teh podjetij je izvedla nekaj ukrepov, da bi še bolj zavarovala pravice potrošnikov in se na ta način približala potrošniku in hkrati GDPR-ju. Vsekakor lahko trdim, da se podjetja zavedajo pomena tega področja in delajo korake v pravo smer.

6 SKLEP

V zvezi z raziskovalnim vprašanjem, kako bo sprejeta Splošna uredba o varstvu osebnih podatkov vplivala na pripravljenost potrošnikov, da svoje osebne podatke posredujejo gospodarskim subjektom, sem na podlagi primerjave pravne ureditve varstva osebnih podatkov potrošnikov v RS pred uveljavitvijo GDPR-ja in po tem, ko je GDPR stopila v veljavo, ugotovil, da se potrošniki zavedajo, da podjetja zbirajo podatke o njih in jih zelo dobro uporabljajo sebi v prid. Potrošniki trdijo, da raje posredujejo osebne podatke podjetjem, ki jim zelo jasno razložijo, zakaj jih bodo uporabili.

Kljub temu pa se vsakih nekaj mesecev pojavi aplikacija, ki uporabniku v zameno za enormno količino osebnih podatkov podari manjše darilo. Dober primer je aplikacija FaceApp, ki jo je v tednu dni preneslo več kot 100 milijonov potrošnikov. Aplikacija te v zameno za odobritev dostopa do prav vseh tvojih slik postara. Poraja se vprašanje, zakaj podjetje, ki stoji za aplikacijo, potrebuje dostop do čisto vseh fotografij. Predvsem pa je zanimivo dejstvo, da ljudje aplikaciji dovolijo dostop s samo enim klikom, ne da bi karkoli prebrali.

V raziskavi sem ugotovil, da ljudje večino pravic dobro poznajo. Morda je torej razlog za brezglavo deljenje osebnih podatkov tudi ta, da se zavedajo, da v večini primerov lahko podatke izbrišejo s spleta. Če neželene informacije lahko zbrišeš z Googlovega brskalnika, potem tako ali tako ni nobene bojazni, da bi se te osebni podatki kadarkoli v prihodnosti lahko razkrili. To je smer, ki bi jo bilo smiselno bolj raziskati.

Zaradi nekakšne naivnosti ljudi oz. potrošnikov je prav, da pristojni organi opozarjajo na pomembnost tega področja in ozaveščajo. Prav tako je pomembno, da opravijo svoje delo, ko pride do večjih kršitev. Veliko vlogo v primeru kršitev opravijo tudi mediji. Predvsem tako, da skrbijo za ozaveščanje.

V delu sem ugotovil, da so podjetja vzela GDPR z vso resnostjo – predvsem velika podjetja. Podjetja ves čas delajo na tem, da bi bile njihove trženjske aktivnosti skladne z trenutno obstoječo zakonodajo. Pred 25. majem 2018 je bila to lokalna zakonodaja – v Sloveniji ZVOP-1, zdaj je to GDPR.

Ne morem trditi, da je GDPR spremenil trženje, vendar je do neke mere dosegel svoj namen. Namen GDPR-ja je bil poenotiti zakonodajo in dvigniti zavest o pomembnosti varstva osebnih podatkov v EU. Ker je v EU veliko tujih multinacionalk, lahko trdimo, da je vpliv GDPR-ja globalen. Iz ZDA prihaja največ podjetij, katerih posel je odvisen od obdelave osebnih podatkov. Drugi najpomembnejši trg, takoj za ZDA, je EU. Redka so podjetja, ki bodo svojo politiko upravljanja z osebnimi podatki prilagodila samo za evropski trg. Če ne takoj, pa malo kasneje bodo to politiko prenesla tudi v ostale države in primeri dobrih praks se tako leto dni za sprejetjem kažejo že v drugih državah.

Slovenski pregovor pravi: tresla se je gora, rodila se je miš. V primeru sprejetja GDPR-ja so za nekakšno paniko med podjetji poskrbele pravne pisarne in podjetja, ki ponujajo programske rešitve za upravljanje z osebnimi podatki, npr. CRM-sisteme. Njihove aktivnosti so bile popolnoma legitimne. Dejstvo je, da mora imeti vsako podjetje, ki obdeluje osebne podatke, primerno poskrbljeno za pravni vidik, prav tako pa morajo imeti zbiranje in obdelavo urejeno sistemsko.

Cilj GDPR-ja je bil hkrati doseči enake pogoje za vsa podjetja. Podjetja, ki obdelujejo osebne podatke, imajo sedaj po zaslugi GDPR-ja bolj urejene baze. Z urejenimi bazami je precej lažje dobiti informacije, ki pomagajo pri sprejemanju odločitev.

Zavedanje pomembnosti področja varstva osebnih podatkov je zaradi GDPR-ja večje. Prav tako so podjetja zaradi sprejetja prevetrila svoje trženjske strategije. Veliko podjetij je začelo svoje baze podatkov (predvsem liste za obveščanje) zbirati na novo. In to je dobro. Zakaj bi tržil nekomu za vsako ceno, če ga tvoja vsebina oz. ponudba ne zanima? Takšna prevetritev

je poskrbela, da so se tržniki ponovno usedli za mizo in premislili o novih načinih, kako pridobivati stranke. Sedaj so trženjska sporočila bolj ciljana in bolj premišljena. Potrošniki so zaradi tega manj obremenjeni s trženjskimi sporočili. Kadar pa do njih pride sporočilo, je to sporočilo bolj zanimivo zanje.

Pomembnosti tega področja se zavedajo tudi podjetja. Vrednost Facebooka je odvisna od tega, koliko časa uporabnik preživi na njihovi platformi. Več časa ko preživiš na platformi, več je priložnosti za predvajanje oglasnih sporočil. Če sporočila niso prilagojena posamezniku, posameznik platformo zapusti. Podjetji Google in Microsoft, ki omogočata pošiljanje elektronske pošte, sta ravno s tem namenom razvili poseben del elektronske pošte, ki se imenuje nezaželena pošta (ang. junk) (Jamnik, 2018).

Podjetja delajo vse, da bi svoje storitve in/ali produkte čim bolj približala potrošniku. Tako bo tudi naprej. Vedno se bo našel nekdo, ki bo tekom teh procesov želel potrošniku ali podjetju škodovati. V takih primerih je pomembno, da je zakonodaja primerno urejena in da se potrošniki zavedajo nevarnosti.

Ključni izziv za podjetja je spremeniti način razmišljanja o področju varstva osebnih podatkov. Če so v preteklosti lahko podatke zbirali brez, da bi vedeli kaj bodo z njimi naredili, morajo sedaj strateško pristopiti k zbiranju podatkov. Kljub dodatnem delu, pa to prinaša prednosti. Podjetja bodo zaradi tega začele s strani potrošnikov začela pridobivati bolj kvalitetne podatke.

Tema, kateri bi bilo v prihodnosti smotrno nameniti več razmisleka, je kako daleč so potrošniki pripravljeni iti, da zadovoljijo svoje potrebe in kaj je potrebno narediti, da tega ne storijo brezglavo. Na kakšen način bi potrošnika lahko čim bolj informirali o morebitnih posledicah.

LITERATURA IN VIRI

1. Accenture PLC. (2018, maj). *Personalization pulse check 2018*. Pridobljeno (3. marca 2019) iz https://www.accenture.com/t20161011T222718Z__w__/us-en/_acnmedia/PDF-34/Accenture-Pulse-Check-Dive-Key-Findings-Personalized-Experiences.pdfla=en
2. Centa, N. (2018). *Vpliv Splošne uredbe o varstvu podatkov na organizacije in potrošnike v Sloveniji* (magistrsko delo). Ljubljana: Fakulteta za družbene vede.
3. Čebulj, J. (1992). *Varstvo informacijske zasebnosti v Evropi in Sloveniji*. Ljubljana: Inštitut za javno upravo pri Pravni fakulteti v Ljubljani.
4. Čebulj, J. & Žurej, J. (2005). *Varstvo osebnih podatkov in informacije javnega značaja*. Ljubljana: Nebra.
5. Dolenc, S. (2018). *Veliko podatkovje in avtonomni subjekt svobodne volje. Pravo in nadzor v dobi velikega podatkovja.* Ljubljana: Inštitut za kriminologijo pri Pravni fakulteti.
6. Drev, M. (2016, 10. oktober). *7 napotkov za zakonit in učinkovit direktni marketing*. Pridobljeno (6. aprila 2019) iz https://www.dmslo.si/zapis/6-napotkov-za-zakonit-in-uinkovit-direktni-marketing
7. Drev, M. (2018). *Splošna uredba o varstvu podatkov – pogled Informacijskega pooblaščenca* (interno gradivo). Šenčur: FrodX d.o.o.

