

UNIVERZA V LJUBLJANI
EKONOMSKA FAKULTETA

MAGISTRSKO DELO

TANJA ŠUŠTAR

UNIVERZA V LJUBLJANI
EKONOMSKA FAKULTETA

MAGISTRSKO DELO
**ZAGOTAVLJANJE VARSTVA OSEBNIH PODATKOV V OBLAKU
PRI REVIDIRANJU**

Ljubljana, november 2015

TANJA ŠUŠTAR

IZJAVA O AVTORSTVU

Spodaj podpisana Tanja Šuštar, študentka Ekonomske fakultete Univerze v Ljubljani, izjavljam, da sem avtorica magistrskega dela z naslovom Zagotavljanje varstva osebnih podatkov v oblaku pri revidiranju, pripravljenega v sodelovanju s svetovalko doc. dr. Meto Duhovnik.

Izrecno izjavljam, da v skladu z določili Zakona o avtorskih in sorodnih pravicah (Ur. l. RS, št. 21/1995 s spremembami) dovolim objavo magistrskega dela na fakultetnih spletnih straneh.

S svojim podpisom zagotavljam, da:

- je predloženo besedilo rezultat izključno mojega lastnega raziskovalnega dela;
- je predloženo besedilo jezikovno korektno in tehnično pripravljeno v skladu z Navodili za izdelavo zaključnih nalog Ekonomske fakultete Univerze v Ljubljani, kar pomeni, da sem:
 - poskrbela, da so dela in mnenja drugih avtorjev oziroma avtoric, ki jih uporabljam v magistrskem delu, citirana oziroma navedena v skladu z Navodili za izdelavo zaključnih nalog Ekonomske fakultete Univerze v Ljubljani, in
 - pridobila vsa dovoljenja za uporabo avtorskih del, ki so v celoti (v pisni ali grafični obliki) uporabljena v besedilu, in sem to v njem tudi jasno zapisala;
- se zavedam, da je plagiatorstvo–predstavljanje tujih del (v pisni ali grafični obliki) kot mojih lastnih–kaznivo po Kazenskem zakoniku (Ur. l. RS, št. 55/2008 s spremembami);
- se zavedam posledic, ki bi jih na osnovi predložene zaključne strokovne naloge/diplomskega dela/specialističnega dela/magistrskega dela/doktorske disertacije dokazano plagiatorstvo lahko predstavljalo za moj status na Ekonomski fakulteti Univerze v Ljubljani v skladu z relevantnim pravilnikom.

V Ljubljani, dne 20. 11. 2015

Podpis avtorice: _____

KAZALO

UVOD	1
1 RAČUNALNIŠTVO V OBLAKU.....	2
1.1 Opredelitev računalništva v oblaku	2
1.2 Vrste računalništva v oblaku.....	5
1.2.1 Zasebni oblak	6
1.2.2 Javni oblak.....	7
1.2.3 Mešani (hibridni) oblak.....	8
1.2.4 Ostali modeli	8
1.3 Prednosti in slabosti računalništva v oblaku.....	9
1.3.1 Prednosti.....	9
1.3.2 Slabosti	10
2 VARSTVO OSEBNIH PODATKOV	11
2.1 Osební podatki	11
2.2 Direktiva Evropskega parlamenta in Sveta 95/46/ES.....	12
2.3 ZVOP-1.....	13
2.3.1 Splošne določbe.....	14
2.3.2 Obdelava osebnih podatkov	15
2.3.3 Institucionalno varstvo osebnih podatkov.....	16
2.3.4 Iznos osebnih podatkov	18
2.4 Smernice glede varovanja osebnih podatkov.....	19
2.4.1 Obdelava osebnih podatkov – splošno	21
2.4.2 Pogodbena obdelava osebnih podatkov	21
2.4.3 Informacijska varnost (zavarovanje osebnih podatkov) – skladnost in revizija .	22
2.4.4 Pravice posameznika	24
2.4.5 Iznos osebnih podatkov v tretje države	24
2.5 Primerjava slovenske zakonodaje z drugimi DČ	26
2.5.1 Obdelava osebnih podatkov	26
2.5.2 Pravice posameznikov.....	35
2.5.3 Institucionalno varstvo osebnih podatkov.....	38
2.5.4 Iznos osebnih podatkov (tretje države) in ozemeljska veljavnost.....	42
2.5.5 Zaključek.....	45
3 RAZISKAVA VARNOSTI OSEBNIH PODATKOV V OBLAKU	47

3.1 Anketiranje slovenskih uporabnikov storitev v oblaku (podjetij in revizijskih družb)	48
3.1.1 Način izbora anketnih vprašanj	48
3.1.2 Anketna vprašanja za podjetja in revizijske družbe	48
3.2 Predstavitev rezultatov anketiranja slovenskih uporabnikov storitev v oblaku	49
3.2.1 Predstavitev rezultatov anketiranja podjetij	49
3.2.3 Skladnost rezultatov anketiranja z zakonskimi zahtevami	63
3.3 Primerjava rezultatov anketiranja z mednarodno raziskavo revizijske mreže KPMG	64
3.3.1 Podobnosti in razlike	64
3.3.2 Sklepne ugotovitve	66
SKLEP	66
LITERATURA IN VIRI	68

Priloga

KAZALO SLIK

Slika 1: Modeli računalništva v oblaku	4
Slika 2: Modeli računalništva v oblaku	6
Slika 3: Struktura revizijskih družb, ki uporabljajo/ne uporabljajo storitve RO v %	49
Slika 4: Struktura ostalih podjetij, ki uporabljajo/ne uporabljajo storitve RO v %	50
Slika 5: Vzroki ne uporabe storitev RO med revizijskimi družbami v %	51
Slika 6: Vzroki ne uporabe storitev RO med ostalimi podjetji v %	51
Slika 7: Ključni cilji, na katerih temelji odnos revizijskih družb do storitev RO v %	52
Slika 8: Ključni cilji, na katerih temelji odnos ostalih podjetij do storitev RO v %	52
Slika 9: Mnenje revizijskih družb glede učinkovitosti in prihrankov RO v %	53
Slika 10: Mnenje ostalih podjetij glede učinkovitosti in prihrankov RO v %	53
Slika 11: Ključni izzivi pri sprejetju RO za revizijske družbe	54
Slika 12: Ključni izzivi pri sprejetju RO za ostala podjetja	54
Slika 13: Prikaz usposobljenosti revizijskih družb pri premagovanju izzivov	55
Slika 14: Prikaz usposobljenosti ostalih podjetij pri premagovanju izzivov	56
Slika 15: Zahtevnost poslovnih področij za revizijske družbe	57
Slika 16: Zahtevnost poslovnih področij za revizijske družbe	58
Slika 17: Prikaz področij poslovanja, kjer revizijske družbe že/še ne uporabljajo RO	59
Slika 18: Prikaz področij poslovanja, kjer ostala podjetja že/še ne uporabljajo RO	60
Slika 19: Področja poslovanja, ki jih bodo revizijske družbe prenesle v oblak	61
Slika 20: Področja poslovanja, ki jih bodo ostala podjetja prenesla v oblak	61
Slika 21: Struktura revizijskih družb, ki imajo osebne podatke zavarovane na način, ki je opredeljen v 24. členu ZVOP-1, v %	62

Slika 22: Struktura ostalih podjetij, ki imajo osebne podatke zavarovane na način, ki je opredeljen v 24. členu ZVOP-1, v %	63
---	----

KAZALO TABEL

Tabela 1: Značilnosti storitev v oblaku	4
Tabela 2: Prednosti in slabosti zasebnega oblaka.....	7
Tabela 3: Prednosti in slabosti javnega oblaka.....	8
Tabela 4: Prednosti in slabosti hibridnega oblaka	8
Tabela 5: Prednosti in slabosti RO	10
Tabela 6: Kontrolni seznam za preverjanje skladnosti 1–3.....	21
Tabela 7: Kontrolni seznam za preverjanje skladnosti 4–8.....	22
Tabela 8: Kontrolni seznam za preverjanje skladnosti 9–15.....	23
Tabela 9: Kontrolni seznam za preverjanje skladnosti 16.....	24
Tabela 10: Kontrolni seznam za preverjanje skladnosti 17–18.....	24

UVOD

Razvoj informacijske tehnologije prinaša spremembe na vseh področjih. Tudi koncept računalniške infrastrukture v podjetjih se spreminja. V zadnjem času se vse pogosteje uporablja izraz računalništvo v oblaku. Enotne opredelitve, kaj naj bi pomenilo računalništvo v oblaku, še ni. Nekateri avtorji pa celo menijo, da gre za staro tehnologijo z novim imenom (Knuth, 2009).

Tudi gospodarske razmere v zadnjih letih so pripomogle k temu, da se je računalništvo v oblaku močno razvilo. Mala in srednje velika podjetja, ki nimajo lastne računalniške infrastrukture, jo raje najamejo. Namesto da bi aplikacije, storitve in infrastrukturo poganjali na lastnem krajevnem računalniku, njihovo uporabo najamejo na strežnikih, ki sestavljajo računalniški oblak (Avram, 2014).

Oblak ponuja večjo mobilnost uporabniku, ta ima dostop do programske opreme kjerkoli in kadarkoli, le da ima dostop do interneta (Chou, 2015).

Problem, do katerega prihaja pri računalništvu v oblaku je, da se v oblak seli vse večja obdelava osebnih podatkov. Vprašanje pa je, kako dobro so ti podatki varovani. Pri tem moramo paziti, da so osebni podatki zavarovani in varovani. Gre za dva različna pojma, oba pa sta za računalništvo v oblaku pomembna. Zavarovanje osebnih podatkov (angl. *data security*) je eden od ukrepov, s katerim se ščiti celovitost, zaupnost in razpoložljivost podatkov. Varstvo osebnih podatkov (angl. *data protection*) pa je precej širši pojem. Podatki so lahko odlično »zaklenjeni«, a kljub temu lahko pride do kršitve varstva osebnih podatkov, ker morda ni pravne podlage za njihovo obdelavo, mogoče se jih uporablja nezakonito, predolgo hrani ipd. Pri računalništvu v oblaku lahko zanašanje zgolj na tehnične metode izboljša varnost podatkov, vendar se s tem ne more izogniti zakonodaji na področju varstva osebnih podatkov (Tomšič, 2011). Magistrsko delo bo obravnavalo izzive, povezane z varstvom osebnih podatkov, s posebnim poudarkom njihovega pomena za podjetja, med njimi pa zlasti za revizijske družbe, ki že uporabljajo ali nameravajo uporabljati računalništvo v oblaku.

Računalništvo v oblaku omogoča dostopnost do računalniških zmogljivosti na ekonomičen in prilagodljiv način kjer koli in kadar koli. Vse te prednosti, ki jih prinaša računalništvo v oblaku, pa ne smejo biti izgovor za nižanje ravni varstva osebnih podatkov.

Namen magistrskega dela je, da na osnovi spoznanj v strokovni literaturi, pravne ureditve varstva osebnih podatkov in lastne raziskave ugotovim, ali slovenska podjetja, med njimi pa zlasti revizijske družbe, zagotavljajo ustrezno varstvo osebnih podatkov v oblaku.

Hipoteza, ki jo bom poskušala potrditi je, da je obdelava osebnih podatkov v oblaku varna. Postavljeno hipotezo bom preverila z anketnim vprašalnikom. Anketirala bom slovenske revizijske družbe in ostala podjetja, ki uporabljajo storitve računalništva v oblaku.

Magistrska naloga bo poleg uvoda, sklepa in literature ter virov sestavljena iz treh delov. V prvem delu bom predstavila pojem računalništvo v oblaku, vrste računalništva v oblaku ter njegove prednosti in slabosti. V drugem delu bom predstavila področje varstva osebnih podatkov. Opredelila bom, kaj je osebni podatek in kateri pravni viri obravnavajo to področje. Predstavila bom Direktivo Evropskega parlamenta in Sveta 95/46/ES in slovenski Zakon o varstvu osebnih podatkov (v nadaljevanju ZVOP-1). V nadaljevanju naloge bom predstavila še Smernice, ki jih je informacijski pooblaščenec pripravil skupaj s Cloud Security Alliance (CSA) Slovenia Chapter, Slovenskim odsekom Information Systems Audit and Control Association (v nadaljevanju ISACA) in Zavodom e-Oblak, Eurocloud Slovenia. Glavni del drugega dela magistrske naloge je predstavitev in primerjava evropske zakonodaje glede varstva osebnih podatkov s slovenskim ZVOP-1. V tretjem delu bom s pomočjo anketnega vprašalnika poskušala potrditi postavljeno hipotezo. Rezultate lastne raziskave bom pred zaključnim delom primerjala z rezultati mednarodne raziskave revizijske mreže KPMG.

1 RAČUNALNIŠTVO V OBLAKU

V prvem poglavju bom na kratko predstavila, kaj sploh pomeni pojem računalništvo v oblaku, kakšne vrste računalništva v oblaku poznamo in kakšne prednosti oz. slabosti prinaša omenjeno računalništvo. V nadaljevanju magistrske naloge bom za računalništvo v oblaku uporabljala kratico RO.

1.1 Opredelitev računalništva v oblaku

RO je nova paradigma gostovanja in zagotavljanja storitev preko interneta. Predstavlja zbliževanje dveh glavnih trendov na področju informacijske tehnologije, to je (a) učinkovitost IT, pri čemer je moč sodobnih računalnikov bolj učinkovito uporabljena z visoko razširljivo strojno in programsko opremo, ter (b) poslovne spretnosti, ki jih je mogoče uporabiti kot konkurenčno orodje (Avram, 2014).

RO je vrsta vzporednega in porazdeljenega sistema, ki sestoji iz zbirke med seboj povezanih in virtualiziranih računalnikov, z dinamično oskrbo in združevanjem enega ali več virov, ki temeljijo na ravni sporazumov med uporabniki in ponudniki storitev (Buyya, Yeo, Venugopal, Broberg, & Brandic, 2009).

Center za RO (Center for Cloud Computing, 2015) na svoji spletni strani navaja, da je RO slog računalništva, ki zagotavlja razširjene virtualizirane računalniške vire kot storitev preko internetne povezave.

National Institute of Standard and Technology (Mell & Grance, 2011) opredeljuje RO kot model, ki omogoča dostop do skupnega prostora nastavljenih računalniških virov (npr. omrežje, strežniki, aplikacije, storitve) prek internetne povezave, kjerkoli s hitrim dostopom in ga je mogoče upravljati z minimalnim naporom.

Plummer (2009), ki povzema definicijo družbe Gartner, pravi, da je RO slog računalništva, kjer so prilagodljive IT-zmogljivosti s pomočjo internetne tehnologije dostopne več odjemalcem oz. strankam.

Rouse (2010) pravi, da je RO splošni izraz za vse gostujoče storitve preko interneta. Oblak je razdeljen na tri ravni storitev, in sicer na infrastrukturo storitev, platformo storitev ter programsko opremo kot storitev.

Informacijski pooblaščenec (2012) pa RO opredeljuje kot vzorec uporabe informacijske tehnologije, ki za zmogljivo programsko opremo ne zahteva velikih investicij. Do aplikacij in storitev se dostopa prek omrežja, za kar je potreben le internet. Dostop je možen z uporabo klasičnega odjemalca, kjer koli in kadar koli, brez potrebe po posebni programski opremi. RO omogoča takojšen dostop do prednastavljenih skupnih informacijskih virov, ki jih ponuja ponudnik (npr. omrežja, strojno opremo, pomnilniške enote, programsko opremo, različne informacijske storitve).

Bistvena lastnost RO je, da uporabnik preko spletnega brskalnika orodja uporablja tako, kot bi jih uporabljal, če bi imel ta orodja nameščena na lastni računalniški postaji (Furuncu & Sogukpinar, 2015). Pri tem moramo razumeti, da RO ni izdelek ali tehnologija niti ni standard, ampak je metoda za zagotovitev fleksibilnih, skupnih IT-storitev (Höllwarth, 2012).

Enotne opredelitve RO ni, čeprav model v svojem bistvu niti ni tako nov. Združuje namreč že znane koncepte skupinskega in porazdeljenega računalništva z modelom plačevanja po porabi. Kot primer lahko vzamemo elektronsko pošto Gmail. Ta deluje v oblaku, česar se mnogi sploh ne zavedajo, v uporabi pa je že zelo dolgo (Pohorec, 2011).

Na spletu je mogoče najti različne definicije različnih avtorjev. Vsem definicijam pa je skupno to, da gre za ponujanje različnih računalniških storitev, ki delujejo s pomočjo omrežja in so za ponudnika hitro dostopne ter poceni.

Höllwarth (2012, str. 36) v svoji knjigi navaja 6 značilnosti, ki naj bi bile značilne za storitev v oblaku:

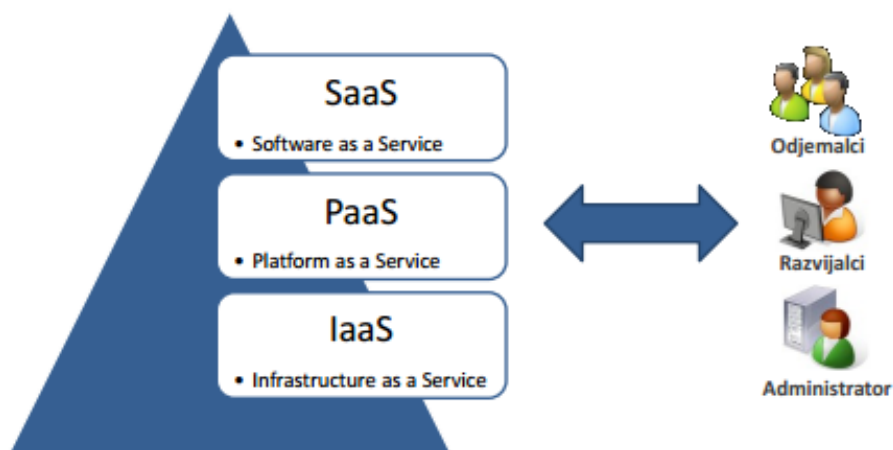
Tabela 1: Značilnosti storitev v oblaku

Značilnosti	Uporabnik
VIRTUALNI VIRI	Izvajanje storitev uporabniku fizično ni vidno. Izvajalec lahko zato storitve optimizira glede na standardizacije in učinkovitosti.
SPOSOBNOST BITI STRANKA	Viri so namenjeni več uporabnikom, za vsakega uporabnika posebej se uporabljajo mehanizmi za zaščito in izolacijo.
PLAČILO NA OSNOVI PORABE	Uporabnik plača le toliko in za tisto, kar dejansko uporablja.
UPORABNIK IMA NADZOR NAD UPORABO	Vire si uporabnik naroči sam in jih nato tudi uporablja brez posredovanja ponudnika storitev.
ELASTIČNOST	Uporabnik si lahko storitve hitro prilagodi glede na svoje potrebe (občutek neomejenosti virov).
PROGRAMSKI NADZOR	Uporabnik si vire nastavi, upravlja in uporablja s pomočjo vmesnikov za programiranje. Uporabniku je tako omogočen dinamičen način uporabe aplikacije.

Vir: T. Höllwarth, Pot v oblak, 2012, str. 36.

Običajno pri RO govorimo o treh že omenjenih storitvenih modelih oz. plasteh, ki so razdeljene hierarhično, kar je vidno na Sliki 1. Storitveni modeli so prikazani v obliki piramide, ker se ti modeli gradijo eden na drugem in so zato med sabo delno povezani.

Slika 1: Modeli računalništva v oblaku



Vir: Gemini, Modeli računalništva v oblaku, 2015.

- **Infrastruktura kot storitev (angl. »Infrastructure as a Service–IaaS«)**

Najosnovnejša oblika RO je infrastruktura v oblaku. Infrastruktura kot storitev ponuja virtualizirane strojne vire (procesor, pomnilnik, diskovni prostor, omrežje) ali najem virtualizirane strežniške infrastrukture, uporabe operacijskega sistema in programskih rešitev (Bešter, 2011). Uporabniki infrastrukture kot storitve so sistemski administratorji. Primer virtualiziranega vira je Amazon Simple Storage Service (S3), ki predstavlja enotno naslovljiv diskovni prostor z navidezno neskončno kapaciteto. Analogni komercialni primer strežniške virtualizacije je Amazon Elastic Compute Cloud (EC2), na katerem je mogoče poganjati lastne slike operacijskega sistema (Sedlar, Bešter & Kos, 2011). Ta model je privlačen, ker omogoča uporabo in avtomatizacijo standardiziranih storitev (Höllwarth, 2012).

- **Platforma kot storitev (angl. »Platform as a Service–PaaS«)**

Platforma kot storitev posreduje določeno platformo, ki omogoča delovanje programske opreme. Uporabnik najame platformo, na kateri uporablja programske rešitve, platforma skrije infrastrukturo in uporabniku ni vidna. Nudi možnost za razvoj aplikacij, vendar pa je ta odvisna od infrastrukture, za katero skrbi nekdo drug (Bešter, 2011). Uporabniki platforme kot storitve so razvijalci. Primer platforme kot storitve predstavlja Google App Engine, ki razvijalcem nudi dinamično in prilagodljivo platformo, ki poganja aplikacijo. Ko razvijalec napiše aplikacijo, jo naloži v oblak in s tem je njegovo delo končano, saj mu pri tem ni potrebno skrbeti za prilagodljivost in upravljanje infrastrukture (Sedlar, et al., 2011).

- **Programska oprema kot storitev (angl. »Software as a Service–SaaS «)**

Programska oprema kot storitev pomeni zagotavljanje celotne infrastrukture skupaj s programsko opremo in nastavitvami za njeno delovanje. Ker ni potrebno ničesar posebej namestiti, lahko uporabnik dostopa do storitev kjer koli, če le ima dostop do interneta. SaaS zagotavlja funkcije za končnega uporabnika. V to kategorijo sodijo poslovne aplikacije ali programska oprema kot storitev (SaaS). Vidnejši ponudniki so salesforce.com, Microsoft (npr. Office 365), Google Apps (vključno z Gmail), CRM (angl. *Customer Relationship Management*) (Furuncu & Sogukpinar, 2015). Primer programske opreme kot storitve predstavlja spletna pošta, kjer se uporabnik prijavi s svojim računom, potem pa mu strežnik postreže podatke, ki se lahko nahajajo na povsem različnih platformah ter na povsem geografsko in logično porazdeljeni infrastrukturi (Sedlar, et al., 2011).

1.2 Vrste računalništva v oblaku

Uporabnik virov in ponudnik virov sta dva glavna udeleženca, ki nastopata pri RO. Ponudnik virov ponuja informacijske vire, uporabnik pa na te vire prenaša svoje sisteme, podatke ali aplikacije. Glede na ponudnike in uporabnike virov poznamo različne modele RO.

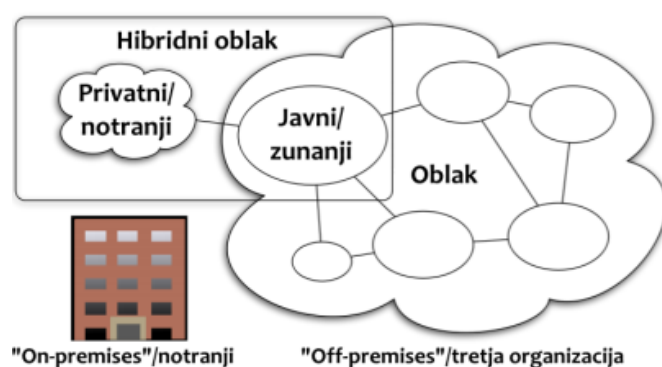
Poznamo tri osnovne modele, to so (Bervar, 2013):

- zasebni model–privatni oblak (angl. *private cloud*);
- javni model–javni oblak (angl. *public cloud*);
- mešani (hibridni) model – hibridni oblak (angl. *hybrid cloud*).

Ostali modeli:

- vertikalni oblak oz. oblak skupnosti (angl. *community cloud*);
- posredovanje do ponudnikov računalništva v oblaku (angl. *cloud brokering*).

Slika 2: Modeli računalništva v oblaku



Vir: Gemini, Modeli računalništva v oblaku, 2015.

1.2.1 Zasebni oblak

Za zasebni oblak je značilno, da je dostopen samo v zasebnem omrežju (npr. znotraj intraneta podjetja) in je primeren za velika podjetja. Infrastruktura oblaka je zagotovljena znotraj podjetja, do storitev dostopajo notranji uporabniki (npr. poslovne enote). Storitve, infrastruktura in upravljanje so lahko pod nadzorom podjetja ali tretje osebe ali kombinacija obeh (Mell & Grance, 2011).

Storitve so dostopne preko interneta ali preko navideznih zasebnih omrežij. Zasebni oblak je primeren za organizacijo, ki želi imeti svoj oblak (Gemini, 2015).

Podjetje se odloči za lasten, zasebni oblak zaradi strateških, operativnih ali kulturnih razlogov. Popolno funkcionalen oblak je oblak, ki je v lasti in upravljanju podjetja. Zasebni oblaki pa so lahko povezani tudi z javnimi oblaki (Höllwarth, 2012). Z njimi je mogoče izkoristiti številne prednosti npr. samopostrežbo storitev, razširljivost in elastičnost, dodaten nadzor ter možnost prilagajanja itd. (Gemini, 2015). Poseben primer je navidezno zaseben oblak, ki ga upravlja ponudnik. Ponudnik v podjetju vzpostavi oblak, kar spada pod zunanje izvajanje storitev (angl. *outsourcing*), podjetje pa je še vedno nosilec IT-

infrastrukture (Marks & Lozano, 2010). Podjetje ima tako nadzor nad tem, kdo, kako in kdaj sme uporabljati storitve iz te infrastrukture (Höllwarth, 2012).

Tabela 2: Prednosti in slabosti zasebnega oblaka

Prednosti	Slabosti
– zasebni oblak omogoča individualne prilagoditve – zasebni oblak bolj varen kot javni oblak	– vnaprej plačanih stroškov investicije pri tem modelu ni možno spremeniti v stroške izvedbe, ker podjetje vnaprej nabavi in sestavi komponente za zasebni oblak, tega pa kasneje ni mogoče nadgraditi

Vir: T. Höllwarth, Pot v oblak, 2012, str. 41.

1.2.2 Javni oblak

Javni oblak se pogosto omenja tudi samo kot oblak. Dostopen je javnosti in ni omejitev glede njegove uporabe. Gre za storitve, ki jih ponuja trg (Höllwarth, 2012). Javni oblak imajo v lasti in ga upravljajo poslovne, akademske in vladne organizacije ali kombinacija navedenega. Ponudnik storitev v oblaku je lastnik infrastrukture (Mell & Grance, 2011).

Do storitev lahko dostopa vsak, ki ima uporabniško ime (primer Gmail). Storitve Gmaila si uporabniki delijo, to pomeni, da imajo dokumente in pošto na istih strežnikih, pa tega niti ne vedo (Gemini, 2015). Uporabnik tako nima nobenega vpliva (ne tehnično ne pogodbeno) na to, kdo vse še uporablja storitev ponudnika. To je tudi glavna značilnost, po kateri prepoznamo javni oblak (Höllwarth, 2012).

Prvi oblaki, ki so se razvili, so bili javni oblaki, npr. Google, Amazon in Salesforce. (Marks & Lozano, 2010).

Ponudniki javnih oblakov pa morajo pri tem ves čas paziti, da je tak oblak tehnično popolno izvršen in varen. Prav varnost je tukaj ključna, saj uporabniki storitev v teh oblakih shranjujejo dokumente in podatke, ki ne smejo biti vidni ostalim uporabnikom. Zagotovljeno mora biti varovanje teh podatkov (Zakrajšek, 2011).

Tabela 3: Prednosti in slabosti javnega oblaka

Prednosti	Slabosti
- plačilo na osnovi uporabe - ni potrebno vlagati v lastno IT (prihranek) - mobilnost (dostop je možen kjerkoli, ne glede na lokacijo)	- pomisleki glede skladnosti, varnosti, dostopnosti, zmogljivosti

Vir: T. Höllwarth, Pot v oblak, 2012, str. 40.

1.2.3 Mešani (hibridni) oblak

Hibridni oblak je kombinacija zgoraj dveh navedenih oblakov (javnega in zasebnega oblaka). Ta vrsta oblaka je nekako najbolj stabilna in zanesljiva (Marks & Lozano, 2010).

Podjetje, ki se odloči za to vrsto oblaka, svoje procese razdeli tako, da del teh procesov gosti v zasebnem oblaku, del pa v javnem oblaku. Tako so občutljivi deli (občutljivi podatki) pod nadzorom podjetja, za manj občutljivo področje pa poskrbi ponudnik storitev v oblaku. S tega vidika je poskrbljeno za varnost podatkov, poleg tega pa lahko podjetje, ki se odloči za to vrsto oblaka, izkorišča prednosti javnega oblaka (Gemini, 2015).

