

**UNIVERZA V LJUBLJANI
FAKULTETA ZA UPRAVO**

**DIPLOMSKO DELO
VISOKOŠOLSKEGA PROGRAMA PRVE STOPNJE UPRAVA**

RAVNANJE Z ZAUPNIMI PODATKI

Katja Mavhar

Ljubljana, oktober 2010

UNIVERZA V LJUBLJANI
FAKULTETA ZA UPRAVO

DIPLOMSKO DELO
VISOKOŠOLSKEGA PROGRAMA PRVE STOPNJE UPRAVA

RAVNANJE Z ZAUPNIMI PODATKI

Kandidatka: Katja Mavhar
Številka indeksa: 04034039

Mentor: doc. dr. Janez Stare

Ljubljana, oktober 2010

IZJAVA O AVTORSTVU DIPLOMSKEGA DELA IN NAVEDBA LEKTORJA

Podpisana Katja Mavhar, študentka Visokošolskega strokovnega študijskega programa Uprava I. stopnja, z vpisno številko 04034039, sem avtorica diplomskega dela z naslovom: »Ravnanje z zaupnimi podatki«.

S svojim podpisom zagotavljam, da:

- je predloženo delo izključno rezultat mojega lastnega raziskovalnega dela,
- sem poskrbela, da so dela in mnenja drugih avtorjev oz. avtoric, ki jih uporabljam v predloženem delu, navedena oz. citirana v skladu s fakultetnimi navodili,
- sem poskrbela, da so vsa dela in mnenja drugih avtorjev oz. avtoric navedena v seznamu virov, ki je sestavni element predloženega dela in je zapisan v skladu s fakultetnimi navodili,
- sem pridobila vsa dovoljenja za uporabo avtorskih del, ki so v celoti prenesena v predloženo delo in sem to tudi jasno zapisala v predloženem delu,
- se zavedam, da je plagiatorstvo – predstavljanje tujih del, bodisi v obliki citata bodisi v obliki skoraj dobesednega parafraziranja bodisi v grafični obliki, s katerim so tuje misli oz. ideje predstavljene kot moje lastne – kaznivo po zakonu (Zakon o avtorstvu in sorodnih pravicah, Ur. list RS, št. 21/95), kršitev pa se sankcionira tudi z ukrepi po pravilih Univerze v Ljubljani in Fakultete za upravo,
- se zavedam posledic, ki jih dokazano plagiatorstvo lahko predstavlja za predloženo delo in za moj status na Fakulteti za upravo,
- je elektronska oblika identična s tiskano obliko diplomskega dela ter soglašam z objavo dela v zbirki »Dela FU«.

Diplomsko delo je lektorirala: prof. slovenščine Nataša Črešnar.

Ljubljana, 2. 10. 2010

Katja Mavhar

POVZETEK

V diplomskem delu z naslovom Ravnanje z zaupnimi podatki so navedene vrste zaupnih podatkov in podroben opis, kako se ti podatki varujejo. Pri zaupnih podatkih je posebej pomembno, katere osebe imajo dostop do le-teh; to so upravičene in pooblaščne osebe. Zaupni podatki se morajo dobro varovati in hraniti. Pogosto prihaja do razkritja in zlorabe, zato so ob sumu zlorabe in izdaje zaupnih podatkov važni pravilni ukrepi. Da ne prihaja do razkritij in zlorab, je bistvena pravilna politika varovanja zaupnih podatkov, ki se zapiše v interni – notranji akt v organizaciji.

S pomočjo anketnega vprašalnika sem ugotovila, kakšnega mnenja so zaposleni glede varovanja zaupnih podatkov v njihovi organizaciji in ali so seznanjeni z predpisi, ki urejajo zaupne podatke.

Ključne besede: zaupni podatki, varovanje zaupnih podatkov, upravičene in pooblaščne osebe, obdelava in hranjenje zaupnih podatkov, varnostna politika zaupnih podatkov.

SUMMARY

In my diploma paper with title Handle with confidential information there are listed numerous types of confidential information and a detailed description of how these information are protected. With confidential information it is extremely important who access them. These are justified and authorized persons. Confidential information must be well kept and protected. Often it comes to disclosure and misuse of this information that is why it is very important to take proper action in order to protect these data. The most important is the correct policy to protect confidential information, which is written in internal act of the organization.

With the help of a questionnaire, I found out, what opinion have the employees about protection of confidential data and if they are familiar with the regulations, that edit these data.

KEY WORDS: confidential information, protection of classified information, justified and authorized person, data processing and storing confidential information, security policy of confidential information.

KAZALO

IZJAVA O AVTORSTVU DIPLOMSKEGA DELA IN NAVEDBA LEKTORJA	i
POVZETEK	II
SUMMARY	III
KAZALO PONAŽORITEV	VI
1 UVOD	1
2 OPREDELITEV IN VAROVANJE ZAUPNIH PODATKOV	4
2.1 SKRIVNOST IN TAJNOST	5
2.2 GOSPODARSKE ZAUPNOSTI	6
2.2.1 Poslovna skrivnost in varovanje poslovne skrivnosti	6
2.2.2 Bančna tajnost in varovanje bančne tajnosti	7
2.3 URADNE ZAUPNOSTI	8
2.3.1 Tajni podatek in varovanje tajnega podatka	8
2.3.1.1 Varnostno preverjanje v NATU	9
2.3.1.2 Varnostno preverjanje v EU	9
2.3.2 Državna tajnost in varovanje državne tajnosti	10
2.3.3 Uradna tajnost in varovanje uradne tajnosti	10
2.3.4 Davčna tajnost in varovanje davčne tajnosti	11
2.3.5 Poklicna tajnost in varovanje poklicne tajnosti	11
2.4 POSAMEZNIKOVE ZAUPNOSTI	12
2.4.1 Osební podatki in varstvo osebnih podatkov	12
3 RAVNANJE Z ZAUPNIMI PODATKI	14
3.1 OSEBE, KI LAHKO DOSTOPAJO DO ZAUPNIH PODATKOV	14

3.2 PRISTOJNOSTI IN PRAVICE INFORMACIJSKEGA POOBlašČENCA DO VPOGLEDA V ZAUPNE PODATKE.....	14
3.3 IZJAVA O VAROVANJU PODATKOV	15
3.4 DOVOLJENJA ZA DOSTOP DO ZAUPNIH PODATKOV	15
4 OBDELAVA IN HRANJENJE ZAUPNIH PODATKOV	17
4.1 SPREJEM IN POSREDOVANJE ZAUPNIH PODATKOV	17
4.2 VAROVANJE PROSTOROV Z ZAUPNIMI PODATKI.....	17
4.3 VAROVANJE OPREME Z ZAUPNIMI PODATKI.....	18
4.4 HRAMBA ZAUPNIH PODATKOV	19
4.5 RAZKRITJE IN ZLORABA ZAUPNIH PODATKOV	20
4.5.1 Motivi za zlorabo in izdajo zaupnih podatkov	20
4.5.2 Ukrepi ob sumu zlorabe in izdaje zaupnih podatkov	21
5 VARNOSTNA POLITIKA ZAUPNIH PODATKOV	23
5.1 POLITIKA VAROVANJA INFORMACIJ.....	23
6 RAZISKAVA: RAVNANJE Z ZAUPNIMI PODATKI.....	26
6.1 SESTAVA IN STRUKTURA ANKETE.....	26
6.2 PREDSTAVITEV REZULTATOV	27
6.3 KONČNE UGOTOVITVE.....	34
7 ZAKLJUČEK	36
LITERATURA.....	38
VIRI	38

KAZALO PONAŽORITEV

SEZNAM GRAFIKONOV

Grafikon 1: Spol zaposlenih	27
Grafikon 2: Starost zaposlenih	27
Grafikon 3: Stopnja izobrazbe zaposlenih.....	28
Grafikon 4: Delovna doba zaposlenih	29
Grafikon 5: Predpisi, ki urejajo zaupne podatke.....	29
Grafikon 6: Sežnanjenost z dolžnostmi varovanja zaupnih podatkov.....	30
Grafikon 7: Zaščita prostorov in opreme, kjer se hranijo zaupni podatki	31
Grafikon 8: Varnostna politika.....	32
Grafikon 9: Razkritje, zloraba zaupnih podatkov s strani zaposlenih	32
Grafikon 10: Zaupni podatki so danes zelo ogroženi, zakaj?	33

SEZNAM SLIK IN TABEL:

Slika 1: Večnivojska varnostna politika	24
Tabela 1: Razdelitev skrivnosti in tajnosti v tri kategorije	6

PRILOGA

Priloga	39
---------------	----

1 UVOD

Z zaupnimi podatki in informacijami se srečujemo občasno. Predvsem jih srečamo takrat kadar opravljamo kakšne naloge za organizacijo, v kateri delamo in jih opredeli kot zaupne.

Zaupne podatke moramo varovati na poseben način zato, da se z morebitnim razkritjem ali zlorabo ne bi povzročile škodljive posledice organizaciji. Zaupni podatek se pojavlja v pisnih virih in v ustnem komuniciranju. Pomen zaupnih podatkov v dokumentarnem in arhivskem gradivu kaže na to, da vse stvari, dogodki, vsebine niso prosto dostopne različnim zainteresiranim skupinam ali posamezniku ampak velja načelo, da se smejo s podatki seznaniti samo upravičeni ter pooblaščen posamezniki, kar je bistvo za ravnanje z zaupnimi podatki. Zaupni podatki so širši javnosti nedostopni in posebej varovani z modernimi fizičnimi in tehničnimi sredstvi.

Varovanje podatkov je zaradi hitrega in nepredvidljivega razvoje informacijskih tehnologij ena izmed vse bolj pomembnih usmeritev tako v podjetjih, kot tudi za državne ustanove. Nove vrste groženj, kot so terorističnih napadi, kriminalna dejanja povezana z Internetom in računalniškimi goljufijami, računalniškimi virusi, nove potrebo po neprekinjenem poslovanju, izpostavljajo vprašanja, kako varovati informacije, kje začeti, kakšne smernice in standarde pri tem uporabiti.

Izhodišče diplomskega dela je, da se na podlagi anketnega vprašalnika ugotovi, kako so z zaupnimi podatki v organizaciji seznanjeni zaposleni.

Namen diplomskega dela je, da se opredeli kateri so zaupni podatki, zakonodajo, ki ureja zaupne podatke, pojma skrivnosti in tajnosti, osebe, ki imajo dostop do zaupnih podatkov, obdelavo in hrambo zaupnih podatkov, razkritje in zlorabe zaupnih podatkov, motive za razkritje in zlorabo ter ukrepe ob sumu zlorabe in izdaje zaupnih podatkov ter varnostno politiko zaupnih podatkov.

Cilji, ki naj bodo doseženi v diplomskem delu, so, da z anketo, ki se bo razdelila med uslužbence, ugotovi, ali so uslužbenci dovolj seznanjeni z zakonodajo, ki ureja zaupne podatke; kako so uslužbenci v organizaciji seznanjeni z varovanjem zaupnih podatkov (priročnik, brošura, interni akti, pogodba o zaposlitvi, izobraževanje ...); ali imajo v organizaciji varno zaščitene zaupne podatke; ali imajo napisano politiko o varovanju informacij (varnostno politiko); kateri so razlogi, da pride do razkritja ali izdaje zaupnih podatkov.

Izvedla se je raziskava na podlagi izpolnjevanja anketnega vprašalnika z vnaprej zastavljenimi vprašanji. Anketni vprašalnik bo služil kot osnova za analizo stanja na področju zaupnih podatkov.

Cilji se glasijo:

- **cilj 1** se glasi: 50 % uslužbencev na svojem delovnem mestu trdi, da so zelo dobro seznanjeni s predpisi, ki urejajo zaupne podatke,
- **cilj 2**: največ anketirancev meni, da imajo v organizaciji zelo dobro zaščitene prostore in opremo, kjer se hranijo zaupni podatki,
- **cilj 3**: organizacija ima napisano politiko o varovanju informacij – varnostno politiko.

Obravnavanje tematike diplomskega dela *Ravnanje z zaupnimi podatki* zahteva uporabo različnih metod, ki so medsebojno prilagojene in usklajene. V nalogi so uporabljeni primarni viri (zakoni, pravilniki, direktive, uredbe), sekundarni viri (knjige, članki, raziskovalna poročila) in tudi terciarni viri (internet, diplomske naloge na podobno temo).

Diplomsko delo je sestavljeno iz dveh delov. Prvi del je teoretičen. Omogoča lažje razumevanje vsebine diplomskega dela. Drugi del je analitičen, v katerem se analizira anketni vprašalnik ter potrdijo ali zavržejo cilji, ki so se zadali na začetku diplomskega dela.

Prvo poglavje predstavlja uvod, v katerem je opisano izhodišče diplomskega dela, namen in cilj raziskave. Navedene so metode in struktura diplomskega dela.

Drugo poglavje s teoretično opredelitvijo omogoča lažje razumevanje vsebine dela. Navedene so vrste zaupnih podatkov, ki se uporabljajo v Sloveniji, ter zakoni, ki te zaupnosti urejajo. Skrivnost in tajnost se razdelita v tri skupine: gospodarske, uradne in posameznikove zaupnosti. V vse tri skupine spadajo različni zaupni podatki, katere podrobneje opisujem, ter navajam, kako se ti zaupni podatki varujejo.

Tretje poglavje predstavlja ravnanje z zaupnimi podatki, katere osebe imajo dostop do zaupnih podatkov, izjava o varovanju zaupnih podatkov, ki jo morajo podpisati zaposleni, ki imajo pravico dostopa do zaupnih podatkov, varnostno preverjanje oseb (pomembno je, da je uslužbenec taka oseba, ki jo poznamo kot osebno stabilno, lojalno, visoko načelno in moralno in za katero zagotovo vemo, da ne bi mogla izkoriščati pridobljenih zaupnih podatkov za namene nezakonitih ali kaznivih dejanj), dovoljenje za dostop do zaupnih podatkov, ki se zapiše v odločbo. Dovoljenja se izdajo po naslednjih stopnjah tajnosti (strogo zaupno, tajno in zaupno).