8. Evropski nadzornik za varstvo podatkov. (2019). *The history of the general data protection regulation*. Pridobljeno (14. marca 2019) iz https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en
9. Edwards, L. (2018, 21. maj). *Data Protection: Enter the General Data Protection Regulation*. Pridobljeno (1. aprila 2019) iz https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3182454
10. Evropska komisija. (2018). *2018 reform of EU data protection rules*. Pridobljeno (3. julija 2019) iz https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en
11. Falque-Pierrotin, I. (2017). *Smernice o pooblaščenih osebah za varstvo podatkov.* Bruselj: Evropska komisija.
12. Farmer, N., Rogers, H. & Smart, L. (2017, 10. november) . *Preparing for GDPR – Guidance from the Article 29 Working Party*. Pridobljeno (26. septembra 2019) iz https://www.clearycyberwatch.com/2017/11/preparing-gdpr-guidance-article-29-working-party/
13. Finžgar, A. (1985). *Osebnostne pravice*. Ljubljana: Slovenska akademija znanosti in umetnosti v Ljubljani.
14. Goodwin, C. (1991). Privacy: Recognition of a Consumer Right. *Journal of Public Policy & Marketing, 10,* 149–166.
15. Godec, A. (2008). *Neposredno trženje in varstvo osebnih podatkov. Računovodstvo, davki, pravo, 1*(7–8), 109-113.
16. Hughes, A. (1994). *Strategic Database Marketing: The Masterplan for Starting and Managing a Profitable, Customer-Based Marketing Program*. Čikago: Probes Publishing.
17. Informacijski pooblaščenec. (2007, 15. december). *Mnenje glede veljavnih oblik privolitve*. Pridobljeno (1. septembra 2019) iz https://www.ip-rs.si/vop/mnenje-glede-veljavnih-oblik-privolitve1302/
18. Informacijski pooblaščenec. (2008). *Oglaševanje oziroma tržno segmentiranje s strani spletnih portalov*. Pridobljeno (1. septembra 2019) iz https://www.ip-rs.si/varstvo-osebnihpodatkov/iskalnik-po-odlocbah-in-mnenjih/odlocbe-in-mnenja-varstvo-osebnihpodatkov
19. Informacijski pooblaščenec. (2009). *Informirani potrošnik - komu dajem katere osebne podatke in zakaj?* Pridobljeno (1. septembra 2019) iz https://www.ip-rs.si/fileadmin/user_upload/Pdf/smernice/Potrosniki_koncna_web
20. Informacijski pooblaščenec. (2018a, december). *Smernice Informacijskega pooblaščenca za oblikovanje izjave o varstvu osebnih podatkov na spletnih straneh*. Pridobljeno (1. septembra 2019) iz https://www.ip-rs.si/publikacije/prirocniki-in-smernice/smernice-informacijskega-pooblascenca-za-oblikovanje-izjave-o-varstvu-osebnih-podatkov-na-spletnih-straneh/
21. Informacijski pooblaščenec. (2018b). *Informirani potrošnik - komu dajem katere osebne podatke in zakaj?* Pridobljeno (1. septembra 2019) iz https://www.ip-rs.si/publikacije/prirocniki-in-smernice/ocene-ucinkov-na-varstvo-podatkov/
22. Informacijski pooblaščenec. (2019, maj). *Letno poročilo Informacijskega pooblaščenca za leto 2018.* Pridobljeno (1. septembra 2019) iz https://www.ip-rs.si/publikacije/letna-porocila/
23. Jamnik, M. (2018). *Kaj prinaša Splošna uredba o varstvu podatkov* (interno gradivo). Ljubljana: FrodX d.o.o.

24. Klemenčič, G., Makarovič, B., Klobučar, T., Bogataj Jančič, M. & Pahor, D. (2003). *Internet in pravo: izbrane teme s komentarjem Zakona o elektronskem poslovanju in elektronskem podpisu.* Ljubljana: Pravna fakulteta.
25. Korže, B. (2016). *Pravo družb in poslovno pravo*. Ljubljana: Uradni list Republike Slovenije.
26. Kovačič, M. (2003). *Zasebnost na internetu*. Ljubljana: Mirovni inštitut za sodobne družbene in politične študije
27. Kotler, P. (1996). *Marketing management - trženjsko upravljanje: analiza, načrtovanje izvajanje in nadzor*. Ljubljana: Slovenska knjiga.
28. Križaj, F. (1989). *Osebne svoboščine in zasebnost v informacijski družbi*. Ljubljana: Gospodarska založba.
29. Možina, D. (2000). *Varstvo osebnih podatkov na spletu*. *Pravna praksa, 19*(36/37), 23-29.
30. Oseben. (1994). Ljubljana: Državna založba Slovenije.
31. Phelps, J., Nowak, G. & Ferrel, E. (2000). *Privacy Concerns and Consumer Willingness to Provide Personal Information*. *Journal of Public Policy & Marketing, 19,* 27-41.
32. Pingitore, G., Rao, V., Cavallaro, K. & Dwivedi, K. (2017, 5. september). *To share or not to share*. Pridobljeno (17. marca 2019) iz https://www2.deloitte.com/insights/us/en/industry/retail-distribution/sharing-personal-information-consumer-privacy-concerns.html
33. Pirc Musar, N., Bien, S., Bogataj, J., Prelesnik, M. & Žaucer, A. (2006). *Zakon o varstvu osebnih podatkov s komentarjem*. Ljubljana: GV založba.
34. Pirc Musar, N., Prelesnik, M. & Bien, S. (2006a). *Predpisi s področja prava varstva osebnih podatkov in dostopa do informacij javnega značaja*. Ljubljana: GV Založba.
35. Pirc Musar, N., Prelesnik, M. & Bien, S. (2006b). *Varstvo osebnih podatkov: vstop v zasebnost prepovedan*. Ljubljana: GV Založba.
36. Praprotnik, D. (2006). *Varovanje podatkov in zasebnosti na internetu* (magistrsko delo). Ljubljana: Ekonomska fakulteta.
37. Quinn, M. & Rogers, D. (2015, oktober). *What Is the Future of Data Sharing*? Pridobljeno (1. aprila 2019) iz https://www8.gsb.columbia.edu/globalbrands/sites/globalbrands/files/images/The_Future_of_Data_Sharing_ColumbiaAimia_October_2015.pdf
38. Statista, Inc. (2016, 28. november). *Level of agreement regarding Internet of Things (IoT) manufacturers sufficiently informing consumers about information the devices can collect in Europe in 2016*. Pridobljeno (1. februarja 2019) iz https://www.statista.com/statistics/609021/trust-in-iot-device-manufacturers-eu/
39. Swirl Networks, Inc. (2015, 10. december). *New Study Reveals That Traditional Retailers Are Failing to Meet Consumer Desires for Amazon-like Personalization*. Pridobljeno (1. maja 2019) iz https://www.prnewswire.com/news-releases/new-study-reveals-that-traditional-retailers-are-failing-to-meet-consumer-desires-for-amazon-like-personalization-300191107.html
40. Tankard, C. (2016). *What the GDPR means for business*. *Digital Pathways, 2016(6),* 5-8.
41. Volokh, E. (2000). *Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People from Speaking about You*. *Stanford Law Review*. *52(5),* 1049-1124.
42. Žagar, K. & Blažič, J. (2017, 8. september). *Varstvo osebnih podatkov*. *Primerjalni pregled*. Pridobljeno (1. aprila 2019) iz https://fotogalerija.dz-rs.si/datoteke/Publikacije/Zborniki_RN/2017/Varstvo_osebnih_podatkov.pdf

PRILOGE

Priloga 1: vprašalnik

Pozdravljeni, kot podiplomski študent Ekonomske fakultete, smer Mednarodno poslovodenje in organizacija, v magistrskem delu raziskujem vpliv Splošne uredbe o varstvu osebnih podatkov potrošnikov na trženje. Anketa je primerna za vse posameznike s stalnim prebivališčem v Sloveniji, ki so starejši od 16 let.
Z izpolnitvijo ankete boste pomagali pridobiti potrebne rezultate za izpeljavo analize. Izpolnjevanje ankete v povprečju vzame 6 minut, vaše sodelovanje pa je anonimno.

Najlepša hvala,
Matevž Kadak

1. Kje se največkrat srečujete z vprašanjem ali privoliti v obdelavo osebnih podatkov? Možnih je več odgovorov.

- Na delovnem mestu
- Pri izpolnjevanju fizičnih dokumentacij
- Ko brskam po spletu
- Ko kupujem v fizičnih trgovinah
- Ko kupujem preko spleta

2. V kolikšni meri se strinjate s spodaj navedenimi trditvami, ki se navezujejo na pravice posameznika s področja varstva osebnih podatkov? Če se s trditvijo ne strinjate, izberite 1 - Sploh se ne strinjam. Bolj kot se s trditvijo strinjate, bolj izberite odgovor na desni strani. Če se s trditvijo zelo strinjate, izberite 5 - Popolnoma se strinjam.