Tabela 4: Prednosti in slabosti hibridnega oblaka

Prednosti	Slabosti
- elastičnost, dinamičnost (ponuja kombinacijo fleksibilnosti javnega oblaka in zanesljivosti zasebnega oblaka)	- zapletenost - uporabnik v zasebnem okolju lahko uporablja več različnih storitev z različnimi uporabniški imeni in gesli, v poslovnem okolju pa lahko uporablja samo eno identiteto

Vir: T. Höllwarth, Pot v oblak, 2012, str. 43.

1.2.4 Ostali modeli

Nekateri avtorji poleg javnega, zasebnega in hibridnega oblaka navajajo tudi vertikalni oblak oz. oblak skupnosti. Gre za obliko javnega oblaka, ki ga uporablja določena skupina uporabnikov, ki imajo skupne interese (npr. poslanstvo, varnostne zahteve, politika in pomisleki o skladnosti). Uporabniki so npr. skupine podjetij, ki med seboj sodelujejo oz. tekmujejo in se oblikujejo v poseben vertikalni trg, kot so npr. finančne storitve (Marks & Lozano, 2010). Za oblak skupnosti je značilno, da je dostopen le omejenemu številu uporabnikov (Gemini, 2015).

V primeru, da podjetju v zasebnem oblaku primanjkuje virov in te vire nadomesti, tako, da enakovredno uporablja vire javnega oblaka, govorimo o razširjanju v javni oblak (angl. *cloudbursting*). Javni oblak je nekakšna rezervna kapaciteta, ki jo ima podjetje na voljo (Gemini, 2015).

Obstaja pa tudi model posredovanja do ponudnikov računalništva v oblaku (angl. *cloud brokering*). Gre za to, da posrednik glede na trenutne potrebe in razmere posreduje storitve najprimernejšega ponudnika storitev v oblaku (Gemini, 2015).

1.3 Prednosti in slabosti računalništva v oblaku

1.3.1 Prednosti

Ponudniki storitev RO nudijo udoben, preprost dostop do storitev, za katere uporabnik plača le toliko, kolikor jih uporablja (angl. *pay per use*). Uporabniku ni potrebno vlagati v strojno in programsko opremo, niti mu ni potrebno najeti IT-osebja, ki bi skrbelo za to opremo. Prednost prehoda v oblak je razširljivost in prilagodljivost IT, ki jo ponuja ponudnik. V primeru povečanja obsega dela uporabnik RO izkorišča prožnost oblaka, saj mu ni potrebno kupovati dodatne opreme, ker plača glede na uporabo storitev v oblaku. Naslednja prednost, ki jo ponuja oblak, je možnost večje mobilnosti uporabnika, ta ima dostop do programske opreme kjer koli in kadar koli, če le ima dostop do interneta (Chou, 2015).

Prednost RO je tudi v virtualizaciji virov, integraciji podatkov in shranjevanju podatkov. RO zmanjšuje stroške in omejitve glede avtomatizacije ter uvedbe računalniškega sistema in stroške vzdrževanja. Razvojne ekipe so namreč usmerjene v reševanje strokovne problematike, za tehnično infrastrukturo pa jim ni potrebno skrbeti, ker zanje skrbi ponudnik storitev RO (Hashem, Yaqoob, Anuar, Mokhtar, Gani & Khan, 2015).

RO je priložnost predvsem za manjša podjetja in za mnoge uporabnike iz držav tretjega sveta, ki so na področju IT manj razviti. Imajo namreč nizke začetne stroške (ni potrebe po vlaganju v strežniške sobe, strežnike, programsko opremo, usposabljanje za to opremo itd.). Do virov strojne opreme lahko dostopajo takoj, brez vnaprejšnjih kapitalskih naložb, kar jim omogoča hitrejši vstop na trg in hitrejši razvoj. Oblak ponuja prilagodljivo infrastrukturo, ki jo lahko uporabljajo različni končni uporabniki na različne načine (Avram, 2014).

1.3.2 Slabosti

Področja tveganja, ki jih predstavlja RO, so varnost in zasebnost podatkov, verodostojnost, povezava z notranjim sistemom, razpoložljivost sistema, kontinuiteta poslovanja, lastništvo ter druge zakonske zahteve. Med omenjenimi področji je najbolj tvegano področje varnost in zasebnost podatkov. Podjetje (uporabnik) podatkov nima shranjenih v svojih prostorih, ampak pri ponudniku storitev v oblaku (Chou, 2015). RO je popolnoma odvisno od razpoložljivosti dostopa do omrežja (internetne povezave) in njegove hitrosti dostopa. Težavo predstavljajo tudi okvare, izpad in druge motnje, ki onemogočajo dostop do aplikacij v oblaku (Avram, 2014).

V tabeli 5 so povzete prej navedene prednosti in slabosti RO:

Tabela 5: Prednosti in slabosti RO

Prednosti	Slabosti
- nizki stroški pri nakupu opreme in nadaljnjem vzdrževanju	- varnost in zasebnost podatkov je vprašljiva
- veliko število potencialnih uporabnikov	- možnost izgube podatkov
- večja mobilnost in fleksibilnost	- potreba po hitrem in stalnem dostopu do interneta
- mala podjetja imajo dostop do sistemov visoke kakovosti	- občutljivost interneta (npr. motnje, kibernetični napadi)
- preprosto, prilagodljivo in pregledno povezovanje različnih tehničnih elementov	- tveganja, povezana s selitvijo in obdelavo podatkov v druge države, ki imajo drugačne predpise
- dostop kjerkoli in kadarkoli, na različnih prenosnih napravah	- obveznosti in pravice uporabnikov/ponudnikov RO so še vedno nejasne
- neomejena kapaciteta hrambe podatkov	
- takojšnje in redne posodobitve programske opreme	

RO prinaša številne prednosti, zaradi katerih se bo vse več uporabnikov (podjetij) odločalo za RO. Privlačno je že zaradi tega, ker je možno storitve RO uporabljati od koder koli, kadar koli in s katere koli naprave. Poleg tega uporaba prinaša podjetjem ogromne prihranke. V prihodnosti je pričakovati, da bo ponudnikov in uporabnikov storitev RO vse več. Pri tem pa bo potrebno zelo veliko pozornosti nameniti področju varovanja podatkov.

2 VARSTVO OSEBNIH PODATKOV

V tem poglavju bom opredelila, kaj je osebni podatek. Na kratko bom predstavila Zakon o varstvu osebnih podatkov (Ur. l. RS, št. 86/2004-UPB1, 67/2007, v nadaljevanju ZVOP-1), ki ga bom v nadaljevanju primerjala z zakoni izbranih evropskih držav. Predstavila bom smernice glede varstva osebnih podatkov pri računalništvu v oblaku, ki jih je informacijski pooblaščenec pripravil v sodelovanju s Cloud Security Alliance (CSA) Slovenia Chapter, Slovenskim odsekom ISACA ter Zavodom e-Oblak, Eurocloud Slovenia. Predstavila pa bom tudi Direktivo 95/46/ES Evropskega parlamenta in Sveta (Direktiva o varstvu podatkov, v nadaljevanju Direktiva) in usklajenost ZVOP-1 z Direktivo.

2.1 Osebni podatki

Ministrstvo za notranje zadeve (2015) opredeljuje osebni podatek kot kateri koli podatek, ki se nanaša na določeno ali določljivo fizično osebo, torej posameznika, ne glede na obliko, v kateri je izražen.

»Določljiva fizična oseba je oseba, ki se jo lahko neposredno ali posredno identificira s pomočjo njenih identifikacijskih števil (npr. EMŠO, davčna številka, številka zdravstvenega zavarovanja, telefonska številka, registrska številka vozila) ali s sklicevanjem na dejavnike, ki so značilni za njeno fizično, fiziološko, duševno, ekonomsko, kulturno ali družbeno identiteto (npr. zaposlitev, naslov, funkcijo, položaj ali status v določenem subjektu, ipd.)« (Informacijski pooblaščenec, 2015).

Osebni podatki se lahko obdelujejo le v primeru, če tako določa zakon oz. če posameznik sam privoli v to. Namen obdelave podatkov mora biti določen z zakonom oz. če se podatki obdelujejo na podlagi privolitve posameznika, mora le-ta biti o namenu predhodno obveščen (Informacijski pooblaščenec, 2015).

Pri nas področje varstva osebnih podatkov ureja ZVOP-1. Zakon je potreben za doseganje ravnotežja med pravico do zasebnosti in legitimnimi razlogi za uporabo osebnih podatkov. Zakonodaja mora posamezniku nuditi varstvo in pravice, hkrati pa omogočati uporabo osebnih podatkov tistim subjektom, ki so do tega upravičeni (Informacijski pooblaščenec, 2006). Podlago za to zagotavlja Ustava Republike Slovenije v 38. členu: »Zagotovljeno je 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. Vsakdo se ima pravico seznaniti z zbranimi osebnimi podatki, ki se nanašajo nanj, in pravico do sodnega varstva ob njihovi zlorabi« (Ustava Republike Slovenije, Ur. l. RS št. 33/91-I, 42/97, 66/2000, 24/03, 69/04, 68/06, 47/13).

2.2 Direktiva Evropskega parlamenta in Sveta 95/46/ES

Evropski parlament in Svet EU sta leta 1995 sprejela Direktivo 95/46/ES o varstvu posameznikov pri obdelavi osebnih podatkov ter o prostem pretoku takih podatkov (Direktiva 95/46/ES, 2015). Direktiva zagotavlja ravnovesje med varstvom zasebnosti posameznika in prostim pretokom osebnih podatkov v EU. Določa stroge meje pri zbiranju in obdelavi osebnih podatkov, zahteva pa tudi, da vsaka država članica vzpostavi neodvisni državni organ za varstvo osebnih podatkov (Europa, 2011).

Namen Direktive je:

- Varovati temeljne pravice in svoboščine fizičnih oseb in predvsem njihovo pravico do zasebnosti pri obdelavi osebnih podatkov.
- Države članice (v nadaljevanju DČ) ne omejujejo in ne prepovedujejo prostega prenosa osebnih podatkov med DČ zaradi varstva teh podatkov.

Direktiva je zakonodajni akt z določenim ciljem, ki ga morajo doseči države članice EU, kako bodo ta cilj dosegle, pa je prepuščeno njim (Europa, 2015).

Direktiva je kot sekundarni pravni akt sestavljena iz dveh delov. Prvi del je pojasnjevalni del, ki ga sestavlja 72 točk. Drugi del je normativen, sestavljen je iz sedmih poglavij in 34 členov.

Prvo poglavje opredeljuje splošne določbe. Vključen je namen Direktive, opredeljeni so vsi pomembni pojmi, ki jih vsebuje Direktiva, in področje, kjer se ta direktiva uporablja, ter uporaba nacionalnega prava.

Sledi drugo poglavje, ki je tudi najobsežnejše in je razdeljeno na devet oddelkov. Na podlagi določb drugega poglavja DČ podrobneje določijo pogoje, pod katerimi je obdelava osebnih podatkov zakonita. Drugo poglavje opredeljuje načela v zvezi s kakovostjo podatkov, ki jih najdemo tudi v našem nacionalnem zakonu ZVOP-1, in sicer v prvem splošnem delu. Sledi oddelek, kjer so opredeljena merila za zakonito obdelavo podatkov. Kadar gre za posebno vrsto podatkov, ki kažejo na rasni ali etični izvor, ali da gre za politična mnenja, verska ali filozofska prepričanja, pripadnost sindikatu ali pa za podatke v zvezi z zdravjem ali spolnim življenjem, se obdelava teh podatkov prepove. Četrty oddelek govori o posredovanju informacij posameznikom, na katere se osebni podatki nanašajo. DČ morajo v svoji zakonodaji določiti, katere informacije mora upravljavec ali njegov predstavnik posredovati posamezniku v primeru, ko se podatki zbirajo od posameznika ali ko podatki niso pridobljeni od posameznika, na katerega se osebni podatki nanašajo. Vsak posameznik mora imeti pravico dostopati do podatkov (Direktiva, 12. člen). DČ pa lahko pravice v zvezi z objavo postopka obdelave (Direktiva, 21. člen), pravico do dostopa (Direktiva, 12. člen), do informacij (Direktiva, 11. in 10. člen) in izpolnitve načel (Direktiva, 6. člen) omeji. To lahko stori, kadar gre za zaščito državne varnosti, obrambe, javne varnosti, preprečevanja, preiskovanja, odkrivanja in pregona kaznivih dejanj,

gospodarskega ali finančnega interesa DČ ali EU ali kadar gre za zaščito posameznika. DČ priznavajo posamezniku, da lahko v določenih primerih ugovarja obdelavi osebnih podatkov. Obdelava osebnih podatkov mora biti zaupna, podatkov se ne sme obdelovati brez navodil upravljavca, razen če tako določa zakon. Poskrbljeno mora biti za tehnične in organizacijske ukrepe za zavarovanje osebnih podatkov.

Tretje poglavje obravnava pravna sredstva, odgovornost in sankcije. Nacionalna zakonodaja DČ mora posamezniku zagotoviti, da ima vsaka oseba v primeru kršitve pravic pravico vložiti pravno sredstvo na sodišču. Oškodovana oseba ima pravico zahtevati odškodnino za škodo od upravljavca, če je zanj odgovoren. Vsaka DČ mora v svoji nacionalni zakonodaji določiti sankcije, ki se naložijo v primeru kršitve določb, določenih v Direktivi.

Četrto poglavje obravnava prenos podatkov v tretje države (v države, ki niso v EU). V tem delu so opredeljena načela in odstopanja glede prenosa podatkov. Direktiva določa, da se DČ in Komisija EU obveščata v primeru, da katera od tretjih držav ne zagotavlja ustreznega varstva osebnih podatkov.

V petem poglavju DČ in Komisija spodbujajo k pripravi kodeksov ravnanja, ki naj bi spodbujali k pravilnemu izvajanju nacionalne zakonodaje. Šesto poglavje določa, da mora vsaka DČ določiti enega ali več javnih organov, ki bodo odgovorni za spremljanje uporabe predpisov, ki so jih sprejele in so v skladu s to direktivo. Ti nadzorni organi so pri izvajanju nalog popolnoma samostojni. Poleg nadzornih organov pa se ustanovi še delovna skupina za varstvo posameznikov pri obdelavi osebnih podatkov. Delovna skupina ima svetovalni status in prav tako deluje samostojno. Nadzorni organi delujejo na nacionalni ravni, delovne skupine pa na nivoju Evropske unije.

Direktiva v sedmem poglavju predvideva še ustanovitev odbora, ki ga sestavljajo predstavniki DČ, predseduje pa mu predstavnik Komisije. Njegova naloga je spremljanje izvajanja Direktive v posamezni DČ. Na koncu končne določbe določajo, da morajo DČ sprejeti zakone in druge predpise za uskladitev z Direktivo, najpozneje v treh letih. Komisija je zavezana poročati Svetu in Evropskemu parlamentu o izvajanju Direktive. Zadnji, 34. člen določa, da je Direktiva naslovljena na vse DČ.

2.3 ZVOP-1

Prvi zakon o varovanju osebnih podatkov v Republiki Sloveniji je bil sprejet leta 1990, v veljavo pa je vstopil leta 1992. V vmesnem obdobju je bilo nekaj dopolnitev tega zakona. Leta 1999 je bil sprejet nov Zakon o varstvu osebnih podatkov ZVOP-A, leta 2001 pa še njegova novela (Informacijski pooblaščenec, 2006). Namen novele je bil uskladitev zakona z določbami konvencije Sveta Evrope in določbami Direktive Evropske unije. Z vstopom v Evropsko unijo je morala Slovenija Zakon o varstvu osebnih podatkov prilagoditi določbam Direktive. Prenovljeni zakon je Državni zbor RS sprejel 15. 7. 2004, veljati pa je

prišel 1. 1. 2005 (Krašovec, Bogataj, Duralija, Jerše, Kalan, Šumah, Kraigher, Pavšič, & Tomšič, 2013). To je po letu 1990 tretji zakon, ki ureja varstvo osebnih podatkov (Čebulj & Žurej, 2005).

Julija 2007 je bila sprejeta novela Zakona o varstvu osebnih podatkov, ZVOP-1A, ki je uvedla dve novosti na področju dostopa posameznikov do njihovih osebnih podatkov, in s tem administrativno ter finančno razbremenila upravljavce osebnih podatkov (Krašovec, et al., 2013). ZVOP-1 je še vedno veljaven zakon na področju varstva osebnih podatkov.

ZVOP-1 povzema vse pomembne opredelitve pojmov, ki jih podaja Direktiva, in dodaja še nekaj svojih razlag. Povzema pa tudi načela. ZVOP-1 določa merila za zakonitost obdelave podatkov, ki jih narekuje Direktiva. Obdelavo podatkov razčleni na javni in zasebni sektor, oboje pa opredeljuje podrobneje kot Direktiva.

2.3.1 Splošne določbe

ZVOP-1 določa pravice, obveznosti, načela in ukrepe, s katerimi se preprečujejo neustavni, nezakoniti in neupravičeni posegi v zasebnost in dostojanstvo posameznika pri obdelavi osebnih podatkov (ZVOP-1, 1. člen).

Temelji na načelih varstva osebnih podatkov, ki so opredeljena v Direktivi. Zakon navaja tri načela: načelo zakonitosti in poštenosti, načelo sorazmernosti ter načelo prepovedi diskriminacije (Čebulj, 2005, str. 26).

- **Načelo zakonitosti in poštenosti** (ZVOP-1, 2. člen) zahteva, da se osebni podatki obdelujejo zakonito in pošteno.
- **Načelo sorazmernosti** (ZVOP-1, 3. člen) zahteva, da so osebni podatki, ki se obdelujejo, ustrezni in po obsegu primerni glede na namene, za katere se zbirajo in v nadaljevanju obdelujejo.
- **Načelo prepovedi diskriminacije** (ZVOP-1, 4. člen) narekuje, da mora biti varstvo osebnih podatkov zagotovljeno vsakemu posamezniku, ne glede na njegovo narodnost, raso, barvo, veroizpoved, etično pripadnost, spol, jezik, politično ali drugo prepričanje, spolno usmerjenost, premoženjsko stanje, rojstvo, izobrazbo, družbeni položaj, državljanstvo, kraj oz. vrsto prebivališča ali katerokoli drugo osebno okoliščino.

ZVOP-1 velja za obdelavo osebnih podatkov, če je upravljavec ustanovljen oz. ima podružnico v Republiki Sloveniji. Prav tako ta zakon velja za upravljavca, ki ni registriran v državi članici EU, vendar za obdelavo osebnih podatkov uporablja opremo, ki se nahaja v RS. Zakon pa velja tudi za diplomatsko-konzularna predstavništva Republike Slovenije v tujini (ZVOP-1, 5. člen).

2.3.2 Obdelava osebnih podatkov

2.3.2.1 Pravne podlage in nameni (ZVOP-1, 8.–17. člen)

V drugem delu ZVOP-1 opredeljuje pravno podlago obdelave osebnih podatkov v javnem in zasebnem sektorju. Občutljivi osebni podatki se lahko obdelujejo samo v primerih, ki so navedeni v nadaljevanju (ZVOP-1, 13. člen):

- če posameznik poda izrecno osebno privolitev, ki je praviloma pisna;
- če je obdelava potrebna zaradi izpolnjevanja obveznosti in posebnih pravic upravljavca osebnih podatkov na področju zaposlovanja v skladu z zakonom;
- če je obdelava nujno potrebna za varovanje življenja ali telesa posameznika, na katerega se osebni podatki nanašajo, kadar le-ta fizično ali poslovno ni sposoben dati svoje privolitve;
- če jih za namene zakonitih dejavnosti obdelujejo ustanove, združenja, društva, verske skupnosti, sindikati ali druge nepridobitne organizacije s političnim, filozofskim, verskim ali sindikalnim ciljem; če se obdelava nanaša na njihove člane ali na posameznike, ki so v zvezi s temi cilji z njimi v rednem stiku, ter če se ti podatki ne posredujejo drugim, brez pisne privolitve;
- če je posameznik, na katerega se nanašajo občutljivi osebni podatki, te javno objavil;
- če jih za namene zdravstvenega varstva prebivalstva in posameznikov ter vodenja ali opravljanja zdravstvenih služb obdelujejo zdravstveni delavci in zdravstveni sodelavci v skladu z zakonom;
- če je to potrebno zaradi uveljavljanja ali nasprotovanja pravnemu zahtevku;
- če tako določa drug zakon zaradi izvrševanja javnega interesa.

Ne glede na prvotni namen zbiranja se lahko osebni podatki obdelujejo tudi za zgodovinsko, statistično in znanstveno-raziskovalne namene (ZVOP-1, 17. člen).

2.3.2.2 Varstvo posameznikov (ZVOP-1, 18.–23. člen)

Vsi podatki, ki se obdelujejo, morajo biti točni in ažurni. Točnost osebnih podatkov se lahko preveri z vpogledom v osebni dokument ali drugo ustrezno listino posameznika, na katerega se podatki nanašajo (ZVOP-1, 18. člen). O obdelavi osebnih podatkov pa je potrebno posameznika obvestiti (ZVOP-1, 19. člen).

Osební podatki se lahko shranjujejo le toliko časa, dokler je potrebno, da se doseže namen, za katerega so se ti podatki zbirali. Ko je namen dosežen, se ti podatki zbríšejo, uničijo, blokirajo ali anonimizirajo (ZVOP-1, 21. člen).

2.3.2.3 Zavarovanje osebnih podatkov (ZVOP-1, 24.–25. člen)

Zbrane osebne podatke morajo zavarovati upravljavci in pogodbeni obdelovalci osebnih podatkov (ZVOP-1, 25. člen).

24. člen ZVOP-1 opredeljuje, kako se te podatke zavaruje, in sicer tako, da se:

- varujejo prostori, oprema in sistemsko programska oprema, vključno z vhodno-izhodnimi enotami;
- varuje aplikativna programska oprema, s katero se obdelujejo osebni podatki;
- preprečuje nepooblaščen dostop do osebnih podatkov pri njihovem prenosu, vključno s prenosom po telekomunikacijskih sredstvih in omrežjih;
- zagotavlja učinkovit način blokiranja, uničenja, izbrisa ali anonimiziranja osebnih podatkov;
- omogoča poznejše ugotavljanje, kdaj so bili posamezni osebni podatki vneseni v zbirko osebnih podatkov, uporabljeni ali drugače obdelani in kdo je to storil, in sicer za obdobje, ko je mogoče zakonsko varstvo pravice posameznika zaradi nedopustnega posredovanja ali obdelave osebnih podatkov.

2.3.2.4 Obveščanje o zbirkah osebnih podatkov (ZVOP-1, 26.–28. člen)

Upravljavec osebnih podatkov za vsako zbirko osebnih podatkov vzpostavi katalog osebnih podatkov. Državnemu nadzornemu organu za varstvo osebnih podatkov mora posredovati podatke, preden vzpostavi zbirko osebnih podatkov (ZVOP-1, 27. člen). Nadzorni organ za varstvo osebnih podatkov vodi in vzdržuje register zbirk osebnih podatkov (ZVOP-1, 28. člen). Ta mora vsakomur dovoliti vpogled v ta register in prepis podatkov, ki se nanašajo nanj (ZVOP-1, 29. in 30. člen).

2.3.3 Institucionalno varstvo osebnih podatkov

Institucionalno varstvo osebnih podatkov po ZVOP-1 opravljata Državni nadzorni organ za varstvo osebnih podatkov in Varuh človekovih pravic (Čebulj, 2005).

2.3.3.1 Nadzorni organ za varstvo osebnih podatkov (ZVOP-1, 37.–45. člen)

Državni nadzorni organ je samostojen državni organ, ki ima položaj nadzornega organa za varstvo osebnih podatkov. Opravlja dve nalogi, in sicer inšpekcijski nadzor nad izvajanjem določb tega zakona in druge naloge po tem zakonu ter zagotavlja enotno uresničevanje ukrepov na področju varstva osebnih podatkov (ZVOP-1, 37. člen).

2.3.3.2 Inšpekcijski nadzor (ZVOP-1, 50.–58. člen)

Inšpekcijski nadzor nad izvajanjem določb ZVOP-1 opravlja neposredno državni nadzornik za varstvo osebnih podatkov. Nadzor opravlja na podlagi ustave in zakonov (ZVOP-1, 52. člen).

Inšpekcijski nadzor obsega (ZVOP-1, 51. člen):

- nadzor zakonitosti obdelave osebnih podatkov;
- nadzor ustreznosti ukrepov in izvajanja postopkov ter ukrepov za zavarovanje osebnih podatkov;
- nadzor izvajanja določb zakona, ki urejajo katalog zbirke osebnih podatkov, register zbirk osebnih podatkov in evidentiranje posredovanja osebnih podatkov posameznim uporabnikom osebnih podatkov;
- nadzor izvajanja določb zakona glede iznosa osebnih podatkov v tretjo državo in o njihovem posredovanju tujim uporabnikom osebnih podatkov.

Ko nadzornik pri opravljanju inšpekcijskega nadzora ugotovi, da je prišlo do kršitve, ima pravico zahtevati, da se nepravilnosti oz. pomanjkljivosti odpravijo v roku, ki ga določi sam. Pravico ima, da prepove obdelavo osebnih podatkov osebam javnega ali zasebnega sektorja, ki ne zagotavljajo ukrepov za zavarovanje osebnih podatkov. Ob ugotovitvi, da se osebni podatki obdelujejo v nasprotju z določbami zakona, lahko odredi prepoved obdelave osebnih podatkov in blokiranje, brisanje, anonimiziranje ali uničenje osebnih podatkov. Prepove lahko tudi iznos osebnih podatkov v tretjo državo ali njihovo posredovanje tujim uporabnikom osebnih podatkov (ZVOP-1, 54. člen).

2.3.3.3 Sodelovanje in zunanji nadzor na področju varstva osebnih podatkov (ZVOP-1, 59.–61. člen)

Varuh človekovih pravic opravlja naloge na področju varstva osebnih podatkov, ki se navezujejo le na javni sektor, in sicer, na državne organe, organe lokalne skupnosti in nosilce javnih pooblastil (ZVOP-1, 59. člen). Varuh vsako leto izda letno poročilo, v

katerem državnemu zboru poroča o ugotovitvah, priporočilih, predlogih in stanju na področju varstva osebnih podatkov (ZVOP-1, 60. člen). To poročilo je dostopno tudi javnosti.

2.3.4 Iznos osebnih podatkov

2.3.4.1 Iznos osebnih podatkov v države članice Evropske unije in Evropskega gospodarskega prostora (ZVOP-1, 62.–71. člen)

Zakon loči med iznosom podatkov v države članice Evropske unije, Evropski gospodarski prostor in tretje države. Za države članice EU velja prost pretok osebnih podatkov, to pomeni, da se ZVOP-1 ne uporablja, ampak se uporablja pravni red države članice, kamor so se posredovali podatki. ZVOP-1 se uporablja samo za tretje države (Čebulj, 2005).

Posredovanje podatkov v tretjo državo je dopustno, če državni nadzorni organ izda odločbo, da država, v katero se iznašajo podatki, zagotavlja ustrezno raven varstva osebnih podatkov (ZVOP-1, 63. člen). Nadzorni organ ugotovi ustreznost ravni varstva osebnih podatkov tako, da (ZVOP-1, 64. člen):

- uvede postopek ugotavljanja ustrezne ravni varstva osebnih podatkov v tretji državi na podlagi inšpekcijskega nadzora ali pravnega interesa, ki ga izkaže pravna ali fizična oseba;
- na podlagi tega pridobi ministrstvo za zunanje zadeve od pristojnega organa tretje države potrebne informacije;
- dodatne informacije lahko državni nadzorni organ pridobi tudi od drugih nadzornih organov in od za to pristojnega organa Evropske unije;
- nato v dveh mesecih od prejema popolnih informacije izda odločbo;
- v primeru, da ugotovi, da tretja država ne zagotavlja ustrezne ravni varstva osebnih podatkov, je dolžan v 15 dneh (od izdaje odločbe) o tem obvestiti organ Evropske unije.

Državni nadzorni organ mora pri odločanju o ustreznosti varstva osebnih podatkov v tretji državi ugotoviti vse okoliščine, ki so povezane z iznosom osebnih podatkov. Pri tem mora upoštevati (ZVOP-1, 68. člen):

- namen uporabe (ali se izneseni osebni podatki uporabljajo le za namen, za katerega so bili izneseni, in ali se namen lahko spremeni na podlagi dovoljenja upravljavca ali na podlagi osebne privolitve posameznika, na katerega se podatki nanašajo, ter ali ima ta posameznik možnost izvedeti, za kakšne namene se njegovi osebni podatki uporabljajo);
- organizacijske in tehnične postopke;
- ukrepe, s katerimi so zavarovani osebni podatki;

- ali je določena kontaktna oseba (pooblaščenca oseba, ki poda informacije posamezniku, na katerega se nanašajo podatki, ali državnemu nadzornemu organu o obdelavi podatkov, ki so izneseni);
- pravna varnost (ali je zagotovljeno pravno varstvo posameznika, katerega podatki so izneseni).