Četrto poglavje opisuje obdelavo in hrambo zaupnih podatkov. Pomemben je sprejem in posredovanje zaupnih podatkov, kako se varujejo prostori in oprema z zaupnimi podatki, roki hrambe zaupnih podatkov, razkritje in zlorabe zaupnih podatkov ter navedba najpogostejših motivov, zakaj pride do zlorabe in izdaje ter kakšni naj bodo ukrepi ob sumu zlorabe in izdaje zaupnih podatkov.

Peto poglavje obravnava varnostno politiko zaupnih podatkov. Varnostna politika je najpomembnejši interni dokument vsake organizacije. Varnostna politika zaupnih

podatkov se razdeli na krovno varnostno politiko, varnostno politiko za posamezna področja ter operativna navodila, interni standardi in postopki za delo.

Šesto, poglavje predstavlja obdelavo anketnega vprašalnika. Anketa je bila razdeljena med uslužbenci v javni upravi. Vsa vprašanja so prikazana v grafikonu, pod katerim je analiza vprašanj. V tem poglavju so ovrednoteni doseženi cilji.

V zadnjem, sedmem poglavju je zapisan zaključek diplomskega dela.

2 OPREDELITEV IN VAROVANJE ZAUPNIH PODATKOV

Z zaupnostjo se varujejo informacije ali podatki o nekem predmetu. Podatek in informacija sta dva različna pojma. Pri informaciji gre za celoto vrednosti o določenem dejstvu, dogodku, stvari, procesu, ideji, dejavnosti ali področju. S podatkom pa označujemo dejstvo, ki o določeni stvari kaj konkretnije pove ali se nanj nanaša (Stare in Lavrič, 2008, str. 2).

Zaupni podatki družbe so podatki, ki so določeni kot zaupni in so tako pomembni, da bi z njihovo izdajo nastale ali bi očitno lahko nastale škodljive posledice za delovanje družbe in njegove koristi (Pravilnik o varovanju zaupnih in osebnih podatkov ter dokumentarnega gradiva, 6. člen).

V slovenski zakonodaji poznamo preko deset vrst poimenovanj zaupnosti, te niso poenotene niti glede označevanja niti glede hrambe. V zakonodaji lahko zasledimo izraza zaupno ali zaupnost, s katerim poimenujemo dostopnost in zavarovanje podatkov ob dejstvu, da se za tako opredeljene podatke zagotavlja dostop do njih le na podlagi načela potrebe in pravice po vedenju¹ (Stare in Lavrič, 2008, str. 2).

Slovenska zakonodaja pozna več poimenovanj zaupnosti (Lavrič, 2008, str. 3):

- **davčna tajnost** (urejeno v zakonu o davčnem postopku),
- **poklicna skrivnost** (urejeno v zakonu o zasebnem varovanju, zakonu o javnih uslužbencih in drugih predpisih),
- **bančna tajnost** (urejeno v bančnem kodeksu Združenja bank Slovenije, zakonu o bančništvu in v drugih predpisih),
- **poslovna skrivnost** (urejeno v zakonu o gospodarskih družbah, v zakonu o bankah in hranilnicah in v drugih predpisih),
- **osebni podatki** (urejeno v zakonu o varstvu osebnih podatkov),
- **tajni podatki** (urejeno v zakonu o tajnih podatkih),
- **uradna tajnost** (urejeno v zakonu o industrijski lastnini, v notranjih predpisih ministrstva ter v drugih predpisih),
- **vojaška tajnost** (urejeno v neusklajenih predpisih organov javne uprave),
- **državna tajnost** (urejeno v zakonu o slovenskih varnostno-obveščevalnih agencijah in v drugih predpisih),
- **industrijska skrivnost** (urejeno v notranjih predpisih gospodarskih družb),
- **zdravniška skrivnost** (urejeno v notranjih predpisih zdravstvenih organizacij).

¹ Potreba po vedenju (angl. need to know) je predpogoj za pridobivanje podatkov zaupne narave. Te izhajajo iz načela upravičene možnosti pridobivanja takih podatkov in se nanaša na delovno mesto, kjer se podatki potrebujejo za različne obdelave.

Informacije in podatki so poleg kapitala, ljudi, naravnih virov in znanja eno najpomembnejših virov organizacij, so sredstva z določeno vrednostjo, ki jo je potrebno ustrezno zaščititi. Varovanje informacij in podatkov se ščiti pred različnimi nevarnostmi, z namenom zagotoviti varno in neprekinjeno poslovanje ter omejiti poslovno škodo na najmanjšo možno raven. Varovanje informacij in podatkov obsega varovanje in zaščito vseh kritičnih, poslovno občutljivih, tajnih, osebnih in drugih občutljivih podatkov ter informacijske sisteme, ki so namenjeni obdelavi (oblikovanju, shranjevanju, spreminjanju, analiziranju ...) teh podatkov v organizaciji (Eršte, 2006, str. 30).

2.1 SKRIVNOST IN TAJNOST

Pojem *tajen* Slovar slovenskega knjižnega jezika (CD-rom) opredeli kot nekaj, kar »javnost, oblast ne ve: imeti taje sestanek; dogodki so ostali tajni; tajna organizacija; tajna radijska postaja; tajno društvo«. V drugem pomenu pa ga opredeli kot »s katerim se javnost, ljudje ne morejo seznaniti: tajno srečanje državnikov, skleniti tajni sporazum, tajna meddržavna pogodba; tajno sojenje, tajno glasovanje za katerega ve ozek krog ljudi«, obenem pa zopet poudari knjižno sopomenko *skrivnost*. Tajnost pa opiše kot »značilnost tajnega« (jamči tajnost glasovanja, zavarovati tajnost dopisovanja, podatki morajo ostati v tajnosti) ali kot nekaj, »kar je tajno« (ti podatki so tajnost, državna, poslovna, službena, vojaška tajnost oziroma skrivnost).

Skrivnost in tajnost v nekaterih zakonih regulirajo varovanje informacij in podatkov, ki so tako pomembni, da bi njihovo razkritje lahko škodovalo delovanju in izvajanju nalog organizacije ali celo interesom Republike Slovenije. Zato lahko namesto besede skrivnost in tajnost uporabljamo primernejši izraz – zaupnost (Lavrič, 2008, str. 3).

Zaupnost je opredelila Mednarodna organizacija za standardizacijo (ISO)² v ISO-17799. Kako jo zagotoviti, da so informacije dostopne le pooblaščenim osebam in je ena od temeljev informacijske varnosti.

Zaupnost se nanaša tudi na etična načela v zvezi z več poklici (npr. medicina, pravo, vera, novinarstvo)

(Wikipedia The Free Encyclopedia. Zaupnost. 11. 10. 2009).

V tabeli so navedene najpogostejše vrste skrivnosti in tajnosti iz zakonodaje, ki so razdeljene v tri kategorije zaupnosti, glede na mesto nastanka zaupnih podatkov. Navedeni sta tudi vojaška in državna tajnost, ki se v Sloveniji ne uporablja več, vsebinsko pa sodita v okolje policijskega in vojaškega delovanja.

² International Organization for Standardization; kratica ISO je mednarodno združenje organizacij za standardizacijo.

Tabela 1: Razdelitev skrivnosti in tajnosti v tri kategorije

Gospodarske zaupnosti	Uradne zaupnosti	Posameznikove zaupnosti
poslovna skrivnost	tajni podatki	osebni podatki
poslovna tajnost	uradna tajnost	
industrijska skrivnost	davčna tajnost	
informacijska skrivnost	vojaška tajnost	
bančna tajnost	državna tajnost	
znanstvena tajnost	zdravniška tajnost	
umetniška tajnost ...	poklicna skrivnost ...	

Vir: (Stare in Lavrič 2008, str. 2)

2.2 GOSPODARSKE ZAUPNOSTI

Gospodarske zaupnosti se uporabljajo pretežno v gospodarskih družbah in so pomembne za vsako organizacijo in njeno izkazovanje na trgu. Zavarovanje podatkov se zagotavlja znotraj družbe in pri potencialnemu pogodbeniku. Družba sprejme notranji (interni) akt za varovanje svojih zaupnih podatkov. Uslužbenci se z zaupnostjo seznani ob podpisu izjave ali s pogodbo o zaposlitvi (Stare in Lavrič, 2008, str. 3).

2.2.1 Poslovna skrivnost in varovanje poslovne skrivnosti

Poslovna skrivnost se je vsebinsko pojavila kot problem s pojavom podjetij. Pojem zasebne lastnine proizvodnih sredstev in svobodno delovanje trga sta ustvarila potrebo po varovanju določenih podatkov, pomembni za doseg gospodarskih prednosti podjetja, torej poslovne skrivnosti (Lavrič, 2006, str. 17).

Kateri podatki se štejejo za poslovno skrivnost, določa Zakon o gospodarskih družbah (v nadaljevanju ZGD-1). Za poslovno skrivnost se štejejo podatki, za katere tako določi družba s pisnim sklepom. S tem sklepom morajo biti seznanjeni družbeniki, delavci, člani organov in druge osebe, ki so poslovno skrivnost dolžne varovati. Ne glede na to ali so določeni s sklepi iz prejšnjega odstavka tega člena, se za poslovno skrivnost štejejo tudi podatki, za katere je očitno, da bi nastala občutna škoda, če bi zanje izvedela nepooblaščen oseba. Družbeniki, delavci, člani organov družbe in druge osebe so odgovorni za kršitev, če so vedeli, ali bi morali vedeti za tak značaj podatkov.

Za poslovno skrivnost se ne morejo določiti podatki, ki so po zakonu javni, ali podatki o kršitvi zakona ali dobrih poslovnih običajih (ZGD-1, 39. člen).

Družba s sklepom ali pravilnikom o poslovni skrivnosti opredeli tudi način varovanja poslovne skrivnosti, odgovornost oseb, zavezanih k njenemu varovanju ter z njimi seznanjeni družbenike, zaposlene, člane organov in druge osebe, ki so poslovno skrivnost dolžne varovati. To niso le osebe, ki so del organizacijske strukture družbe, pač pa tudi bivši družbeniki ali zaposleni, poslovni partnerji ali pa osebe, ki z družbo še niso vzpostavile poslovnega razmerja, se pa z njo dogovarjajo za sodelovanje. Poleg obveze varovanja poslovnih skrivnosti ZGD-1 tudi prepoveduje ravnanja, s katerimi bi osebe izven družbe skušale pridobiti podatke, ki so poslovna skrivnost družbe. Takšno ravnanje je v nasprotju z zakonom ali voljo družbe (Lavrič, 2006, str. 20).

V delovnem pravu se v zvezi s prepovedjo konkurence srečujemo s konkurenčno prepovedjo in s konkurenčno klavzulo. Konkurenčna prepoved pomeni, da delavec ne sme brez pisnega soglasja delodajalca za svoj ali tuj račun opravljati del oziroma sklepati poslov, ki sodijo v dejavnost, ki jo dejansko opravlja delodajalec in bi za delodajalca lahko pomenili konkurenco. Smisel konkurenčne prepovedi je varovanje delodajalčevega poslovnega interesa, zato bo delavec lahko opravljal takšna dela, če bo delodajalec s tem pisno soglašal.

Konkurenčna klavzula pomeni prepoved opravljanja konkurenčne dejavnosti po prenehanju pogodbe o zaposlitvi in se lahko dogovori samo v tistih primerih, ko delavec pri svojem delu ali v zvezi z njim pridobiva tehnična, proizvodna ali poslovna znanja ter zveze, ki so značilne za tega delodajalca in ki jih drugje delavec ne bi mogel pridobiti. Biti mora takšna, da prepreči opravljanje konkurenčne dejavnosti v določenem obdobju, s čimer zaščiti delodajalca, vendar mora biti to obdobje čim krajše, da se zaščiti interes delavca, ki je omejen pri izbiri zaposlitve (Sindikalnik območne organizacije ZSSS, 2. 9. 2009).

Poslovna skrivnost je vse, kar bi konkurenca rada vzela s seboj (Kop, 1995, str. 43).

2.2.2 Bančna tajnost in varovanje bančne tajnosti

V Zakonu o bančništvu (v nadaljevanju ZBan-1) mora banka kot zaupne varovati vse podatke, dejstva in okoliščine o posamezni stranki, s katerimi razpolaga, ne glede na način, na katerega je pridobila te podatke (ZBan-1, 214. člen).

Bančna tajnost so vsi podatki, dejstva in okoliščine, ki izhajajo iz poslovnega odnosa banke s stranko – komitentom ali so z njim kakorkoli povezani.

Dolžnost varovanja bančne tajnosti imajo:

- **delavci banke** – člani organov, družbeniki, delničarji in bančni delavci; ti so zavezani k temu, da pri delu v banki za take podatke, dejstva in okoliščine, ki so mu znani, zaupani ali dostopni, varujejo. Ne smejo jih izdati, objaviti ali sporočiti tretjim osebam, niti jih sami izkoriščati;

- bančno tajnost so dolžni varovati tudi **zunanji sodelavci** – zunanji sodelavci so izvedenci, predstavniki državnih organov, kontrolni, inšpekcijski in nadzorni organi, ki pri delu v banki ali zunaj nje zvedo za take podatke. Na to dolžnost jih mora banka opozoriti, preden pričnejo opravljati nalogo;
- k varovanju bančne tajnosti so zavezane tudi **zainteresirane tretje osebe** – varuhi, skrbniki, zastopniki, pooblaščenici, pričakujoči dediči, izvršitelji oporoke, prisilni upravitelji in likvidatorji, poroki, hipotekarni zavezanci.