1. Sploh se ne strinjam
2. Se ne strinjam
3. Se niti ne strinja, niti strinjam
4. Se strinjam
5. Popolnoma se strinjam

- Zelo dobro poznam Splošno uredbo o varovanju osebnih podatkov.
- Poznam pravice, ki mi jih nudi zakonodaja na področju varstva osebnih podatkov.
- Če mi podjetje omogoči uveljavljanje pravic posameznika, se lažje odločim za nakup.
- Podjetja, ki imajo urejeno področje varstva osebnih podatkov, so zaupanja vredna podjetja.
- Podjetja načeloma jasno zapišejo pravice, ki mi jih omogočajo na področju varstva osebnih podatkov.

3. V kolikšni meri se strinjate s spodaj navedenimi trditvami, ki se navezujejo na pravice posameznika s področja varstva osebnih podatkov? Če se s trditvijo ne strinjate, izberite 1 - Sploh se ne strinjam. Bolj kot se s trditvijo strinjate, bolj izberite odgovor na desni strani. Če se s trditvijo zelo strinjate, izberite 5 - Popolnoma se strinjam.

1. Sploh se ne strinjam
2. Se ne strinjam
3. Se niti ne strinja, niti strinjam
4. Se strinjam
5. Popolnoma se strinjam

- Brez težav pustim osebne podatke, če podjetje to zahteva.
- Brez težav delim lastne osebne podatke, če sem seznanjen s svojimi pravicami.
- Brez težav delim lastne osebne podatke, če zaradi tega dobim personalizirano vsebino/ponudbo.
- Brez težav delim lastne osebne podatke, če v zameno dobim brezplačne storitve.

4. V kolikšni meri se strinjate s spodaj navedenimi trditvami, ki se navezujejo na pravice posameznika s področja varstva osebnih podatkov? Če se s trditvijo ne strinjate, izberite 1 - Sploh se ne strinjam. Bolj kot se s trditvijo strinjate, bolj izberite odgovor na desni strani. Če se s trditvijo zelo strinjate, izberite 5 - Popolnoma se strinjam.

   - Pravica do izbrisa.
   - Pravica do popravka.
   - Pravica do prenosljivosti.
   - Pravica do pozabe.
   - Pravica do omejitve obdelave.
   - Pravica do vpogleda.

5. Podjetja zbirajo veliko informacij o svojih kupcih in o njihovih aktivnostih. Kako zelo ste oz. niste zaskrbljeni zaradi tega.

1. Sploh nisem zaskrbljen/a
2. Nisem zaskrbljen/a
3. Nisem niti nezaskrbljen/a niti zaskrbljen/a
4. Sem zaskrbljen/a
5. Sem zelo zaskrbljen/a

   - Zbiranje osebnih podatkov na javnem mestu (na cesti, vlaku, avtobusu, prireditvah itd.).
   - Zbiranje osebnih podatkov prek mobilnega telefona ali z uporabo aplikacij na mobilnih telefonih (poslušanje klicev, uporaba geo-lokacije itd.).
   - Zbiranje informacij preko ti. kartic zvestobe (personalizacija ponudbe, oglaševanje, analiza nakupnih vzorcev itd.).
   - Zbiranje informacij preko plačilnih kartic.
   - Zbiranje osebnih podatkov preko spleta (zgodovina, prenos datotek, dostop do vsebin na spletnih straneh itd.).

6. V kolikšni meri se strinjate s spodaj navedenimi trditvami, ki se navezujejo na pravice posameznika s področja varstva osebnih podatkov? Če se s trditvijo ne strinjate, izberite 1 - Sploh se ne strinjam. Bolj kot se s trditvijo strinjate, bolj izberite odgovor na desni strani. Če se s trditvijo zelo strinjate, izberite 5 - Popolnoma se strinjam.

1. Sploh se ne strinjam
2. Se ne strinjam
3. Se niti ne strinja, niti strinjam
4. Se strinjam
5. Popolnoma se strinjam

   - Podjetja bi morala bolje poskrbeti za varstvo osebnih podatkov.
   - Zavedam se, da podjetja upravljajo z mojimi osebnimi podatki.

- Bolj zaupam podjetjem, ki jasno komunicirajo, kako skrbijo za varstvo osebnih podatkov.
- Podjetju, ki jasno predstavijo moje pravice, lažje dovolim uporabo mojih osebnih podatkov.

7. Za konec bi vas prosil, da mi zaupate naslednje demografske podatke. Spol:

   - Moški
   - Ženska

8. V katero starostno skupino spadate

   - do 20 let
   - 21 – 40 let
   - 41 – 60 let
   - 61 let ali več

9. Vaša dokončana izobrazba

   - Osnovna šola ali manj
   - Nižja ali srednja poklicna izobrazba
   - Srednja strokovna izobrazba
   - Visoka strokovna izobrazba
   - Visoka univerzitetna izobrazba
   - Specialistična povišolska izobrazba, magisterij, doktorat

10. V kateri regiji prebivate?

    - Pomurska
    - Podravska
    - Koroška
    - Savinjska
    - Zasavska
    - Jugozahodna Slovenija
    - Osrednjeslovenska
    - Gorenjska
    - Notranjokraška
    - Goriška
    - Obalnokraška

11. Kakšen je vaš neto mesečni dohodek (brez prevoza in malice) v EUR:

    - do 500
    - od 501 do vključno 900
    - od 901 do vključno 1300
    - od 1301 do vključno 1700
    - od 1701 do vključno 2100
    - nad 2101

Priloga 2: analiza spletnih strani

Analiza spletnih strani mikro podjetij

Ars pharmae d.o.o oz. www.arspharmae.com

Piškotki 2018

Na spletni strani podjetja, z dne 7. 1. 2018, je takoj ob prihodu v levem kotu spodaj mogoče videti pasico, ki uporabnika sili v strinjanje z uporabo vseh piškotkov.

Piškotki 2019

Pri definiciji ni nobenih sprememb. Sporočilnost ostaja popolnoma enaka. Drugačen je zgolj zapis, ki sedaj deluje nekoliko bolj pregleden za uporabnika.

Prijava na spletne novice 2018

Dobrih 10 sekund po začetku brskanja po spletni strani se pojavi pojavno okno ti. pop up, ki uporabnika nagovarja k oddaji elektronske pošte v zameno za pridobivanje e-novic in nasvetov, ter kupon za 15% popust na vse izdelke. Pravno varnost zagotavljajo s pripisom: »*Spoštujemo vašo zasebnost. Zato vaših podatkov nikoli ne bomo posredovali nobeni tretji osebi*«.

Prijava na spletne novice 2019

V pojavnem oknu je jasno razbrati, da se novice pošiljajo enkrat do dvakrat tedensko. Dejstvo pa je, da jih pošiljajo vsakodnevno, zato bi bilo ta del potrebno dopolniti. Jasno je izraženo kaj je v teh sporočilih. Prejemanja sporočil ne pogojujejo z ničemer. V ti. drobnem tisku je jasno zapisano za katere dva namene se podatki zbirajo. Jasno je zapisano tudi kakšne so pravice posameznika in kako jih lahko uveljavi.

Pravno obvestilo 2018

V pravnem obvestilu podjetje ne zagotavlja točnosti in zanesljivosti objavljenih podatkov. Iz tega je težko razbrati katere podatke mislijo. Podjetje trdi, da bodo vsi pridobljeni osebni podatki uporabljeni izključno v namene, za katere so bili pridobljeni. S spletne strani je nemogoče razbrati, kateri so te osebi podatki. Podjetje trdi, da jih ne bodo posredovali nikomur brez posameznikove privolitve.

Posameznik se z uporabo spletnega mesta, strinja s temi pogoji.

Pravno obvestilo 2019

V pravnem obvestilu, z vidika varstva osebnih podatkov, ni nobenih sprememb.

Velcom d.o.o oz. www.cityport.si

Piškotki

Podjetje piškotkov na spletni strani ne uporablja.

Kontakt 2018

Obvezna je oddaja imena, priimka in elektronske pošte. Nikjer na spletni strani ni zaznano kaj se s temi podatki zgodi, ko jih oseba odda.

Kontakt 2019

Opaziti ni nobenih sprememb.

Pravno obvestilo 2018

Na spletni strani ni mogoče najti pravnega obvestila.

Pravno obvestilo 2019
Opaziti ni nobenih sprememb.