V nadaljevanju ZVOP-1 opredeljuje še kazenske določbe in prehodne ter končne določbe.

2.4 Smernice glede varovanja osebnih podatkov

Področje varovanja osebnih podatkov obravnavajo tudi Smernice glede varstva osebnih podatkov pri računalništvu v oblaku, ki so bile izdane leta 2012. Informacijski pooblaščenec jih je pripravil skupaj s Cloud Security Alliance (CSA) Slovenia Chapter, Slovenskim odsekom ISACA in Zavodom e-Oblak, Eurocloud Slovenia (Musar, 2012).

Pravno podlago za izdajo teh smernic informacijskemu pooblaščenцу daje 49. člen ZVOP-1, ki pravi, da lahko pooblaščenec daje neobvezno mnenje o skladnosti kodeksov poklicne etike, neobvezna mnenja, pojasnila in stališča o vprašanjih s področja varstva osebnih podatkov. Mnenja, zahteve, odločbe in sklepe pa lahko objavlja na spletni strani ali na drug primeren način. Izdaja lahko tudi notranje glasilo in strokovno literaturo (ZVOP-1, 49. člen).

Omenjene smernice so namenjene upravljavcem zbirk osebnih podatkov, uporabnikom storitev računalništva v oblaku, nadzornim, revizorskim in svetovalnim inštitucijam. S pomočjo teh smernic naj bi upravljavci dobili priporočila, kako naj v praksi izpolnjujejo zahteve ZVOP-1 (Informacijski pooblaščenec, 2012).

»Namen smernic je podati skupne praktične napotke za upravljavce zbirk osebnih podatkov na jasn, razumljiv in uporaben način in s tem odgovoriti na najpogostejše zastavljena vprašanja s področja varstva osebnih podatkov, s katerimi se srečujejo posamezni upravljavci zbirk osebnih podatkov. S pomočjo smernic naj bi upravljavci dobili priporočila, kako naj v praksi zadostijo zahtevam ZVOP-1« (Informacijski pooblaščenec, 2012).

Obravnavajo vprašanja, ki izhajajo iz pogodbenih razmerij med uporabnikom in ponudnikom storitev RO, ter na vprašanja v zvezi z zaščito podatkov na tem področju. Poleg tega ponujajo različne pristope k skladnosti obdelovanja osebnih podatkov, ki je značilen za RO (EuroCloud, 2012).

Vidiki varstva osebnih podatkov, ki so najbolj izpostavljeni so (Informacijski pooblaščenec, 2012):

- Pogodbena obdelava osebnih podatkov

Določen del osebnih podatkov upravljavec zaupa pogodbenemu obdelovalcu. Pri RO je ponudnik storitev tisti, ki določa pogoje uporabe, raven zavarovanja podatkov in druge pomembne elemente poslovanja, in ne naročnik. Medsebojne pravice in obveznosti uredita s pogodbo, ki mora biti sklenjena v pisni obliki. Med drugim mora vsebovati dogovor o postopkih in ukrepih, s katerimi bodo podatki zavarovani pred slučajnim ali namernim nepooblaščenim uničevanjem, njihovo spremembo ali izgubo ter njihovo nepooblaščno obdelavo.

- Zavarovanje osebnih podatkov

Informacijska varnost je bistveni del in eno temeljnih načel področja varstva osebnih podatkov, to pomeni varovanje celovitosti, zaupnosti in razpoložljivosti osebnih podatkov. Zunanjemu izvajalcu je potrebno zaupati v celoti, gre za zaupanje v varnostne postopke, ukrepe, zanesljivost, dostopnost in stanovitnost obratovanja. Na strani naročnika pa je, da oceni ali ponujene storitve ustrezajo njegovim in zakonskim zahtevam. Za oceno pa potrebuje zadostne in transparentne informacije s strani ponudnika in analizo tveganj, ki jih predstavlja sprejem ponudbe. Naročnik mora vedeti, kje se bodo obdelovali njegovi podatki, kako bo zagotovljena njihova zaupnost, celovitost in razpoložljivost, v katerih tretjih državah se bodo obdelovali, kdaj in kako bodo uničeni, kateri so podizvajalci in kako bodo sodelovali pri obdelavi podatkov itd.

- Iznos osebnih podatkov v tretje države

Pravo vprašanje zavarovanja in varnosti osebnih podatkov se pojavlja pri izvozu osebnih podatkov v tretje države (izven EU), ki ne zagotavljajo enake ravni varstva osebnih podatkov kot domača zakonodaja. Eden najpogostejših inštrumentov zavarovanja so standardne pogodbene klavzule. Gre za pisno pogodbo med upravljavcem in pogodbenim obdelovalcem osebnih podatkov, v kateri so razvidne pravice in obveznosti, vsebuje pa tudi dogovor o postopkih in ukrepih za zavarovanje osebnih podatkov. V porastu je tudi uporaba zavezujočih poslovnih pravil. Gre za interne akte multinacionalnih korporacij – skupin podjetij, ki imajo določena podjetja locirana v tretjih državah. V internem aktu je določena politika korporacije glede iznosa podatkov - v skladu z zahtevami, ki so določene v Direktivi o varstvu osebnih podatkov glede iznosa podatkov v tretje države. Na podlagi internega akta ni mogoče prenašati podatkov podjetjem zunaj korporacije. Velja pa prost pretok osebnih podatkov znotraj te korporacije, tudi če so njihovi člani izven EU. Eden manj uveljavljenih inštrumentov zavarovanja so Zavezujoča poslovna pravila za pogodbene obdelovalce (Explanatory Document on the Processor Binding Corporate Rules, 2013).

Smernice so torej namenjene dvigu stopnje ozaveščenosti o tveganjih, ki jih prinaša obdelava osebnih podatkov pri RO. Poleg tega pa ponujajo kontrolni seznam, s pomočjo katerega je lažje ugotoviti skladnost z zahtevami ZVOP-1. Določene kontrole s tega seznama izpolni naročnik, določene pa ponudnik. Te kontrole predstavljajo minimalne zahteve, ki morajo biti izpolnjene, ko se naročnik odloča za storitve RO (Informacijski pooblaščenec, 2012).

Kontrolni seznam je v nadaljevanju predstavljen v obliki tabel.

2.4.1 Obdelava osebnih podatkov – splošno

V prvi del so uvrščene prve tri kontrolne točke. Prva točka obravnava pravno podlago obdelave osebnih podatkov, s katero mora razpolagati naročnik. Naročnik (N) je seznanjen s kategorijo osebnih podatkov, ki jih bo iznašal v oblak. Preveri pa tudi, ali ponudnik (P) storitev ustreza vsem pogojem, ki mu jih je postavil. Prvo in tretjo kontrolno točko obravnava tudi ZVOP-1 v 8., 9. in 10. členu. V tej tabeli je vidno, da vse tri kontrolne točke izpolnita oba, naročnik (N) in ponudnik (P).

Tabela 6: Kontrolni seznam za preverjanje skladnosti 1–3

Zap. št.	Kontrolna točka	DA	NE	N	P	Zakonska referenca
1	Naročnik razpolaga s pravno podlago za obdelavo osebnih podatkov.			X	X	8., 9., 10. člen ZVOP-1
2	Naročnik ve, katere kategorije osebnih podatkov bo iznašal v oblak.			X	X	
3	Ponudnik ustreza vsem pogojem uporabe storitve, ki jih je postavil naročnik.			X	X	8., 9., 10. člen ZVOP-1

Vir: Informacijski pooblaščenec, Varstvo osebnih podatkov & računalništvo v oblaku, 2012, str. 16.

2.4.2 Pogodbena obdelava osebnih podatkov

Ta del obravnava področje, ko naročnik in ponudnik storitev skleneta pisno pogodbo. V ta del sodijo kontrolne točke od 4 do 8, ki jih izpolnita oba, ponudnik in naročnik storitev. V ZVOP-1 so obravnavane v 11., 8. in 21. členu. Pogodba med naročnikom in ponudnikom storitev mora vključevati dogovor o postopkih in ukrepih za zavarovanje osebnih podatkov. Prav tako mora biti v pogodbi opredeljeno, katere obdelave osebnih podatkov

naj bi izvajal ponudnik storitev in kakšna pooblastila ima. V primeru, da so v posel vključeni tudi podizvajalci, mora biti naročnik o tem seznanjen. Naročnik in ponudnik se morata v pogodbi dogovoriti tudi o tem, da se po prekinitvi pogodbe uničijo vsi shranjeni osebni podatki.

Tabela 7: Kontrolni seznam za preverjanje skladnosti 4–8

Zap. št.	Kontrolna točka	DA	NE	N	P	Zakonska referenca
4	S ponudnikom računalništva v oblaku smo sklenili pisno pogodbo.			X	X	2. odst. 11. člena ZVOP-1
5	Pisna pogodba s ponudnikom računalništva v oblaku vključuje konkretiziran dogovor o postopkih in ukrepih za zavarovanje osebnih podatkov.			X	X	2. odst. 11. člena ZVOP-1
6	V pogodbi s ponudnikom računalništva v oblaku je opredeljeno, katere obdelave osebnih podatkov izvaja ponudnik in kakšna so njegova pooblastila.			X	X	2. odst. 11. člena ZVOP-1
7	Naročnik mora biti v vsakem trenutku seznanjen z vsemi podizvajalci, ki v imenu in za račun ponudnika izvajajo obdelavo osebnih podatkov naročnika, ter z vrsto obdelave (načelo transparentnosti). Ponudnik mora naročniku dati razumen rok pred uporabo storitev novega podizvajalca, v katerem se lahko naročnik odloči, da bo odstopil od pogodbe, če se z uporabo storitev novega podizvajalca ne bo strinjal. Prenos osebnih podatkov podizvajalcu, s katerim se naročnik ne strinja, ni dopusten.			X	X	8. člen ZVOP-1
8	Po preteku pogodbe ali na zahtevo naročnika bo ponudnik storitev računalništva v oblaku uničil vse osebne podatke, vključno z morebitnimi kopijami.			X	X	21. člen ZVOP-1

Vir: Informacijski pooblaščenec, Varstvo osebnih podatkov & računalništvo v oblaku, 2012, str. 17–19.

2.4.3 Informacijska varnost (zavarovanje osebnih podatkov) – skladnost in revizija

V ta del so vključene kontrolne točke od 9. do 15., v ZVOP-1 so obravnavane v 24. in 11. členu. Naročnik lahko sam ali pa s pomočjo tretje osebe izvede analizo tveganja. Naročnik

mora vedeti za lokacijo, kjer naj bi se nahajali osebni podatki. Ves čas ima pravico tudi izvesti revizijo informacijskih sistemov ponudnika. Revizijo pa lahko izvede tudi ponudnik sam in o rezultatih obvešča stranke. Da je poskrbljeno za varnost osebnih podatkov, ki se prenašajo zunaj ali znotraj oblaka, jih mora ponudnik šifrirati. Naročnik mora biti seznanjen o vsakem incidentu, tudi o pristopu večstanovskosti, ki ga ponudnik uporablja za deljenje virov.

Tabela 8: Kontrolni seznam za preverjanje skladnosti 9–15

Zap. št.	Kontrolna točka	DA	NE	N	P	Zakonska referenca
9	Pred uporabo storitev računalništva v oblaku je naročnik sam ali s pomočjo zaupanja vredne tretje stranke izvedel analizo tveganja.			X		24. člen ZVOP- 1
10	Fizična lokacija osebnih podatkov je znana v vseh fazah obdelave osebnih podatkov			X	X	24. člen ZVOP- 1
11	Naročnik ima pogodbeno pravico do revizije informacijskega sistema ponudnika oz. ponudnik redno izvaja zunanje neodvisne revizije celotnega informacijskega sistema. Ponudnik strankam objavlja rezultate revizij informacijskega sistema in varnostnih pregledov v skladu z zakonodajo in varnostnimi standardi.			X	X	2. odst. 11. člena ZVOP-1
12	Ponudnik šifrira osebne podatke, ki se prenašajo v ali znotraj oblaka po nezaščitenih komunikacijskih omrežjih.			X	X	24. člen ZVOP- 1
13	Naročnik je obveščen o dejanskih incidentih in o načinih odkrivanja ter rokovanja z incidenti, vključno s sredstvi pri ponudniku, ki so načrtovani in opisani v načrtu odziva na incidente.			X	X	24. člen ZVOP- 1
14	Naročnik mora biti seznanjen s pristopom, ki ga ponudnik uporablja za deljenje virov in s tehničnimi ter drugimi ukrepi, s katerimi ponudnik naslavlja varnostne vidike večstanovskosti (angl. multi-tenancy).			X	X	24. člen ZVOP- 1
15	Ponudnik varuje svojo večstanovsko infrastrukturo in z načini varovanja seznanjeni naročnika.			X	X	

Vir: Informacijski pooblaščenec, Varstvo osebnih podatkov & računalništvo v oblaku, 2012, str. 20–23.

2.4.4 Pravice posameznika

ZVOP-1 obravnava 16. kontrolno točko v 30., 31. in 32. členu, in sicer vsak posameznik mora imeti dostop do osebnih podatkov. Infrastruktura in postopki ponudnika pa morajo to omogočati.

Tabela 9: Kontrolni seznam za preverjanje skladnosti 16

Zap. št.	Kontrolna točka	DA	NE	N	P	Zakonska referenca
16	Naročnik je preveril, da postopki in infrastruktura ponudniku omogočata enostaven dostop do osebnih podatkov v primeru zahteve posameznika po seznanitvi z lastnimi osebnimi podatki v okviru predpisanih zakonskih rokov.			X	X	30.–32. člen ZVOP-1

Vir: Informacijski pooblaščenec, Varstvo osebnih podatkov & računalništvo v oblaku, 2012, str. 24.

2.4.5 Iznos osebnih podatkov v tretje države

V ta zadnji del sodita 17. in 18. kontrolna točka. V ZVOP-1 sta opredeljeni od 63.–71. člena. V tem delu se preveri, ali je naročnik seznanjen, v katere tretje države se bodo osebni podatki iznašali. Za iznos osebnih podatkov mora obstajati pravna podlaga.

Tabela 10: Kontrolni seznam za preverjanje skladnosti 17–18

Zap. št.	Kontrolna točka	DA	NE	N	P	Zakonska referenca
17	Naročnik je seznanjen s podatkom, v katere tretje države se bodo iznašali osebni podatki.			X		63.–71. člen
18	Pravne podlage za iznos osebnih podatkov v vsako izmed navedenih tretjih držav					
	Država, iz katere je ponudnik oblaka, oz. v kateri bodo (tudi če le za kratek čas) hranjeni podatki, je na seznamu Informacijskega pooblaščenca, v celoti ali delno zagotavlja varnost osebnih podatkov (Švica, ZDA – Varni pristan, Makedonija) odločba ni potrebna.			X	X	2. odst. 63. člena

se nadaljuje

nadaljevanje

Zap. št.	Kontrolna točka	DA	NE	N	P	Zakonska referenca
	Ponudnik oblaka je zavezan Varnemu pristanu ¹ in izpolnjuje vse ostale kontrolne točke (odločba IP ni potrebna).			X	X	3. odstavek 63. člena
	Ponudnik oblaka je zavezan Varnemu pristanu ¹ in izpolnjuje vse ostale kontrolne točke (odločba IP ni potrebna).			X	X	3. odstavek 63. člena
	Iznos bo opravljen na podlagi ene izmed navedenih izjem (odločba IP ni potrebna, tudi če država ne zagotavlja ustrezne ravni varstva OP): tako določa drug zakon ali obvezujoča mednarodna pogodba; podana je osebna privolitev posameznika, iznos je potreben za izpolnitev pogodbe med posameznikom, na katerega se nanašajo osebni podatki, in upravljavcem osebnih podatkov ali za izvršitev predpogodbenih ukrepov, sprejetih kot odgovor na zahtevo posameznika, na katerega se nanašajo osebni podatki; iznos je potreben za sklenitev ali izvršitev pogodbe, ki je v korist posameznika, na katerega se nanašajo osebni podatki, sklenjene med upravljavcem osebnih podatkov in tretjo stranko; iznos je potreben, da se pred hujšim ogrožanjem zavaruje življenje ali telo posameznika, na katerega se nanašajo osebni podatki; iznos se opravi iz registrov, javnih knjig ali uradnih evidenc, ki so po zakonu namenjene zagotavljanju informacij javnosti in so na voljo za vpogled javnosti na splošno ali katerikoli osebi, ki lahko izkaže pravni interes, da so v posameznem primeru izpolnjeni pogoji, ki jih za vpogled določa zakon.			X	X	1.–6. točka 1. odstavka 70. člena ZVOP-1
	Država, v kateri bodo podatki, je na seznamu Evropske komisije (odločba Informacijskega pooblaščenca je potrebna!).			X		1. odstavek 63. in 67. člen ZVOP-1

se nadaljuje

¹ VARNI PRISTAN (angl. *Safe Harbor*) – gre za dogovor organizacij iz tretjih držav, da bodo spoštovale načela obdelovanja osebnih podatkov. To zagotavlja, da organizacija ustrezno varuje osebne podatke. Dogovor Varni pristan naj bi omogočil lažjo izmenjavo podatkov. Organizacija iz Slovenije pred prenosom podatkov organizaciji v ZDA, ki je zavezana načelom Varnega pristani, ne potrebuje posebnega dovoljenja, ki ga izda Informacijski pooblaščenec za iznos podatkov v tretje države.

nadaljevanje

Zap. št.	Kontrolna točka	DA	NE	N	P	Zakonska referenca
	S ponudnikom oblaka, ki mu bomo zaupali osebne podatke, smo sklenili standardne pogodbene klavzule (odločba Informacijskega pooblaščenca je potrebna!).			X	X	7. točka 1. odstavka 70. člena ZVOP-1
	Ponudnik oblaka ima potrjena Zavezujoča poslovna pravila – odločba Informacijskega pooblaščenca je potrebna!			X	X	7. točka 1. odstavka 70. člena ZVOP-1
	S ponudnikom oblaka smo sklenili drugo pogodbo, s katero zagotavljamo ustrezno raven varstva osebnih podatkov (zgled so standardne pogodbene klavzule) – odločba Informacijskega pooblaščenca je potrebna!			X	X	7. točka 1. odstavka 70. člena ZVOP-1

Vir: Informacijski pooblaščenec, Varstvo osebnih podatkov & računalništvo v oblaku, 2012, str. 24–26 .

2.5 Primerjava slovenske zakonodaje z drugimi DČ

Za primerjavo sem vzela 4 države, ki so članice EU in imajo tako kot Slovenija svojo zakonodajo usklajeno z Direktivo 95/46/ES, in sicer Nemčijo, Avstrijo, Litvo in Dansko. Razlog, da sem izbrala Nemčijo je, da Slovenija zelo veliko posluje z Nemčijo. Avstrija je naša sosed, ki postaja gospodarsko vse močnejša. Litvo sem izbrala, ker je glede na velikost in število prebivalcev zelo podobna Sloveniji. Od skandinavskih držav pa sem si izbrala Dansko.

2.5.1 Obdelava osebnih podatkov

V tem delu poglavja bom predstavila, kdaj se osebni podatki lahko obdelujejo in kdaj ne. Za kaj vse mora obdelovalec osebnih podatkov poskrbeti, ko obdeluje, zbira in uporablja osebne podatke in kdaj so taki podatki lahko objavljeni.

2.5.1.1 Nemčija

Zvezni zakon o varstvu podatkov dopušča zbiranje, obdelavo in uporabo osebnih podatkov le, če je to predpisano z zakonom ali drugo zakonsko določbo ali če oseba, na katero se nanašajo osebni podatki, sama privoli v to. Upravitelj mora osebo, o kateri se zbirajo

osebni podatki, obvestiti o identiteti upravljavca, namenu zbiranja, obdelave in uporabe podatkov in v primeru, da se podatki prenašajo, tudi vrsto prejemnika (Data Protection Act, 4. člen, v nadaljevanju FDPA).

Če oseba privoli v zbiranje, obdelavo in uporabo osebnih podatkov, mora za to podati soglasje. Soglasje se poda v pisni obliki, v njem pa mora biti določeno, na katere podatke se to soglasje nanaša (FDPA, 4. a člen).

Zakon zahteva, da se vsak postopek avtomatizirane obdelave podatkov prijavi pri pristojnem nadzornem organu. Velja pa izjema, da postopka ni potrebno prijaviti v primeru, ko odgovorna enota imenuje pooblaščenca za varstvo osebnih podatkov. Obvezna prijava se opusti tudi v primeru, če upravljavec zbira, obdeluje in uporablja osebne podatke za svoje lastne namene in se s tem ukvarja stalno največ devet ljudi. Prijava tudi ni potrebna, če oseba poda soglasje oz. so ti podatki potrebni za izvedbo pravno-poslovne obveznosti. Oprostitev obvezne prijave pa ne velja v primeru, ko gre za avtomatizirano obdelavo poslovnih osebnih podatkov, kjer se ti podatki shranjujejo na določenem mestu, z namenom anonimnega posredovanja ali raziskovanja trga (FDPA, 4. d člen).

Javni in zasebni organi, ki avtomatsko obdelujejo osebne podatke, imenujejo pooblaščenca za varstvo osebnih podatkov. Zasebni organi so dolžni imenovati pooblaščenca v roku enega meseca od začetka opravljanja dejavnosti (FDPA, 4. f člen).

Če upravljavec pri zbiranju, obdelavi ali uporabi osebnih podatkov povzroči škodo osebi, na katero se osebni podatki nanašajo, je dolžan zagotoviti odškodnino za povzročeno škodo (DPA, 7. člen). Enako velja, kadar javni organ v primeru avtomatiziranega zbiranja, obdelave ali uporabe podatkov osebe pri tem povzroči škodo. V tem primeru je organizacija dolžna poravnati škodo. V hudih primerih kršenja zasebnosti je posameznik, na katerega se nanašajo podatki, upravičen do denarne odškodnine (FDPA, 8. člen).

Za zagotovitev čim manjšega obsega kršitev je potrebno, da javni in zasebni organi, ki obdelujejo osebne podatke v svojem imenu ali imenu drugih, sprejmejo v ta namen ustrezne tehnične in organizacijske ukrepe, ki so potrebni za zagotovitev izvajanja določb zveznega zakona (FDPA, 9. člen). Ponudniki sistemov in programov za obdelavo podatkov in organi, ki izvajajo obdelavo podatkov, da bi izboljšali varstvo osebnih podatkov, lahko svoje strategije varstva podatkov ter tehnične zmogljivosti dajo preučiti in oceniti ter rezultate revizije tudi objavijo (FDPA, 9. a člen).

Zakon ločeno obravnava obdelavo podatkov s strani javnih organov celotne federacije, ki ne sodelujejo s konkurenčnimi podjetji javnega prava. Če deželni zakoni o varstvu osebnih podatkov tega področja ne obravnavajo, veljajo določbe zveznega zakona tudi za javne organe dežel ter deželne komisarje za varstvo podatkov (FDPA, 12. člen).

Zbiranje osebnih podatkov je dopustno, če je to potrebno za opravljanje nalog organov. Kadar se osebni podatki zbirajo od zasebnega organa in ne od osebe, je ta organ obveščen

o zakonskih določbah takega pridobivanja podatkov. Zbiranje posebnih vrst podatkov je dovoljeno le:

- če je to določeno z zakonom;
- če posameznik, na katerega se nanašajo osebni podatki, v to privoli;
- če je to potrebno za zaščito posameznika, na katerega se podatki nanašajo, ali tretje osebe, kadar posameznik, na katerega se osebni podatki nanašajo, fizično ali poslovno ni sposoben dati svoje privolitve;
- če so podatki posameznika, na katerega se ti podatki nanašajo, postali javni;
- če je zbirka potrebna za zagotavljanje javnega reda;
- če je zbirka potrebna za namene zdravstvenega varstva, diagnoze in preventive ter za opravljanje zdravstvenih storitev;
- če je zbirka pomembna za znanstvene raziskave;
- če je zbirka potrebna za opravljanje nalog javnega organa federacije ali za humanitarne namene.

Prenos podatkov s kreditno preiskovalne agencije v primeru, ko terjatev ni bila pravočasno poravnana, je upravičen v primeru zaščite upravičenih interesov upravljavca ali tretje osebe. Oseba, na katero se nanašajo osebni podatki, mora prejeti vsaj dva pisna opomina po datumu zapadlosti (FDPA, 28. člen).

Osebni podatki se lahko obdelujejo ali uporabljajo le za namen, za katerega so bili zbrani. Če so osebni podatki zbrani ali shranjeni za znanstveno-raziskovalne namene, se lahko obdelujejo ali uporabljajo samo za te namene, podatki pa se morajo anonimizirati. Organi, ki izvajajo znanstvene raziskave, lahko objavijo osebne podatke samo v primeru, če oseba, na katero se nanašajo podatki, v to privoli ali če je to nujno potrebno za predstavitev raziskovalnih spoznanj (FDPA, 40. člen).

2.5.1.2 Avstrija

Avstrijski zakon določa, da mora biti uporaba podatkov poštena in zakonita. Podatki se zbirajo za posebne, zakonite namene in se naprej ne smejo obdelovati na način, ki ni združljiv z nameni, za katere so bili podatki zbrani. Podatki se hranijo v obliki, ki dopušča identifikacijo posameznika, dokler je to potrebno za namen, za katerega so bili podatki zbrani. Daljše obdobje skladiščenja podatkov pa se lahko določi le s posebnimi zakoni (npr. zakon v zvezi z arhivi) (Datenschutzgesetz 2000, 6. člen, v nadaljevanju DSG).

Podatki se lahko obdelujejo, če za to obstajajo pravna dovoljenja ali če je oseba, na katero se nanašajo osebni podatki, dala soglasje. To soglasje lahko oseba prekliče kadar koli, po preklicu pa je vsakršna uporaba teh podatkov nezakonita. Podatki se lahko obdelujejo tudi na podlagi interesov osebe, na katero se nanašajo podatki, ali na podlagi zakonitih interesov upravljavca ali tretje stranke, ki so ji posredovani podatki (DSG 2000, 6. člen).

Tajnost glede uporabe občutljivih podatkov se ne krši, če (DSG 2000, 9. člen):

- je oseba, na katero se nanašajo osebni podatki, sama javno objavila podatke,
- je obvezno po zakonu ali ima uporabnik pooblastilo za uporabo takih podatkov in je to pomembno za javni interes;
- podatke uporablja upravljavec javnega sektorja pri izpolnjevanju svojih obveznosti – zagotavljanju pomoči med organi;
- je oseba, na katero se nanašajo osebni podatki, dala svojo privolitve, ki jo lahko prekliče kadarkoli, po preklicu pa je vsaka nadaljnja uporaba takih podatkov nezakonita;
- je uporaba podatkov v interesu osebe, na katero se podatki nanašajo, ni pa mogoče pravočasno pridobiti njenega soglasja;
- uporaba je v interesu tretje osebe;
- je uporaba podatkov potrebna za uveljavljanje, izvajanje ali obrambo pravnih zahtev;
- se podatki uporabljajo za zasebne namene, za znanstvene raziskave ali statistične podatke, za anketiranje ali za primere naravnih nesreč (katastrof);
- je uporaba v skladu s pravicami in dolžnostmi upravljavca na področju delovnega prava;
- so podatki potrebni za namene preventivne medicine, medicinske diagnoze, za zagotovitev zdravstvene oskrbe in zdravljenja ali za opravljanje zdravstvenih storitev.

Podatki o politični usmerjenosti, filozofskem prepričanju, verski ali sindikalni pripadnosti se ne razkrivajo, če oseba, na katero se ti podatki nanašajo, ne da privolitve.

Upravljavec lahko zaposli obdelovalca podatkov, če ta jamči, da bo legitimno in varno uporabljal podatke. Upravljavec mora o tem obvestiti Komisijo za varstvo podatkov, razen če je to izvedeno na podlagi pravnega dovoljenja. Obdelovalec podatkov ima poleg pogodbenih obveznosti še obveznosti, ki jih določa zakon. Te obveznosti so opredeljene v 11. členu. Ne glede na pogodbene obveznosti imajo vsi obdelovalci obveznost, da uporabljajo podatke po navodilih upravljavca, prenos uporabljenih podatkov je prepovedan. Sprejeti morajo vse potrebne varnostne ukrepe (delavci se morajo zavezati k zaupnosti). V primeru vključitve dodatnega obdelovalca osebnih podatkov je potrebno pridobiti dovoljenje nadzornika in obvestiti upravljavca. Po obdelavi je potrebno vse rezultate obdelave in dokumentacijo, ki vsebuje občutljive podatke, uničiti ali predati upravljavcu. Upravljavec mora imeti na voljo vse informacije, potrebne za nadzor. Dogovori med upravljavcem in obdelovalcem podatkov se določijo v pisni obliki (DSG 2000, 11. člen).