Banka in vsi zavezanci k varovanju bančne tajnosti so kazensko in materialno odgovorni za njeno kršitev. Obveznost varovanja bančnih tajnosti traja tudi po prenehanju delovnega razmerja oziroma po prenehanju poslovnega posla z banko. Pravica do zaščite bančne tajnosti je strogo vezana na osebo – komitenta kot upravičenca do njegovega varovanja, brez njegovega dovoljenja (Bančni kodeks in Združenje Bank Slovenije, 2. 9. 2009).

2.3 URADNE ZAUPNOSTI

Uradne zaupnosti nastanejo najpogosteje v javnem sektorju, omogočajo pa varovanje informacij ali podatkov, ki se nanašajo na delo v organih javne uprave. Zavarovanje podatkov se mora zagotavljati znotraj vsakega upravnega organa. Pogodbeniki so lahko tudi gospodarske družbe, ki so obvezani varovati zaupnosti.

Sprejeti sistemski zakoni s podzakonskimi akti podrobno urejajo dostop in prejem zaupnih podatkov, organi pa lahko sprejmejo interne akte za izvajanje varovanja teh zaupnosti. Uslužbenci se lahko seznaniijo z zaupnimi podatki po podpisu izjave, na podlagi pravice po vedenju, pridobljenem varnostnem dovoljenju in udeležbi na usposabljanju (Stare, Lavrič, 2008, str. 3).

2.3.1 Tajni podatek in varovanje tajnega podatka

Tajni podatek je dejstvo ali sredstvo z delovnega področja organa, ki se nanaša na javno varnost, obrambo, zunanje zadeve ali obveščevalno in varnostno dejavnost države, ki ga je treba zaradi razlogov določenih v Zakonu o tajnih podatkih (v nadaljevanju ZTP) zavarovati pred nepoklicanimi osebami, in ki je skladno z zakonom določeno in označeno za tajno (ZTP, 2. člen).

Za varovanje tajnih podatkov sprejme država predpise, s katerimi definira sistem označevanja, varovanja, dostopa in nadzora nad njimi. Slovenija je temelje na področju varovanja tajnih podatkov postavila leta 2004, s sprejemom ZTP. V njem je jasno in natančno definirano, kaj je tajni podatek, kdo ga kot tajnega lahko označi, kakšen je dostop do tajnih podatkov, kako se te podatke varuje itd. (Lavrič, 2006, str. 35).

Eden izmed temeljnih pogojev, ki jih je morala sprejeti Republika Slovenija pred vstopom v EU³ in NATO⁴, je vzpostavitev ustreznega sistema obravnavanja tajnih podatkov. Standardi obeh organizacij predstavljajo, da je način varovanja tajnih podatkov pri vsaki članici na taki ravni, da omogoča popolno medsebojno zaupanje pri izmenjavi podatkov brez dodatnega varnostnega dogovarjanja ali ukrepanja. S sprejemom ZTP je Republika Slovenija področje tajnih podatkov uskladila s standardi omenjenih organizacij, kar sta tudi obe potrdili in ocenili – Slovenija je na tem področju vredna zaupanja (Predlog Zakona o spremembah in dopolnitvah ZTP).

2.3.1.1 Varnostno preverjanje v NATU

Slovenija se je z vstopom v evroatlantske povezave zavezala, da bo uredila tudi pomembno področje, kot je varovanje tajnih podatkov.

Temeljni akt, ki v NATU ureja varovanje tajnih podatkov, je dokument z naslovom Varnost v okviru organizacije Severnoatlantskega sporazuma C-M (2002)⁵, ki je sestavljen iz direktiv za vsa področja varovanja tajnih podatkov in je zamenjal dokument Varnost v okviru organizacije Severnoatlantskega sporazuma C-M(55)15(FINAL).

V dokumentu C-M(2002)49 so zajeti in določeni politika varovanja podatkov, sredstev in objektov, pomembnih za delovanje in uresničevanje ciljev Nata, ter minimalni varnostni ukrepi in postopki pri obravnavanju podatkov; opravljanja nekaterih dejavnosti ali pri uporabi določene infrastrukture, na primer objektov, predmetov in naprav, morajo upoštevati organi in članice Nata (Čaleta, 2004. str. 60–62).

2.3.1.2 Varnostno preverjanje v EU

EU področju varnosti ni namenjala tolikšne pozornosti kot Nato. To je razvidno tudi iz predpisov, ki so v Natu veliko natančnejši, pa tudi več jih je.

V EU zakonsko podlago in obenem ključni akt predstavljajo Varnostna pravila Sveta EU (Security regulations 2001/264/ES, Council Decision 19. MAR 200). Predpisi za varovanje tajnih podatkov veljajo za vse institucije EU, države članice ter druge posameznike, ki pri svojem delu prihajajo v stik s tajnimi podatki EU. Države članice pa morajo sprejeti ustrezne ukrepe znotraj države in s tem zagotoviti upoštevanje vsaj minimalnih standardov EU (Črnčec, 2004, str. 54).

³ Evropska unija.

⁴ North Atlantic Treaty Organisation, ustanovljena 1949, kot obrambna organizacija suverenih držav. Njen glavni namen in cilj je bil varovanje miru in svobode vseh članic s političnimi kot tudi z vojaškimi sredstvi.

⁵ »Security within the North Atlantic Treaty Organization« dokument C-M (2002) 49.

2.3.2 Državna tajnost in varovanje državne tajnosti

Državno tajnost opredeljuje 52. člen Zakona o Slovenski varnostno-obveščevalni agenciji (v nadaljevanju SOVA), ki določa, da so do sprejema zakona, ki bo urejal določanje in varovanje zaupnih podatkov v državnih organih, podatki, ki jih agencija pridobi pri izvajanju nalog s tajnim sodelovanjem in posebnimi oblikami pridobivanja podatkov, državna tajnost.

Zakon o policiji (v nadaljevanju ZPol-UPB) v 56. členu določa, da mora policist varovati državno, uradno ali drugo tajnost, s katero se seznani pri opravljanju nalog. Dolžnost varovanja državne, uradne ali druge tajnosti traja tudi po prenehanju delovnega razmerja policista. Policist je dolžan varovati tajnost vira prijave, sporočila oziroma pritožbe. Minister lahko v utemeljenem primeru, kadar to terjajo interesi izvedbe kazenskega postopka in če s tem ne ogroža življenja ali osebne varnosti posameznika, na zahtevo pristojnih organov razreši policista ali posameznika, ki je pomagal policiji pri opravljanju z zakonom določenih nalog, varovanja tajnosti.

2.3.3 Uradna tajnost in varovanje uradne tajnosti

Za uradno tajnost se štejejo podatki, ki so z zakonom, z drugim predpisom, splošnim aktom ali s sklepom pristojnega organa, ki so izdani na podlagi zakona, razglašeni za uradno tajnost in so tako pomembni, da so z njihovo izdajo nastale ali bi lahko nastale hujše škodljive posledice za službo. Uradna oseba ali druga oseba, ki v nasprotju s svojimi dolžnostmi varovanja uradne tajnosti sporoči ali izroči komu podatke, ki so uradna tajnost, ali mu kako drugače omogoči, da pride do njih, ali zbira take podatke z namenom, da jih izroči nepoklicani osebi, se kaznuje z zaporom do treh let. Če je dejanje storjeno iz koristoljubnosti⁶ ali z namenom objave ali uporabe podatkov v tujini, se storilec kaznuje z zaporom do petih let. Če je dejanje storjeno iz malomarnosti⁷, se storilec kaznuje z zaporom do enega leta. Enako se kaznuje, kdor z namenom, da jih neupravičeno uporabi, na protipraven način pride do podatkov, ki se varujejo kot uradna tajnost, kakor tudi kdor take podatke brez dovoljenja javno objavi. Ne kaznuje se oseb, katere razkrijejo uradno tajnost, katere vsebina je v nasprotju z ustavnim redom Republike Slovenije, posreduje za objavo ali objavi z namenom, da javnosti razkrije nepravilnosti pri organiziranju, delovanju in vodenju službe, če objava za državo nima škodljivih posledic (KZ-UPB-1, 266. člen).

Uradno tajnost opredeljuje Zakon o industrijski lastnini (v nadaljevanju ZIL), ki v 8. členu določa, da so spisi v zvezi s patentno prijavo in prijavo modela, uradna tajnost vse do njihove objave v uradnem glasilu. Takšna določba je pomembna, saj podjetje s pravicami industrijske lastnine dosežejo učinkovito zaščito, vendar šele po preteku določenega

⁶Koristoljubje pomeni namenski dogodek posameznika, ki se s pridobljenim podatkom lahko materialno ali drugače okoristi in je nastal načrtno, zavestno.

⁷Malomarnost je posledica posameznika nepoučenosti ali nevestnosti, s katerimi se povzroči škodni dogodek, vendar je kazenski ukrep ponavadi milejši, saj dogodek ne nastane načrtno z drugim namenom, ki bi prinesel neko korist.

časa od prijave patenta ali modela. S prijavo pa že razkrijejo pomembne podatke, ki bi lahko, če bi bili znani, povzročili škodo njihovemu nosilcu, zato so varovani kot uradna tajnost, čeprav spadajo po vsebini in definiciji bolj med industrijske skrivnosti.

2.3.4 Davčna tajnost in varovanje davčne tajnosti

Davčna tajnost je opredeljena v Zakonu o davčnem postopku (v nadaljevanju ZDavP-2). Davčni organ mora kot zaupne varovati podatke, ki jih zavezanec za davek v davčnem postopku posreduje davčnemu organu, ter druge podatke v zvezi z davčno obveznostjo zavezancev za davek, s katerimi razpolaga davčni organ (ZDavP-2, 15. člen).

Uradne in druge osebe davčnega organa, izvedenci, tolmači, zapisnikarji in druge osebe, ki sodelujejo ali so sodelovale pri pobiranju davkov, in vse druge osebe, ki so zaradi narave svojega dela prišle v stik s podatki, ki so davčna tajnost, teh podatkov ne smejo sporočiti tretjim osebam, razen v primerih, določenih z zakonom, niti jih ne smejo same uporabljati ali omogočiti, da bi jih uporabljale tretje osebe (ZDavP-2, 16. člen).

Vsak podatek oziroma vsak dokument ali zbirka podatkov, ki vsebuje podatke, ki so davčna tajnost, mora biti vidno označen kot tak, razen, če minister za finance določi drugače. Dostop do podatkov, ki so davčna tajnost, imajo vse zaposlene osebe davčnega organa, vendar le v obsegu, ki je potreben za opravljanje njihovih delovnih nalog. Dovoljenje za dostop pridobijo z začetkom delovnega razmerja in podpisom izjave, da so seznanjene s tem zakonom in da se zavezujejo s podatki, ki so davčna tajnost. Nihče ne sme dobiti podatka, ki je davčna tajnost, prej in v večjem obsegu, kot je to potrebno za opravljanje njegovih delovnih nalog. Davčni organ mora vzpostaviti sistem postopkov in ukrepov varovanja podatkov, ki so davčna tajnost, ki onemogoča razkritje podatkov nepooblaščenim osebam. Davčni organ mora vzpostaviti in voditi nadzor ter pregled nad razkritjem podatkov, ki so davčna tajnost, osebam zunaj davčnega organa. Iz pregleda mora biti razvidno, kdaj in komu zunaj davčnega organa so bili podatki, ki so davčna tajnost, razkriti. Minister za finance predpiše podrobnejše fizične, organizacijske in tehnične ukrepe ter postopke za varovanje podatkov, ki so davčna tajnost (ZDavP-2, 17. člen).

2.3.5 Poklicna tajnost in varovanje poklicne tajnosti

Poklicne tajnosti so navadno zajete v kodeksih poklicne etike, ki jih morajo ob nudenju svojih storitev držati različne agencije, posredniki, zastopniki, saj imajo pri tem dostop do informacij, ki lahko predstavljajo tudi poslovne skrivnosti naročnika (Lavrič, 2006, str. 50).

Zakon o zasebnem varovanju (v nadaljevanju ZZasV) v 39. členu opredeljuje, da so odgovorne osebe za opravljanje zasebnega varovanja, varnostniki, varnostni tehniki, pooblašeni inženirji varnostnih sistemov in operaterji v varnostno-nadzornih centrih v zadevah, ki jih opravljajo oziroma, ki so jim bile zaupane, zavezane k molčečnosti.

V Zakonu o poklicnem in strokovnem izobraževanju (v nadaljevanju ZPSI) je v 86. členu zapisano, da so svetovalni delavci dolžni podatke iz 10. točke prvega odstavka tega člena varovati kot poklicno skrivnost. Te podatke so kot poklicno skrivnost dolžni varovati tudi drugi strokovni delavci, ki so jim podatki posredovani zaradi narave njihovega dela.

V kodeksu odvetniške poklicne etike je poklicna tajnost opredeljena v 51., 52. in 53. členu. Odvetnik mora varovati kot tajnost, kar mu je stranka zaupala ali kar je kot zaupno izvedel. Tudi sam mora vestno oceniti, kar stranka želi varovati kot tajno. Dolžnost varovanja poklicne tajnosti velja tudi za vsebino odvetnikovega spisa in to tudi po prenehanju zastopanja in pri uničenju arhiva končanih zadev. Varovanje poklicne tajnosti zavezuje odvetnika, da odkloni podatke o tem, ali je nekomu nudil pravno pomoč. Izjemoma je odvetnik razrešen dolžnosti varovanja tajnosti, če ga stranka odveže varovanja tajnosti, če je odkritje tajnosti v očitno korist stranke in če je to potrebno zaradi varovanja njegovih pomembnih osebnih interesov. Odvetnik pa tudi v interesu stranke ne sme odkriti tajnosti, če mu stranka izrecno prepove, razen če to terjajo izredne okoliščine v osebnem interesu stranke (Odvetniška zbornica Slovenije. Kodeks odvetniške poklicne etike, 9. 9. 2009).