Analiza spletnih strani malih podjetij

FrodX d.o.o oz. www.frodx.com
Piškotki 2018
Na spletni strani podjetja, z dne 1. 1. 2018, je takoj ob prihodu spodaj mogoče videti pasico, ki uporabnika sili v strinjanje z uporabo vseh piškotkov. Klik na več o piškotkih, pa uporabnika pripelje na podstran, ki ga izobrazi o piškotkih. Kaj so piškotki, za kaj se uporabljajo, skladno s katero zakonodajo se jih uporablja (ZEK-om1).
Piškotki 2019
Pri definiciji ni nobenih sprememb. Sporočilnost ostaja popolnoma enaka.

Prenos priročnika 2018
Po nekaj klikih na spletni strani se pojavi pojavno okno, ki uporabnika nagovarja k oddaji elektronske pošte v zameno za pridobivanje e-novic in nasvetov. Podjetje trdi, da pravno varnost zagotavljajo skladno z ZVOP-1.

Prenos priročnika 2019
V pojavnem oknu je jasno razbrati, da se novice pošiljajo enkrat tedensko. Jasno je izraženo kaj je v teh sporočilih. Prejemanja sporočil ne pogojujejo z ničemer. V ti. drobnem tisku je jasno zapisano za katere dva namene se podatki zbirajo. Jasno je zapisano tudi kakšne so pravice posameznika in kako jih lahko uveljavi. Za prejemanje sporočil je potrebna oddaja zgolj elektronske pošte v nadaljnjih korakih, ob prenosih priročnika pa tudi ime, priimek, podjetje in telefonska številka.

Pravno obvestilo 2018
Podjetje trdi, da bo osebne podatke uporabljajo izključno za seminarje/dogodke in obvestila povezana izključno z dejavnostjo podjetja. Podatke pa bodo varovali v skladu z ZVOP-1.

Pravno obvestilo 2019
Od pregledanih podjetij je podjetje FrodX d.o.o je v letu dni zelo dobro dodelalo pravno obvestilo. Pravno obvestilo oz. politika varstva osebnih podatkov, kot jo imenujejo, je sestavljena iz uvodnih pojasnil, podatkih o upravljalcu, DPO-ju, osebnih podatki, ki se jih zbira, uporabnikih, času hrambe, skrbjo za varnost, pravicami posameznika, postopkom uveljavljanja pravic, pravico do vložitve pritožbe in veljavnostjo politike.

Ceneje d.o.o oz. www.ceneje.si
Piškotki 2018
Na spletni strani podjetja, z dne 24. 2. 2018, je takoj ob prihodu desno spodaj mogoče videti pasico, ki uporabnika sili v strinjanje z uporabo vseh piškotkov. Klik na podrobnosti o piškotkih, pa uporabnika pripelje na podstran, ki mu pove kaj so piškotki in zakaj se uporabljajo. Zelo podrobno, tudi slikovno, so predstavljeni piškotki, ki jih podjetje uporablja.

Piškotki 2019
Pri definiciji ni nobenih sprememb. Sporočilnost ostaja popolnoma enaka.

Prijava na spletne novice 2018

Na prvi strani spodaj se nahaja pojavno okno, ki od uporabnika zahteva elektronski naslov, v zameno za prejemanje spletnih novic. Jasno je opredeljeno kakšne te novice so in kaj uporabnik dobi v zameno. Prijavi se lahko na tri različne oblike novic. Nameni obdelave in načini hrambe pa so opredeljeni v pravnem obvestilu.

Prenos priročnika 2019
Ni bilo zaznati nobenih sprememb.

Pravno obvestilo 2018
Jasno je zapisano katere osebne podatke podjetje hrani. Zelo podrobno so opredeljeni nameni obdelave. Prav tako je jasno, tudi slikovno, predstavljeno vsako orodje, ki ga podjetje uporablja za namen obdelave osebnih podatkov. Jasno so predstavljene pravice posameznika in kako jih posameznik lahko uveljavlja.

Pravno obvestilo 2019
Zaznati ni nobenih bistvenih sprememb.

Analiza spletnih strani srednje velikih podjetij

Euro plus d.o.o oz. www.nicelabel.com
Piškotki 2018
Na spletni strani podjetja, z dne 14. 1. 2018, je takoj ob na vrhu mogoče videti pasico, ki uporabnika sili v strinjanje z uporabo vseh piškotkov. Pasico lahko zgolj zapreš s klikom na gumb X. Na podstrani Privacy policy je mogoče prebrati nekaj več splošnega o piškotkih.

Piškotki 2019
Ob prihodu se pasica neopazno skriva levo spodaj. Uporabnik lahko sliko v obliki palete odpre in upravlja z različnimi piškotki. Definicija je sedaj razširjena in uporabniku omogoča, da se sam odloči kdaj bo uporabil katere piškotke. Podjetje se poslužuje uporabe opt-out načina.

Prenos priročnika 2018
V zameno za prenos priročnika, mora uporabnik pustiti ime, priimek, naziv podjetje, elektronski naslov, telefon in industrijo podjetja. Strinjati se mora z splošnimi pogoji, ki niso opredeljeni.

Prenos priročnika 2019
Ni bilo zaznati nobenih sprememb. Ni zaznati delovanju v želji po približevanju GDPRju.

Pravno obvestilo 2018
Pravno obvestilo je zapisano zelo splošno. Podjetje piše o podatkih katere mogoče zbira mogoče pa tudi ne. Podjetje ne želi sprejeti nobene odgovornosti v primeru vdora v sistem.

Pravno obvestilo 2019
Pravno obvestilo je sedaj precej razširjeno in dodelano. Opisano je katere podatke podjetje zbira, namen, varnost podatkov, prenos podatkov, pravice posameznika, kako uveljavljati pravice.

Fibran d.o.o oz. www.fibran.si

Piškotki 2018
Na spletni strani podjetja, z dne 11. 1. 2018, je spodaj mogoče videti pasico, ki uporabnika sili v strinjanje z uporabo vseh piškotkov. S klikom na gumb več informacij, pa je mogoče prebrati več splošnega o piškotkih.

Piškotki 2019
Ni bilo zaznanih nobenih sprememb.

Kontakt 2018
Za kontakt je potrebno deliti ime, priimek in elektronsko pošto. Nikjer ni zaznati kaj se s temi podatki zgodi kasneje.
Kontakt 2019
Ni bilo zaznati nobenih sprememb.

Pravno obvestilo 2018
Pravnega obvestila ni bilo zaznati na spletni strani.
Pravno obvestilo 2019
Pravno obvestilo je sedaj mogoče najti, sicer skrito nekje na spletni strani. Pravno obvestilo je razdeljeno na dva dokumenta: nameni obdelave osebnih podatkov, ki precej razširjeno in dodelano opiše kako in zakaj se podatki hranijo, ter pravice posameznika, kjer je razloženo kaj so in kako jih je mogoče uveljavljati.

DIH Technology oz. www.hocoma.com
Piškotki 2018
Na spletni strani podjetja, z dne 4. 1. 2018, ni mogoče razbrati, da podjetje uporablja piškotke.

Piškotki 2019
Takoj ob prihodu na spletno stran se spodaj pojavi pasica, ki uporabnika obvešča, da spletna stran uporablja piškotke. Piškotke je mogoče tudi spremeniti glede na način uporabe spletne strani.

Prijava na spletne novice 2018
Za prijavo je potrebno deliti ime, priimek, elektronsko pošto, namen uporabe (zaseben, posloven), jezik in državo. Nikjer ni zaznati kaj se s temi podatki zgodi kasneje. Strinjati se moraš s prijavo v posebnem okencu, to pa potrdiš še z prijavo na gumb *subscribe*.

Prijava na spletne novice 2019
Podjetje sedaj zahteva zgolj ime, priimek, državo in elektronski naslov. Jasno je zapisano zakaj so te podatki potrebni. Če uporabnika zanima več, lahko to preveri na izbrani podstrani.

Pravno obvestilo 2018
Pravno obvestilo je obsežno, vendar v njemu ni mogoče razbrati ničesar o varstvu osebnih podatkov.

Pravno obvestilo 2019
Ko uporabnik zapre pasico z obvestilom o uporabi piškotkov, se pojavi nova, ki pravi, da ima podjetje sedaj urejeno varstvo osebnih podatkov. Jasno je razloženo katere podatke zbirajo o obiskovalcih, na kakšen način, kako jih uporabljajo, kako jih varujejo. Nikjer ni jasno zapisano kakšne so pravice posameznika

Analiza spletnih strani velikih podjetij

Adriatic slovenica d. d.

Piškotki 2018

Na spletni strani podjetja, z dne 24. 2. 2018 je spodaj pasica, ki uporabnika obvešča o uporabi piškotkov. Na podstrani tukaj, je jasno in pregledno razbrati katere piškotke uporabljajo in za kateri namen.

Piškotki 2019

Takoj ob prihodu na spletno stran se spodaj pojavi pasica, ki uporabnika obvešča, da spletna stran uporablja piškotke. Piškotke je mogoče tudi spremeniti glede na način uporabe spletne strani.