2.5.1.3 Danska

Zakon se uporablja za avtomatske in druge oblike obdelav osebnih podatkov. Velja pa tudi za primere, ko se osebni podatki ročno prenašajo drugim upravnim organom. Zakon velja tudi za obdelavo podatkov, ki jih izvajajo kreditno informacijske agencije, in pri obdelavi osebnih podatkov v zvezi z video nadzorom. V določenih primerih pa lahko uporabo tega

zakona določi tudi pristojni minister (The Act on Processing of Personal Data, 1. člen, v nadaljevanju TAPPD).

Predpisi, določeni v drugih zakonih, ki nudijo boljšo pravno zaščito osebnih podatkov, so nad tem zakonom. V zakonu pa je določeno tudi to, da se zakon ne uporablja, če je v nasprotju z določbami Evropske konvencije o varstvu človekovih pravic in temeljnih svoboščinah. Zakon se ne uporablja še v naslednjih primerih (TAPPD, 2. člen):

- pri obdelavi podatkov, ki jih izvajajo fizične osebe za uresničevanje osebnih dejavnosti;
- pri obdelavi podatkov, ki se izvajajo v imenu sodišča, na področju kazenskega prava;
- pri obdelavi podatkov, ki se izvajajo v imenu danskega parlamenta in z njim povezanimi institucijami;
- pri obdelavi podatkov, ki jih zajema Zakon o podatkovnih zbirkah, ki jih upravlja medij;
- pri že objavljenih podatkih (besedila, slike, zvočni posnetki);
- pri obdelavi podatkov, ki se izvajajo v imenu obveščevalnih služb policije in nacionalne obrambe.

Podatki se zbirajo za določene in zakonite namene. Podatki, ki se obdelujejo, morajo biti primerni in ustrezni. Obdelava pa mora biti organizirana na način, ki zagotavlja posodobitve teh podatkov. Zagotoviti je potrebno tudi nek nadzor, ki zagotavlja, da so zbrani podatki točni. V primeru, da so podatki netočni ali zavajajoči, jih je potrebno izbrisati ali pa napake takoj odpraviti. Zbrani podatki se ne smejo hraniti v obliki, ki omogoča identifikacijo osebe, na katero se podatki navezujejo, in se ne smejo hraniti daljše obdobje, kot je potrebno za namene, za katere so bili podatki zbrani (TAPPD, 5. člen).

Osebni podatki se lahko obdelujejo le (TAPPD, 6. člen):

- če je oseba, na katero se nanašajo ti podatki, dala svojo izrecno privolitev;
- če je obdelava potrebna za izvajanje pogodbe;
- če je obdelava potrebna za skladnost z zakonom;
- če je obdelava potrebna za varstvo posameznika, na katerega se podatki nanašajo;
- če je obdelava potrebna za izvajanje naloge, ki se izvaja v javnem interesu;
- če je obdelava potrebna za namene zakonitih interesov upravljavca ali tretje stranke, ki so ji posredovani podatki.

Družba, ki ima podatke o potrošniku, ne sme razkriti teh podatkov tretji družbi, razen v primeru, ko je potrošnik za to dal soglasje (TAPPD, 6. člen).

Ne obdelujejo se osebni podatki, ki razkrivajo rasno ali etično poreklo, politična mnenja, verska ali filozofska prepričanja, članstvo v sindikatu, ali podatki v zvezi z zdravjem ali spolnim življenjem. To pa ne velja, če (TAPPD, 7. člen):

- je oseba, na katero se nanašajo podatki, dala soglasje za obdelavo podatkov;
- je obdelava potrebna za varstvo življenjskih interesov posameznika, na katerega se nanašajo podatki;
- se obdelava nanaša na podatke, ki so javno dostopni;

- je obdelava potrebna za uveljavljanje, izvajanje ali obrambo pravnih zahtevkov.

Obdelava podatkov je dovoljena za namene preventivne medicine, zdravstvene diagnoze, za zagotovitev oskrbe, zdravljenja ali vodenja zdravstvenih storitev, ali kadar te podatke obdeluje zdravstveni delavec v skladu z zakonodajo (TAPPD, 7. člen).

Podatki o kaznivih dejanjih, resnih socialnih težavah in drugih osebnih zadevah se lahko obdelujejo v javni upravi samo, če je obdelava potrebna za opravljanje njenih nalog. Ti podatki se ne smejo razkriti nobeni tretji osebi, razen v primeru, da (TAPPD, 8. člen):

- je oseba, na katero se nanašajo osebni podatki, dala soglasje za razkritje;
- so javni ali zasebni interesi večji od interesov osebe, na katero se podatki nanašajo;
- je razkritje potrebno za opravljanje nalog državnih organov.

Podatki se lahko obdelujejo v primeru, da obdelava poteka izključno za namene statističnih in znanstvenih študij, ki so bistvene za javni pomen. Ti podatki pa se nato ne smejo obdelovati za druge namene. Enako velja tudi za ostale podatke, ki se obdelujejo izključno samo za statistične in znanstvene namene (TAPPD, 10. člen).

12. člen je namenjen obdelavi podatkov za tržne namene. Obdelujejo se lahko podatki o imenih, naslovih, poklicih, e-poštnih naslovih, telefonskih številkah, podatki iz trgovinskih registrov, v skladu z zakonom in predpisi, ter drugi podatki, če je oseba, na katero se ti podatki nanašajo, dala soglasje. Minister za pravosodje lahko določi dodatne omejitve glede dostopa do obdelave nekaterih vrst podatkov.

Podatki se lahko arhivirajo v skladu s pravili, ki jih določa Zakon o arhivih (TAPPD, 14. člen).

Podatki o dolgovih do javnih organov se smejo razkriti kreditno informacijskim agencijam v skladu z določbami zakona (TAPPD, 15. člen). Podatki se lahko razkrijejo, če je to dovoljeno z zakonom ali predpisi, ko skupni znesek v plačilo zapadlega dolga doseže vrednost 7500 DKK, vendar pa ta znesek ne sme vsebovati sporazuma za podaljšanje časa za plačilo ali plačilo na obroke. Pred razkritjem je potrebno dolžnika o tem pisno obvestiti (TAPPD, 16. člen).

Kreditne informacijske agencije lahko obdelujejo samo podatke, ki so pomembni za oceno finančnega položaja in bonitete (TAPPD, 23. člen), pri tem pa morajo pridobiti pooblastilo od Agencije za varstvo podatkov (TAPPD, 19. člen). Podatki, ki so stari več kot 5 let, ne smejo biti obdelani, razen v določenih primerih. Podatki o finančnem položaju in kreditni sposobnosti se lahko izdajo le v pisni obliki. Agencija pa lahko ustno razkrije zbirne podatke naročnikov, pod pogojem, da se ime in naslov spraševalca zabeleži za najmanj 6 mesecev. Objave iz kreditno informacijskih agencij lahko vsebujejo le podatke v obliki povzetka, ki se ga razdeli le osebam ali družbam, ki so naročeni na obvestila agencije. Publikacija ne sme navajati identifikacijske številke osebe, na katero se nanašajo osebni podatki (TAPPD, 23. člen).

Kadar se ugotovi, da so podatki netočni in zavajajoči, jih je potrebno popraviti ali izbrisati. Če je te podatke že prejela tretja oseba, pa mora agencija pisno obvestiti o netočnosti in o popravkih njo in osebo, na katero se ti podatki navezujejo (TAPPD, 24. in 25. člen).

Glede slikovnih in zvočnih posnetkov, ki vsebujejo osebne podatke, zakon dovoljuje razkritje le, če je oseba, na katero se podatki nanašajo, v to privolila, če tako zahteva zakon ali če to zahteva policija. Ti podatki se morajo v 30 dneh od posnetja teh podatkov izbrisati, shranijo se lahko le v posebnih primerih (TAPPD, 26. a člen).

Posamezniki in podjetja, ki opravljajo delo za upravljavca ali obdelovalca in imajo dostop do podatkov, lahko te obdelujejo samo po navodilih upravljavca, razen če z zakonom ali drugimi predpisi ni določeno drugače (TAPPD, 41. člen). Upravljavec mora ves čas zagotavljati tehnične in organizacijske ukrepe za zaščito podatkov. Glede varnostnih ukrepov lahko podrobnejša pravila določi tudi minister za pravosodje. Če za upravljavca izvaja obdelavo drug obdelovalec, mora to razmerje med njima urejati pogodba. V pogodbi mora biti določeno, da obdelovalec deluje po navodilih upravljavca. Če ima obdelovalec podatkov sedež v drugi državi članici EU, mora pogodba določati tudi varnostne ukrepe, ki veljajo za to državo članico (TAPPD, 42. člen).

Področje obveščanja o obdelavi podatkov za javno upravo obravnava 43. člen. V tem primeru mora upravljavec obvestiti Agencijo za varstvo podatkov, preden začne z obdelavo podatkov. Enako mora upravljavec storiti pred začetkom kakršnekoli obdelave podatkov, ki se izvaja v imenu zasebnega upravljavca (TAPPD, 48. člen).

Pred začetkom kakršne koli obdelave podatkov, ki se izvaja v imenu zasebnega upravljavca, morata upravljavec ali njegov zastopnik obvestiti Agencijo za varstvo podatkov (TAPPD, 48. člen). Obdelovalci podatkov, ki imajo sedež na Danskem, in ponujajo elektronske storitve obdelave podatkov, morajo o začetku postopka obdelave podatkov obvestiti Agencijo za varstvo podatkov (TAPPD, 53. člen).

2.5.1.4 Litva

Upravljavec podatkov mora zagotoviti, da so osebni podatki (Law on Legal Protection of Personal Data, 3. člen, v nadaljevanju LLPPD):

- zbrani za določene in zakonite namene ter da se ti podatki kasneje ne obdelujejo za namene, ki niso združljivi s predhodnimi;
- obdelani natančno, pošteno in zakonito;
- natančni, za namene obdelave pa tudi posodobljeni; netočne ali nepopolne podatke je upravljavec dolžan popraviti, dopolniti, zbrisati ali blokirati;
- shranjeni v obliki, ki sicer dopušča identifikacijo posameznika, vendar ne več, kot je potrebno za namene, za katere so bili podatki zbrani;
- identični, ustrezni in ne pretirani glede na namen, za katerega so zbrani.

Osební podatki, ki so zbrani za druge namene, se lahko obdelujejo za statistične, zgodovinske in znanstveno-raziskovalne namene le v primeru, ki jih določa zakonodaja. Pri tem morajo biti sprejeti določeni ukrepi varovanja podatkov (LLPPD, 3. člen). Hramba podatkov ne sme biti nikoli daljša, kot je to potrebno za namene obdelave podatkov. Ko podatki niso več potrebni za namene obdelave, jih je potrebno uničiti. Velja izjema, in sicer za podatke, ki morajo biti preneseni v državne arhive (LLPPD, 4. člen).

Osební podatki se lahko obdelujejo, če (LLPPD, 5. člen):

- oseba, na katero se podatki nanašajo, da privolitev;
- se sklene pogodba z osebo, na katero se nanašajo podatki;
- obstaja pravna obveznost, določena z zakonom, da upravljavec podatkov obdeluje osebne podatke;
- je obdelava potrebna za zaščito interesov osebe, na katero se podatki nanašajo;
- je obdelava podatkov potrebna za izvajanje javne oblasti (v državnih ali občinskih institucijah, agencijah, podjetjih ali za tretjo osebo, ki so ji posredovani podatki);
- je obdelava potrebna za namene zakonitih interesov upravljavca ali tretje osebe, ki so ji posredovani podatki.

Osební podatki se lahko obdelujejo tudi, če (LLPPD, 5. člen):

- je obdelava potrebna za namene zaposlitve ali civilne službe;
- je to potrebno za zaščito življenjskih interesov posameznika, na katerega se nanašajo osebni podatki, in ta ne more privoliti zaradi telesne prizadetosti ali pravne nesposobnosti;
- se obdelava osebnih podatkov izvaja za politične, filozofske, verske namene ali namene v zvezi s sindikati, združenji ali drugimi neprofitnimi organizacijami, pod pogojem, da osebne podatke obdelujejo izključno člani te organizacije; takšni osebni podatki se ne smejo razkriti tretji stranki brez privolitve posameznika, na katerega se podatki nanašajo;
- so osebni podatki osebe, na katero se nanašajo podatki, javno objavljeni;
- so podatki potrebni pri preiskovanju kaznivih dejanj ali drugih nezakonitih dejavnosti;
- so podatki potrebni za sodno obravnavo.

V primeru, ko se osebni podatki razkrijejo, je potrebno skleniti pogodbo o razkritju osebnih podatkov med upravljavcem podatkov in prejemnikom podatkov. Pogodba mora vsebovati namen, za katerega se bodo uporabili osebni podatki, pravno podlago za razkritje, pogoje uporabe in obseg razkritja osebnih podatkov (LLPPD, 6. člen).

7. člen določa, kdaj se lahko uporablja EMŠO. Osebna identifikacijska številka se dodeli osebi, v skladu s postopkom, določenim v zakonu o registru prebivalstva. Osebna identifikacijska številka se ne sme objaviti, niti se ne sme zbirati in obdelovati za namene neposrednega trženja. Ta številka se lahko uporablja samo v primeru soglasja posameznika. Soglasje pa ni potrebno:

- če je z zakonom določeno kako drugače;

- v primeru znanstvenega ali statističnega raziskovanja;
- pri obdelavi podatkov v državnih in institucionalnih registrih, če so ti ustanovljeni v skladu z Zakonom o državnih registrih in informacijskih sistemov;
- pri obdelavi podatkov s strani pravnih oseb, ki sodelujejo pri dejavnostih, povezanih z odobritvijo posojil in izterjavo dolgov, zavarovanju ali finančnem leasingu, zdravstvu in socialnem zavarovanju, kot tudi pri dejavnostih institucij, ki izvajajo in upravljajo socialno varstvo in znanstveno-izobraževalne ustanove.

V primeru obdelave osebnih podatkov s strani medijev, ki obdelujejo podatke z namenom informiranja javnosti, umetniškega in literarnega izražanja, te nadzoruje inšpektor za novinarsko etiko. Njegove pristojnosti so določene v Zakonu o zagotavljanju informacij javnosti (LLPPD, 8. člen). Za namene socialnega zavarovanja in socialnega varstva si pristojne institucije izmenjujejo osebne podatke brez privolitve posameznika, na katerega se podatki nanašajo (LLPPD, 9. člen).

Osebne podatke o zdravju posameznika (njegovo stanje, diagnoza, prognoza, zdravljenje itd), lahko obdelujejo le pooblaščen zdravstveni delavci. Zdravje posameznika se obravnava kot poslovna skrivnost. Osebni podatki o zdravju posameznika se lahko obdelujejo avtomatsko za znanstveno medicinsko raziskovalne namene. V tem primeru mora državni inšpektorat za varstvo podatkov izvesti predhodno preverjanje (LLPPD, 10. člen).

Osebni podatki se lahko obdelujejo za namene znanstvenih raziskav pod pogojem, da je oseba, na katero se nanašajo osebni podatki, dala privolitev. Brez privolitve se lahko podatki za namene znanstvenih raziskav obdelujejo samo v primeru, ko se o tem obvesti inšpektorat za varstvo podatkov. V tem primeru mora inšpektorat za varstvo podatkov izvesti predhodni pregled. Podatke, ki se uporabljajo v znanstvenih raziskavah, je potrebno spremeniti v tako obliko, ki ne omogoča identifikacije. Zbrani podatki, ki se uporabljajo v znanstveno-raziskovalne namene, se ne smejo uporabljati za druge namene. Rezultati raziskav se lahko skupaj z osebnimi podatki objavijo samo v primeru, če je oseba, na katero se nanašajo osebni podatki, v to privolila (LLPPD, 12. člen). Drugače je v primeru, ko se podatki zbirajo in obdelujejo za statistične namene, kjer zakon v določenih primerih dopušča razkritje in uporabo teh podatkov za druge namene (LLPPD, 13. člen).

Osebni podatki, ki se obdelujejo za namene trženja, se lahko obdelujejo, če oseba, na katero se nanašajo osebni podatki, da privolitev. Pri zbiranju podatkov je treba določiti rok hrambe osebnih podatkov (LLPPD, 14. člen).

Obdelavo osebnih podatkov na področju elektronskih komunikacij ureja Zakon o elektronskih komunikacijah (LLPPD, 15. člen).

Upravljavca podatkov ima pravico do obdelave in razkritja podatkov oseb, ki niso pravočasno izpolnile svoje finančne obveznosti. Upravljavca sme razkriti podatke dolžnika pod pogojem, da je pred tem poslal pisni opomin o njegovem neplačilu in v tridesetih dneh od datuma opomina ta dolg še ni poravnal (LLPPD, 21. člen). Banke in druge kreditne institucije ter finančna podjetja, ki se ukvarjajo s krediti in finančno dejavnostjo, lahko

druga drugi razkrijejo podatke posameznika, vendar pod pogojem, da je ta oseba v to privolila (LLPPD, 22. člen).

Splošne zahteve glede organizacijskih in tehničnih ukrepov za varstvo podatkov določi državni inšpektorat za varstvo podatkov. Kadar upravljavec dovoli obdelovalcu podatkov obdelavo osebnih podatkov, mora obdelovalec dati jamstvo glede ustreznih tehničnih in organizacijskih ukrepov varovanja podatkov. Odnos med upravljavcem in obdelovalcem podatkov mora biti urejen s pisno pogodbo, razen če je to urejeno z zakoni ali drugimi pravnimi akti. Zaposleni, ki delajo pri upravljavcu ali obdelovalcu, morajo upoštevati zaupnost podatkov, ta obveza velja tudi po prenehanju službe (LLPPD, 30. člen).

Osební podatki se lahko obdelujejo z avtomatskimi sredstvi le, kadar upravljavec obvesti državni inšpektorat za varstvo podatkov, veljajo pa izjeme, ko to ni potrebno (LLPPD, 31. člen). Upravljavec ima pravico, da za varstvo podatkov imenuje osebo ali enoto. Ta skrbi, da upravljavec deluje v skladu s postopkom, ki ga določi vlada, da se podatki obdelujejo v skladu z določbami zakona, sprejema ukrepe za odpravo kršitev, lahko pa tudi pisno obvesti državni inšpektorat za varstvo podatkov, da upravljavec osebnih podatkov pri obdelovanju osebnih podatkov krši določbe zakona in druge akte o varstvu podatkov in kršitve noče odpraviti (LLPPD, 32. člen). V določenih primerih državni inšpektorat za varstvo podatkov izvaja tudi predhodna preverjanja.

2.5.2 Pravice posameznikov

V tem delu poglavja bom za vsako državo posebej opredelila, kakšne pravice imajo osebe, katerih podatki se zbirajo, obdelujejo in uporabljajo.

2.5.2.1 Nemčija

Oseba, o kateri se zbirajo osebni podatki, ima pravico zahtevati informacije v zvezi s shranjevanjem podatkov, informacije o prejemnikih, ki so jim posredovani ti podatki, in informacije o namenu shranjevanja podatkov. Informacij pa se ne posreduje v primeru, da bi to škodilo pravilnemu opravljanju nalog upravljavca ali javni varnosti. Informacije o shranjevanju podatkov se ne razkrivajo osebi, na katero se osebni podatki nanašajo, kadar mora biti varovana skrivnost v skladu s predpisi ali zaradi njihove narave, predvsem na račun upravičenega interesa tretje osebe (FDPA, 19. člen). Če so podatki zbrani brez vednosti osebe, na katero se nanašajo osebni podatki, jo je potrebno obvestiti o skladiščenju, o identiteti upravljavca, namenu zbiranja, obdelave in uporabe. Osebo je potrebno obvestiti tudi o prejemnikih podatkov. Obvestilo o prenosu podatkov je potrebno zagotoviti v času prvega prenosa (FDPA, 19. a člen).

V primeru, da so zbrani osebni podatki nepravilno shranjeni, je potrebno to popraviti. Osebni podatki, ki se obdelujejo z avtomatskimi postopki ali so shranjeni v neavtomatiziranih zbirkah, se zbrisejo, če je njihovo shranjevanje nedopustno ali jih upravljavec za opravljanje njegovih nalog ne potrebuje več. Osebni podatki so blokirani, če zakon, statut ali pogodba izključujejo izbris podatkov. Podatki se blokirajo, če obstaja razlog za domnevo, da bi izbris škodoval osebi, na katero se ti podatki nanašajo, ali v primeru, da izbris ni mogoč ali je otežen zaradi posebne vrste skladiščenja teh podatkov. O popravkih napačnih podatkov, blokiranju spornih podatkov in izbrisu ali blokiranju podatkov zaradi nedopustnega skladiščenja, se obvesti organe, katerim se ti podatki posredujejo v shranjevanje (FDPA, 20. člen).

Vsakdo, ki meni, da so mu bile kršene pravice, se lahko pritoži Zveznemu komisarju za varstvo podatkov in svobodo informacij (FDPA, 21. člen).

2.5.2.2 Avstrija

Vsakdo ima pravico do tajnosti osebnih podatkov. To je izključeno v primeru, kadar podatki ne morejo biti predmet pravice do tajnosti zaradi njihove splošne dostopnosti. Vsaka oseba ima, če se njeni osebni podatki namenjeni avtomatski ali ročni obdelavi, pravico do informacij o tem, kdo podatke obdeluje, kateri podatki se obdelujejo in kateri podatki se prenašajo. Če so ti podatki nepravilni, ima pravico do popravka, če pa so podatki nezakonito obdelani, ima pravico do izbrisa (DSG 2000, 1. člen).

Vsaka oseba, na katero se nanašajo podatki, ima pravico biti obveščena. Upravljavec mora osebo, na katero se nanašajo podatki, obvestiti o namenu uporabe podatkov in o imenu ter naslovu upravljavca, če tega podatka oseba zaradi posebnih okoliščin ni mogla pridobiti. Zakon ne dovoljuje, da se podatki obdelujejo v skupnem informacijskem sistemu. Če upravljavec izve, da so podatki zlorabljeni in lahko to povzroči škodo osebi, na katero se nanašajo ti podatki, mora o tem takoj obvestiti osebo. Tega pa ni potrebno storiti, če je škoda majhna oz. so stroški informiranja osebe o škodi previsoki (DSG 2000, 24. člen).

Informacije se lahko posredujejo pisno, v primeru soglasja pa tudi ustno. Informacije pa se ne smejo dati, če je to nujno za zaščito osebe, ki zahteva informacije ali zaradi javnega interesa. Javni interes lahko izhaja iz potrebe po zaščiti ustavnih institucij Avstrije, varovanja operativne pripravljenosti vojske, varovanje interesov nacionalne obrambe, zunanje politike, gospodarskih in finančnih interesov Avstrije ali Evropske unije ali preprečevanja in pregona zločinov. Zahtevo glede posredovanja informacij se lahko izpolni, zavrne ali delno izpolni v roku osmih tednov. Informacije se dajejo brezplačno, če oseba v tekočem letu še ni vložila zahtevka za informacije in upravljavec ni isti. V nasprotnem primeru je potrebno plačati pavšalno nadomestilo v višini 18,89 € (DSG 2000, 26. člen).

Upravljalavec mora popraviti ali brisati podatke, ki so netočni ali so bili obdelani v nasprotju z določbami zakona. Takoj, ko podatki niso več potrebni za namen uporabe, se morajo izbrisati, razen če je njihovo arhiviranje zakonsko dovoljeno, dostop do teh podatkov pa posebej zavarovan. Popravek ali izbris mora upravljalavec opraviti v roku osmih tednov po prejemu zahtevka. Upravljalavec mora zagotavljati, da so zbrani podatki točni. Če so bili podatki posredovani, preden so bili popravljeni ali izbrisani, mora upravljalavec o tem obvestiti prejemnika podatkov (DSG 2000, 27. člen).

Če z zakonom uporaba podatkov ni dovoljena, ima oseba, na katero se nanašajo osebni podatki, pravico vložiti ugovor upravljalcu. V tem primeru je upravljalavec dolžan izbrisati podatke v osmih tednih (DSG 2000, 28. člen).

2.5.2.3 Danska

Zakon v 31. členu opredeljuje pravice osebe do informiranja o obdelavi podatkov, ki se nanašajo nanjo. Upravljalavec mora osebo, na katero se nanašajo podatki, informirati o namenu obdelave, kateri podatki se obdelujejo, kdo prejema te podatke in vse razpoložljive informacije o viru teh podatkov. Sporočilo mora biti v pisni obliki.

V primeru, da podjetje razkrije podatke o potrošniku tretji družbi za namene trženja, mora preveriti, ali je potrošnik za to dal privolitev. Potrošnik lahko v roku dveh tednov izrazi nestrinjanje z razkritjem podatkov. V tem času se podatki ne smejo razkriti. To področje posebej obravnava tudi Zakon o marketingu (TAPPD, 36. člen).

Oseba, na katero se nanašajo podatki, ima pravico zahtevati, da podatke, ki so netočni ali zavajajoči ali se obdelujejo v nasprotju z zakonom in drugimi predpisi, upravljalavec izbriše, blokira ali popravi. Oseba lahko zahteva tudi, da se o popravkih, izbrisu ali blokiranju podatkov obvesti tretjo stranko, ki so ji bili ti podatki posredovani (TAPPD, 37. člen).

V primeru, da je oseba, na katero se nanašajo podatki, dala soglasje, da se ti podatki lahko posredujejo in obdelujejo, lahko to soglasje tudi umakne (TAPPD, 38. člen). Oseba, na katero se nanašajo podatki, ima pravico vložiti pritožbo na ustrezen nadzorni organ v zvezi z obdelavo njenih podatkov (TAPPD, 40. člen).

2.5.2.4 Litva

Vsaka oseba, katere podatki se obdelujejo, ima pravico biti seznanjena z obdelavo njenih podatkov in z načinom obdelave podatkov. Pravico ima zahtevati popravek ali uničenje osebnih podatkov. Prepove pa lahko tudi nadaljnjo obdelavo svojih osebnih podatkov. Upravljalavec mora dopuščati uveljavljanje teh pravic. So pa v zakonu določene izjeme, ko to ni mogoče, in sicer, kadar gre za:

- državno varnost ali obrambo;
- javni red;
- preprečevanje, preiskovanje, odkrivanje in pregon kaznivih dejanj;
- pomembne ekonomske ali finančne interese države;
- preprečevanje, preiskovanje in odkrivanje kršitev poklicne etike;
- varstvo pravic in svoboščin osebe, na katero se nanašajo osebni podatki.

Kadar oseba, na katero se nanašajo podatki, ne more uveljavljati svojih pravic, ji mora upravljavec za to podati razlago. Odgovor mora sporočiti v 30 dneh od datuma, ko je upravljavec dobil prošnjo za uveljavljanje pravic. Oseba ima pravico, da se nad odločitvijo upravljavca pritoži (LLPPD, 23. člen).

Če oseba ugotovi, da so njeni osebni podatki nepravilni, nepopolni ali netočni, jih mora upravljavec popraviti in prepovedati obdelavo takšnih podatkov. V primeru, da se podatki nezakonito ali neupravičeno obdelujejo, mora upravljavec brez odlašanja in brezplačno, na pisno zahtevo posameznika, uničiti osebne podatke in prepovedati obdelavo takšnih podatkov. Upravljavec mora o popravku, uničenju ali prepovedi obdelave obvestiti tudi prejemnika teh podatkov, razen v primeru, da je število prejemnikov, ki prejemajo te podatke, preveliko in so s tem povezani stroški preveliki. V takem primeru je potrebno obvestiti državni inšpektorat za varstvo osebnih podatkov (LLPPD, 26. člen).

V primeru neposrednega trženja mora upravljavec osebnih podatkov obvestiti osebo, na katero se nanašajo podatki, o obdelavi njenih osebnih podatkov. Ta ima pravico do ugovora (pisno, ustno ali v kateri koli drugi obliki). Če je ugovor upravičen, mora upravljavec brezplačno prekiniti obdelavo njenih osebnih podatkov in o tem obvestiti prejemnike podatkov (LLPPD, 27. člen).

Osebe, na katere se nanašajo osebni podatki, imajo pri dostopu do svojih osebnih podatkov na voljo pomoč, ki jo nudi državni inšpektorat za varstvo podatkov (LLPPD, 29. člen).

2.5.3 Institucionalno varstvo osebnih podatkov

V tem poglavju bom opredelila, katere institucije so pristojne za varstvo osebnih podatkov v posameznih državah in kakšne so njihove naloge.

2.5.3.1 Nemčija

Za varstvo osebnih podatkov je zadolžen in za to izvoljen zvezni komisar za varstvo osebnih podatkov in svobodo obveščanja. Izvoljen je na predlog zvezne vlade. Izvoljeni komisar opravi prisego pred zveznim ministrom za notranje zadeve. Izvoljen je za dobo 5 let, z možnostjo ponovne izvolitve (FDPA, 22. člen).