2.4 POSAMEZNIKOVE ZAUPNOSTI

Posameznikove zaupnosti so osebni podatki posameznika, sem vključujemo podatke o letu in kraju rojstva, imenu, priimku ter naslovu prebivališča, EMŠO številki, davčno številko pri fizičnih osebah, podatke o rasnem, narodnem poreklu, političnem, verskem prepričanju, zdravstvenem stanju. Varstvo posameznikove informacije zasebnosti je ena izmed človekovih pravic, ki je kot taka varovana s konvencijo Organizacije združenih narodov, ustavah in zakonih vseh demokratičnih držav (Stare, Lavrič, 2008, str. 4).

2.4.1 Osebni podatki in varstvo osebnih podatkov

Podlago za sprejem zakonodaje o varstvu osebnih podatkov zagotavlja Ustava Republike Slovenije (v nadaljevanju Ustava RS) (1991), ki v 38. členu določa:

»... 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 ima pravico seznaniti se z zbranimi osebnimi podatki, ki se nanašajo nanj, in pravico do sodnega varstva ob njihovi zlorabi« (Nataša Pirc Musar et. al., str. 7).

Temeljni zakon, ki določa področje varstva osebnih podatkov, je Zakon o varstvu osebnih podatkov (v nadaljevanju ZVOP-1), ki sistemsko določa splošna pravila, obveznosti in ukrepe, s katerimi se preprečuje nezakoniti, neustavni in neupravičeni poseg v zasebnost posameznika pri obdelavi osebnih podatkov.

Osebni podatek je katerikoli podatek, ki se nanaša na posameznika, ne glede na obliko, v kateri je izražen (ZVOP-1, 6. člen).

ZVOP-1 in drugi zakoni, ki podrobneje predpisujejo obdelavo osebnih podatkov na posameznem področju, se neposredno uporabljajo tudi v določbi **Konvencije o varstvu posameznikov glede na avtomatsko obdelavo osebnih podatkov**⁸ (Bogataj, 2004, str. 113).

Namen te konvencije je zagotovitev na ozemlju vsake pogodbenice vsakemu posamezniku ne glede na državljanstvo in prebivališče spoštovanje njegovih pravic in temeljnih svoboščin in v tem okviru še posebej spoštovanje pravice do zasebnosti glede na avtomatsko obdelavo osebnih podatkov, ki se nanašajo nanj (»zaščita podatkov«) (Konvencije o varstvu posameznika in avtomatska obdelava osebnih podatkov, 1. člen).

Načela konvencije so bila povzeta tudi v **Direktivo o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku teh podatkov**⁹.

Namen direktive o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku teh podatkov:

1. v skladu s to direktivo države članice varujejo temeljne pravice in svoboščine fizičnih oseb in predvsem njihovo pravico do zasebnosti pri obdelavi osebnih podatkov;
2. države članice ne omejujejo niti ne prepovedujejo prostega prenosa osebnih podatkov med državami članicami zaradi razlogov, povezanih z varstvom, ki je zagotovljeno na podlagi odstavka 1 (Direktive o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku teh podatkov, 1. člen).

⁸ Uradni list RS-MK št. 11/1994, Mednarodne pogodbe, 3/1994.

⁹ Uradni list št. L 281 23.11. 1995.

3 RAVNANJE Z ZAUPNIMI PODATKI

3.1 OSEBE, KI LAHKO DOSTOPAJO DO ZAUPNIH PODATKOV

Temeljno načelo varovanja zaupnih podatkov je zagotavljanje njegove nedostopnosti. Nedostopnost pomeni, da so informacije in podatki namenjeni le ožjemu krogu oseb oziroma posameznikom, ki se morajo seznaniti z informacijo ali podatkom, ki je zaupne narave. Načelo varovanja zaupnosti vključuje tudi način varovanja, ki je lahko fizične ali tehnične narave.

Zaupnost ni mogoče varovati, v kolikor je informacija ali podatek posredovan množici ljudi. Pomembno je, da se z zaupnimi podatki seznanijo le majhen krog oseb, torej tistih, ki jih potrebujemo pri svojem delu.

Osebe, ki lahko dostopajo do zaupnih podatkov, morajo biti upravičene in pooblašene.

Upravičena oseba je posameznik, ki zaseda tako pomembno delovno mesto (funkcionar, direktor, vodja, poveljnik), da se lahko z zaupno vsebino seznanijo že zaradi opravljanja svoje funkcije oziroma po svoji uradni dolžnosti.

Pooblaščen oseba je posameznik, ki ima pisno ali ustno pooblastilo, da sploh lahko dostopa do zaupnih podatkov (Stare, Lavrič, 2008, str. 7).

3.2 PRISTOJNOSTI IN PRAVICE INFORMACIJSKEGA POOBLAŠČENCA DO VPOGLEDA V ZAUPNE PODATKE

Informacijski pooblaščenec je dobil s svojim nastankom precej pooblastil do vpogleda v zaupne podatke. Konkretni določbi, ki informacijskemu pooblaščenцу omogočata dostop do zaupnih podatkov, sta ZDIJZ (31. Člen ZDIJZ-A) in ZTP (zadnja alineja 3. člena).

Zakon o dostopu informacij javnega značaja v tretjem odstavku 31. člena pravi: *»Ne glede na določbe zakona, ki ureja tajne podatke, ima brez dovoljenja dostop do tajnih podatkov tudi pooblaščenec (državni funkcionar)«*.

Ti določbi pravita, da ima pooblaščenec dostop do tajnih podatkov vseh stopenj brez pridobivanja dovoljenj, kot jih določa ZTP. Tako izjemno pooblastilo imajo glede na 3. člen ZTP le najvišji državni funkcionarji, ob dejstvu, da dobijo te osebe dovoljenje z začetkom opravljanja funkcije in podpisom izjave.

3.3 IZJAVA O VAROVANJU PODATKOV

Vsi zaposleni morajo podpisati formalno **izjavo o varovanju podatkov**, za katere zvejo pri svojem delu, kar velja tako za čas trajanja delovnega razmerja kot tudi po prenehanju le-tega. Če zaposleni ne podpišejo zaposlitvene pogodbe glede varovanja podatkov, veliko pogosteje pride do razkritja zaupnih podatkov (razkritje družinskim članom in prijateljem, ob službenem klepetu, ob odhodu k drugemu delodajalcu, ...).

Organizacija pa mora posebej ustrezno ravnati z vsemi podatki, ki so označeni s stopnjo strogo zaupno, tajno, zaupno in interno (po Priporočilu za pripravo informacijske varnosti str. 25).

Posameznik, ki prekrši obveznost varovanja zaupnih podatkov je lahko na podlagi določil pogodbe o zaposlitvi in drugih predpisov, v kolikor mu je krivda dokazana, kaznovan. Zakon najpogosteje predpisuje denarno kazen, možni pa so tudi drugi disciplinski ukrepi, kot je odpoved pogodbe o zaposlitvi, premestitev na drugo delovno mesto, odvzem primera, suspenz, varnostni ali vzgojni ukrep, zaporna kazen, plačilo kazni. Za najbolj odgovorne funkcije v državi, kot so predsednik republike, vlade ali ministri, lahko ustavno sodišče na podlagi sklepa o obtožbi, posredovanega s strani državnega zbora, v primeru kršitve ustave ali hujše kršitve zakona odloči, da začasno ne sme več opravljati svoje funkcije ali pa da mu funkcija preneha (Stare in Lavrič, 2008, str. 8).

3.4 DOVOLJENJA ZA DOSTOP DO ZAUPNIH PODATKOV

Izdaja dovoljenja za dostop do zaupnih podatkov se zapiše v odločbo. To je časovno vezana odločba. Vendar imajo te odločbe pomembno posebnost. Dovoljenje mora opredeliti tudi obseg pravice v smislu določitve stopnje tajnosti podatkov, do katerih ima stranka pravico dostopa.

Izdaja teh dovoljenje ureja ZTP, ki v 13., 22. in 23. členu določa, da se dovoljenja za dostop do podatkov izdajajo po naslednjih stopnjah tajnosti in za določen čas veljavnosti:

- stopnja »strogo zaupno« se nanaša na tajne podatke, katerih razkritje nepoklicani osebi bi ogrozilo vitalne interese Republike Slovenije ali jim nepopravljivo škodovalo – za to stopnjo se dovoljenja izdajajo za pet let;
- stopnja »tajno« se nanaša na tajne podatke, katerih razkritje nepoklicani osebi bi lahko škodovalo varnosti ali interesom RS – za to stopnjo se dovoljenja izdajo za pet let;
- stopnja »zaupno«, ki se določi za tajne podate, katerih razkritje nepoklicani osebi bi lahko škodovalo varnosti ali interesom RS – za to stopnjo se dovoljenja izdajo za deset let.

Imetniki dovoljenja so osebe, ki za svoje področje oziroma za svoje zaposlene potrebujejo dostop do zaupnih podatkov zaradi opravljanja funkcij ali izvajanja nalog na delovnih mestih v organih.

Tako dovoljenje se mora prekiniti, ko uslužbenec zamenja delovno mesto ali je prerazporejen v drugo organizacijo oziroma na druge objektivne ali subjektivne okoliščine (invalidnost, duševna bolezen) (Kovač, članek , Pravna praksa str. 11–13).

V vseh organizacijah (tako v javnem sektorju, kjer ureja položaj javni uslužbenec in sistemski zakoni, kot v gospodarskih družbah, kjer so poslovne skrivnosti opredeljene v statutu in internih aktih) so uslužbenci dolžni varovati kot zaupne informacije vse, kar zvedo pri svojem delu tudi na podlagi določil pogodbe o zaposlitvi. Ne glede na to, ali imajo posebno dovoljenje za dostop do zaupnih podatkov, s pridobljenimi informacijami ne smejo ravnati na način, da bi povzročilo razkritje, zlorabo oziroma izdajo podatka. Zaupne podatke so dolžne varovati tudi osebe¹⁰, ki so imele kot druge osebe v postopku priznано pravico udeležbe zaradi varstva svojih pravnih koristi (Lavrič, 2008, str. 4–6).

¹⁰ Osebe, ki nastopajo v postopku, so lahko: stranke, stranski udeleženci, začasni zastopniki, skupni predstavniki, pooblaščenici, zakoniti zastopniki, strokovni pomočniki, svetovalci, skrbniki, priče, izvedenci, tolmači, dediči, predstavniki banke, zavarovalnice, osebe, udeležene na javni dražbi itd. Posebna izjema so tudi uradne osebe, kot so: inšpektorji, računski revizorji, državni tožilec, pravobranilec, policisti, odvetniki, duhovniki, ki morajo take podatke že po službeni dolžnosti varovati kot poklicno tajnost.

4 OBDELAVA IN HRANJENJE ZAUPNIH PODATKOV

Organizacije, ki imajo opravke z zaupnimi podatki, morajo za delo z zaupnimi podatki zagotoviti ustrezne pogoje. Prostori za obdelavo in hrambo zaupnih podatkov morajo biti zgrajeni v skladu s predpisi s področja varovanja zaupnih podatkov tako, da omogočajo operativno obdelavo in pripravo dokumentov za potrebe organa oziroma drugih služb, in da omogočajo tudi njihovo obravnavo (MUPP, 2007, str. 21).

4.1 SPREJEM IN POSREDOVANJE ZAUPNIH PODATKOV

Zaupne podatke je dovoljeno prenašati z informacijskimi, telekomunikacijskimi in drugimi sredstvi le ob izvajanju postopkov in ukrepov, ki nepooblaščenim osebam preprečujejo prilaščanje ali uničenje podatkov ter neupravičeno seznanjanje z njihovo vsebino. Zbirajo in obdelujejo se lahko samo tisti podatki, ki imajo ustrezno zakonsko osnovo (Pravilnik o varovanju zaupnih ter osebnih podatkih ter varovanja dokumentarnega gradiva 26.–29. člen).

4.2 VAROVANJE PROSTOROV Z ZAUPNIMI PODATKI

Prostori, kjer se nahajajo zaupni podatki, se imenujejo varovani prostori. Varovani prostori morajo biti varovani s fizičnimi, tehničnimi in organizacijskimi ukrepi, ki onemogočajo nepooblaščenim osebam dostop do podatkov (Pravilnik o varovanju zaupnih ter osebnih podatkih ter varovanja dokumentarnega gradiva 7. člen).

Dostop v prostore je možen in dopusten le v delovnem času. Izven delovnega časa pa le na podlagi upravičene pooblaščen osebe. Varovani prostori ne smejo ostati nadzorovani oziroma se morajo zaklepiti ob odsotnosti delavca, ki jih nadzoruje. Izven delovnega časa morajo biti omare in pisalne mize z nosilci podatkov zaklenjene. V varovane prostore nezaposleni ne smejo vstopati brez spremstva ali prisotnosti delavca. Delavec, ki dela v varovanih prostorih, mora vestno in skrbno nadzorovati prostor in ga ob zapustitvi zakleniti. Delavec, ki pri svojem delu obdeluje zaupne podatke, ne sme med delovnim časom puščati zaupnih podatkov na pisalni mizi ali jih kako drugače izpostavljati nevarnosti vpogleda nepooblaščenim osebam. Zaposleni tehnično vzdrževalni delavci in čistilke se lahko gibljejo v varovanih prostorih izven delovnega časa in brez prisotnosti odgovornega delavca le, če so nosilci podatkov shranjeni na način, ki ga določa pravilnik o varovanju zaupnih in osebnih podatkov ter o varovanju dokumentarnega gradiva. S štipaljkami, papirjem z glavo podjetja in drugimi pripomočki, s katerimi bi bilo mogoče ponarediti dokumente, je potrebno ravnati kot z zaupnimi podatki (Pravilnik o varovanju zaupnih ter osebnih podatkih ter varovanja dokumentarnega gradiva 8. in 9. člen).