Kontakt 2018

Za kontakt svetovalca je potrebno deliti ime, priimek, elektronsko pošto, mobilno številko, naslov. Nikjer ni zaznati kaj se s temi podatki zgodi kasneje.

Kontakt 2019

Podjetje je dodalo okence, kjer mora uporabnik svoje strinjanje jasno potrditi z gumbom dajem izrecno privolitev. V primeru, da posameznika zanima s čim se strinja, to lahko prebere s pritiskom na podstran preberite vsebino privolitve.

Pravno obvestilo 2018

Podjetje trdi, da so osebni podatki posameznika namenjeni za uporabo zgolj njihovega podjetja in, da jih varujejo skladno z ZVOP-1 in Zakonom o zavarovalništvu.

Pravno obvestilo 2019

Dodana je bila nova podstran: varstvo osebnih podatkov. Jasno je razloženo katere podatke zbirajo o obiskovalcih, na kakšen način, kako jih uporabljajo, kako jih varujejo. Jasno je zapisano kaj so pravice posameznika in kako jih lahko uveljavlja.

Iskratel d.o.o

Piškotki 2018

Na spletni strani podjetja, z dne 29. 12. 2017, se takoj ob prihodu na spletno stran spodaj pojavi pasica, ki uporabnika obvešča, da spletna stran uporablja piškotke. Z klikom na gumb, je na podstrani mogoče razbrati več o piškotkih.

Piškotki 2019

Ni bilo zaznati nobenih sprememb.

Prijava na spletne novice 2018

Za prijavo je potrebno deliti elektronsko pošto. Nikjer ni zaznati kaj se s temi podatki zgodi kasneje.

Prijava na spletne novice 2019

Prijava na spletne novice je bila umaknjena s spletne strani. Razlog je lahko v strateški odločitvi podjetja, lahko pa je v tem, da ne želi hraniti osebnih podatkov, če to ni nujno potrebno.

Pravno obvestilo 2018

Pravnega obvestila ni mogoče najti na spletni strani.

Pravno obvestilo 2019
Zaznanih ni bilo nobenih sprememb.

Petrol d.d.
Piškotki 2018
Na spletni strani podjetja, z dne 4. 1. 2018, je desno spodaj jasno predstavljeno, da podjetje uporablja piškotke. Je edino izmed analiziranih podjetij, ki omogoča anonimnost.

Piškotki 2019
Takoj ob prihodu na spletno stran se spodaj pojavi pasica, ki uporabnika obvešča, da spletna stran uporablja piškotke. Piškotke je mogoče tudi spremeniti glede na način uporabe spletne strani.

Prijava na spletne novice 2018
Za prijavo je potrebno deliti elektronsko pošto. Nikjer ni zaznati kaj se s temi podatki zgodi kasneje.

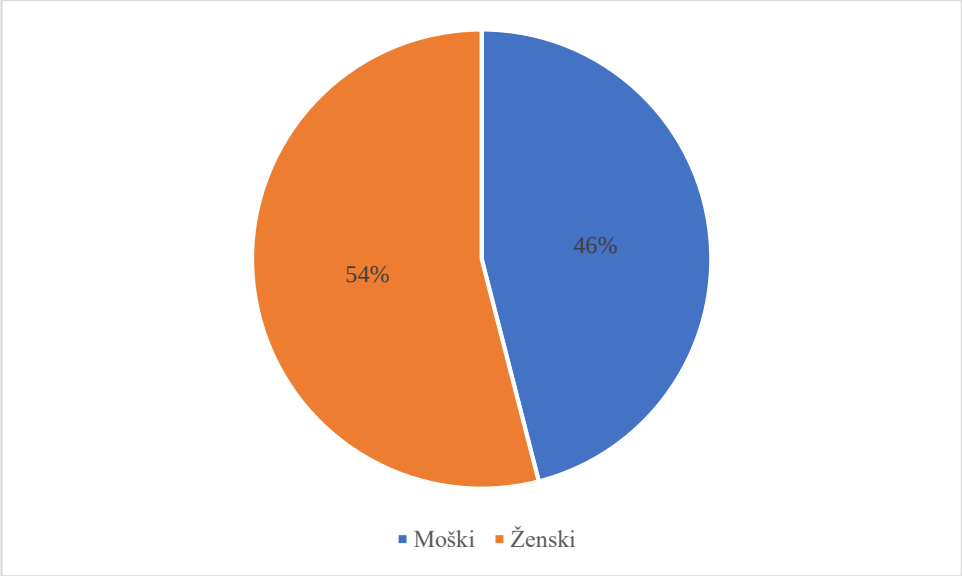
Prijava na spletne novice 2019
Prijava na spletne novice je sedaj urejena preko aplikacije Moj Petrol. To podjetju omogoča večji nadzor. Prijavo pogojujejo z registracijo v spletno aplikacijo. Odjava od spletnih novic pa je omogočena že na tej podstrani in je bolj enostavna kot sama prijava.

Pravno obvestilo 2018
Pravno obvestilo je zelo obsežno. Zaradi obsežnosti tudi precej nepregledno. Lastnika osebnih podatkov kljub temu opozori na namen zbiranja, hrambo, varnost in pravice.

Pravno obvestilo 2019
Ko uporabnik zapre pasico z obvestilom o uporabi piškotkov, se pojavi nova, ki pravi, da ima podjetje sedaj urejeno varstvo osebnih podatkov. Jasno je razloženo katere podatke zbirajo o obiskovalcih, na kakšen način, kako jih uporabljajo, kako jih varujejo. Nikjer ni jasno zapisano kakšne so pravice posameznika.

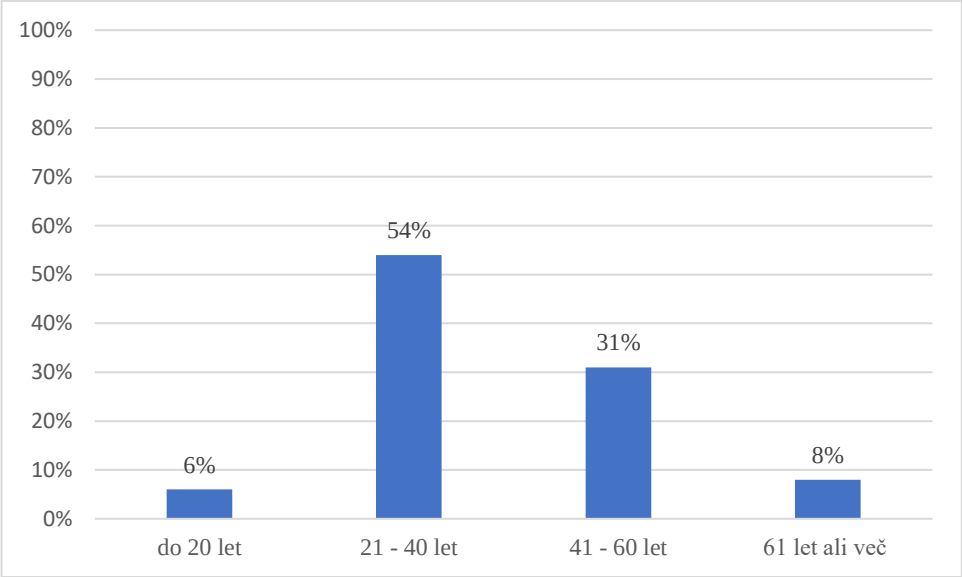
Priloga 3: rezultati ankete

Graf 1: Spol anketirancev



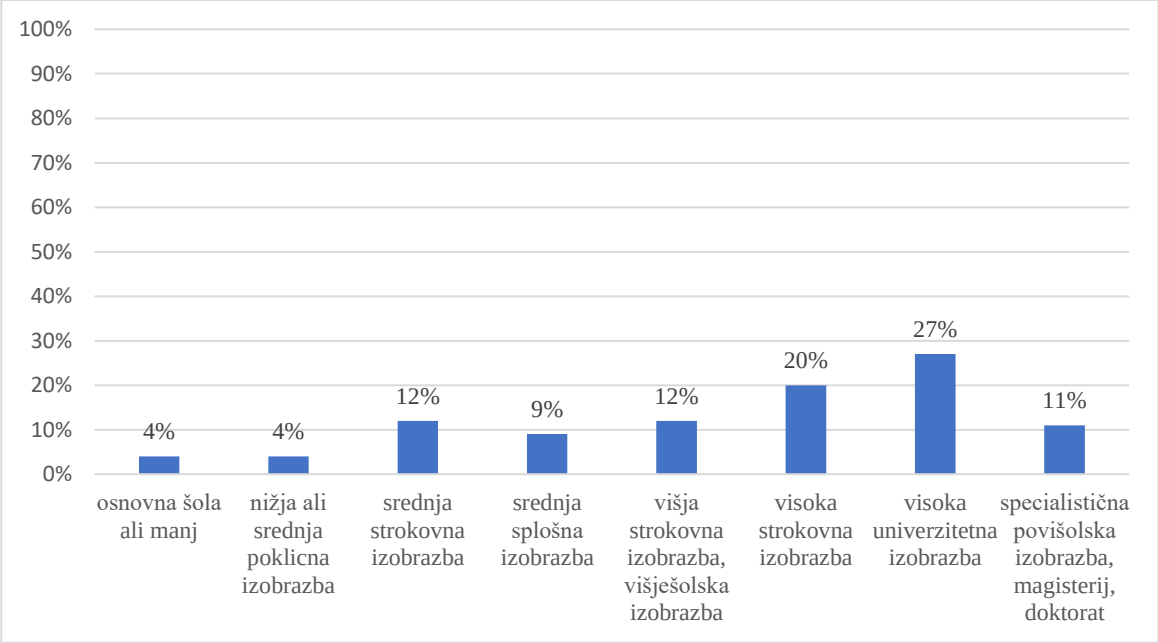
Vir: lastno delo.