Mandat zveznega komisarja za varstvo podatkov in svobodo informacij se prične s potrditvijo njegovega imenovanja. Konča pa se ob izteku njegovega mandata ali v primeru njegove razrešitve. Zvezni komisar ne sme opravljati drugih funkcij ali kakršne koli pridobitne dejavnosti, za katero bi dobival plačilo. O vseh prejetih darilih mora obvestiti Zvezno ministrstvo za notranje zadeve (FDPA, 23. člen).

Zvezni komisar na vsaki dve leti izda poročilo o svojem delu, poda ocene in priporočila za izboljšave (FDPA, 26. člen).

Za nadzor nad varstvom osebnih podatkov so pristojni nadzorni organi, in sicer v vsaki zvezni deželi posebej. Nadzorni organ spremlja izvajanje zakona in drugih predpisov o varstvu podatkov, ureja avtomatsko obdelavo osebnih podatkov oz. predelavo ali uporabo osebnih podatkov iz neavtomatiziranih zbirk. Poleg tega svetuje in podpira uradnike ter nadzornike za varstvo podatkov. V primeru, da ugotovi kršitev zakona ali drugih predpisov o varstvu podatkov, pozove posameznike, da kršitev prijavijo ustreznim organom, ki so odgovorni za pregon in kazni. Najmanj vsaki dve leti objavi poročilo o svoji dejavnosti. Nadzorni organ vodi register avtomatiziranih postopkov obdelave. V ta register imajo vpogled vsi. Uradi, ki so predmet nadzora, in osebe, ki vodijo te urade, morajo na zahtevo nadzornega organa priskrbeti informacije, ki so potrebne za opravljanje njihovih nalog. Osebe, ki jih nadzorni organ imenuje za opravljanje nadzora, imajo pravico, kadar je to potrebno za izpolnitev nalog, da med uradnimi urami vstopijo v prostore ali na zemljišče in opravijo ogled. Da bi se ta zakon upošteval, lahko nadzorni organ sprejme ukrepe za odpravo kršitev v času zbiranja, obdelave ali uporabe osebnih podatkov ali tehničnih ali organizacijskih nepravilnosti. V primeru resnih kršitev ali nepravilnosti lahko nadzorni organ prepove zbiranje, obdelavo ali uporabo posameznih postopkov, če kršitve ali napake niso bile odpravljene v ustreznem času (FDPA, 38. člen).

2.5.3.2 Avstrija

V Avstriji za varstvo podatkov skrbita dva organa, in sicer Komisija za varstvo podatkov in Svet za varstvo podatkov. Najvišjo izvršilno oblast ima Komisija za varstvo podatkov (DSG 2000, 35. člen). Komisijo sestavlja šest članov, vsi člani morajo imeti pravno znanje in izkušnje na področju varstva podatkov. Eden od članov pa mora biti sodnik. Komisija za varstvo podatkov pripravi poročilo o svojem delu vsaj vsako drugo leto (DSG 2000, 36. člen). Ena od nalog, ki jih opravlja, je vodenje registra osebnih podatkov. Dostop do registra ima vsaka oseba, ki zaprosi za vpogled, če lahko dokaže, da se osebni podatki nanašajo nanjo. Zvezni kancler bolj natančno določi predpise o vodenju registra (pravilnost, popolnost, jasnost, dostop). Izbrisi iz registra in druge spremembe se v registru izvedejo na podlagi obvestila o spremembi (DSG 2000, 16. člen).

Vsak ima pravico, da Komisiji prijavi domnevno kršitev njegovih pravic. Komisija ima na podlagi tega pravico do vpogleda v podatkovne aplikacije. Dostop do aplikacij in ustreznih

dokumentov mora omogočiti upravljavec ali obdelovalec podatkov. Informacije, ki jih Komisija za varstvo podatkov pridobi pri pregledu, se uporabljajo samo za namene nadzora v okviru izvrševanja predpisov o varstvu podatkov (npr. za namene sodnih postopkov na sodiščih). Za vzpostavitev zakonitega stanja lahko Komisija za varstvo podatkov izda priporočila. Če ta priporočila v ustreznem roku niso upoštevana, lahko Komisija ukrepa po uradni dolžnosti (DSG 2000, 30. člen). Sankcije so odvisne od vrste prekrška:

- kazenska ovadba;
- v primeru hudih prestopkov s strani upravljavca zasebnega sektorja vloži tožbo na pristojno sodišče;
- v primeru prestopka s strani organa pravne osebe vloži tožbo pri najvišjem pristojnem organu; ta organ mora v primernem roku, ki ne presega dvanajst tednov, sprejeti ukrepe, ki zagotavljajo, da je priporočilo Komisije za varstvo podatkov izpolnjeno, ali da Komisijo za varstvo podatkov obvesti, zakaj priporočilo ni izpolnjeno – razlog lahko objavi (DSG 2000, 30. člen).

Komisija za varstvo podatkov je tista, ki odloča o pritožbah oseb, ki so jim bile kršene njihove pravice do tajnosti, pravice do popravka ali izbrisa podatkov (DSG 2000, 31. člen). Če pri reševanju pritožb uporablja nacionalne predpise druge države članice Evropskega gospodarskega prostora, mora zaprositi tuji pristojni nadzorni organ za pomoč (DSG 2000, 34. člen).

Svet za varstvo podatkov ima možnost, da izrazi svoje mnenje o zapisih ministrstva, če so ti pomembni za varstvo podatkov. Svet ima pravico zahtevati informacije in dokumente od upravljavcev javnega sektorja, če je to pomembno za oceno projektov, ki imajo vpliv na varstvo podatkov v Avstriji. Pravico ima zahtevati tudi poročila in dokumente od Komisije za varstvo podatkov. Nadzornike zasebnega sektorja oz. njihove predstavnike lahko zaprosi, da podajo svoje mnenje o njihovi zaskrbljenosti in pozornosti, ki jo namenjajo varstvu podatkov. Svet posreduje svoje pripombe, pomisleke in predloge za izboljšave na področju varstva podatkov (DSG 2000, 41. člen).

48. člen se dotakne tudi področja novinarstva, če medijska podjetja in njihovi delavci uporabljajo podatke neposredno za novinarske namene. Bolj podrobno obravnava to področje še Zakon o medijih.

V nadaljevanju je še opredeljeno, kako je z uporabo podatkov v primeru katastrofe doma, ali če pride do katastrofe v tujini (posredovanje podatkov v tretje države). V tem primeru so regulatorji javnega sektorja pooblaščen za dostop do podatkov in njihovo uporabo.

2.5.3.3 Danska

Na Danskem sta za varstvo osebnih podatkov pristojna nadzorni organ in Agencija za varstvo podatkov. Nadzorni organ vodi register osebnih podatkov. Za varstvo podatkov pa skrbi Agencija za varstvo podatkov. Agencija je sestavljena iz Sveta in sekretariata. Odgovorna je za nadzor vseh postopkov obdelave podatkov (APPD, 55. člen). Pri izvajanju nalog je popolnoma samostojna. Agencija za varstvo podatkov nadzoruje, da se obdelava podatkov izvaja v skladu z določbami zakona (TAPPD, 58. člen).

Agencija za varstvo podatkov lahko na lastno pobudo ali na zahtevo druge DČ preveri, ali je postopek obdelave podatkov, ki se opravlja na Danskem, zakonit, ne glede na to, ali postopek obdelave podatkov ureja zakonodaja druge DČ. Agencija lahko razkrije podatke nadzornim organom drugih DČ, če je to v skladu z določbami danskega zakona ali zakonodaje o varstvu podatkov druge DČ (TAPPD, 64. člen).

Agencija predloži letno poročilo o svoji dejavnosti danskemu parlamentu. Poročilo se objavi tudi javno. Agencija pri izpolnjevanju svojih nalog sodeluje tudi z danskim upravnim sodiščem (TAPPD, 65. člen). Uprava danskega sodišča nadzoruje obdelavo podatkov, ki se izvaja v imenu sodišča. Takšen nadzor vključuje obdelavo podatkov glede upravnih zadev na sodiščih (TAPPD, 67. člen).

2.5.3.4 Litva

Izvajanje zakona o varstvu podatkov nadzoruje Inšpektorat za varstvo podatkov. Inšpektorat je državna institucija, ki se financira iz državnega proračuna in je odgovorna vladi. Predpise v zvezi z Inšpektoratom odobri vlada. Inšpektorat mora biti javna pravna oseba s svojim bančnim računom. Cilj delovanja Inšpektorata je nadzor nad upravljavci pri obdelavi podatkov, pri spremljanju zakonitosti obdelave, preprečevanju kršitev obdelave podatkov in zagotavljanju varstva pravic posameznika. Velja izjema, da Inšpektorat nima pravice spremljati obdelave osebnih podatkov na sodiščih (LLPPD, 36. člen).

Inšpektorat vodi direktor, ki mora biti javni uslužbenec. Izvoljen je za obdobje petih let. Razreši ga lahko le predsednik vlade. Oseba, ki postane direktor, mora v obdobju svojega mandata, prekiniti članstvo v politični stranki (LLPPD, 38. člen).

Naloge državnega inšpektorata za varstvo podatkov so (LLPPD, 40. člen):

- upravlja državni register osebnih podatkov, nadzoruje dejavnosti upravljavcev podatkov, ki se nanašajo na obdelavo osebnih podatkov;
- preučuje zahteve oseb v skladu s postopkom, določenim v zakonu;
- obravnava pritožbe;
- preverja zakonitost obdelave osebnih podatkov in sprejema odločitve v zvezi s kršitvami pri obdelavi osebnih podatkov;

- izdaja dovoljenja za upravljavce podatkov pri prenosu osebnih podatkov uporabnikom v tretje države;
- pripravlja in objavlja letna poročila o svojih dejavnostih;
- posvetuje se z upravljavcem podatkov in pripravlja metodološka priporočila o varstvu osebnih podatkov, ki jih objavlja na spletu;
- drugim državam zagotavlja informacije o pravnih aktih Republike Litve glede varstva podatkov;
- opravlja predhodno preverjanje in daje sklepe upravljavcu podatkov o namenu obdelave podatkov;
- sodeluje s tujimi institucijami, pristojnimi za varstvo osebnih podatkov, institucijami Evropske unije, agencijami in mednarodnimi organizacijami;
- izvaja določbe Konvencije o varstvu posameznikov glede avtomatske obdelave osebnih podatkov.

2.5.4 Iznos osebnih podatkov (tretje države) in ozemeljska veljavnost

V zadnjem delu tega podpoglavja pa bom opredelila, kje obravnavani zakoni veljajo in kdaj se lahko osebni podatki iznašajo v druge države.

2.5.4.1 Nemčija

Nemški zakon o varstvu podatkov ne velja, če se upravljavec nahaja v drugi državi članici Evropske unije ali v drugi državi podpisnici Sporazuma o Evropskem gospodarskem prostoru. Se pa zakon uporablja, če se upravljavec ne nahaja v državi članici Evropske unije ali drugi državi podpisnici Sporazuma o Evropskem gospodarskem prostoru, vendar zbira, obdeluje ali uporablja osebne podatke v Nemčiji.

2.5.4.2 Avstrija

Določbe zakona o varstvu podatkov veljajo za uporabo osebnih podatkov v Avstriji in v drugih državah članicah EU, če se podatki uporabljajo za namene glavnega podjetja ali podružnice upravljavca v Avstriji. Pravo države, v kateri ima upravljavec sedež, se uporablja, kadar upravljavec zasebnega sektorja, ki ima sedež v drugi državi članici EU, uporablja osebne podatke v Avstriji za namen, ki ga ni mogoče pripisati kateremu od obratov v Avstriji. Določbe o iznosu podatkov v tretje države se ne uporabljajo, če se podatki posredujejo upravljavcu osebnih podatkov, pogodbenemu obdelovalcu ali uporabniku osebnih podatkov, ki je ustanovljen, ima sedež ali je registriran v državi članici Evropske unije ali Evropskega gospodarskega prostora. Ta zakon se ne uporablja tudi v

primeru, ko se podatki posredujejo samo preko avstrijskega ozemlja (DSG 2000, 3. člen). Upravljavce podatkov, ki ne prebiva v Evropski uniji, mora imenovati predstavnika v Avstriji (DSG 2000, 6. člen).

Če se podatki prenašajo izven meja, v države podpisnice Evropskega gospodarskega prostora, ni potrebno pridobiti posebnega dovoljenja. Dovoljenja tudi ni potrebno imeti, če so prejemniki podatkov iz tretjih držav, ki imajo ustrezno raven varstva podatkov. Države, ki imajo ustrezno raven varstva podatkov, so našteje v odloku zveznega kanclerja. Dovoljenja pa ni potrebno imeti še v naslednjih primerih (DSG 2000, 12. člen):

- podatki so zakonito objavljeni v Avstriji;
- podatki se do prejemnika prenašajo le posredno;
- čezmejni prenos je podprt s predpisi, ki so enakovredni zakonu v avstrijskem pravnem sistemu;
- oseba, na katero se nanašajo osebni podatki, je dala svoje soglasje za čezmejni prenos;
- pogodbe med upravljavcem in osebo, na katero se nanašajo osebni podatki, ni mogoče izpolniti drugače kot s čezmejnimi prenosom podatkov;
- gre za uveljavljanje, izvajanje ali obrambo pravnih zahtevkov pred tujimi organi (podatki morajo biti zbrani zakonito);
- gre za izmenjavo podatkov z avstrijskimi državnimi predstavništvi v tujih državah.

Kadar zakon zahteva, da mora upravljavec zaprositi za posebno dovoljenje za iznos podatkov v tretje države, ga ta dobi pri Komisiji za varstvo podatkov. Obdelovalec podatkov lahko zaprosi za dovoljenje, da si pridobi določenega obdelovalca podatkov izven Avstrije. To se lahko stori samo s soglasjem upravljavca. Upravljavce o tem poroča Komisiji za varstvo podatkov, ta pa to vpiše v register za obdelavo podatkov. Prenos podatkov predstavništvom tujih vlad ali medvladnim institucijam v Avstriji se obravnava kot čezmejna izmenjava podatkov, ki zahteva izdajo dovoljenja (DSG 2000, 13. člen).

2.5.4.3 Danska

Zakon se uporablja za obdelavo podatkov, ki se izvaja v imenu upravljavca, ki ima sedež na Danskem, če se dejavnosti izvajajo na ozemlju Evropske skupnosti. Zakon velja tudi za danska diplomatska predstavništva. Velja pa tudi za upravljavca, ki ima sedež v tretji državi, podatke pa obdeluje z uporabo opreme, ki se nahaja na Danskem, in v primeru, da se podatki zbirajo na Danskem, obdelava teh podatkov pa bo potekala v tretji državi. V tem primeru mora upravljavec imenovati zastopnika, ki ima sedež na Danskem in o tem pisno obvestiti Urad za varstvo podatkov (TAPPD, 4. člen).

Zakon se uporablja tudi, kadar se podatki obdelujejo na Danskem v imenu upravljavca, ki ima sedež v drugi DČ, in v primeru, da se podatki obdelujejo na Danskem v imenu upravljavca s sedežem v državi, ki ima sklenjen sporazum z Evropsko skupnostjo. Sporazum vsebuje pravila, ki so določena tudi v Direktivi (TAPPD, 4. člen).

Zakon dovoljuje iznos podatkov v tretjo državo samo v primeru, če tretja država zagotavlja ustrezno raven varstva podatkov. Ustreznost ravni, se oceni glede na okoliščine postopka prenosa podatkov, vrsto podatkov, namen in trajanje postopka obdelave, države porekla in namembne države, pravna pravila, ki veljajo v tretji državi, in varnostne ukrepe (TAPPD, 27. člen).

Podatki se lahko prenesejo v tretjo državo samo v primeru, če (TAPPD, 27. člen):

- oseba, na katero se nanašajo osebni podatki, da privolitev;
- je prenos potreben za izvajanje pogodbe med osebo, na katero se nanašajo osebni podatki, in upravljavcem;
- je prenos potreben za sklenitev ali izvajanje pogodbe, sklenjene med upravljavcem in tretjo stranko, v korist osebe, na katero se nanašajo osebni podatki;
- je prenos potreben, ker tako zahteva zakon ali gre za javni interes;
- je prenos potreben, da bi zavarovali življenjske interese osebe, na katero se nanašajo podatki;
- se opravi prenos iz registra, ki je na voljo in ima dostop do njega javnost ali katerakoli druga oseba, ki lahko izkaže zakoniti interes, če so izpolnjeni pogoji, ki jih določa zakon;
- je prenos potreben za preprečevanje, preiskovanje ali pregon kaznivih dejanj in izvrševanje kazni ali varstvo oseb;
- je prenos potreben za zaščito javne varnosti, obrambe ali nacionalne varnosti.

Dovoljenje za prenos osebnih podatkov v tretjo državo, ki nima ustrezne zaščite varstva podatkov, daje Agencija za varstvo podatkov. Agencija mora o izdaji dovoljenja obvestiti Evropsko komisijo in druge DČ. Prenos osebnih podatkov v tretje države se lahko opravi brez dovoljenja na podlagi pogodbe v skladu s standardnimi pogodbenimi klavzulami, ki jih je odobrila Evropska komisija (27. člen).

2.5.4.4 Litva

Zakon se uporablja pri obdelavi osebnih podatkov, kadar je upravljavec podatkov ustanovljen in deluje na ozemlju Litve. Zakon velja tudi za podružnice in predstavništva iz drugih DČ Evropske unije ali drugih držav Evropskega gospodarskega prostora, ki so ustanovljene in delujejo v Litvi. Upravljavec, ki je ustanovljen zunaj ozemlja Litve, je vezan na zakone Litve, na podlagi mednarodnega javnega prava. Sem sodijo tudi diplomatska in konzularna predstavništva. V primeru, da ima upravljavec podatkov sedež v tretji državi, podatke pa obdeluje v Litvi, mora v takem primeru imeti svojega predstavnika (sedež podružnice ali predstavništva v Litvi) (LLPPD, 1. člen).

Zakon se ne uporablja v primeru, ko fizična oseba obdeluje osebne podatke v okviru svoje osebne dejavnosti, ki ni povezana s poslovanjem ali njenim poklicem. Kadar se osebni podatki obdelujejo za namene državne varnosti in obrambe, se ta zakon uporablja le, če

druga zakonodaja v Litvi ne določa drugače. Zakon ne omejuje ali prepoveduje prostega pretoka osebnih podatkov pri izpolnjevanju zavez članstva v Evropski uniji (LLPPD, 1. člen).

Osebnih podatki, katerih prejemniki so iz držav članic EU, se prenašajo pod enakimi pogoji, kot veljajo za prejemnike v Republiki Litvi. Če pa se podatki prenašajo v tretje države, morajo imeti odobritev državnega inšpektorata za varstvo osebnih podatkov. Ta odobri ali zavrne zahtevo v dveh mesecih. Dovoljenje se izda le v primeru, da obstaja ustrezna raven pravnega varstva v tretji državi. Če tretja država tega ne zagotavlja, mora to zagotavljati upravljavec podatkov, kar pa mora biti potrjeno pisno (LLPPD, 35. člen).

2.5.5 Glavne ugotovitve

Za institucionalno varstvo osebnih podatkov v vsaki državi po zakonu skrbita dva organa, razen v Litvi, kjer za varstvo osebnih podatkov skrbi le en organ. Ti organi se po državah razlikujejo glede na naziv in po opravljanju nalog.

V Sloveniji področje in naloge Varuha človekovih pravic ureja poseben zakon, Zakon o varuhu človekovih pravic. To je tudi razlog, da v ZVOP-1 o funkciji Varuha glede varstva osebnih podatkov ni prav veliko napisanega. Tudi inšpekcijski nadzor, ki ga opravlja nadzorni organ, se lahko dopolnjuje z Zakonom o inšpekcijskem nadzoru, če ZVOP-1 ne določa drugače. Kar se tiče varstva podatkov v Nemčiji, je potrebno opozoriti na to, da v Nemčiji poleg Zveznega zakona o varstvu podatkov za varstvo podatkov skrbijo še Deželni zakoni o varstvu podatkov. Na podlagi tega sklepam, da nemški zakon za primerjavo s slovenskim ZVOP-1 ni ravno najboljši primer, saj lahko deželni zakoni precej podrobneje obravnavajo določeno področje kot Zvezni zakon o varstvu podatkov. Nemški zakon o varstvu podatkov nima posebej člena, ki bi izpostavil, da naloge nadzornega organa opravlja nadzornik. V nadaljevanju pa nato tudi niso opredeljene pristojnosti, ki jih ima nadzornik, niti ne ukrepi, ki jih lahko sprejme v primeru kršitev. Za razliko od slovenskega zakona pa nemški zakon določa, da nadzorni organ ob ugotovitvi kršitve pozove posameznike, da kršitev prijavijo ustreznim organom, ki so odgovorni za pregon in kazni.

Avstrijski zakon zelo natančno opredeljuje sestavo Komisije za varstvo podatkov. Vsak član mora imeti ustrezno izobrazbo in izkušnje. Delo Komisije je tako bolj kakovostno. Slovenski ZVOP-1 tega posebej ne opredeljuje. Ima sicer zelo nazorno prikazane naloge nadzornega organa in nato posebej še naloge, pristojnosti in ukrepe nadzornika. Nikjer tudi ni zapisano, da lahko nadzorni organ v primeru hudih kršitev sodeluje s sodiščem. V avstrijskem zakonu je to precej bolj poudarjeno. V Avstriji ima Komisija za varstvo podatkov veliko večjo vlogo tudi glede odločanja o pritožbah oseb, ki so jim bile kršene pravice. V Sloveniji ima to vlogo Varuh človekovih pravic. Slovenski ZVOP-1 tudi ne omenja ničesar v zvezi z reševanjem pritožb, če se pri tem uporablja nacionalne predpise druge države članice Evropskega gospodarskega prostora.

V danskem zakonu je mogoče zaslediti, da ima glede varstva osebnih podatkov veliko večjo vlogo Agencija za varstvo osebnih podatkov. Nadzorni organ vodi register osebnih podatkov, medtem ko ima nadzor nad izvajanjem zakonite obdelave podatkov Agencija za varstvo osebnih podatkov.

Od vseh predstavljenih primerov je Litva edina, ki ima le en organ, ki skrbi za varstvo osebnih podatkov. Ta organ je samostojna institucija in opravlja vse naloge glede varstva osebnih podatkov sama. To pa ne pomeni, da je v Litvi slabše poskrbljeno za varstvo podatkov. Inšpektorat namreč opravlja vse naloge, ki jih pri nas opravljata nadzorni organ in Varuh človekovih pravic. Poleg tega, tako kot Slovenija, tudi Litva izvaja določbe Konvencije o varstvu posameznikov glede avtomatske obdelave osebnih podatkov.

Glede iznosa osebnih podatkov v tretje države nemški zakon ne določa ničesar. Danski zakon je glede iznosa podatkov v tretje države zelo podoben slovenskemu ZVOP-1. Razlikuje se v tem, da v Sloveniji izda dovoljenje za prenos osebnih podatkov v tretjo državo nadzorni organ, medtem ko na Danskem dovoljenje izda Agencija za varstvo podatkov. Tako v Avstriji kot tudi na Danskem, v Litvi in v Sloveniji mora upravljavec, ki nima sedeža oz. ni registriran v državi članici EU, za to imenovati predstavnika. Litva in Slovenija določata, da mora v primeru, ko tretja država ne zagotavlja ustrezne ravni varstva podatkov, to zagotoviti upravljavec podatkov sam. To pa mora biti potrjeno pisno. Litva v svojem zakonu zelo slabo opredeljuje področje iznosa podatkov v tretje države. Glede iznosa osebnih podatkov v tretje države ima avstrijski zakon zelo podobne določbe kot slovenski ZVOP-1. Razlika je v tem, da slovenski ZVOP-1 dovoljuje iznos podatkov tudi v primeru, če se ta opravi iz registrov, javnih knjig ali uradnih evidenc.

V vseh obravnavanih zakonih, tako v slovenskem kot tudi v nemškem, avstrijskem, danskem in v litvanskem, ima posameznik, o katerem se zbirajo osebni podatki, pravico zahtevati informacije v zvezi s shranjevanjem, obdelovanjem in posredovanjem informacij. Večjih posebnosti glede tega področja ni, razen to, da so pravice posameznika v slovenskem ZVOP-1 natančneje opredeljene kot v nemškem zakonu. Nemški zakon ne določa, kakšen je postopek seznanitve, niti posebej ne opredeli postopka v primeru dopolnitve, popravka, blokiranja, izbrisa in ugovora. V Avstriji je rok glede posredovanja informacij 8 tednov, medtem ko je v Sloveniji in Litvi mogoče informacije dobiti najkasneje v 30 dneh. V Avstriji, Sloveniji in na Danskem mora upravljavec osebnih podatkov na zahtevo posameznika obvestiti o popravkih le zadevne osebe. V Nemčiji pa je o popravku potrebno obvestiti tudi nadzorni organ oz. v Litvi državni inšpektorat za varstvo osebnih podatkov, če je število prejemnikov, ki prejemajo te podatke, preveliko in so s tem povezani stroški preveliki.

Od predstavljenih zakonov je slovenski ZVOP-1 edini, ki ločeno določa pravno podlago obdelave podatkov za javni sektor in ločeno za zasebni sektor. Slovenski zakon ne določa, da se vsak postopek avtomatizirane obdelave osebnih podatkov prijavi pri nadzornem organu. V zvezi s tem pa nato nima opredeljene niti izjeme, kdaj se lahko prijava opusti. Nemški zakon določa tudi, da javni in zasebni organi, ki avtomatsko obdelujejo osebne podatke, imenujejo pooblaščenca za varstvo osebnih podatkov. Razlika med nemškim in

slovenskim zakonom je tudi pri obdelavi občutljivih osebnih podatkov. Nemški zakon dovoljuje obdelavo občutljivih osebnih podatkov pri zagotavljanju javnega reda in za humanitarne namene. Tega v slovenskem ZVOP-1 ni. Je pa v slovenskem zakonu dovoljena obdelava podatkov s strani ustanov, združenj, društev in drugih organizacij s političnimi, filozofskimi, verskimi ali sindikalnimi cilji, kadar se obdelava nanaša na njihove člane.

Avstrijski zakon je edini zakon, ki dopušča, da se podatki hranijo v obliki, ki dopušča identifikacijo posameznika, daljše obdobje hranjenja podatkov se določi s posebnim zakonom. Avstrijski zakon, za razliko od slovenskega, dovoljuje obdelavo osebnih podatkov tudi, če se ti uporabljajo za zasebne namene, znanstvene raziskave ali statistične podatke, za anketiranje ali primere naravnih nesreč (katastrof) ter v primeru uporabe, ki je v skladu s pravicami in dolžnostmi upravljavca na področju delovnega prava. Tako slovenski kot tudi avstrijski zakon predvidevata, da lahko upravljavec osebnih podatkov posamezna opravila preda pogodbenemu upravljavcu s to razliko, da avstrijski zakon zahteva, da se o tem obvesti Komisijo za varstvo podatkov. Slovenska zakonodaja tega ne zahteva.

Danski zakon določa uporabo zakona za avtomatsko obdelavo osebnih podatkov in za ročno prenašanje osebnih podatkov. Slovenski zakon tega ne določa. Danski zakon je tudi edini od predstavljenih zakonov, ki določa, da so predpisi, določeni v drugih zakonih, ki nudijo boljšo pravno zaščito osebnih podatkov, nad tem zakonom. V zakonu je določeno tudi, da mora biti obdelava organizirana na tak način, da omogoča posodobitve. Tega slovenski zakon izrecno ne določa. Danski zakon posebej določa še to, da mora v primeru, ko za upravljavca določena dela izvaja pogodbeni obdelovalec, ki ima sedež v drugi državi članici EU, pogodba vsebovati tudi varnostne ukrepe, ki veljajo zanjo. Vse obdelave podatkov, ki se izvajajo za javno upravo, in obdelave, ki se izvajajo v imenu zasebnega upravljavca, se morajo prijaviti Agenciji za varstvo osebnih podatkov. Slovenski ZVOP-1 tega ne določa.

Litvanski zakon, za razliko od slovenskega, dovoljuje obdelavo osebnih podatkov tudi za primere zaposlitve ali civilne službe in v primeru sodnih obravnav.

Lahko zaključim, da so si vsi predstavljeni zakoni med sabo podobni, saj vsi upoštevajo določbe Direktive. Po moji oceni pa so v avstrijskem zakonu posamezna področja varstva osebnih podatkov precej bolj opredeljena kot v zakonih drugih predstavljenih držav. Če upoštevam še velikost Avstrije in njeno sosedsko lego, je ta zakon najboljši primer za presojo določil slovenskega ZVOP-1.