Osebe lahko nezakonito vstopijo z namenom kraje, poškodovanja ali povzročanje drugih motenj v delovanju. Okolje varovanega prostora mora biti zavarovano pred nepooblaščenim dostopom. Pozornost je potrebno nameniti strehi, stropu in oknom brez privarjenih rešetk. Namestiti je potrebno alarmni sistem. Preučiti je potrebno uporabo video nadzora in rednega snemanja. Vzpostaviti je potrebno jasen pregled nad pooblastili dostopa, kdo skrbi za varnost prostora. Pri vhodih v varovano območje je potrebno vzpostaviti kontrolne vstopne točke, kjer se vstop odobri ali zavrne. Vstopne točke morajo biti zavarovane pred nasilnim vdorom. Obiskovalci varovanih prostorov morajo nositi na vidnem mestu priponko »obiskovalec«. Obiskovalce morajo vedno spremljati pooblaščen osebe. Obiskovalci morajo biti vpisani v dnevnik. V dnevnik se zapiše datum, ura prihoda in odhoda ter razlog vstopa v varovani prostor (MUPP, 2007, str. 58–63).

4.3 VAROVANJE OPREME Z ZAUPNIMI PODATKI

Dostop do opreme in nosilcev podatkov je potrebno ustrezno zaščititi. Občutljivo gradivo mora biti shranjeno v zaklenjenem pohoštvu ali sefu. Zelo občutljivi zaupni podatki morajo biti shranjeni v ognjevarnih in vodotesnih omarah. Ostajati mora seznam pooblaščenih zaposlenih s ključi oziroma kodami za zaklenjeno pohoštvo.

Dostop do računalniške programske opreme mora biti varovan na način, ki omogoča dostop samo upravičenim in določenim pooblaščenim delavcem ter delavcem, ki za organizacijo poslovnega odnosa opravljajo servisiranje računalniške in programske opreme. Vzdrževanje in popravilo strojev in programske opreme je dovoljeno samo z vednostjo pooblaščenih oseb, izvajajo pa ga lahko samo pooblašчени servisi in vzdrževalci. Vzdrževalci prostorov, strojne in programske opreme, obiskovalci in poslovni partnerji se smejo gibati v teh prostorih samo z vednostjo pooblaščen osebe. Dostop do programske opreme mora biti varovan tako, da dovoljuje dostop samo za to v naprej določenim zaposlenim ali pravnim in fizičnim osebam, ki opravljajo dogovorjene storitve. Popravljanje, spreminjanje in dopolnjevanje systemske in aplikativne programske opreme je dovoljeno samo na podlagi odobritve pooblaščen osebe, izvajajo pa ga lahko samo pooblašчени servisi. Izvajalci morajo spremembe in dopolnitve systemske in programske aplikativne opreme ustrezno dokumentirati. Zaposleni ne smejo namestiti programske opreme brez vednosti pooblaščen osebe za posamezno delovno področje. Prav tako ne smejo odnašati programske opreme iz organizacije brez odobritve pooblaščen osebe. Pristop do podatkov preko aplikativne programske opreme se varuje s sistemom gesel za avtorizacijo in identifikacijo uporabnikov programov in podatkov. Vsa gesla in postopki, ki se uporabljajo za vstop in administriranje mreže osebnih računalnikov, administriranje elektronske pošte in administriranje programov se hranijo v zapečatenih ovojnica in se jih varuje kot zaupni podatek. Uporabi se jih lahko samo v izrednih okoliščinah oziroma v nujnih primerih. Vsaka uporaba vsebine zapečatenih ovojnic se dokumentira. Pri vsaki takšni uporabi se določi nova vsebina gesel. Za potrebe restavriranja računalniškega sistema ob okvarah in drugih izjemnih situacijah se zagotavlja redna izdelava kopij

mrežnega strežnika in lokalnih postaj (če se podatki nahajajo tam). Te kopije se hranijo v zato določenih mestih, ki morajo biti ognjevarna, zavarovana proti poplavam in elektromagnetnim motnjam, v okviru predpisanih klimatskih pogojev ter zaklenjena. Dokumenti z zaupnimi podatki morajo na vidnem mestu imeti označbo, da so zaupni. Tako označbo morajo imeti tudi vse njihove priloge. Pri izdelavi dokumentov, ki vsebujejo podatke, ki so zaupni, se na originalu označi, v koliko izvodih je bil izdelan (napisan, natiskan, narisano, razmnožen) in komu je bil posredovan. Vsak izvod takega dokumenta mora imeti svojo evidenčno številko. Dokumenti z oznakami tajnosti morajo biti vedno zaklenjeni v železnih omarah, ki so tehnično varovane ali zaklenjenih ter zapečatenih železnih blagajnah, razen, če niso pod neposredno kontrolo delavca, ki mu je to gradivo bilo dano v delo (Pravilnik o varovanju zaupnih ter osebnih podatkih ter varovanja dokumentarnega gradiva 14.–25. člen).

4.4 HRAMBA ZAUPNIH PODATKOV

S hrambo zagotavljamo varovanje zaupnega gradiva za dolgo časa, in sicer ne glede na obliko ali medij, v katerem se nahaja. Zaupni podatki prihajajo v arhiv še vedno večinoma na papirju, vendar je vedno več tudi digitalnih zapisov. Vse več pa je tudi različnih baz podatkov, ki se vzdržujejo samo v digitalni obliki.

Zaupne podatke je pri hrambi potrebno obravnavati strožje. Tako Uredba o upravnem poslovanju v 191. členu kot Uredba o varstvu dokumentarnega in arhivskega gradiva v 42. členu določata, da se dokumentarno gradivo, ki vsebuje tajne podatke po ZTP¹¹ v skladu s posebnimi predpisi, hrani ločeno, za hrambo pa se uporabljajo določbe predpisov o varovanju tajnih podatkov.

Vsem zaupnim podatkom rok zaupnosti nekoč poteče. V kolikor zaupnost ni preklicana, postane tak dokument dostopen šele po 40-ih letih od njenega nastanka oziroma po 75-ih letih od nastanka, v primeru osebnih podatkov. Ta rok lahko glede na določila Zakona o varstvu dokumentarnega in arhivskega gradiva ter arhivih Vlade RS na obrazložen zahtevek arhivske komisije podaljša, če obstaja interes. Lahko pa ga tudi skrajša, če obstaja močnejši javni interes (Lavrič, 2008, str. 46–49).

¹¹ Deloma velja smiselno tudi za ostale zaupnosti, npr. poslovna skrivnost, davčna tajnost, bančna tajnost.

4.5 RAZKRITJE IN ZLORABA ZAUPNIH PODATKOV

Z razkritjem zaupnih podatkov se srečamo takrat, ko se informacije ali podatki objavijo v javnosti z namenom, da prikažejo neko zasebno stanje. Razkritje informacije ali podatka se za škodljivo in kaznivo izkaže, ko se posreduje osebi, ki do zaupnega podatka ni upravičena niti pooblaščen. Dejanje, ko ta oseba zaupni podatek sporoči tretji osebi in ta oseba preko medija javnosti, povzroči popolno razkritje zaupnosti, ki nosi kazenske in odškodninske posledice (Lavrič, 2008, str. 6).

Pri delu se pogosto zgodi, da se s kakšnim zaupnim podatkom srečajo naključni sodelavci, ki mimogrede pogledajo na sosednjo mizo, ko pridejo na sestanek, stranke pri okencih, ki čakajo na obdelavo podatkov pri uslužbencih z vpogledom na listine na njegovi mizi, v pogovorih med uslužbencih ter strankami in doma v pogovoru s partnerjem. Visoka stopnja zavarovanja zaupnih podatkov se lahko zagotavlja v organizacijah z majhnim številom uslužbencev in kjer poteka poslovanje brez obiskovalcev. Sistema, ki bi bil popolnoma zanesljiv proti razkritjem ali zlorabam podatkov, ni.

Zloraba in izdaja je nedovoljena pridobitev, uporaba, prenos, izdaja, uničenje ali kakršnakoli drugačna uporaba zaupnega podatka, ki je s predpisom določen kot zaupen. Zloraba zaupnega podatka se obravnava šele ob razkritju nedovoljenega podatka. Med »skrite« zlorabe prištevamo aktivnosti posameznika na delovnem mestu, kjer znanja vanj vlaga delodajalec, ta pa v popoldanskem delu to znanje prodaja strankam (siva ekonomija), zaposlitev v drugi službi in odnašanje pomembnih podatkov iz prejšnjega podjetja kljub konkurenčni prepovedi, prenos službenih informacij o sodelavcih in posameznih strankah ter sporočanje teh informacij tretjim osebam, prevzemanje avtorskih idej, ... (Stare in Lavrič, str. 6–7).

4.5.1 Motivi za zlorabo in izdajo zaupnih podatkov

Motivov za zlorabo in izdajo zaupnih podatkov je več. Pomembno je, da pozna organizacija čim več motivov, saj ima organizacija s tem več možnosti, da prepreči takšno delovanje.

Motivi za zlorabo in izdajo so:

- *želja po uspehu*: željo po uspehu ima vsakdo, toda pri nekaterih je tako močna, da premaga številne ovire moralnega značaja. Če ima tak človek pri svojem delu dostop do zaupnih podatkov in če meni, da mu to poznavanje lahko pomaga do uspeha, so ti zaupni podatki že obsojeni na zlorabo;
- *prihranek pri stroških*: to je eden izmed osnovnih motivov za zlorabo. O njem govorimo, kadar se nekdo pripravlja, da bo ustanovil svojo organizacijo in pri tem uporablja skrivno znanje svojega sodelavca. Uspeh mu je zagotovljen, saj nima nobenih stroškov z razvojem in lahko konkurira sedanjemu delodajalcu z nižjo ceno in enako kakovostjo. Ta motiv je tesno povezan z željo po uspehu;

- *časovna stiska*: interesent pride pri svojem razvojnem delu v časovno stisko. Izhod vidi le v razvojnem delu nekoga drugega in meni, da bi z njim skrajšal čas, ki je potreben, da bi uspešno končal delo;
- *boj za tržne deleže*: ta motiv je povezan z željo po uspehu. Z njim imamo opravka, ko je tekmelec že navzoč na trgu in bi si rad na tuj račun povečal svoj tržni delež;
- *boj za preživetje*: ko človeku grozi nevarnost, se oprijemlje vsega, kar mu je dosegljivo. To velja tudi za organizacije, ki pred grozečim polomom vidijo rešitev v zaupnih podatkih svojega uspešnejšega tekmeca na trgu;
- *obeti v poklicu*: ta motiv je najpogostejši v zvezi z izdajo. Interesent si izbere človeka, za katerega ve, da dobro pozna zaupne podatke, in da pri sedanjem delodajalcu nima možnosti napredovanja. Obljublja, da bo pri njem takoj zasedel zelo dobro plačano delovno mesto, če bo prinesel s seboj določene zaupne podatke;
- *nezadovoljstvo pri delu*: tisti, ki s svojim delovnim mestom ni zadovoljen, je za ponudbo interesenta zelo dovzeten;
- *denarne težave*: človek, ki živi s svojimi finančnimi zmožnostmi, je za interesenta zelo zanimiv, za imetnika zaupnih podatkov pa predstavlja stalno tveganje;
- *želja po denarju*: pri ljudeh z izrazito željo po denarju interesent ve, da bo s svojimi predlogi razmeroma lahko uspel (Kop, 1995, str. 64–67).

Največjo nevarnost za izdajo zaupnih podatkov predstavljajo razočarani in nezadovoljni zaposleni. Kot zaposleni imajo direkten dostop do informacij in do določenih podatkov, ki jih lahko posredujejo naročniku. Veliko nevarnost izdaje podatkov predstavljajo tudi osebe ob zamenjavi zaposlitve, saj v dobi sodobne informacijske tehnologije ni potrebno prekopirati dokumentov, temveč jih preprosto odnesejo na izmenljivih nosilcih (Schmid v: Hartman, 2007, str. 62).

4.5.2 Ukrepi ob sumu zlorabe in izdaje zaupnih podatkov

Ob sumu zlorabe in izdaje zaupnih podatkov je treba poskrbeti, da je o tem kar najhitreje obveščeno vodstvo organizacije. Vsaka takšna sporočila je potrebno jemati z vso resnostjo, ne glede na to, s katerega področja v organizaciji prihajajo. Priporočljivo je, da vodstvo organizacije s svojimi člani ustanovi posebno delovno skupino, ki uvede preiskavo. Število članov mora biti omejeno. Upoštevati je potrebno tudi dejstvo, da nihče nikoli zanesljivo ne ve, kdo vse je v zadevo morda vpleten. Preiskava mora potekati na skrivaj, saj drugače ni mogoče upati na uspeh pri ugotavljanju resnice. Če preiskava potrdi upravičenost suma zlorabe ali izdaje, je na vrsti pravna služba oziroma pravni

zastopnik organizacije, ki mora v pomembnih primerih kar se da hitro navezati stik z javnim tožilstvom in preko njega doseči pomoč organu (Kop, 1995, str. 141–142).

5 VARNOSTNA POLITIKA ZAUPNIH PODATKOV

5.1 POLITIKA VAROVANJA INFORMACIJ

Vsaka organizacija naj bi imela izdelano politiko varovanja informacij. Ta dokument naj bi bil osnova za vse ostale dokumente, ki varnostno problematiko obravnavajo bolj podrobno in so namenjeni reševanju specifičnih problemov. Politiko mora vedno potrditi najvišje vodstvo organizacije.

V varnostni politiki morajo biti natančno definirani cilji varovanja, vloge in odgovornosti ter merila, načela in postopki za njeno uvedbo in nadzor. Politika varovanja informacij je interni akt organizacije, ki določa jasna navodila v zvezi z varnostjo in odgovornostmi zaposlenih za izvajanje te politike (Rakovec, 2005, str. 18).

Varnostno politiko delimo na tri nivoje, in sicer:

- krovna varnostna politika,
- varnostna politika za posamezna področja na srednjem nivoju in
- delovna navodila, procedure in obrazci na nižjem nivoju.