Graf 2: Starostna skupina anketirancev



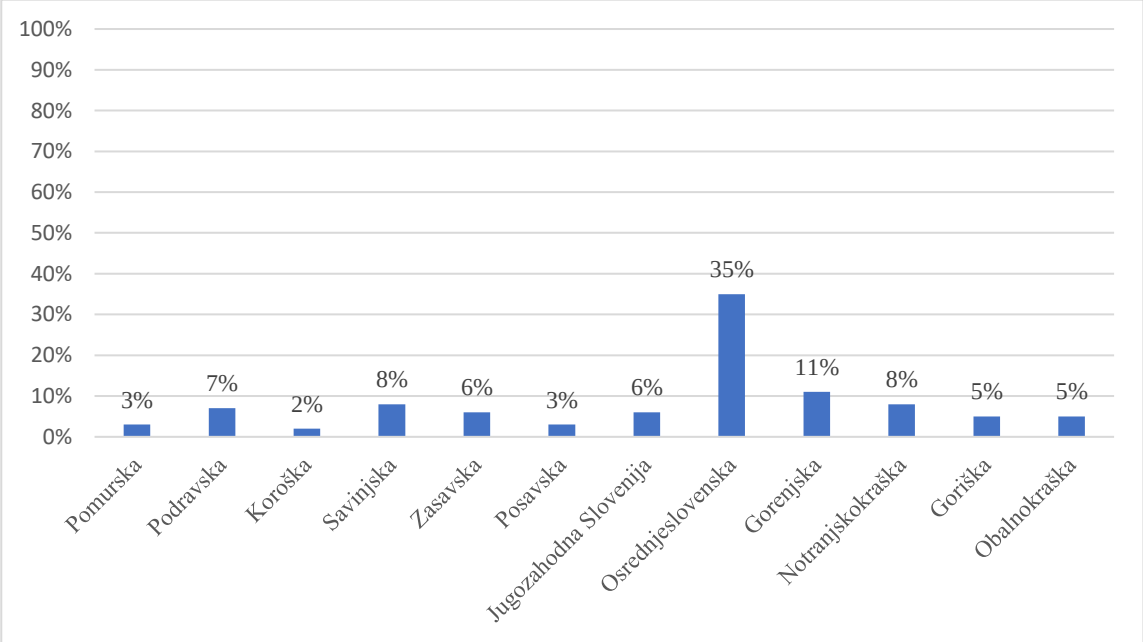
Vir: lastno delo.

Graf 3: Izobrazba anketirancev



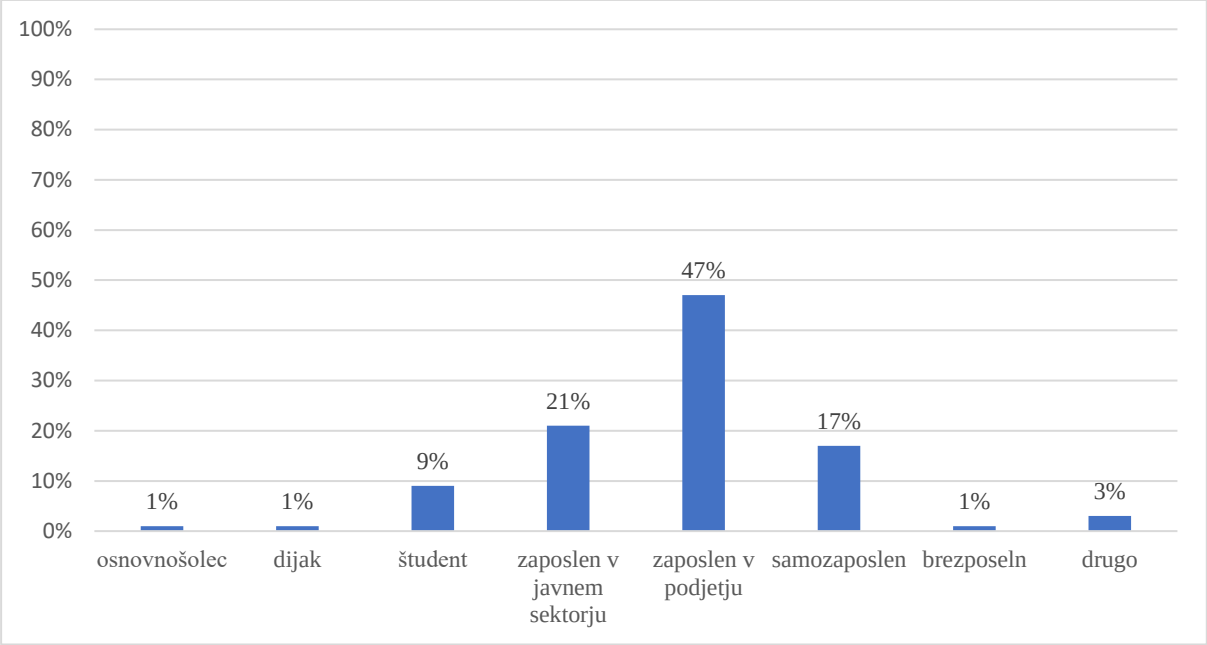
Vir: lastno delo.

Graf 4: Regija bivanja anketirancev



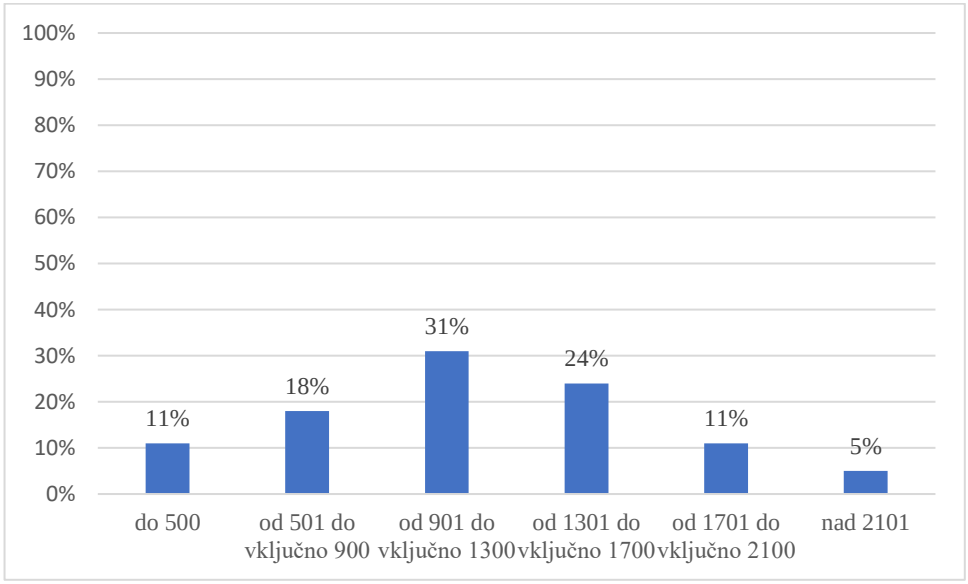
Vir: lastno delo.