3 RAZISKAVA VARNOSTI OSEBNIH PODATKOV V OBLAKU

Zadnji del magistrske naloge temelji na predstavitvi rezultatov anketiranja, ki sem ga izvedla med slovenskimi revizijskimi družbami in ostalimi podjetji. Da bi lahko ugotovila,

kakšno je zagotavljanje varnosti osebnih podatkov v primeru uporabe RO pri revidiranju, bom posebej analizirala izide anket revizijskih družb in jih primerjala z izidi za druga podjetja. Na podlagi rezultatov ankete bom lahko potrdila (oz. zavrnila) hipotezo, ki sem si jo zastavila v začetku magistrske naloge. Rezultate lastne ankete pa bom primerjala tudi z rezultati raziskave, ki jo je izvedla revizijska mreža KPMG.

3.1 Anketiranje slovenskih uporabnikov storitev v oblaku (podjetij in revizijskih družb)

Anketo sem ustvarila s programsko rešitvijo Google Obrazci (angl. *Google Forms*), ki je enostavna in brezplačna. Do njih sem dostopala z lastnim Google računom (Gmail), ki je prav tako brezplačen. Gmail, Googlovi obrazci in odgovori anketirancev so dostopni/shranjeni na Googlovih strežnikih. Gre za primer javnega oblaka.

Googlovi obrazci omogočajo oblikovanje različnih vrst vprašanj, omogočajo dodajanje slik in video posnetkov. Njihova velika prednost je, da sem lahko vsakodnevno spremljala odziv anketirancev in da je dostop povsem brezplačen. Vse odzive pa tudi sproti beleži v Googlovo razpredelnico (angl. *Google Spreadsheet*). Po končanem anketiranju sem lahko vse zbrane podatke enostavno izvozila v Excelov dokument, kjer sem jih analizirala.

3.1.1 Način izbora anketnih vprašanj

Anketni vprašalnik sem sestavila v obliki zaprtih vprašanj. Vsak anketiranec je imel tako že vnaprej ponujene možnosti izbire enega ali več odgovorov. Za ta tip vprašanj sem se odločila, ker sem predpostavljala, da so anketiranci (direktorji, vodje IT-oddelkov), ki jim je bila anketa namenjena, omejeni s časom.

Anketni vprašalnik je vseboval 10 vprašanj. Če je anketiranec izbral možnost, da v podjetju ne uporabljajo storitev RO, je odgovarjal samo na dve vprašanji. Ostali anketiranci, ki so izbrali eno od možnosti uporabe storitve RO, pa so odgovarjali na devet vprašanj. Z načinom izbire vrste in števila vprašanj sem zagotovila, da je bil anketni vprašalnik hitro rešljiv.

Anketni vprašalnik sem sestavila na podlagi vprašanj, ki so predstavljena v prispevku *The cloud takes shape*. Gre za prispevek mednarodne raziskave, ki jo je izvedla revizijska mreža KPMG, in ga bom v nadaljevanju primerjala z lastno raziskavo.

Moja raziskava se od mednarodne raziskave loči po tem, da ima v anketnem vprašalniku vključeno tudi vprašanje, ki se nanaša na področje varstva osebnih podatkov. To mi bo namreč pomagalo pri potrditvi ali zavrnitvi na začetku zastavljene hipoteze.

3.1.2 Anketna vprašanja za podjetja in revizijske družbe

Anketo sem razposlala vsem revizijskim družbam v Sloveniji, teh je 55, glede na seznam, ki je bil dostopen 21. julija 2015 na spletni strani Slovenskega inštituta za revizijo (Register revizijskih družb, 2015). Poleg revizijskih družb pa sem v anketo zajela tudi

podjetja, različna tako po velikosti kot tudi po dejavnosti, letu njihovega nastanka in regiji, v kateri imajo sedež. Anketa je bila poslana 3843 podjetjem. Do spletnih naslovov sem dostopala preko spletnih strani podjetij, Slovenskega inštituta za revizijo, AJPES in Gospodarske zbornice Slovenije.

V spremnem pismu, ki sem ga razposlala skupaj z anketnim vprašalnikom, sem prosila, da na anketo odgovori direktor družbe oz. vodja IT-oddelka. Anketo sem razpošiljala v obdobju od julija do konca septembra. Nanjo je odgovorilo 167 podjetij (vključno z revizijskimi družbami). Čeprav je bil odziv na anketo razmeroma slab, ocenjujem, da iz prejetih odgovorov lahko strnem nekaj temeljnih zaključkov, povezanih z RO.

3.2 Predstavitev rezultatov anketiranja slovenskih uporabnikov storitev v oblaku

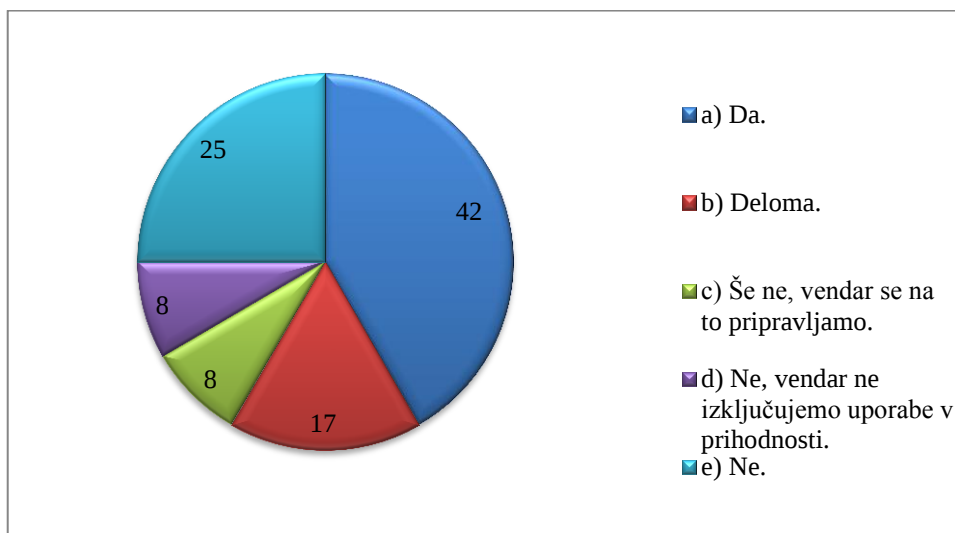
Sledi predstavitev rezultatov ankete v opisni in slikovni obliki. Podatke bom prikazala posebej za revizijske družbe in posebej za ostala podjetja.

3.2.1 Predstavitev rezultatov anketiranja podjetij

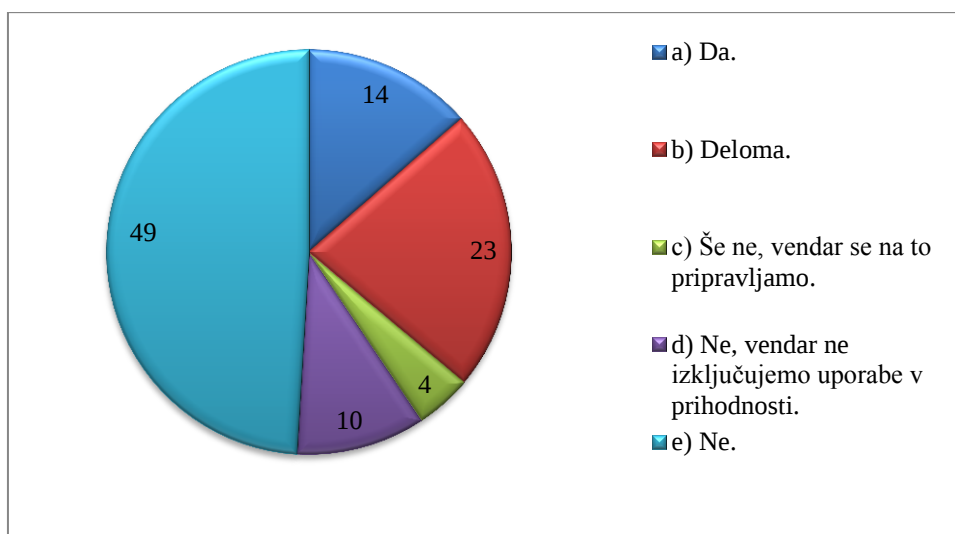
a) Prvo vprašanje: Ali v vašem podjetju pri obdelavi in shranjevanju osebnih podatkov uporabljate storitve RO?

Na vprašanje je odgovorilo 167 podjetij (med njimi 12 revizijskih družb). Rezultati so vidni v spodnjih dveh strukturnih krogih.

Slika 3: Struktura revizijskih družb, ki uporabljajo/ne uporabljajo storitve RO v %



Slika 4: Struktura ostalih podjetij, ki uporabljajo/ne uporabljajo storitve RO v %



79 podjetij (47 %) od skupaj 167 anketiranih podjetij storitev RO ne uporablja in jih tudi v prihodnosti ne namerava uporabljati. 42 % anketiranih revizijskih družb storitve RO uporablja, 25 % jih ne uporablja, 17 % pa le deloma. Med ostalimi podjetji je le 14 % takih, ki storitve RO uporablja, in 49 %, ki storitev RO ne uporablja.

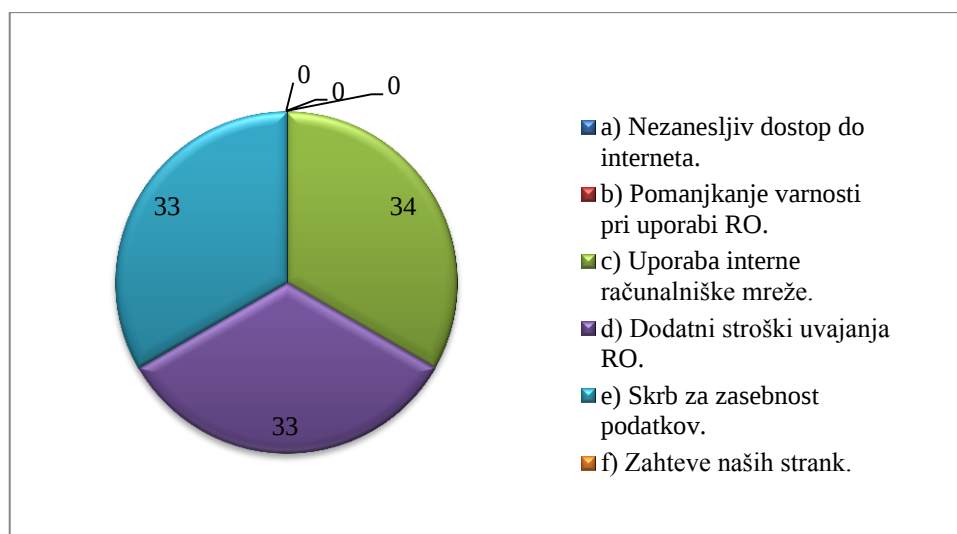
Na sliki 3 je vidno, da so revizijske družbe veliko bolj naklonjene uporabi storitev RO kot pa ostala podjetja (slika 4). Tudi delež revizijskih družb, ki se na uporabo RO še pripravljajo, je večji v primerjavi z ostalimi podjetji.

Po rezultatih sodeč lahko zaključim, da več kot polovica v raziskavo zajetih podjetij in revizijskih družb storitev RO sploh še ne uporablja. So pa revizijske družbe storitvam RO bolj naklonjene.

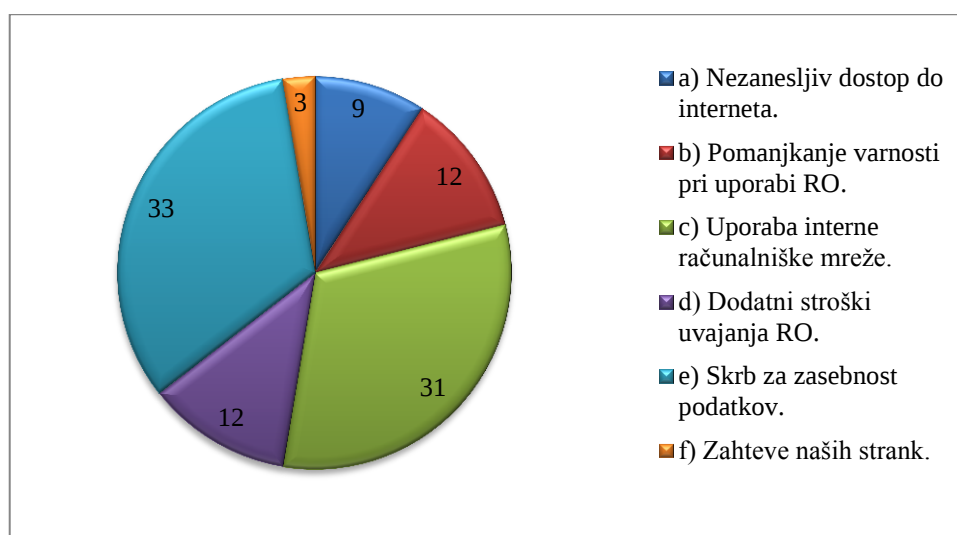
b) Drugo vprašanje: Kaj je tisto, kar vas odvrča od uporabe RO?

Na vprašanje je odgovorilo 79 podjetij, ki v dogledni prihodnosti ne nameravajo uporabljati storitev RO.

Slika 5: Vzroki ne uporabe storitev RO med revizijskimi družbami v %



Slika 6: Vzroki ne uporabe storitev RO med ostalimi podjetji v %



Od devetih revizijskih družb, ki so na anketo odgovorile, so tri take, ki storitev RO ne uporabljajo. Ne uporabljajo jih, ker jim uvajanje RO v njihovo poslovanje predstavlja dodaten strošek, zaradi skrb za zasebnost podatkov in ker uporabljajo interno računalniško mrežo. Podatki so prikazani na sliki 5.

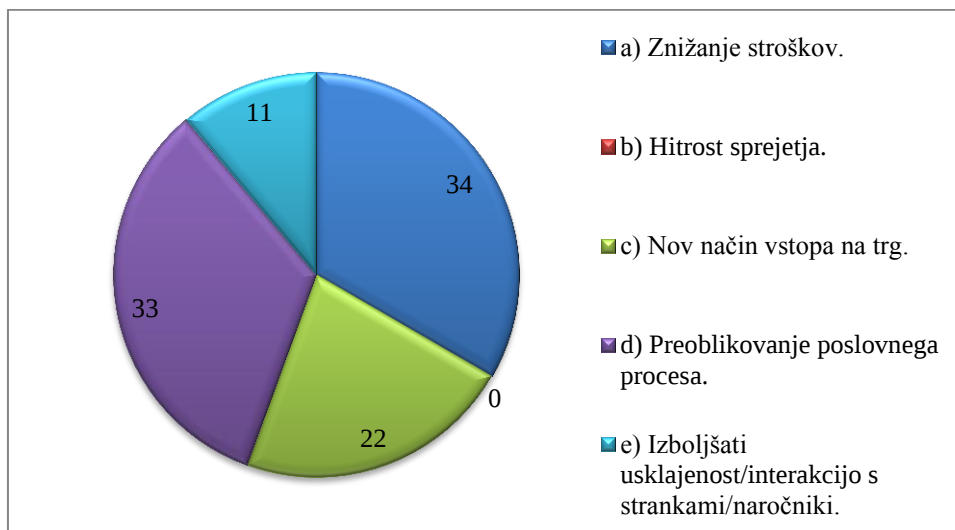
Med ostalimi podjetji je 33 % podjetij, ki RO ne uporabljajo, ker jih skrbi zasebnost podatkov, in 31 % podjetij, ki uporabljajo interno računalniško mrežo. Najmanjši delež, to je 3 % ostalih podjetij, RO ne uporablja zaradi zahtev njihovih strank.

Kot vidimo, sta dva najpogostejša vzroka, zakaj podjetja ne uporabljajo storitev RO, uporaba interne računalniške mreže oz. skrb za zasebnost podatkov.

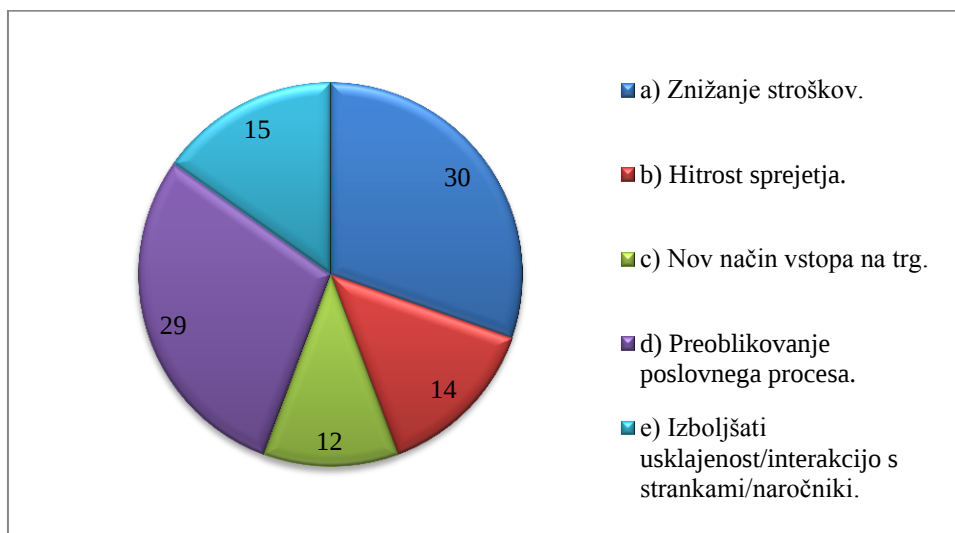
c) Tretje vprašanje: Kateri so ključni cilji, na katerih temelji vaš odnos do RO?

Na vprašanje je odgovorilo 9 revizijskih družb in 79 ostalih podjetij, ki uporabljajo, delno uporabljajo oz. imajo namen uporabljati storitve RO.

Slika 7: Ključni cilji, na katerih temelji odnos revizijskih družb do storitev RO v %



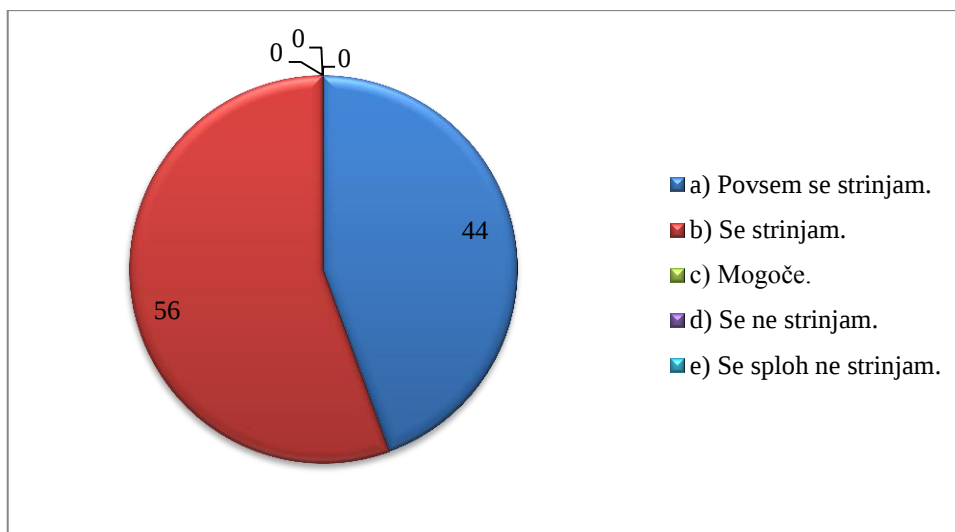
Slika 8: Ključni cilji, na katerih temelji odnos ostalih podjetij do storitev RO v %



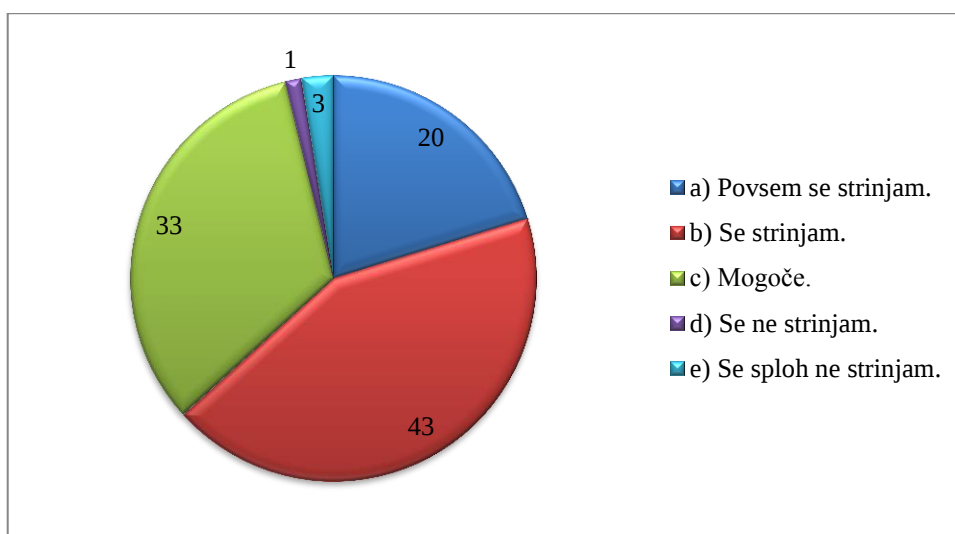
Eden od ciljev, ki ga podjetja skušajo doseči z uporabo storitev RO, je znižanje stroškov. Omenjeni cilj je ključen 34 % revizijskim družbam oz. 30 % ostalim podjetjem. Drugi pomemben cilj je preoblikovanje poslovnega procesa. Razlika med revizijskimi družbami in ostalimi podjetji je v tem, da hitrost sprejetja RO revizijskim družbam ne predstavlja cilja, ki ga hočejo doseči pri uporabi storitev RO.

d) Četrto vprašanje: Ali se strinjate, da v današnjem okolju RO zagotavlja večjo učinkovitost in prihranke?

Slika 9: Mnenje revizijskih družb glede učinkovitosti in prihrankov RO v %



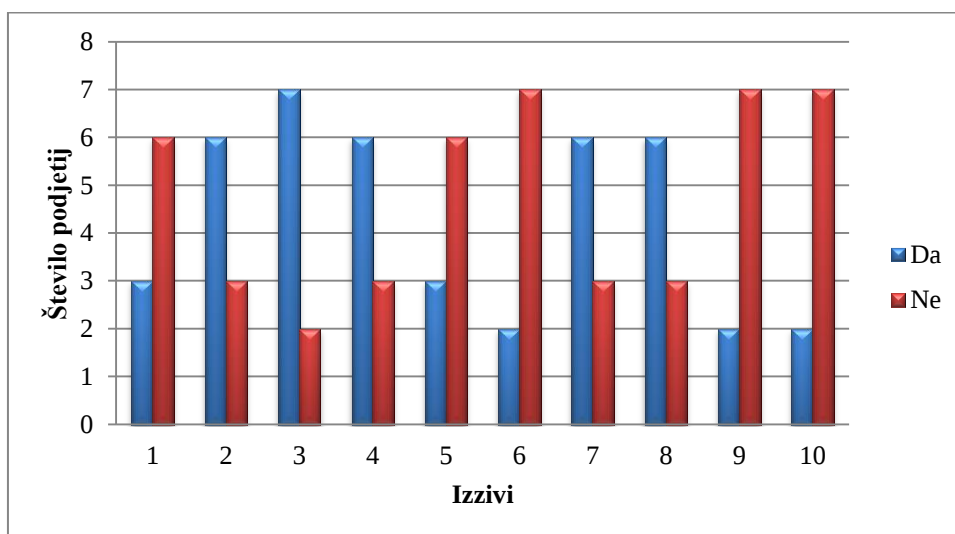
Slika 10: Mnenje ostalih podjetij glede učinkovitosti in prihrankov RO v %



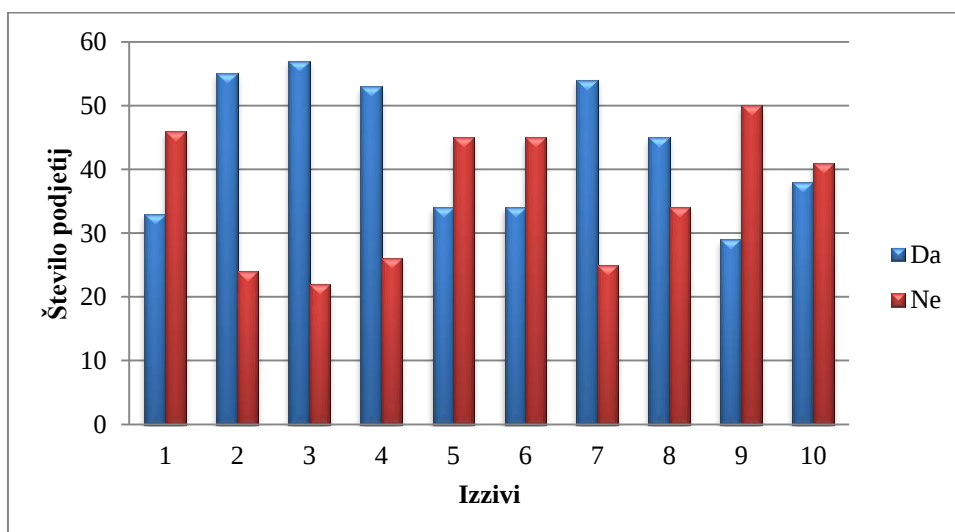
Od skupaj 88 anketiranih podjetij se jih 67 % strinja, da RO zagotavlja večjo učinkovitost in prihranke. V obeh prikazih, ki sta vidna na sliki 9 in 10, je vidno, da je delež podjetij, ki se strinja oz. se povsem strinja, da RO zagotavlja večjo učinkovitost in prihranke, zelo velik. Revizijske družbe pri tem odstopajo, saj se vse strinjajo z omenjeno trditvijo. Med ostalimi podjetji je 33 % takih, ki niso povsem prepričani, da RO zagotavlja večjo učinkovitost in prihranke, 3 % ostalih podjetij pa se s tem sploh ne strinja.

e) Peto vprašanje: Kateri od naštetih izzivov je za vas ključen pri sprejetju RO?

Slika 11: Ključni izzivi pri sprejetju RO za revizijske družbe



Slika 12: Ključni izzivi pri sprejetju RO za ostala podjetja



Opomba: Legenda velja za oba prikaza.

Legenda:

- 1 Previsoki stroški izvedbe, prehoda in integracije.
- 2 Integracija z obstoječo infrastrukturo.
- 3 Izguba podatkov in zasebnosti.
- 4 Izguba kontrole.
- 5 Nepoznavanje prihodnosti povpraševanja (povezano s stroški).
- 6 Pomanjkanje standardov med ponudniki RO.
- 7 Splošno tveganje varnosti.
- 8 Tveganje kraje intelektualne lastnine.
- 9 Skladnost z zakoni in drugimi predpisi.
- 10 Preglednost operativnih kontrol in podatkov.

Na vprašanje je odgovorilo 88 anketiranih podjetij. Na sliki 11 je razvidno, da revizijskim družbam predstavlja največji izziv izguba podatkov in zasebnosti. To je razumljivo, saj razpolagajo z veliko količino podatkov, ki jih pridobijo pri reviziji podjetij. Med pomembnimi izzivi, s katerimi se soočajo revizijske družbe, so tudi integracija z obstoječo infrastrukturo, splošno tveganje varnosti in tveganje kraje intelektualne lastnine. Podobni rezultati veljajo tudi za ostala podjetja, s tem da druga podjetja vidijo v oblaku manjšo nevarnost za krajo intelektualne lastnine kot revizijske družbe. Najpomembnejši izziv jim predstavlja izguba podatkov in zasebnosti, najmanjši izziv pa skladnost z zakoni in drugimi predpisi.

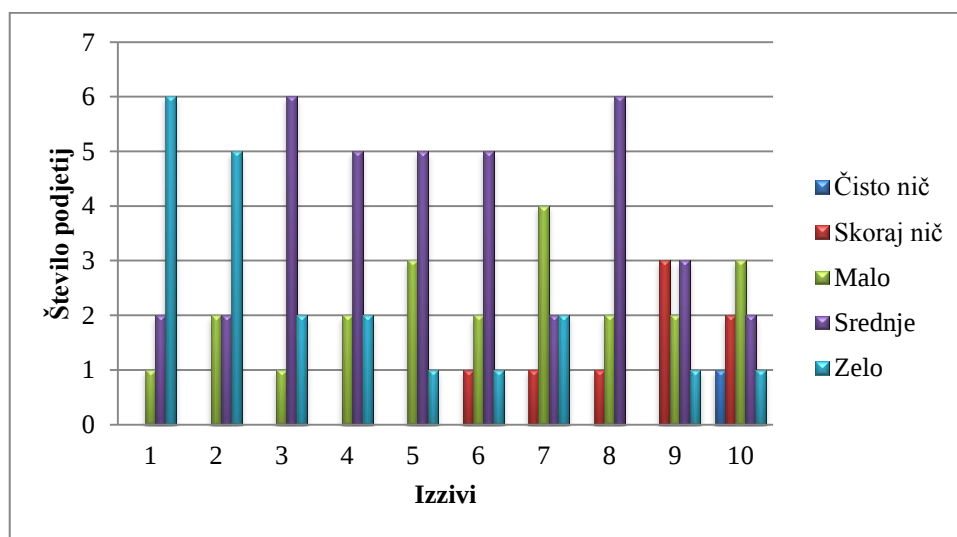
Od skupaj 88 vseh anketiranih podjetij je 67 % takih, ki jim pomemben izziv predstavlja tudi izguba kontrole.