Z nivoji dosežemo prehod od strateških usmeritev in ciljev prek mehanizmov do konkretnih postopkov in tehnologij, ki se bodo uporabili za izpolnitev zastavljenih ciljev. Cilji so dolgoročni in niso vezani samo na trenutno obdobje; tehnologija, ki je na voljo za varovanje informacijskih virov, pa se s časom spreminja. Z ločitvijo v nivoje dosežemo tudi boljšo preglednost dokumentacije in tudi možnost, da do različnega nivoja dokumentov dostopajo različni uporabniki.

V varnostni politiki se natančno določi, kaj je potrebno v organizaciji ščititi in na kakšen način bomo to storili.

Priporočljivo je, da je varnostna politika v internih aktih opredeljena kot obvezujoči akt, ki ga morajo zaposleni spoštovati. V organizacijah je potrebno za njeno morebitno neupoštevanje predpisati sankcije (Eršte, 2006, str. 51).

Slika 1: Večnivojska varnostna politika



Vir: Rakovec, 2005, str. 32

Na najvišjem nivoju je krovna varnostna politika, ki predstavlja temeljni dokument za varovanje informacij v organizaciji. Osnovni cilj dokumenta je pridobivanje podpore in priprava organizacije na izgradnjo celovitega sistema varovanja.

Krovna varnostna politika podaja generalne, od varnostnih tehnologij povsem neodvisne, usmeritve posloводства v zvezi z varovanjem informacij in sistemom podrejenih – elementarnih politik, navodil in obrazcev za izvajanje posamezne politike, ki podrobneje urejajo posamezno področje.

Varnostna politika za posamezna področja so dokumenti srednjega nivoja, ki natančneje opisujejo posamezna področja in sklope, a še vedno ne omenjajo imen konkretnih oseb, niti konkretne računalniške opreme.

Varnostna politika za posamezno področje oziroma elementarna varnostna politika pokriva najbolj pomembne oziroma kritične poslovne procese v organizaciji.

Na najnižjem nivoju dokumentacije se nahajajo operativna navodila, interni standardi in postopki za delo, ki pa zelo natančno določajo postopke za posamezna področja.

Pod temi pojmi razumemo dokumentirane postopke, ki opisujejo, kako izvesti posamezna dela, postopke ali dejavnosti, ki običajno v politiki niso dovolj podrobno opisani (Eršte, 2006 str. 52–53).

Najpomembnejši varnostni ukrepi v varnostni politiki so:

- ovrednotenje informacijskih virov ter prepoznavanje groženj in ranljivosti,
- opredelitev lastništva, skrbništva ter nadzorstva nad vsemi informacijskimi viri,
- oblikovanje ustrezne organizacijske enote z osebo, ki skrbi za varovanje informacij in podatkov,
- kodiran dostop do informacijskih sistemov in uporaba licenčne programske opreme,
- ustrezna protivirusna programska oprema in protipožarne pregrade,
- skrb zaposlenih za stalno prisotnost v primeru obiskov,
- politika »prazne delovne mize« in »praznega računalniškega zaslona«,

- pozornost pri posredovanju zaupnih podatkov preko telefonskih pogovorov, elektronske pošte, navadne pošte, interneta, oglasnih desk, elektronskih zaslonov,
- obveznosti glede varovanja informacij zaposlenih, ki delajo v organizaciji po pogodbi,
- odmetavanje odvečne papirne dokumentacije v koš brez uničevanja in način uničevanja (rezanje) pomožnega gradiva v uničevalcih papirja,
- opredelitev varnostnih pogojev (pri prenosu podatkov med organi) za nasprotno stranko, na način, kot jih določi lastnik ali upravitelj zaupnih podatkov,
- stalno investiranje v posodabljanje sistema varovanja in zaščite,
- pazljivost pri vnosu različne opreme v poslovne prostore,
- stalno usposabljanje in izpolnjevanje uslužbencev s poudarkom na varovanje zaupnih podatkov, ...

Varnostna politika vključuje rešitve, kako zaščititi dostop do zaupnih podatkov v organizaciji ter zagotoviti neprekinjeno poslovanje in omejevanje poslovne škode na najmanjšo možno raven (Stare, Lavrič, str. 12–13).

6 RAZISKAVA: RAVNANJE Z ZAUPNIMI PODATKI

6.1 SESTAVA IN STRUKTURA ANKETE

Anketa je bila opravljena na upravni enoti v Slovenski Bistrici, meseca maja 2010. Sestavlja jo deset vprašanj, na katera so zaposleni odgovarjali prosto in z obkroževanjem.

Upravna enota Slovenska Bistrica, s sedežem na Kolodvorski ulici 10, zavzema pet naravnih območij: Polskavsko dolino, Ložniško dolino, Pohorje, Dravinjsko dolino in ožje mestno bistriško območje. V skladu z zakonom je Upravna enota Slovenska Bistrica organizirana za območje lokalnih skupnosti – občine Slovenska Bistrica in Oplotnica. Po površini obsega 370 km² in šteje 35.600 prebivalcev.

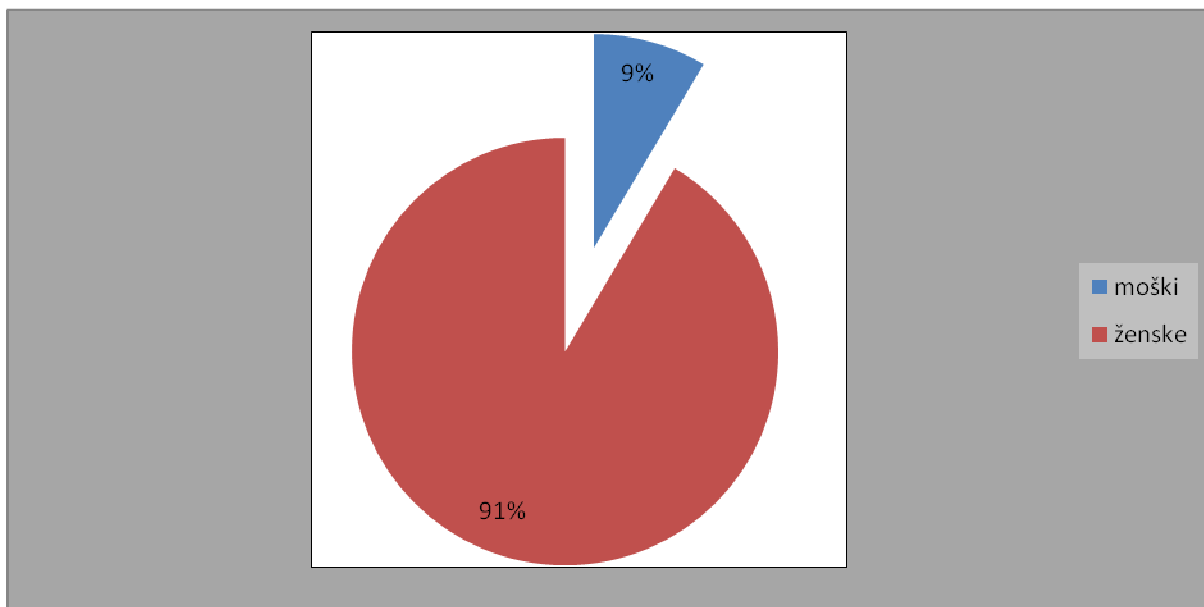
V Upravni enoti Slovenska Bistrica je zaposlenih 43 javnih uslužbencev. V anketi niso sodelovali vsi uslužbenci. Na anketo je odgovorilo 35 javnih uslužbencev.

S pomočjo opravljene ankete so se pridobili želeni podatki in odgovori glede na to, kako zaposleni dojemajo zaupne podatke.

Podatki so bili zbrani s pomočjo anketnega vprašalnika z deskriptivno metodo. Odgovori so analizirani tako, da so opisani in predstavljeni v obliki grafikonov.

6.2 PREDSTAVITEV REZULTATOV

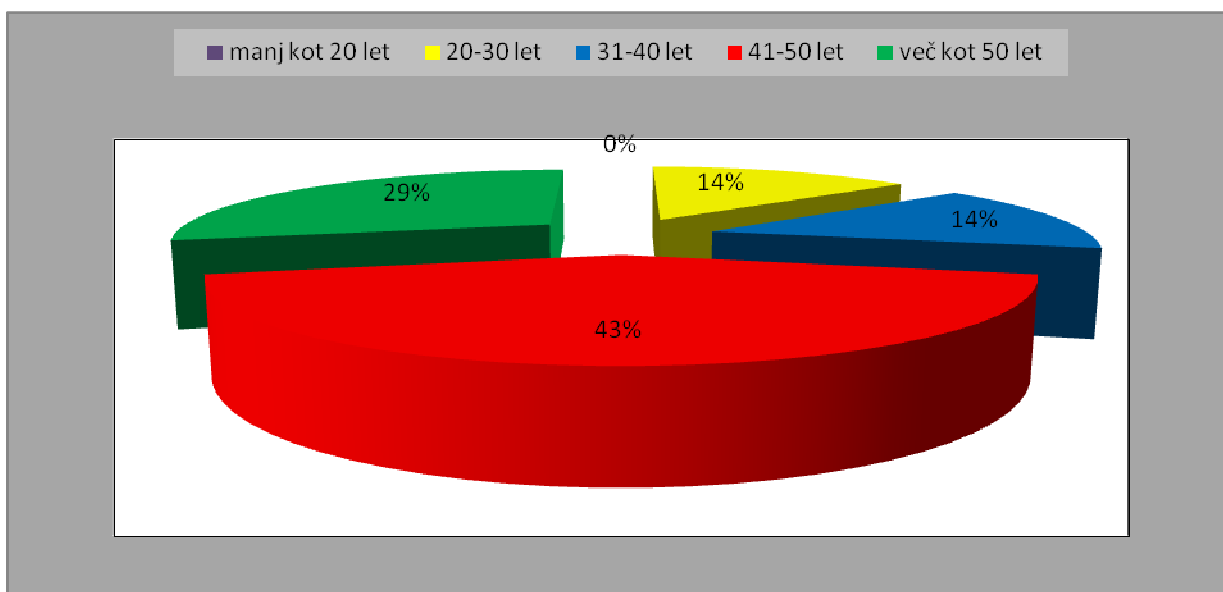
Grafikon 1: Spol zaposlenih



Vir: lastni (2010)

Na anketna vprašanja je odgovorilo petintrideset zaposlenih na Upravni enoti Slovenska Bistrica, od tega je bilo 9 % moškega spola in 91 % ženskega spola.

Grafikon 2: Starost zaposlenih

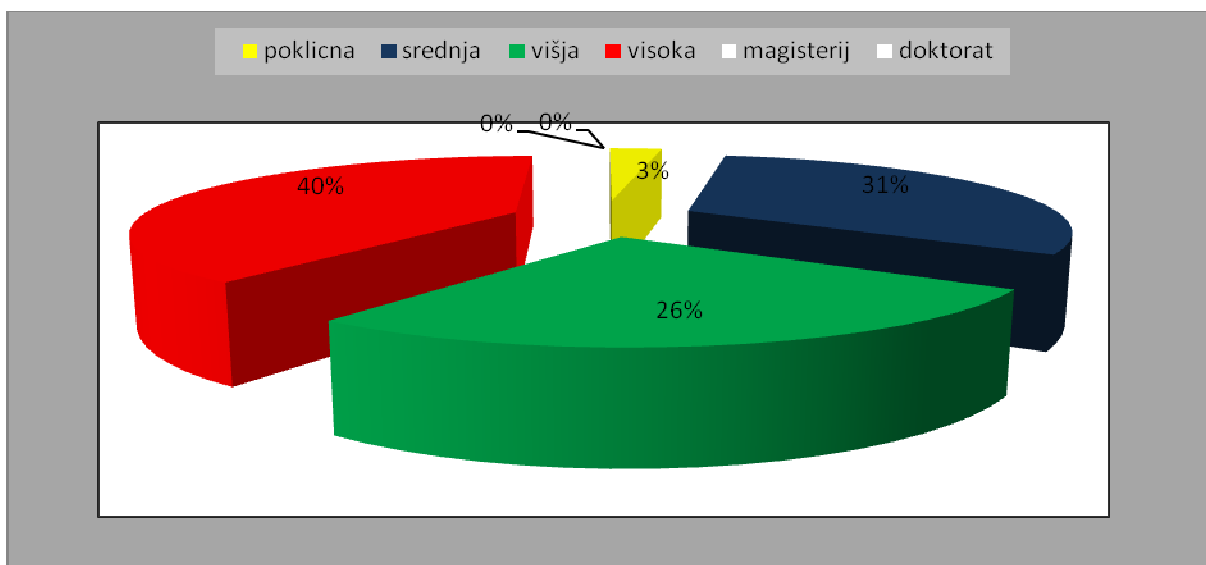


Vir: lastni (2010)

Grafikon 2 prikazuje rezultate ankete glede starosti anketirancev. V anketi ni sodeloval noben anketiranec, ki bi bil star manj kot 20 let, nad 20 do 30 let je bilo starih 14 %, od

31 do 40 let prav tako 14 %, nad 41 do 50 let 43 % anketirancev in nad 51 let 29 % anketirancev. Ker na anketo niso odgovorili vsi zaposleni, se ne more sklepati, da Upravna enota Slovenska Bistrica nima zaposlenih, ki bi bili mlajši od 20 let, lahko pa se predvideva, da je to število zelo nizko. Predvidevam pa lahko tudi, da je največ zaposlenih starih med 40 in 50 let, kar pomeni, da ti zaposleni že imajo nekaj delovnih izkušenj.