Graf 5: Zaposlitveni status anketirancev



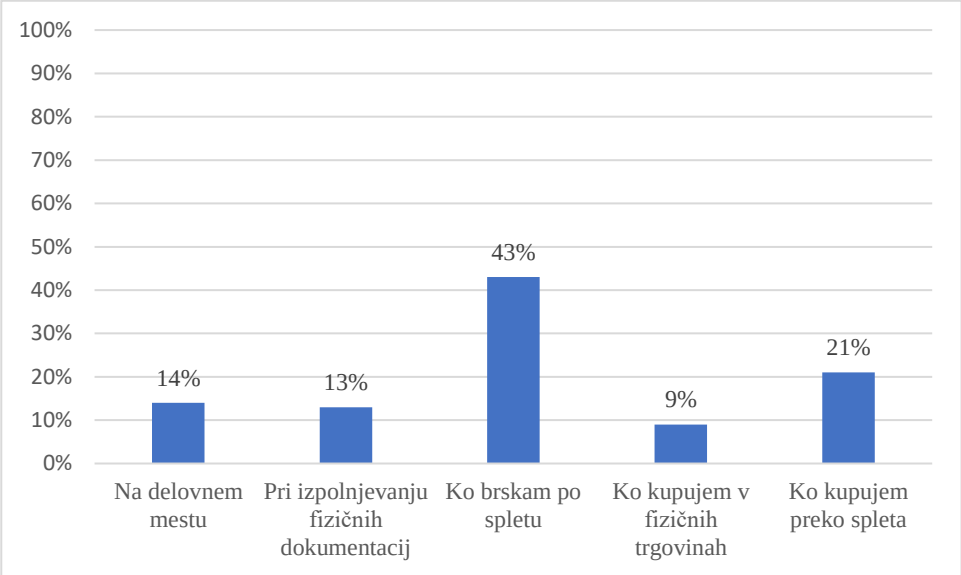
Vir: lastno delo.

Graf 6: Neto mesečni dohodek anketirancev



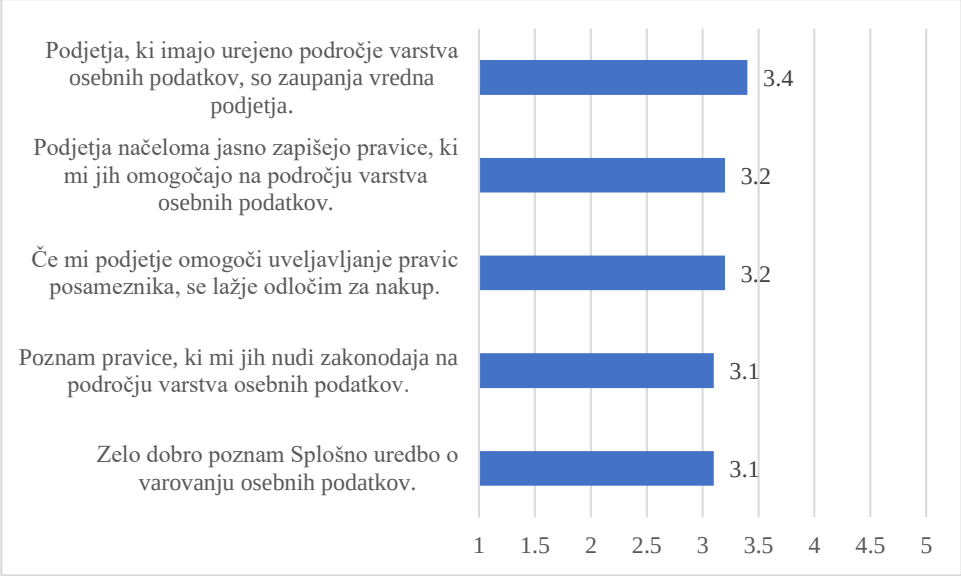
Vir: lastno delo.

Graf 7: Najpogostejše srečanje z vprašanjem ali s privolitvijo v obdelavo osebnih podatkov



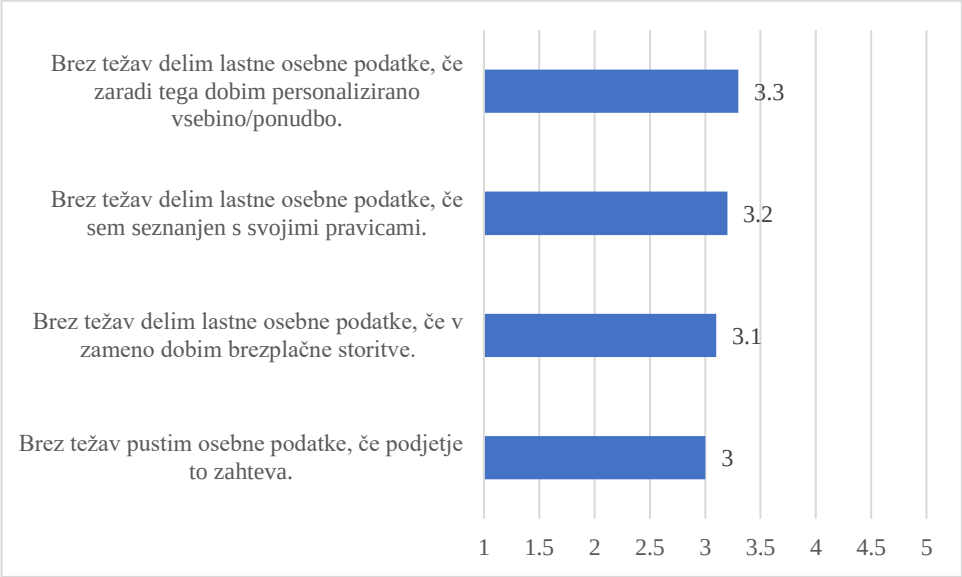
Vir: lastno delo.

Graf 8: Povprečne vrednosti za trditve, ki se navezujejo na pravice posameznika s področja varstva osebnih podatkov



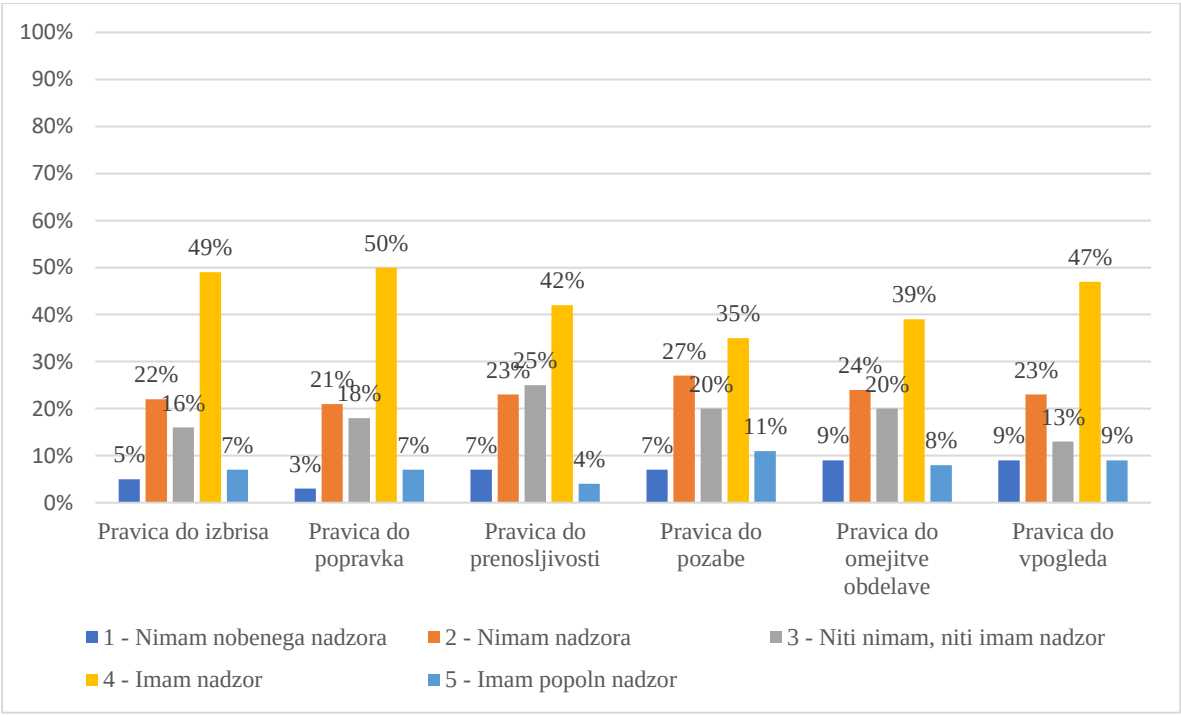
Vir: lastno delo.