Pomanjkanje standardov med ponudniki RO, skladnost z zakoni in predpisi, preglednost operativnih kontrol in podatkov, previsoki stroški in nepoznavanje prihodnosti povpraševanja so za vsa anketirana podjetja manj zahtevni izzivi.

Na slikah 11 in 12 je razvidno, da se revizijske družbe pri izzivih, s katerimi se srečujejo pri RO, ne razlikujejo prav veliko od ostalih podjetij.

f) Šesto vprašanje: Kako usposobljeno je vaše podjetje pri premagovanju naslednjih izzivov?

Slika 13: Prikaz usposobljenosti revizijskih družb pri premagovanju izzivov



Legenda:

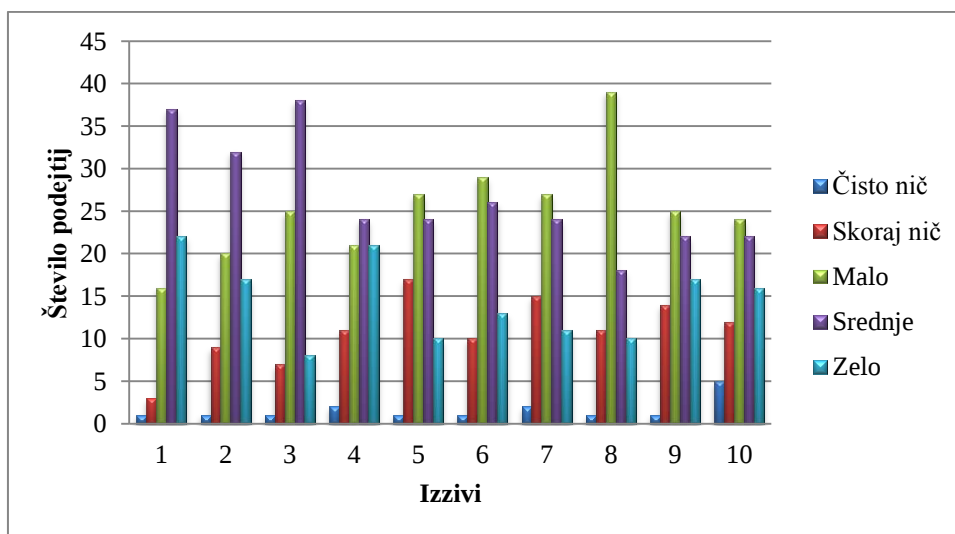
- 1 Skladnost z zakoni in drugimi predpisi.
- 2 Negotovost davčnih posledic.
- 3 Nezadovoljstvo s ponudbo/predstavitvijo/ceno prodajalcev.
- 4 Tveganje razpoložljivosti sistema in neprekinjenosti poslovanja.
- 5 Previsoki stroški izvedbe, prehoda in integracije.
- 6 Merjenje donosnosti naložbe.
- 7 Pomanjkanje standardov med ponudniki oblakov.
- 8 Pomanjkanje celovite ponudbe.

- 9 Integracija z obstoječo infrastrukturo.
- 10 Negotovost glede obljub o realizaciji RO v okolju.

Na vprašanje je odgovorilo 9 revizijskih družb. Na sliki 13 je razvidno, da so izzivi od 1 do 5 izzivi, za katere so revizijske družbe usposobljene vsaj malo, srednje oz. zelo. Namreč nobena revizijska družba ni za omenjene izzive izbrala možnosti, da ni skoraj nič oz. čisto nič usposobljena. Pri izzivih 1 in 2 lahko na sliki 13 vidimo, da se več kot polovica revizijskih družb čuti zanj zelo usposobljena. Izzivi, ki se nahajajo pod številki 3, 4, 5, 6 in 8, so izzivi, za katera je več kot polovica revizijskih družb srednje usposobljena.

Integracija z obstoječo infrastrukturo je eden izmed izzivov, pri katerem revizijske družbe niso dovolj usposobljene. Samo ena revizijska družba se čuti zelo usposobljeno, tri revizijske družbe pa skoraj nič. Negotovost glede obljub o realizaciji RO v okolju je naslednji izziv, za katerega revizijske družbe niso prav dosti usposobljene. Sklepam, da sta izziva 9 in 10 bolj kritična zato, ker je RO za Slovenijo še vseeno dokaj nova storitev, na katero podjetja še niso dovolj pripravljena. Izziv pod številko 10 pa je izziv, na katerega podjetja tudi nimajo prav veliko vpliva.

Slika 14: Prikaz usposobljenosti ostalih podjetij pri premagovanju izzivov



Legenda:

- 1 Skladnost z zakoni in drugimi predpisi.
- 2 Negotovost davčnih posledic.
- 3 Nezadovoljstvo s ponudbo/predstavitvijo/ceno prodajalcev.
- 4 Tveganje razpoložljivosti sistema in neprekinjenosti poslovanja.
- 5 Previsoki stroški izvedbe, prehoda in integracije.
- 6 Merjenje donosnosti naložbe.
- 7 Pomanjkanje standardov med ponudniki oblakov.
- 8 Pomanjkanje celovite ponudbe.

- 9 Integracija z obstoječo infrastrukturo.
 10 Negotovost glede obljub o realizaciji RO v okolju.

Na vprašanje je odgovorilo 79 podjetij. Na sliki 14 je vidno, da se ostala podjetja za premagovanje izzivov 1, 2, 3, in 8 čutijo vsaj malo oz. srednje usposobljena.

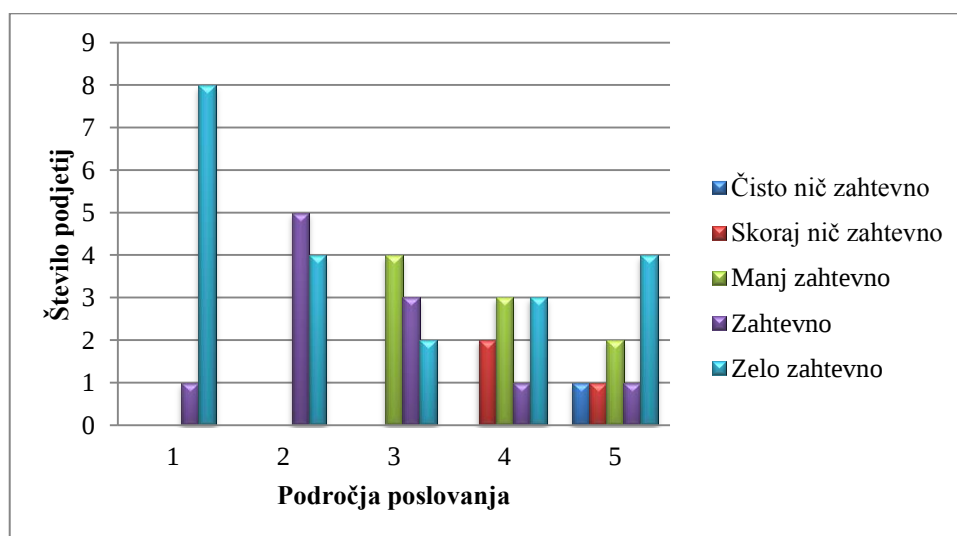
Že na sliki 12 je vidno, da podjetjem pri RO predstavlja velik izziv integracija z obstoječo infrastrukturo, vzrok za to lahko vidimo na sliki 14, saj so glede tega podjetja razmeroma slabo usposobljena. Negotova so tudi glede obljub ponudnikov RO o realizaciji RO v okolju.

Tako kot za revizijske družbe sta izziva 9 in 10 tudi za ostala podjetja bolj kritična. Izziv pod številko 10 pa je izziv, na katerega podjetja tudi nimajo prav veliko vpliva.

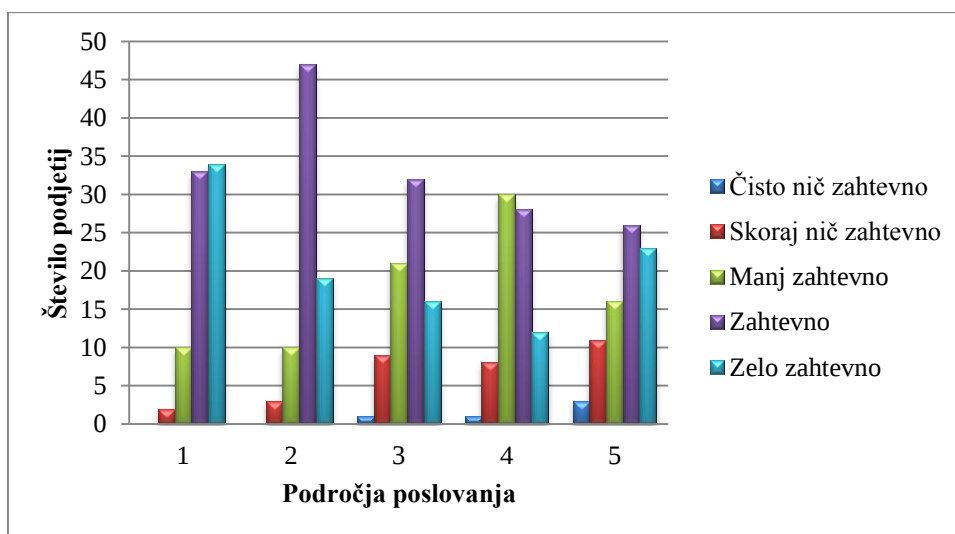
V povprečju se vse anketirane revizijske družbe in ostala podjetja, ki uporabljajo storitve RO, čutijo malo do srednje usposobljeni pri premagovanju naštetih izzivov.

g) Sedmo vprašanje: Kako zahtevno je po vašem mnenju vsako od naštetih področij?

Slika 15: Zahtevnost poslovnih področij za revizijske družbe



Slika 16: Zahtevnost poslovnih področij za revizijske družbe



Opomba: Legenda velja za oba prikaza.

Legenda:

- 1 Izguba podatkov in tveganje zasebnosti.
- 2 Splošno tveganje varnosti.
- 3 Tveganje kraje intelektualne lastnine.
- 4 Skladnost z zakoni in drugimi predpisi.
- 5 Tveganje razpoložljivosti sistema in neprekinjenosti poslovanja.

Od skupaj 88 podjetij je 47 % takih, ki jim izguba podatkov in tveganje zasebnosti predstavlja najbolj zahtevno področje. To lahko vidimo v obeh prikazih, vidnih na slikah 15 in 16.

Revizijske družbe pri tem zelo izstopajo, saj jih je več kot polovica takih, ki ocenjujejo področje 1 kot zelo zahtevno.

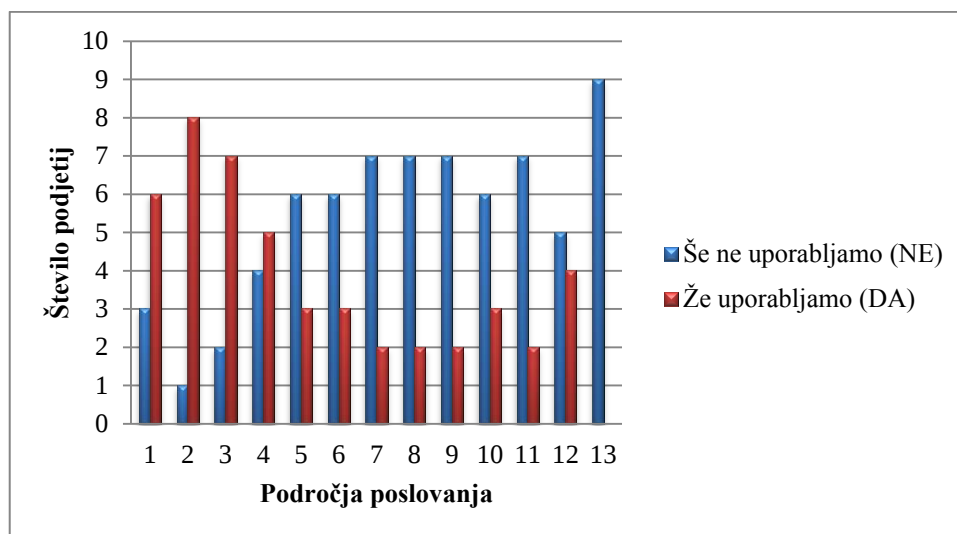
Zahtevno področje predstavlja za vse tudi področje splošnega tveganja varnosti. 59 % od skupaj 88 podjetij je označilo to področje kot zahtevno področje. Tukaj bolj kot revizijske družbe izstopajo ostala podjetja, saj jih je več kot polovica odgovorilo, da je to zanje zahtevno področje.

Področje tveganja kraje intelektualne lastnine je za 45 % revizijskih družb manj zahtevno področje, za 33 % zahtevno in za 22 % zelo zahtevno področje. Ostala podjetja so na tem področju malo bolj občutljiva kot revizijske družbe. 41 % ostalih podjetij je mnenja, da je to zahtevno področje, za 20 % je to zelo zahtevno področje, za 27 % pa malo manj zahtevno področje.

Za področje skladnosti z zakoni in drugimi predpisi je 38 % ostalih podjetij odgovorilo, da je to zanje manj zahtevno področje, 36 % pa da je zahtevno. Revizijske družbe pri tem ne izstopajo. Ponovno se opazi, da so področja, povezana z varnostjo, označena pod 1, 2 in 3, zahtevna področja, kar je razvidno tudi na slikah 11, 12, 13 in 15.

h) Osmo vprašanje: Na katerih področjih vašega poslovanja že uporabljate RO?

Slika 17: Prikaz področij poslovanja, kjer revizijske družbe že/še ne uporabljajo RO



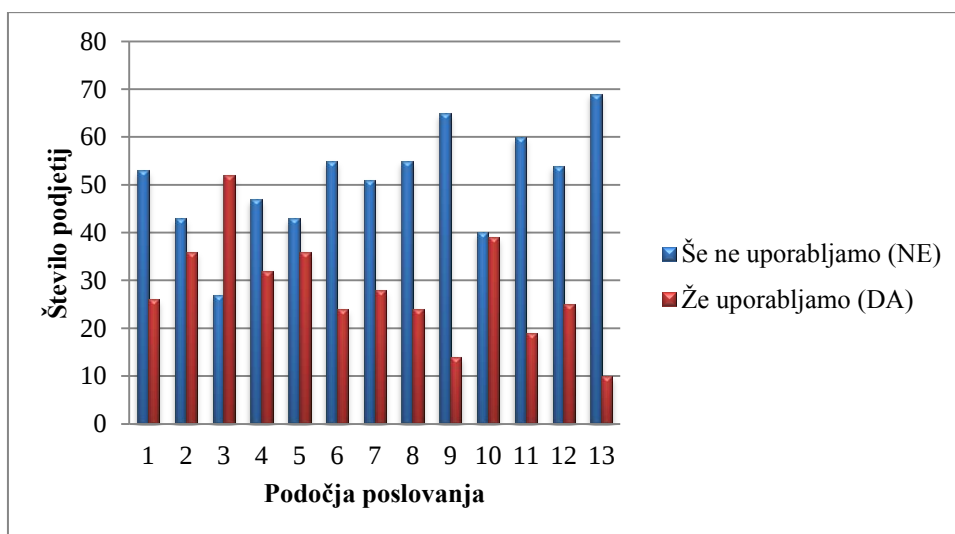
Legenda:

- 1 Človeški viri (HRM).
- 2 Upravljanje z informacijskim sistemom.
- 3 Elektronska pošta.
- 4 Prodaja, marketing.
- 5 Odnos s strankami.
- 6 Oskrbovalno veriga in logistika.
- 7 Računovodstvo in finance.
- 8 Poslovne analize.
- 9 Upravljanje varnosti.
- 10 Upravljanje s spletnimi vsebinami.
- 11 Oskrbovalna veriga.
- 12 Davki.
- 13 Proizvodnja.

Od skupaj 9 revizijskih družb jih 8 uporablja RO na področju upravljanja z informacijskim sistemom. Področja, ki po uporabi RO še izstopajo, so področja označena pod števili 1, 3 in 4. Področja 7, 8, 9 in 11 so področja, pri katerih je uporaba RO najmanjša. Za področje 13 pa je pričakovano, da ga revizijske družbe še niso prenesle v oblak, saj nimajo proizvodnje.

Kako revizijske družbe zaupajo oblaku na področju, na katerem opravljajo svojo dejavnost, je razvidno iz uporabe storitev v oblaku na področju 7 (računovodstvo in finance), ki sta ga zgolj dve revizijski družbi od devetih že prenesli v oblak.

Slika 18: Prikaz področij poslovanja, kjer ostala podjetja že/še ne uporabljajo RO



Legenda:

- 1 Človeški viri (HRM).
- 2 Upravljanje z informacijskim sistemom.
- 3 Elektronska pošta.
- 4 Prodaja, marketing.
- 5 Odnos s strankami.
- 6 Oskrbovalno veriga in logistika.
- 7 Računovodstvo in finance.
- 8 Poslovne analize.
- 9 Upravljanje varnosti.
- 10 Upravljanje s spletnimi vsebinami.
- 11 Oskrbovalna veriga.
- 12 Davki.
- 13 Proizvodnja.

Kar 66 % od 79 ostalih podjetij uporablja RO na področju elektronske pošte. To je tudi edino področje, ki izstopa po uporabi oblaka. Na sliki 18 je razvidno, da več kot polovica ostalih podjetij RO še ne uporablja na področjih 6, 8, 9, 11, 12 in 13. Tudi na sliki 17 je vidno, da so ta področja pri revizijskih družbah manj prenesena v oblak.

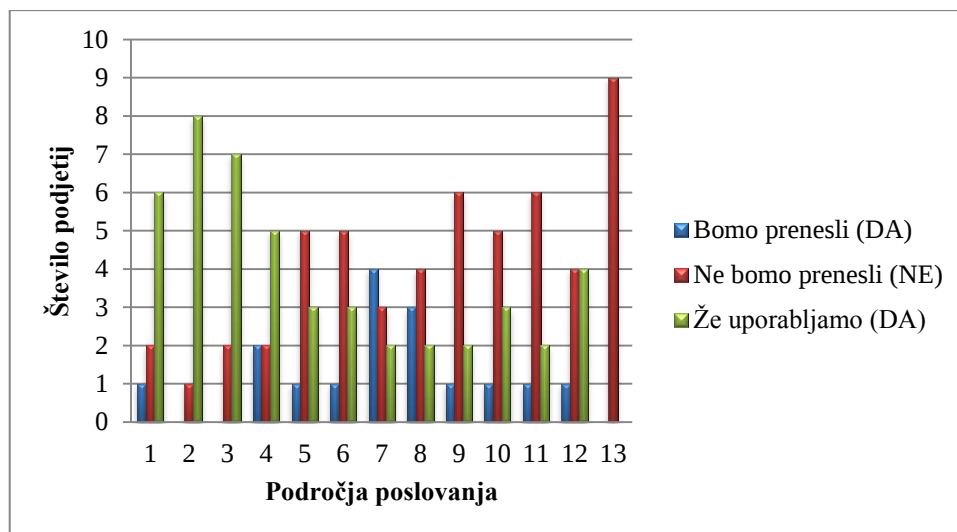
Do razlik med revizijskimi družbami in ostalimi podjetji prihaja na področjih 1 in 2. Revizijske družbe imajo ti dve področji v večini že prenesene v oblak, medtem ko ostala podjetja še ne.

Razlog, da je področje 2 pri revizijskih družbah preneseno v oblak v večjem številu kot pri ostalih podjetjih, bi lahko bil v tem, da so revizijske družbe precej bolj usposobljene glede informacijskih sistemov, saj pri svojih strankah izvajajo tudi revizijo informacijskih sistemov. Pričakovati je, da se na tem področju stalno izpopolnjujejo in so mogoče tudi ene izmed prvih v Sloveniji, ki so to področje prenesli v oblak. Izkušnje, ki jih pri tem pridobivajo, pa jim pomagajo pri njihovem delu.

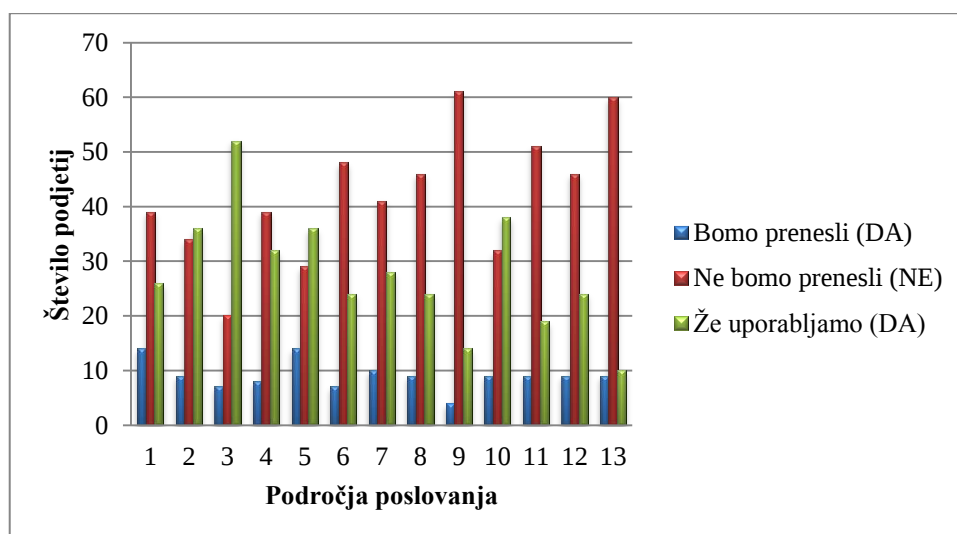
Na drugi strani so podjetja bolj optimistična kot revizijske družbe pri zaupanju RO na področju računovodstva in financ (področje 7).

i) Deveto vprašanje: Katera področja vašega poslovanja boste v prihodnje (čez 18 mesecev) preselili v oblak?

Slika 19: Področja poslovanja, ki jih bodo revizijske družbe prenesle v oblak



Slika 20: Področja poslovanja, ki jih bodo ostala podjetja prenesla v oblak



Legenda (velja za sliki 19 in 20):

- 1 Človeški viri (HRM).
- 2 Upravljanje z informacijskim sistemom.
- 3 Elektronska pošta.
- 4 Prodaja, marketing.
- 5 Odnos s strankami.
- 6 Oskrbovalno veriga in logistika.
- 7 Računovodstvo in finance.
- 8 Poslovne analize.
- 9 Upravljanje varnosti.
- 10 Upravljanje s spletnimi vsebinami.
- 11 Oskrbovalna veriga.
- 12 Davki.

Na vprašanje je odgovorilo 9 revizijskih družb in 79 ostalih podjetij. Na slikah 19 in 20 je vidno, da je v povezavi z RO največji odpor do prenosa podatkov na področjih upravljanja varnosti, oskrbovalne verige in proizvodnje. Pri revizijskih družbah izstopa področje proizvodnje, ki ga revizijske družbe nimajo in zato v prihodnosti ne bo prihajalo do prenosa tega področja v oblak.

Proizvodnja je področje, ki ga tudi ostala podjetja še niso prenesla v oblak (vidno na sliki 20). Od 79 ostalih podjetij, je le 11 % takih, ki nameravajo proizvodnjo prenesti v oblak, 13 % vprašanih jo je že preneslo, preostalih 76 % pa tega ne namerava.

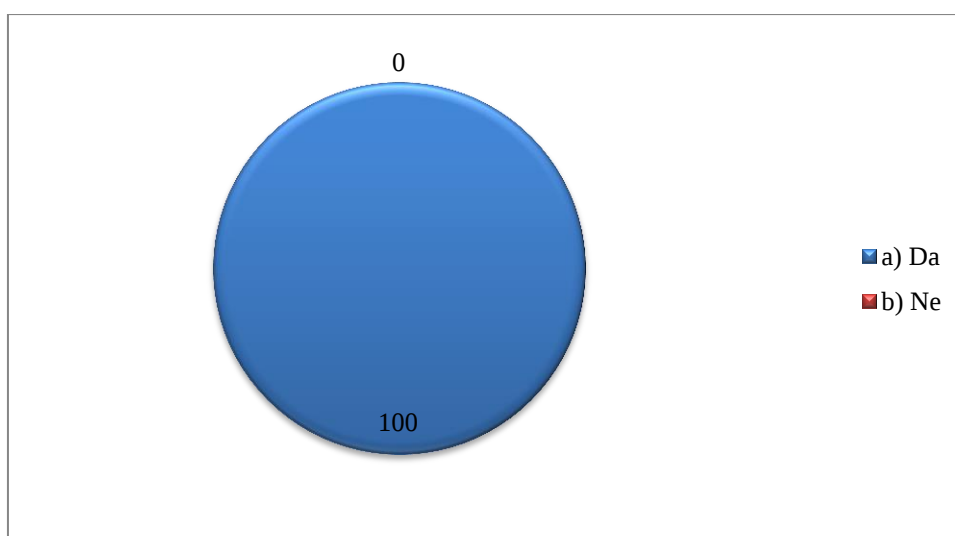
Poslovno področje upravljanja varnosti je naslednje področje, ki ga večina podjetij ne namerava prenašati v oblak. Gre za občutljivo področje, ki ga bo večina podjetij čim manj izpostavljala nevarnostim morebitne prekinitve dostopa do interneta.

Področji, ki ju bodo revizijske družbe prenesle v oblak in v primerjavi z ostalimi poslovnimi področji tudi najbolj izstopata, sta računovodstvo in finance ter poslovne analize (vidno na sliki 19). Področje računovodstva in financ namerava v oblak prenesti 45 % revizijskih družb, 22 % anketiranih revizijskih družb ga je že preneslo, preostalih 33 % pa ga ne namerava. Področje poslovnih analiz pa namerava prenesti v oblak 33 % revizijskih družb od devetih, 45 % pa tega ne namerava storiti.

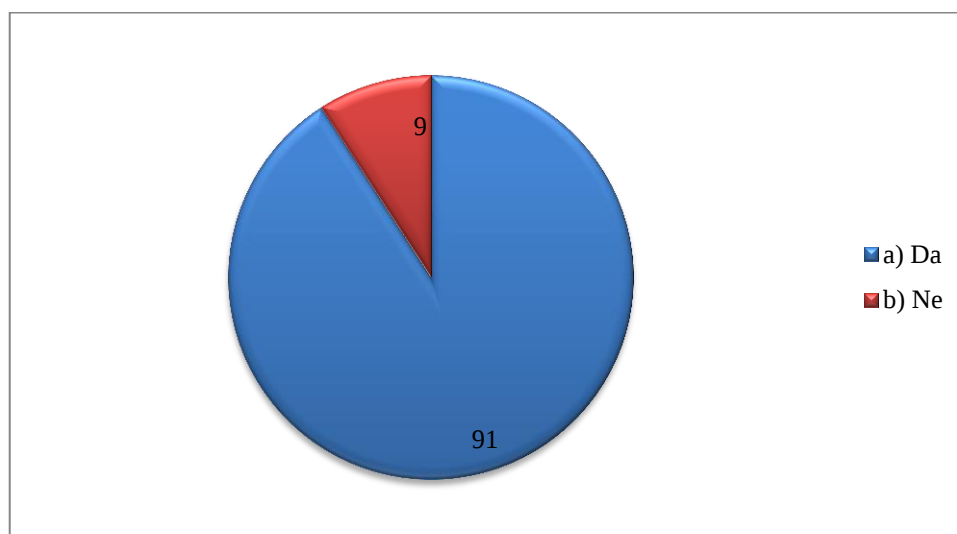
Pri ostalih podjetjih bo do večjih prenosov v oblak prišlo na področju človeških virov in na področju odnosov s strankami.

j) Deseto vprašanje: Eno glavnih vprašanj pri uporabi RO je varstvo osebnih podatkov. Ali imate osebne podatke zavarovane na način, ki je opredeljen v 24. členu ZVOP-1?

Slika 21: Struktura revizijskih družb, ki imajo osebne podatke zavarovane na način, ki je opredeljen v 24. členu ZVOP-1, v %



Slika 22: Struktura ostalih podjetij, ki imajo osebne podatke zavarovane na način, ki je opredeljen v 24. členu ZVOP-1, v %



Na vprašanje je odgovorilo 88 podjetij. Na sliki 21 je vidno, da vse revizijske družbe varujejo osebne podatke v skladu s 24. členom ZVOP-1.

Pri ostalih podjetjih je slika malo drugačna (slika 22). 91 % ostalih podjetij varuje osebne podatke na način, ki je opredeljen v 24. členu, ostalih 9 % pa ne.