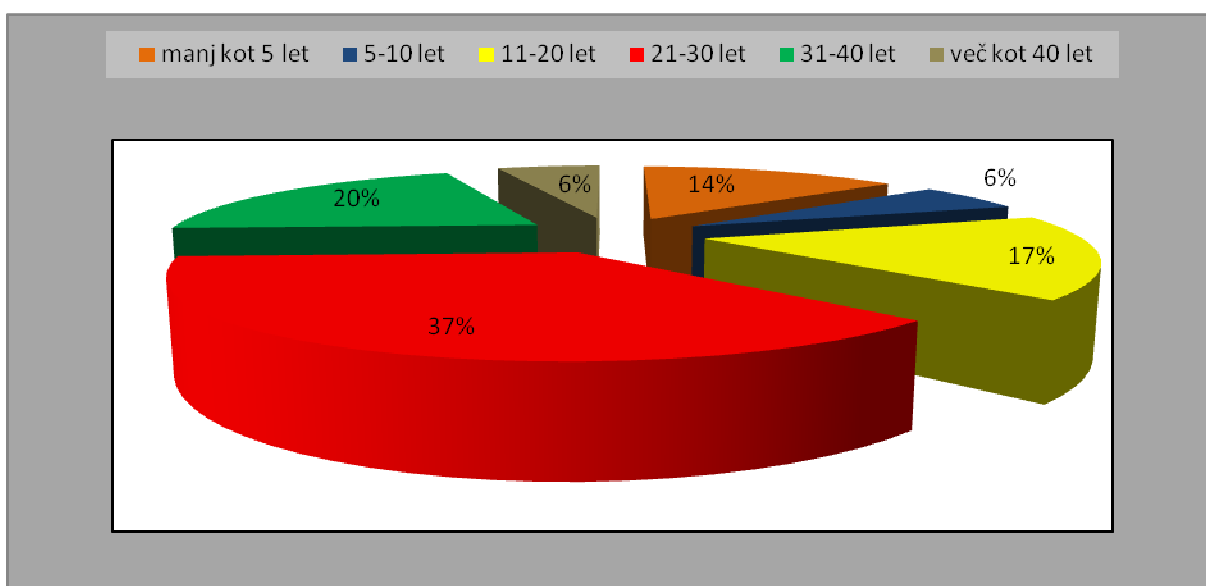
Grafikon 3: Stopnja izobrazbe zaposlenih



Vir: lastni (2010)

Grafikon 3 prikazuje stopnjo izobrazbo zaposlenih. Na Upravni enoti Slovenska Bistrica je največ zaposlenih z visoko šolo, in sicer kar 40 % anketirancev, sledi višja izobrazba s 26 %, srednjo šolo ima 31 % anketirancev ter poklicno izobrazbo 3 % anketirancev. Na anketni vprašalnik mi ni odgovoril nihče z magisterijem ali doktoratom.

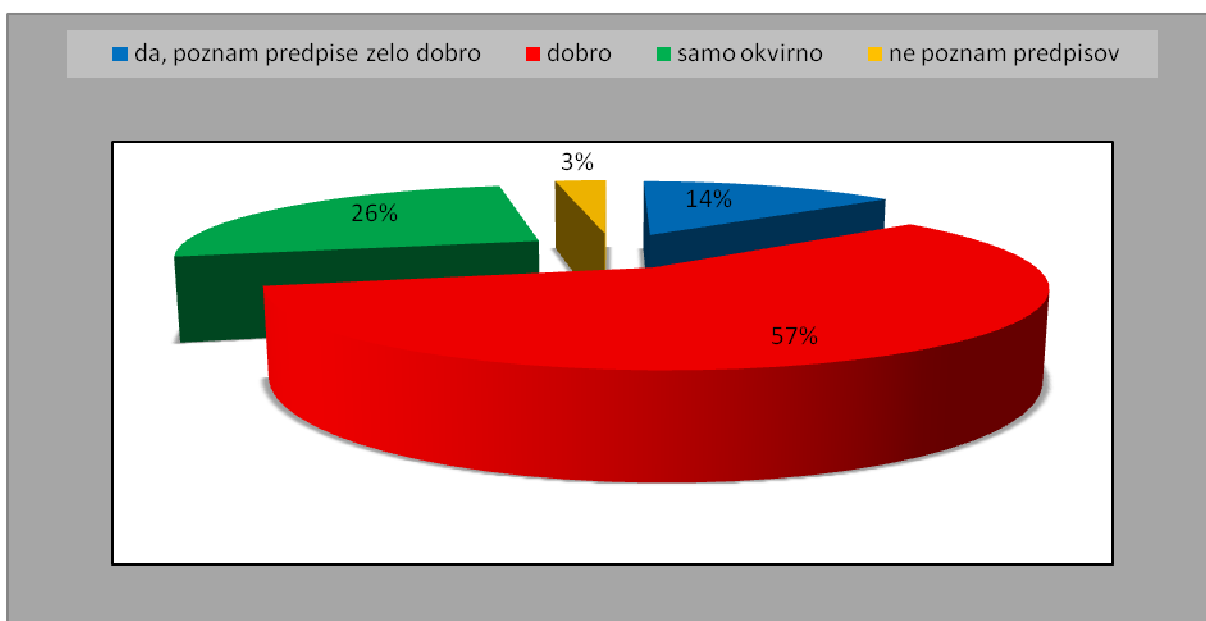
Grafikon 4: Delovna doba zaposlenih



Vir: lastni (2010)

Grafikon 4 prikazuje delovno dobo anketirancev na Upravni enoti Slovenska Bistrica. Največ anketirancev ima delovno dobo med 21 in 30 let, in sicer kar 37 %, med 31 in 40 let ima delovno dobo 20 % anketirancev, med 11 in 20 let ima delovno dobo 17 % anketirancev, manj kot 5 let ima 14 % anketirancev delovne dobe ter 6 % je anketirancev, ki ima 5–10 let in več kot 40 let delovne dobe.

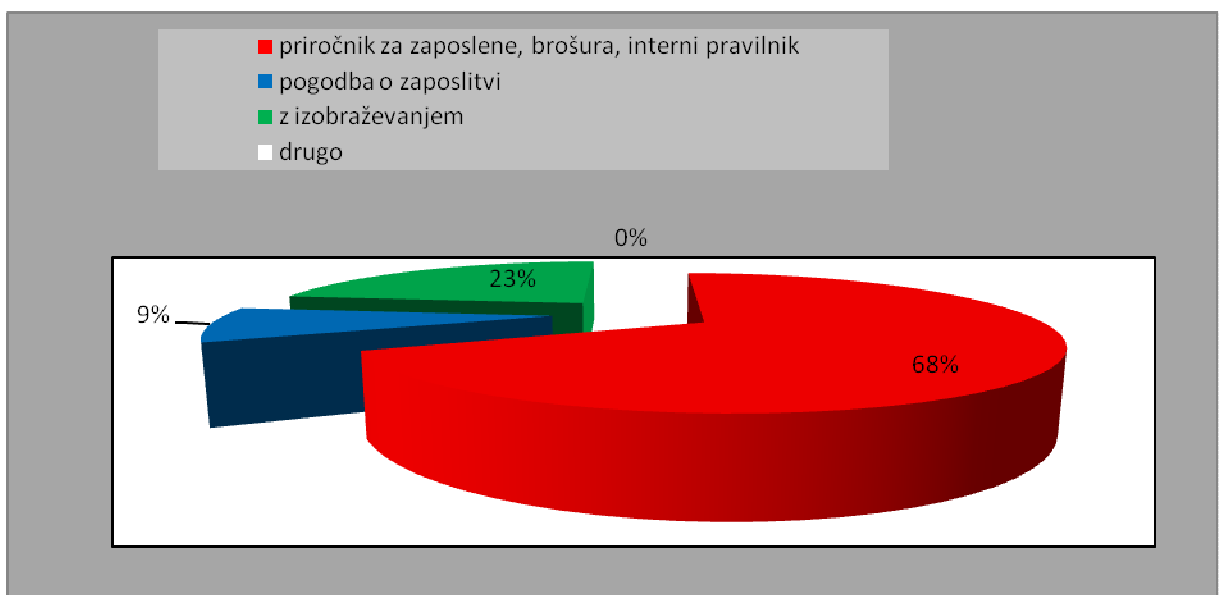
Grafikon 5: Predpisi, ki urejajo zaupne podatke



Vir: lastni (2010)

Na vprašanje *Ali menite, da ste dovolj seznanjeni s predpisi, ki urejajo zaupne podatke* sem ugotovila, da največ anketirancev meni, da so dobro seznanjeni s predpisi, ki urejajo zaupne podatke, in sicer kar 57 %. 26 % anketirancev meni, da so samo okvirno seznanjeni s predpisi, ki urejajo zaupne podatke. 14 % anketirancev meni, da poznajo predpise zelo dobro ter 3 % anketirancev meni, da ne poznajo predpisov, ki urejajo zaupne podatke.

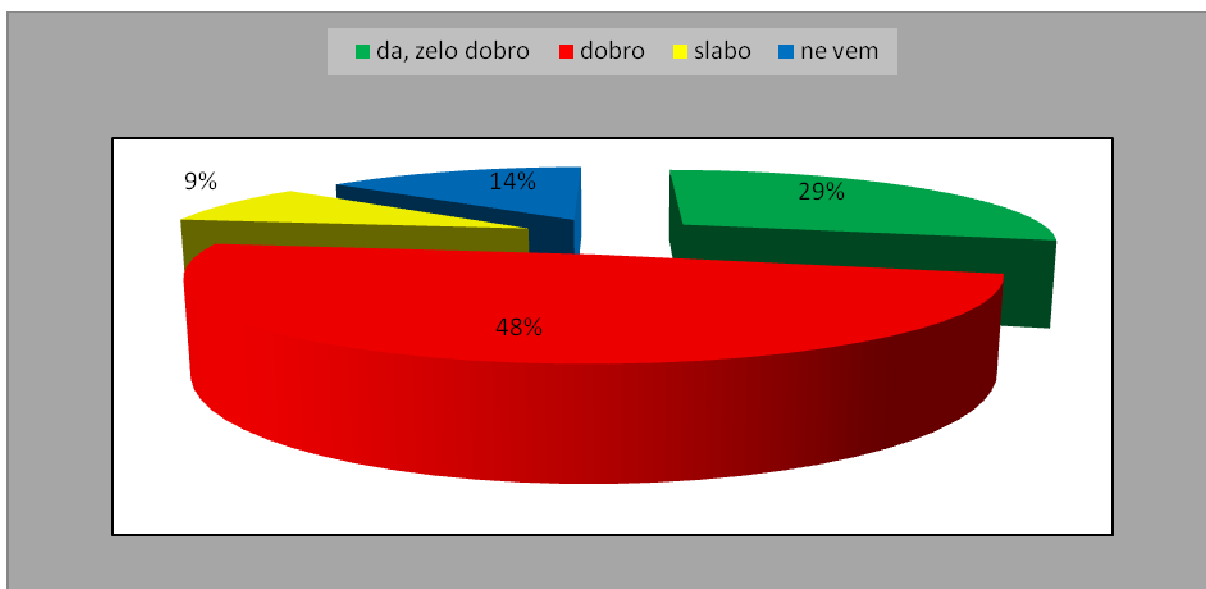
Grafikon 6: Seznanjenost z dolžnostmi varovanja zaupnih podatkov



Vir: lastni (2010)

Za šesto vprašanje *Kako ste v vaši organizaciji seznanjeni z dolžnostmi varovanja zaupnih podatkov?* 69 % anketirancev pravi, da so seznanjeni preko priročnika za zaposlene, preko brošure o varovanju informacij ali internega pravilnika (akta). 23 % anketirancev je seznanjenih z izobraževanjem, 8 % anketirancev pa meni, da v pogodbi o zaposlitvi.

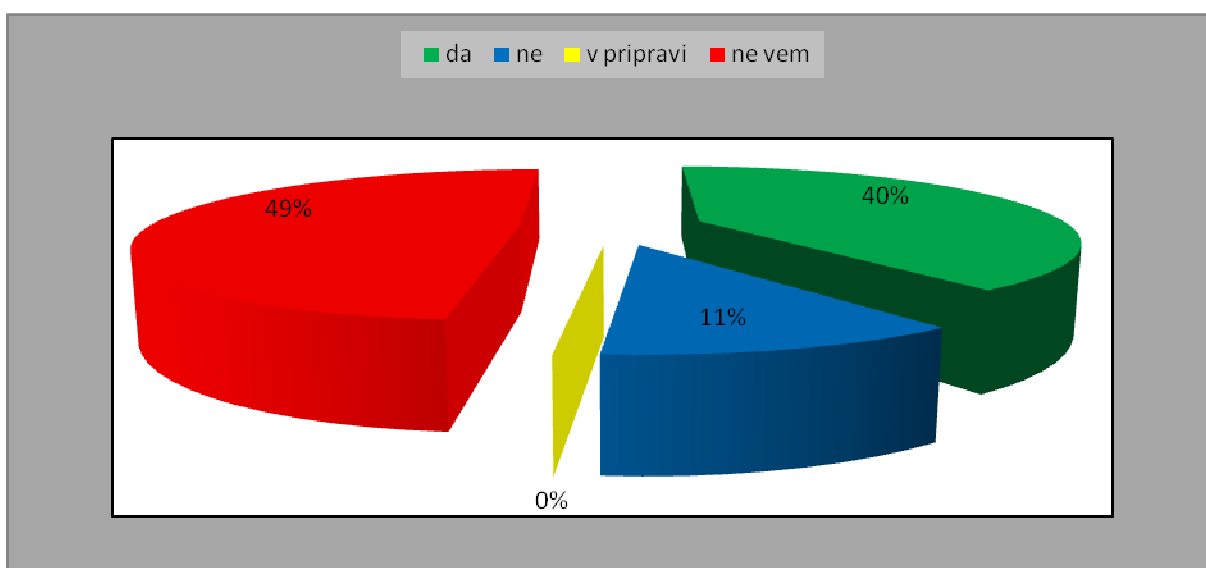
Grafikon 7: Zaščita prostorov in opreme, kjer se hranijo zaupni podatki



Vir: lasnti (2010)

Ali imate v vaši organizaciji varno zaščitene prostore in opremo, kjer hranite zaupne podatke? Na to vprašanje je 48 % anketirancev mnenja, da imajo dobro varovane prostore in opremo, kjer hranijo zaupne podatke. 29 % anketirancev je odgovorilo, da imajo zelo dobro varovan prostore in opremo. 14 % anketirancev sploh ne ve, kako imajo varovane prostore in opremo in 9 % anketirancev meni, da imajo slabo varovane prostore in opremo, kjer hranijo zaupne podatke.