Graf 9: Povprečne vrednosti za strinjanje anketirancev s trditvami, ki se navezujejo na personalizacijo vsebine



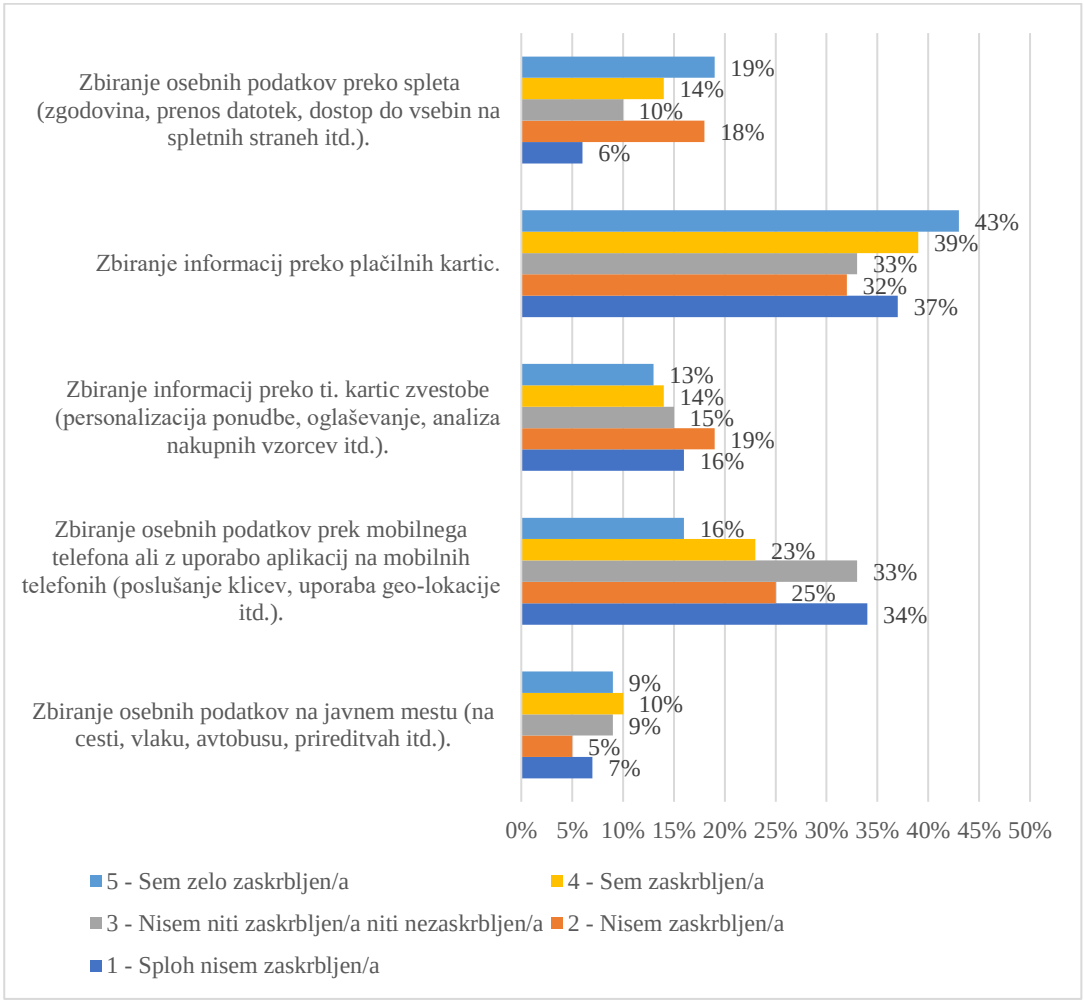
Vir: lastno delo.

Graf 10: Ocenjevanje anketirancev, koliko nadzora imajo nad uveljavljanjem naštetih pravic v zvezi z obdelavo osebnih podatkov



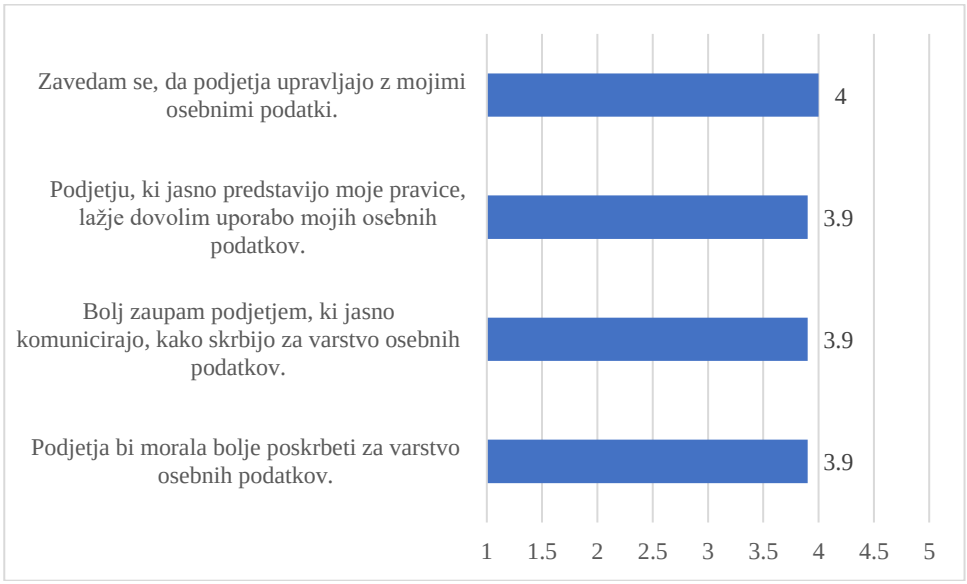
Vir: lastno delo.

Graf 11:Zaskrbljenost anketirancev zaradi tega, ker podjetja zbirajo informacije o svojih kupcih in njihovih aktivnostih

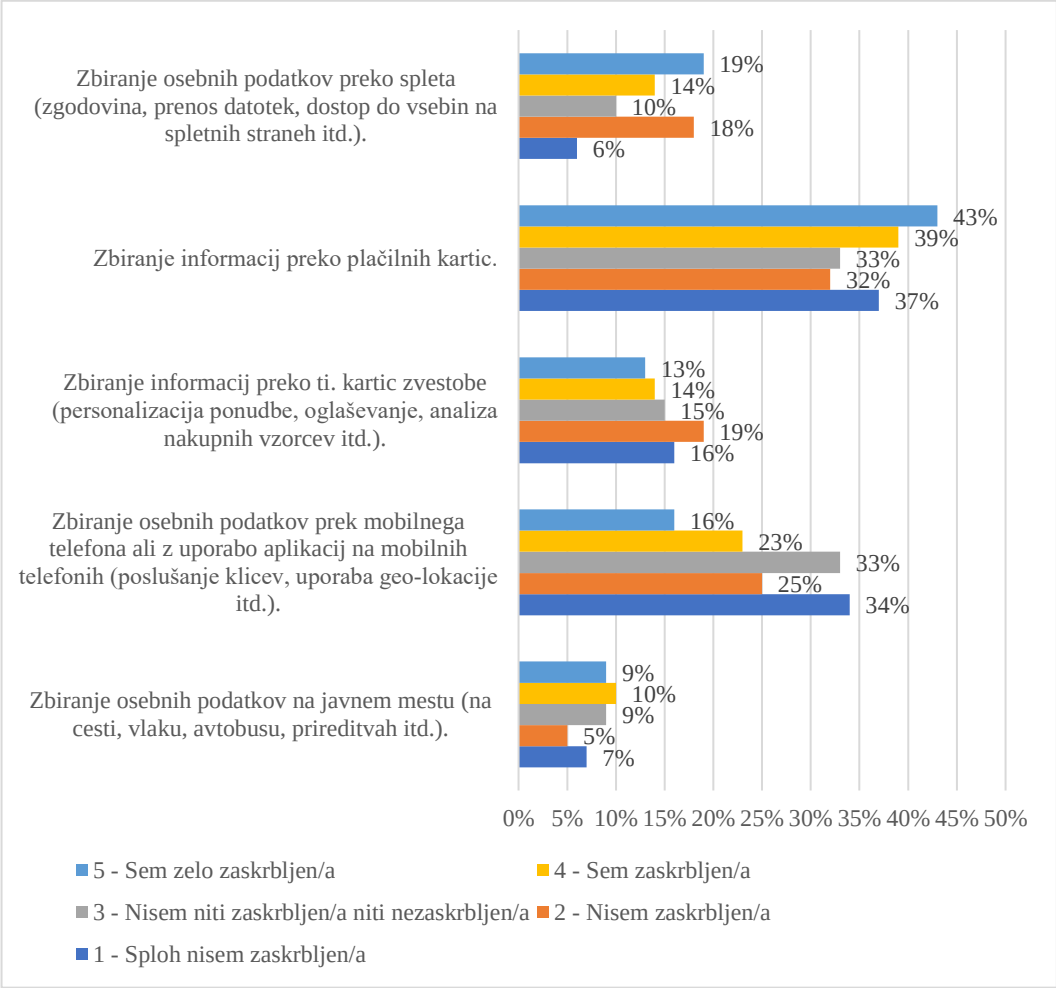


Vir: lastno delo.

Graf 12: Strinjanje anketirancev s trditvami, ki se navezujejo na varstvo osebnih podatkov



Graf 13: Zaskrbljenost anketirancev zaradi tega, ker podjetja zbirajo informacije o svojih kupcih in njihovih aktivnostih



Vir: lastno delo.