3.2.3 Skladnost rezultatov anketiranja z zakonskimi zahtevami

24. člen ZVOP-1 narekuje, da morajo podjetja osebne podatke zavarovati tako, da sprejmejo ustrezne tehnične, logično-tehnične in organizacijske postopke ter ukrepe, s katerimi se varujejo osebni podatki in s tem preprečijo slučajno ali namerno uničenje podatkov, njihovo spremembo ali izgubo oz. nepooblaščenno obdelavo (ZVOP-1). Člen je podrobneje predstavljen že v drugem poglavju.

Eno od vprašanj v anketi je bilo, ali revizijske družbe in podjetja varujejo osebne podatke na način, ki je opredeljen v 24. členu ZVOP-1. Rezultati so vidni na slikah 21 in 22, kjer je razvidno, da vse revizijske družbe in velika večina ostalih podjetij osebne podatke ustrezno varuje. Na slikah 11, 12, 15 in 16 je razvidno, da so področja, povezana z varnostjo, zahtevna področja in predstavljajo za vsa podjetja velik izziv. Na slikah 17 in 19 lahko vidimo, da so revizijske družbe v primerjavi z ostalimi podjetji veliko pogumnejše pri vpeljavi oblaka na področje človeških virov in področje upravljanja z informacijskim sistemom. Področje človeških virov je področje, kjer lahko najdemo veliko osebnih podatkov. Področje upravljanja informacijskih sistemov pa je področje, ki je povezano z vsemi ostalimi področji, tudi s področjem človeških virov. Dobro upravljanje informacijskih sistemov omogoča, da ima podjetje vzpostavljeno varno in zmožljivo infrastrukturo. Iz teh rezultatov lahko sklepam, da se revizijske družbe, pa tudi ostala podjetja, ki se odločajo svoje poslovne procese prenesti v oblak, zavedajo največjih tveganj, ki jih prinaša RO, in se skušajo pred njimi ustrezno zavarovati. Prav tako anketa potrjuje formalno spoštovanje zakonskih določil. Na podlagi teh ugotovitev lahko na

začetku postavljeno hipotezo, da je obdelava osebnih podatkov v oblaku varna, formalno potrdim, za vsebinsko potrditev pa bi bilo potrebno nadaljnje raziskovanje o tem, ali so vsi podatki, ki se prenašajo v RO, ustrezno šifrirani, ali so gesla za zaščito dostopa ustrezna (najmanj štirinajstmestna) in ali so strežniki locirani na mestih, ki so varna, podatki, ki se shranjujejo, pa ustrezno dodatno zavarovani (»backup«). Visoka stopnja varnosti je še zlasti pomembna za revizijske družbe, ki razpolagajo z osebnimi podatki velikega števila naročnikov. Zato skrb za varnost podatkov, s katerimi razpolagajo, ni nič manj pomembna kot skrb za opravljanje revizijskih postopkov v skladu z Mednarodnimi standardi revidiranja. Čas bo pokazal, ali so revizijske družbe prestale preizkus, ki ga je prinesel RO.

3.3 Primerjava rezultatov anketiranja z mednarodno raziskavo revizijske mreže KPMG

Revizijska mreža KPMG je leta 2013 v prispevku z naslovom *The cloud takes shape* predstavila rezultate mednarodne raziskave, ki jo je izvedla leta 2012 v 16 državah po svetu (v Avstraliji, Braziliji, Kanadi, Franciji, Nemčiji, Indiji, Izraelu, Italiji, Japonski, Kitajski, Nizozemski, Savdski Arabiji, Singapurju, Združenih arabskih emiratih, Veliki Britaniji in ZDA). Gre za razvite in manj razvite države. Raziskavo je izvedla skupaj s partnerjem *Forbes Insight*. Namen raziskave pa je bil ugotoviti, kakšno je stanje in vpliv oblaka po svetu.

3.3.1 Podobnosti in razlike

Raziskava, ki jo je izvedla revizijska mreža KPMG (v nadaljevanju mednarodna raziskava), je bila izvedena v različnih državah po svetu. Moja raziskava pa je bila izvedena samo za Slovenijo. Glede na vzorec v mednarodni raziskavi (674 enot) je moj vzorec, ki je vseboval 167 enot, velik, saj je bila moja raziskava opravljena za zelo majhno državo v svetovnem okviru.

Mednarodna raziskava je pokazala, da je za podjetja po svetu ključen cilj, ki ga hočejo doseči z oblakom, zmanjšanje stroškov. Drugi najpomembnejši cilj je hitrost sprejetja oblaka v njihov poslovni proces, tretji cilj pa nov način vstopa na trg.

Slovenska podjetja so glede glavnega cilja oblaka primerljiva s podjetji v mednarodnem prostoru. Na slikah 7 in 8 je vidno, da je za slovenska podjetja najpomembnejši cilj znižanje stroškov. Tudi pri drugem cilju prihaja zgolj do manjših razlik, saj je za slovenska podjetja drugi najpomembnejši cilj preoblikovanje poslovnega procesa, kar je primerljivo z mednarodno raziskavo. Slovenski vzorec nekoliko odstopa od mednarodne raziskave v povezavi s tretjim ciljem, ki je pri nas usmerjen v izboljšanje usklajenosti s strankami oz. naročniki, v mednarodnem prostoru pa v nov način vstopa na trg. Vsekakor pa sta tudi ta dva cilja med seboj povezana.

Tako tuja kot tudi slovenska podjetja soglašajo, da v današnjem okolju RO prinaša večjo učinkovitost in prihranke.

Mednarodna raziskava kaže, da so največji izzivi RO povezani z izvajanjem. Ena tretjina vprašanih je ugotovila, da so bili stroški izvedbe, prehoda in integracije bistveno višji, kot so sprva pričakovali. Drugi pomemben izziv v mednarodnem okolju pa je bila integracija obstoječe IT-infrastrukture z oblakom. Omenjeni izziv je bil tudi za slovenska podjetja eden glavnih izzivov (glejte slike 11 in 12), čeprav slovenska podjetja tega izziva ne postavljajo na prvo mesto. Zanje predstavlja najpomembnejši izziv izguba podatkov in zasebnosti, iz česar bi se dalo sklepati, da podjetja še ne čutijo, da je v ponujene storitve RO vgrajena zadostna stopnja varnosti. Poleg tega revizijske družbe (bolj kot ostala podjetja) izpostavljajo tveganje kraje intelektualne lastnine.

Velika zaskrbljenost glede storitev v oblaku se kaže tudi pri izgubi kontrole, do katere lahko pride ob selitvi podatkov in procesov v oblak. Ta problem izpostavljajo predvsem ameriška podjetja, ki so glede storitev RO bolj izkušena kot druga. Na slikah 11 in 12 je razvidno, da je to tudi za slovenska podjetja eden ključnih problemov.

Podjetja po svetu so ocenila, da imajo najmanj znanja na področju integracije oblaka z obstoječo infrastrukturo. Podoben problem imajo tudi slovenska podjetja, vendar pri tem ne gre za področje, ki izrazito izstopa, ampak je problem usposobljenosti dokaj enakomerno porazdeljen med področja 5 (obvladovanje stroškov izvedbe, prehoda in integracije), 6 (merjenje donosnosti naložbe), 7 (ustreznost presoje zaradi pomanjkanja standardov med ponudniki), 9 (integracija z obstoječo infrastrukturo) in 10 (obvladovanje negotovosti, povezane z obljubami o realizaciji RO v okolju), izstopa pa področje 8, ki predstavlja pomanjkljivo usposobljenost v okolju pomanjkanja celovite ponudbe. Za slovenske revizijske družbe je usposobljenost manj problematična, osredotočene so predvsem na integracijo z obstoječo infrastrukturo in na predvidevanje negotovosti, povezane z obljubami o realizaciji RO v okolju (slike 13 in 14). Tako tuja kot tudi slovenska podjetja, med njimi še posebej revizijske družbe, se čutijo najbolj usposobljena pri zagotavljanju skladnosti z zakoni in drugimi predpisi.

Kljub temu pa podjetja v storitvah RO vidijo veliko pozitivnih učinkov, saj nameravajo svoje poslovne procese delno oz. v celoti prenašati v oblak tudi v prihodnje, s tem pa tudi občutljive podatke.

Mednarodna raziskava je pokazala, da največ podjetij uporablja RO na področjih človeških virov (HRM), upravljanja z informacijskim sistemom, elektronske pošte, prodaje in marketinga ter odnosov s strankami. Treba je opozoriti, da je bila ta raziskava opravljena leta 2012 in se je do danes lahko že marsikaj spremenilo. Poslovna področja, ki naj bi jih podjetja najbolj prenašala v oblak v naslednjih 18 mesecih po raziskavi, pa so bila: davki, oskrbovalna veriga, upravljanje s spletnimi vsebinami, poslovne analize, računovodstvo in finance. Slovenske revizijske družbe in ostala podjetja se po prenosih poslovnih področij v oblak razlikujejo. Revizijske družbe najpogosteje uporabljajo RO za področja človeških virov, upravljanje z informacijskimi viri in elektronsko pošto, medtem ko je pri ostalih podjetjih uporaba RO enakomernije porazdeljena med različnimi področji. Med najpogosteje prenesenimi področji v naslednjih 18 mesecih bosta pri slovenskih revizijskih družbah predvidoma področji računovodstva in financ ter poslovnih analiz, pri ostalih podjetjih pa področji človeških virov in odnosov s strankami.

3.3.2 Sklepne ugotovitve

Na splošno so rezultati moje raziskave podobni rezultatom mednarodne raziskave, le na določenih področjih prihaja do manjših razlik. Glede na to, da je bila mednarodna raziskava izvedena že leta 2012, moja pa v letu 2015, sem pričakovala, da bodo razlike večje. Na drugi strani pa so izidi raziskave dokaz, da so problemi, s katerimi se soočamo pri nas, primerljivi s problemi v svetovnem okviru, kar obenem kaže tudi na primerljivo raven razvitosti področja RO.

SKLEP

Računalništvo v oblaku za razvite države po svetu postaja nekaj vsakdanjega. Multinacionalni, kot sta Google in Microsoft, namreč ponujata storitve v oblaku že nekaj let. Gre za koncept, ki ga podjetja vse pogosteje uporabljajo pri svojem poslovanju. Tudi slovenska podjetja počasi vpeljujejo oblak v svoje poslovanje, kar je vidno iz rezultatov raziskave. Pri tem revizijske družbe izstopajo, saj so uporabi storitev RO bolj naklonjene kot ostala podjetja. Skoraj polovica anketiranih slovenskih podjetij (47 %) storitev RO še ne uporablja.

Kot je pokazala raziskava, je eden glavnih problemov RO varnost. Sem sodi tudi varstvo osebnih podatkov. Z uporabo storitev RO se namreč vse več osebnih podatkov prenese v oblak. Podjetja, še posebej pa revizijske družbe, morajo biti zato zelo previdna, da imajo te podatke ustrezno varovane.

Kljub problemu varnosti pa revizijske družbe najpogosteje v oblak prenašajo ravno področja, kjer se shranjuje velika količina osebnih podatkov. Ta področja so človeški viri (HRM), elektronska pošta in upravljanje z informacijskim sistemom. Po drugi strani pa so prav za revizijske družbe največja tveganja na področju uporabe RO povezana z možno izgubo podatkov in zasebnosti, z možno izgubo kontrole, s splošno varnostjo in z možno krajo intelektualne lastnine. Čeprav se zdi, da s spoštovanjem določil ZVOP-1 revizijske družbe obvladujejo tovrstna tveganja, kar potrjuje moja hipoteza (Obdelava osebnih podatkov v oblaku je varna), pa deklarirano spoštovanje zakonskih določil ni nobeno zagotovilo za to, da so vsi podatki, ki se prenašajo v RO, ustrezno šifrirani, da so gesla za zaščito dostopa dovolj dolga (najmanj štirimestna) in vsebujejo ustrezno kombinacijo alfa numeričnih znakov in da so strežniki locirani na mestih, ki so varna, podatki, ki se shranjujejo, pa ustrezno dodatno zavarovani (»backup«). Zato je moje magistrsko delo izziv za nadaljnje raziskave na teh področjih.

Čas bo pokazal, ali so revizijske družbe prestale preizkus, ki ga je prinesel RO. Množična uporaba RO pa bo z leti najverjetneje privedla do tega, da bo morala zakonodaja biti tudi

na področju varstva osebnih podatkov mnogo bolje prilagojena uporabnikom v konkretni pravni ureditvi.

LITERATURA IN VIRI

1. Avram, M. G. (2014). Advantages and challenges of adopting cloud computing from an enterprise perspective. *Procedia Technology*, (12), 529–534.
2. Bešter, T. (2011). Računalništvo v oblaku. *Knjižničarske novice*, 21(12), 22–25. Najdeno 11. januarja 2015 na spletnem naslovu <http://www.nuk.uni-lj.si/knjiznicarskenovice/v2/podrobnostClanek.aspx?id=552>
3. Bervar, J. (2013). NIL-ov vodnik po storitvah računalništva v oblaku. Najdeno 11. januarja 2015 na spletnem naslovu <http://www.nil.si/assets3554/wp-content/uploads/2013/04/nil-ov-vodnik-po-oblaku.pdf>.
4. Buyya, R., Yeo, C. S., Venugopal, S., Broberg, J., & Brandic, I. (2009). Cloud Computing and Emerging IT Platforms: Vision, Hype, and Reality for Delivering Computing as the 5th Utility. *Future Generation of Computer Systems*, (25), 599–616.
5. Chou, D. C. (2015). Cloud computing: A value creation model. *Computer Standards & Interfaces*, (38), 72–77.
6. Center for Cloud Computing. (2015). What is cloud computing? Najdeno 8. januarja 2015 na spletnem naslovu <http://www.cloud.si/cloud/>.
7. Čebulj, J., & Žurej, J. (2005). *Varstvo osebnih podatkov in informacije javnega značaja*. Ljubljana: Nebra.
8. Datenschutzgesetz 2000–DSG 2000 (Bundesgesetz über den Schutz personenbezogener Daten). (1999) Najdeno 24. februarja 2015 na spletnem naslovu <https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=bundesnormen&Gesetzesnummer=10001597>.
9. Direktiva 95/46/ES (2015). Direktiva 95/46/ES Evropskega parlamenta in Sveta z dne 24. oktobra 1995 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov. Najdeno 7. februarja 2015 na spletnem naslovu https://www.ip-rs.si/fileadmin/user_upload/Pdf/razno/Direktive_E_parlament_a_in_Sveta.pdf.
10. EuroCloud Slovenija (2012, februar). EuroCloud vodič po področju računalništva v oblaku. EuroCloud vodič po področju računalništva v oblaku. Najdeno 31. januarja 2015 na spletnem naslovu <http://eurocloud.si/wp-content/uploads/EuroCloud-smernice-prevedeno-in-prilagojeno1.pdf>.
11. Europa. (2011, februar). Varstvo osebnih podatkov. Povzetki zakonodaje EU. Najdeno 1. februarja 2015 na spletnem naslovu http://europa.eu/legislation_summaries/information_society/data_protection/l14012_sl.htm.
12. Europa. (2015, februar). Uredbe, direktive in drugi akti. Pravo EU. Najdeno 7. februarja 2015 na spletnem naslovu http://europa.eu/eu-law/decision-making/legal-acts/index_sl.htm.
13. Explanatory Document on the Processor Binding Corporate Rules. (2013, april). Najdeno 8. januarja 2015 na spletnem naslovu [68](http://ec.europa.eu/justice/data-</div><div data-bbox=)

- protection/article-29/documentation/opinion-recommendation/files/2013/wp204_en.pdf.
14. Federal Data Protection Act (2015, februar). Najdeno 20. februarja 2015 na spletnem naslovu http://www.gesetze-im-internet.de/englisch_bdsf/federal_data_protection_act.pdf
 15. Furuncu, E., & Sogukpinar, I. (2015). Scalable risk assessment method for cloud computing using game theory (CCRAM). *Computer Standards & Interfaces*, (38), 44–50.
 16. Gemini (2015). Modeli računalništva v oblaku. Storitveni modeli računalništva v oblaku. Najdeno 11. januarja 2015 na spletnem naslovu <http://www.geministyle.si/print/racunalnistvo/splosno/racunalnistvo-v-oblaku-4.html>.
 17. Hashem, I. A. T., Yaqoob, I., Anuar, N. B., Mokhtar, S., Gani, A., & Khan, S. U., (2015). The rise of “big data” on cloud computing: Review and open research issues. *Information Systems*, (48), 98–115.
 18. Höllwarth, T. (2012). *Pot v oblak*. Ljubljana: Pasadena.
 19. Informacijski pooblaščenec (2012, 15. junij). Varstvo osebnih podatkov & računalništvo v oblaku. Najdeno 8. januarja 2015 na spletnem naslovu https://www.ip-rs.si/fileadmin/user_upload/Pdf/smernice/Smernice_rac_v-oblaku.pdf.
 20. Informacijski pooblaščenec (2015). Varstvo osebnih podatkov. Najdeno 18. januarja 2015 na spletnem naslovu <https://www.ip-rs.si/pogosta-vprasanja/varstvo-osebni-podatkov/#c301>.
 21. Knuth, G. (2009, 13. oktober). Why I think "cloud" is a buzzword encapsulating all other buzzwords. A Buzzword Cloud, if you will. Najdeno 18. januarja 2015 na spletnem naslovu <http://www.brianmadden.com/blogs/gabeknuth/archive/2009/10/13/why-i-think-quot-cloud-quot-is-a-buzzword-encapsulating-all-other-buzzwords-a-buzzword-cloud-if-you-will.aspx>.
 22. Krašovec, B. M., Bogataj, J., Duralija, J., Jerše, A., Kalan, E., Šumah, K. K., Kraigher, T., Pavšič, B., & Tomšič, A. (2013). Letno poročilo informacijskega pooblaščenca. Najdeno 25. januarja 2015 na spletnem naslovu https://www.ip-rs.si/fileadmin/user_upload/Pdf/porocila/Letno_porocilo_2013_Web.pdf.
 23. Law on legal protection of personal data. *February 2008, No. X-1444*. Najdeno 28. februarja 2015 na spletnem naslovu http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=315633.
 24. Marks, E. A., & Lozano, B. (2010). *Executive's Guide to Cloud Computing*. Hoboken, New Jersey: John Wiley & Sons, Inc.
 25. Mell, P. & Grance, T. (2011, september). The NIST Definition of Cloud Computing. Recommendations of the National Institute of Standards and Technology. Najdeno 8. januarja 2015 na spletnem naslovu <http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf>.
 26. Ministrstvo za notranje zadeve (2015). Osebni in tajni podatki. Najdeno 18. januarja 2015 na spletnem naslovu http://www.mnz.gov.si/si/mnz_zasvas/osebni_in_tajni_podatki.

27. Musar, P. N. (2012, 15. junij). Smernice glede varstva osebnih podatkov pri računalništvu v oblaku. Najdeno 31. januarja 2015 na spletnem naslovu <https://www.ip-rs.si/novice/detajl/informacijski-pooblastenec-izdal-smernice-glede-varstva-osebnih-podatkov-pri-racunalnistvu-v-obl/?cHash=d7a663aed23ce669459cb407f4be5c56>
28. Musar, P. N., Prelesnik, M., & Bien, M. (2006). *Varstvo osebnih podatkov: vstop v zasebnost prepovedan*. Informacijski pooblaščenec. Ljubljana: Narodna in univerzitetna knjižnica Ljubljana.
29. Plummer, D. C. (2009, 27. januar). Experts Define Cloud Computing: Can we get a Little Definition in our definitions? Najdeno 8. januarja 2015 na spletnem naslovu http://blogs.gartner.com/daryl_plummer/2009/01/27/experts-define-cloud-computing-can-we-get-a-little-definition-in-our-definitions/.
30. Pohorec, S. (2011, 28. september). Skrite pasti računalništva v oblaku. *MonitorPro*. Najdeno 9. januarja 2015 na spletnem naslovu <http://www.monitorpro.si/106191/praksa/skrite-pasti-racunalnistva-v-oblaku/>.
31. Register revizijskih družb (2015, 21. julij). Najdeno 21. julija 2015 na spletnem naslovu <http://www.si-revizija.si/revizijskedruzbe/revizijske-druzbe>.
32. Rouse, M. (2010, 21. december). Cloud Computing. Najdeno 8. januarja 2015 na spletnem naslovu <http://searchcloudcomputing.techtarget.com/definition/cloud-computing>.
33. Sedlar, U., Bešter, J., & Kos, A. (2011). *Računalništvo v oblaku v telekomunikacijah in primeri uporabe*. Ljubljana: Laboratorij za telekomunikacije, Fakulteta za elektrotehniko, Univerza v Ljubljani.
34. The Act on Processing of Personal Data. (Act No. 429 of 31 May 2000). Najdeno 25. februarja 2015 na spletnem naslovu <http://www.datatilsynet.dk/english/>.
35. The cloud takes shape. Global cloud survey: the implementation challenge. (2013). Najdeno 27. januarja 2015 na spletnem naslovu <https://www.kpmg.com/FR/fr/IssuesAndInsights/ArticlesPublications/Documents/the-cloud-takes-shape.pdf>.
36. Tomšič, A. (2011). Zasebnost v oblaku. *Konferenca ARNES, str. 15*. Najdeno 20. januarja 2015 na spletnem naslovu https://skupnost.sio.si/sio_arhiv/sirikt/www.sirikt.si/fileadmin/Sirikt2011/konferenca-arnes/clanki/tomsic-zasebnost-v-oblaku.pdf.
37. Ustava Republike Slovenije. *Uradni list RS* št. 33/91-I, 42/97, 66/2000, 24/03, 69/04, 68/06 in 47/13.
38. Zakon o varstvu osebnih podatkov. *Uradni list RS* št. 94/2007 - UPB1.
39. Zakrajšek, G. (2011, 13. marec). Vpliv računalništva v oblaku na organizacije. Najdeno 11. januarja 2015 na spletnem naslovu <http://esistemi.si/component/content/article/45-google-apps/110-vpliv-raunalnitva-v-oblaku-na-organizacije>.

PRILOGA

Priloga: Anketni vprašalnik

1. Ali v vašem podjetju pri obdelavi in shranjevanju osebnih podatkov uporabljate storitve računalništva v oblaku (v nadaljevanju RO)?

- a) Da.
- b) Deloma.
- c) Še ne, vendar se na to pripravljamo.
- d) Ne, vendar ne izključujemo uporabe v prihodnosti.
- e) Ne.

Če ste na zgornje vprašanje odgovorili z NE (odgovor pod e), odgovorite samo še na 2. vprašanje.

Če na zgornje vprašanje niste odgovorili z NE (odgovori pod a, b, c, d), 2. vprašanje preskočite in izpolnite anketo do konca.

2. Kaj vas odvrača od uporabe RO?

- a) Nezanesejliv dostop do interneta.
- b) Pomanjkanje varnosti pri uporabi RO.
- c) Uporaba interne računalniške mreže.
- d) Dodatni stroški uvajanja RO.
- e) Zahteve naših strank.

3. Kateri so ključni cilji, na katerih temelji vaš odnos do RO?

- a) Znižanje stroškov.
- b) Hitrost sprejetja.
- c) Nov način vstopa na trg.
- d) Preoblikovanje poslovnega procesa.
- e) Izboljšati usklajenost/interakcijo s strankami/naročniki.

4. Ali se strinjate, da v današnjem okolju RO zagotavlja večjo učinkovitost in prihranke?

- a) Povsem se strinjam.
- b) Se strinjam.
- c) Mogoče.
- d) Se ne strinjam.
- e) Se sploh ne strinjam.

5. Kateri od naštetih izzivov je za vas ključen pri sprejetju RO?

Izzivi	DA	NE
1. Previsoki stroški izvedbe, prehoda in integracije.		
2. Integracija z obstoječo infrastrukturo.		
3. Izguba podatkov in zasebnosti.		
4. Izguba kontrole.		
5. Nepoznavanje prihodnosti povpraševanja (povezano s stroški).		
6. Pomanjkanje standardov med ponudniki RO.		
7. Splošno tveganje varnosti.		
8. Tveganje kraje intelektualne lastnine.		
9. Skladnost z zakoni in drugimi predpisi.		
10. Preglednost operativnih kontrol in podatkov.		

6. Kako usposobljeno je vaše podjetje pri premagovanju naslednjih izzivov?

Izzivi/lestvica	1 čisto nič	2 skoraj nič	3 malo	4 srednje	5 zelo
Skladnost z zakoni in drugimi predpisi.					
Negotovost davčnih posledic.					
Nezadovoljstvo s ponudbo/predstavitvijo/ceno prodajalcev.					
Tveganje razpoložljivosti sistema in neprekinjenosti poslovanja.					
Previsoki stroški izvedbe, prehoda in integracije.					
Merjenje donosnosti naložbe.					
Pomanjkanje standardov med ponudniki oblakov.					
Pomanjkanje celovite ponudbe.					
Integracija z obstoječo infrastrukturo.					
Negotovost glede obljub o realizaciji RO v okolju.					

7. Kako zahtevno je po vašem mnenju vsako od naštetih področij?

Področje/lestvica	1 čisto nič zahtevno	2 skoraj nič zahtevno	3 manj zahtevno	4 zahtevno	5 zelo zahtevno
Izguba podatkov in tveganje zasebnosti.					
Splošno tveganje varnosti.					
Tveganje kraje intelektualne lastnine.					
Skladnost z zakoni in drugimi predpisi.					
Tveganje razpoložljivosti sistema in neprekinjenosti poslovanja.					

8. Na katerih področjih vašega poslovanja že uporabljate RO?

Funkcije	Že uporabljamo (DA)	Še ne uporabljamo (NE)
Človeški viri (HRM)		
IT-management		
Elektronska pošta		
Prodaja, marketing		
Odnos s strankami		
Oskrbovalno veriga in logistika		
Računovodstvo in finance		
Poslovne analize		
Upravljanje varnosti		
Upravljanje s spletnimi vsebinami		
Oskrbovalna veriga		
Davki		
Proizvodnja		

9. Katera področja vašega poslovanja boste v prihodnje (čez 18 mesecev) preselili v oblak?

Funkcije	Bomo prenesli (DA)	Ne bomo prenesli (NE)
Človeški viri (HRM)		
IT-management		
Elektronska pošta		
Prodaja, marketing		
Odnosi s strankami		
Oskrbovalno veriga in logistika		
Računovodstvo in finance		
Poslovne analize		
Upravljanje varnosti		
Upravljanje s spletnimi vsebinami		
Oskrbovalna veriga		
Davki		
Proizvodnja		

10. Eno glavnih vprašanj pri uporabi RO je varstvo osebnih podatkov. Ali imate osebne podatke zavarovane na način, ki je opredeljen v 24. členu ZVOP-1?

24. člen

(1) Zavarovanje osebnih podatkov obsega organizacijske, tehnične in logično-tehnične postopke in ukrepe, s katerimi se varujejo osebni podatki, preprečuje slučajno ali namerno nepooblaščen uničevanje podatkov, njihova sprememba ali izguba ter nepooblaščen obdelava teh podatkov tako, da se:

- 1. varujejo prostori, oprema in sistemsko programska oprema, vključno z vhodno-izhodnimi enotami;*
 - 2. varuje aplikativna programska oprema, s katero se obdelujejo osebni podatki;*
 - 3. preprečuje nepooblaščen dostop do osebnih podatkov pri njihovem prenosu, vključno s prenosom po telekomunikacijskih sredstvih in omrežjih;*
 - 4. zagotavlja učinkovit način blokiranja, uničenja, izbrisa ali anonimiziranja osebnih podatkov;*
 - 5. omogoča poznejše ugotavljanje, kdaj so bili posamezni osebni podatki vneseni v zbirko osebnih podatkov, uporabljeni ali drugače obdelani in kdo je to storil, in sicer za obdobje, ko je mogoče zakonsko varstvo pravice posameznika zaradi nedopustnega posredovanja ali obdelave osebnih podatkov.*
- (2) V primeru obdelave osebnih podatkov, ki so dostopni preko telekomunikacijskega sredstva ali omrežja, morajo strojna, sistemska in aplikativna programska oprema zagotavljati, da je obdelava osebnih podatkov v zbirkah osebnih podatkov v mejah pooblastil uporabnika osebnih podatkov.*
- (3) Postopki in ukrepi za zavarovanje osebnih podatkov morajo biti ustrezni glede na tveganje, ki ga predstavlja obdelava in narava določenih osebnih podatkov, ki se obdelujejo.*
- (4) Funkcionarji, zaposleni in drugi posamezniki, ki opravljajo dela ali naloge pri osebah, ki obdelujejo osebne podatke, so dolžni varovati tajnost osebnih podatkov, s katerimi se seznanijo pri opravljanju njihovih funkcij, del in nalog. Dolžnost varovanja tajnosti osebnih podatkov jih obvezuje tudi po prenehanju funkcije, zaposlitve, opravljanja del ali nalog ali opravljanja storitev pogodbene obdelave.*

- a) Da
- b) Ne