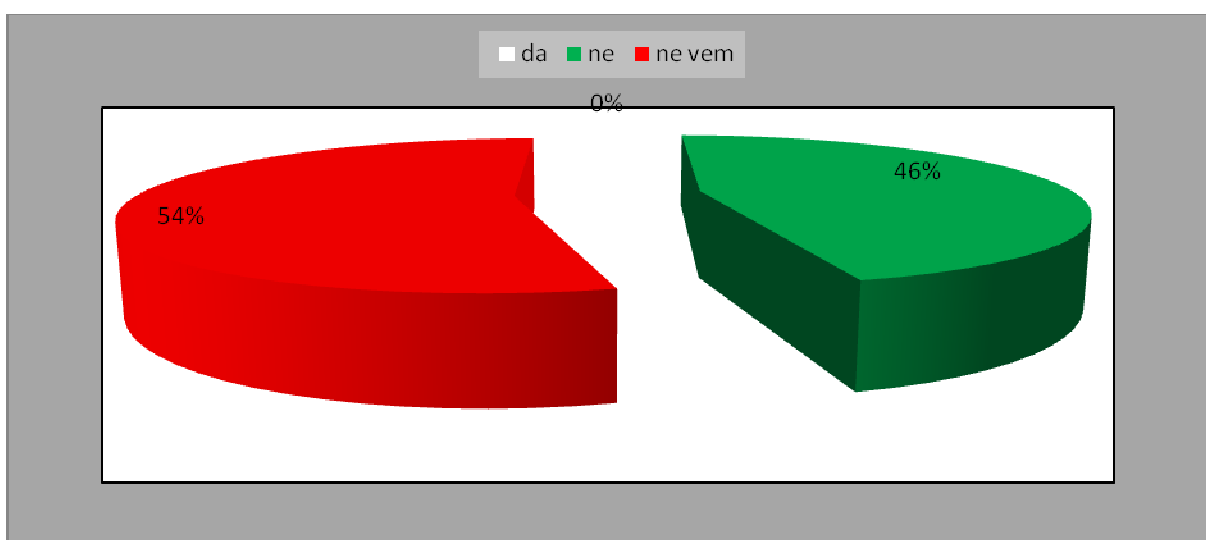
Grafikon 8: Varnostna politika



Vir: lastni (2010)

Osmo vprašanje se glasi: »Ali ima vaša organizacija napisano politiko o varovanju informacij (varnostno politiko)?« Največ anketirancev mi je odgovorilo, da ne vedo, ali imajo napisano varnostno politiko, kar 49 %. 40 % anketirancev mi je odgovorilo, da imajo napisano varnostno politiko. 11 % anketirancev meni, da sploh nimajo napisane varnostne politike in nihče ni odgovoril, da imajo varnostno politiko v pripravi.

Grafikon 9: Razkritje, zloraba zaupnih podatkov s strani zaposlenih

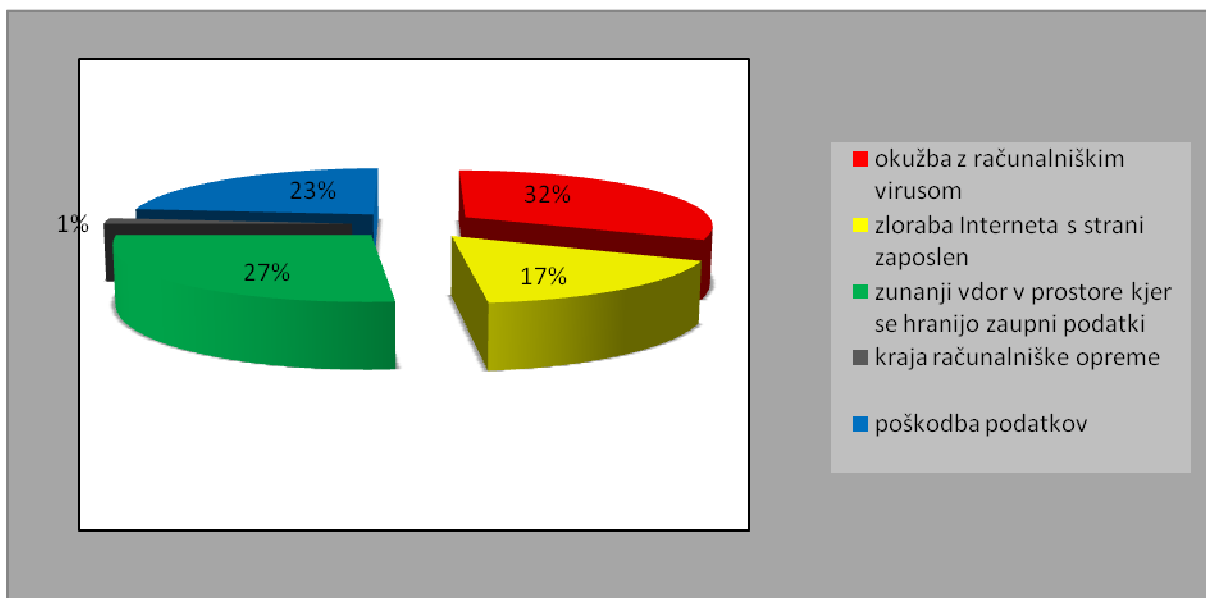


Vir: lastni (2010)

Deveto vprašanje se glasi: »Je že prišlo v vaši organizaciji do kakšnega razkritja, zlorabe zaupnih podatkov s strani zaposlenih?« 54 % anketirancev je odgovorilo, da ne vedo, ali

je že prišlo do razkritja, zlorabe zaupnih podatkov. 46 % anketirancev pa meni, da še ni prišlo do razkritja, zlorabe zaupnih podatkov. Nihče ni odgovoril, da je že prišlo do razkritja, zlorabe zaupnih podatkov.

Grafikon 10: Zaupni podatki so danes zelo ogroženi, zakaj?



Vir: lastni (2010)

Deseto vprašanje se glasi: »Zaupni podatki so danes zelo ogroženi, zakaj? (izpostavite po vašem mnenju dva najpogostejša vzroka).« 32 % anketirancev meni, da so zaupni podatki najpogostejše ogroženi zaradi okužbe z računalniškim virusom, 27 % anketirancev meni, da zaradi zunanjega vdora v prostore, kjer se hranijo zaupni podatki, 23 % anketirancev je odgovorilo, da zaradi poškodbe podatkov, 17 % anketirancev meni, da zaradi zlorabe interneta s strani zaposlenih ter 1 % anketirancev meni, da zaradi kraje računalniške opreme.

6.3 KONČNE UGOTOVITVE

S pomočjo ankete sem ugotovila, da je na Upravni enoti Slovenska Bistrica zaposlenih več žensk kot moških. Največ zaposlenih je starih med 40 in 50 let. Najpogostejša stopnja izobrazbe je visoka šola. Zaposleni, ki so sodelovali v anketi, imajo najpogosteje delovno dobo med 20 in 30 leti.

Na začetku izdelave diplomskega dela sem si zastavila tri cilje. S pomočjo ankete je bila ugotovljena pravilnost teh ciljev.

Cilj 1 se glasi: 50 % zaposlenih na svojem delovnem mestu meni, da so zelo dobro seznanjeni s predpisi, ki urejajo zaupne podatke, kar sem ugotovila s pomočjo petega vprašanja v anketi, ki se glasi: »Menite, da ste dovolj seznanjeni s predpisi, ki urejajo zaupne podatke?« Na vprašanje so anketiranci lahko obkrožili a) da, poznam predpise, zelo dobro, b) dobro, c) samo okvirno, d) ne poznam predpisov.

Cilj, ki sem si ga zastavila, ni potrjen, kajti le 14 % anketirancev meni, da so zelo dobro seznanjeni s predpisi, ki urejajo zaupne podatke. Vendar pa kar 57 % anketirancev meni, da so samo dobro seznanjeni s predpisi, ki urejajo zaupne podatke.

Cilj 2 se glasi: največ anketirancev meni, da imajo v organizaciji zelo dobro zaščitene prostore in opremo, kjer se hranijo zaupni podatki. Sedmo vprašanja v anketi se glasi: »Zaupni podatki se morejo ustrezno obdelovati in hraniti. Ali imate v vaši organizaciji varno zaščitene prostore in opremo, kjer hranite zaupne podatke?« Na vprašanje so anketiranci lahko obkrožili z: a) da, zelo dobro, b) dobro, c) slabo, d) ne vem. S pomočjo tega vprašanja sem ugotovila, da največ anketirancev meni, da imajo dobro varovane prostore in opremo, kjer se hranijo zaupni podatki, in sicer kar 48 %. 29 % anketirancev je mnenja, da imajo zelo dobro varovane prostore in opremo, kjer se hranijo zaupni podatki. Cilj, ki sem si ga zastavila, ni potrjen, saj je več anketirancev odgovorilo, da imajo le dobro varovane prostore in opremo, kjer se hranijo zaupni podatki.

Cilj 3 se glasi: organizacija ima napisano politiko o varovanju informacij – varnostno politiko. Osmo vprašanja v anketi se glasi: »Ali ima vaša organizacija napisano politiko o varovanju informacij (varnostno politiko)?« Na vprašanje so imeli anketiranci možnost obkrožiti a) da, b) ne, c) v pripravi, d) ne vem. 49 % anketirancev je odgovorilo, da ne vedo, ali imajo napisano varnostno politiko. Vendar je 40 % anketirancev odgovorilo, da imajo napisano varnostno politiko. Cilj, ki sem si ga zastavila, je potrjen.

Anketiranci so večinoma odgovorili, da ne vedo za primer, da bi prišlo do razkritij ali zlorabe zaupnih podatkov s strani zaposlenih, čeprav menim, da je že prišlo do takšnega dejanja. Glede na to, da je bilo že veliko takšnih razkritij in zlorab objavljenih v medijih. Na vprašanje, zakaj so najpogosteje ogroženi zaupni podatki, so anketiranci odgovorili, da

zaradi zunanjega vdora v prostor, kjer se hranijo zaupni podatki in poškodba teh podatkov.

7 ZAKLJUČEK

V Sloveniji poznamo preko deset vrst poimenovanja zaupnosti. Te zaupnosti niso poenotene niti z označevanjem niti glede hrambe.

Skrivnost in tajnost v nekaterih zakonih regulirajo varovanje informacij in podatkov, ki so tako pomembni, da bi njihovo razkritje lahko škodovalo delovanju in izvajanju nalog organizacije ali celo interesom Republike Slovenije. Zato lahko namesto besede skrivnost in tajnost uporabljamo primernejši izraz – zaupnost.

Najpogostejše vrste skrivnosti in tajnosti, ki so razdeljene v tri kategorije zaupnosti, glede na mesto nastanka zaupnih podatkov, so: gospodarske zaupnosti, uradne zaupnosti in posameznikove zaupnosti. Gospodarske zaupnosti so poslovna skrivnost, poslovna tajnost, industrijska skrivnost, informacijska skrivnost, bančna tajnost, znanstvena tajnost, umetniška tajnost,... Uradne zaupnosti so tajni podatki, uradna tajnost, davčna tajnost, vojaška tajnost, državna tajnost, zdravniška tajnost, poklicna skrivnost,... Posameznikove zaupnosti pa so osebni podatki.

Temeljno načelo varovanja zaupnih podatkov je zagotavljanje njegove nedostopnosti. Pomembno je, da se z zaupnimi podatki seznanijo le majhen krog oseb. Osebe, ki lahko dostopajo do zaupnih podatkov, morajo biti upravičene in pooblaščenice.

Informacijski pooblaščenec je s svojim nastankom dobil veliko pooblastil do vpogleda v zaupne podatke. Pooblaščenec ima dostop do tajnih podatkov vseh stopenj brez pridobivanja dovoljenja, kot jih določa Zakon o tajnih podatkih. Takšno pooblastilo imajo le najvišji državni funkcionarji, ob dejstvu, da dobijo te osebe dovoljenje z začetkom opravljanja funkcije in podpisom izjave.

Vsi zaposleni, ki imajo dostop do zaupnih podatkov, morajo podpisati formalno izjavo o varovanju podatkov. Posameznik, ki prekrši obveznosti varovanja zaupnih podatkov, je lahko kaznovan, če mu je krivda dokazana. Zakon o tajnih podatkih ureja izdajo dovoljenja za dostop do zaupnih podatkov, ki se zapiše v odločbo. Dovoljenja za dostop do zaupnih podatkov se izdajo za določen čas v treh stopnjah. Imetniki dovoljenja za dostop do zaupnih podatkov so osebe, ki potrebujejo dostop do zaupnih podatkov zaradi opravljanja svoje funkcije.

Pri zaupnosti gre predvsem za odgovornost vodstva, da lažje obvladuje določene aktivnosti, saj so praviloma zaupane le ožjemu krogu oseb. A prevečkrat se zgodi, predvsem v množičnih medijih, da smo priča razkritju informacij, ki so zaupne narave. Ker je dostop do zaupnih podatkov precej enostaven (vemo namreč, kdo z zaupnimi podatki upravlja), je načinov, kako do take informacije ali podatkov priti, več. Lahko gre za spontan pogovor s sogovornikom, ki mimogrede izda zanimiv zaupni podatek, grožnje osebi, podkupovanje, malomarnost pri pospravljanju zaupne dokumentacije v omare, do odtekanja informacij zaradi škodovanja organizacij.

Organizacije, ki imajo opravke z zaupnimi podatki, morajo za delo z zaupnimi podatki zagotoviti ustrezne pogoje. Varovanje prostorov z zaupnimi podatki mora biti varovano s fizičnimi, tehničnimi in organizacijskimi ukrepi. Varovanje opreme z zaupnimi podatki je potrebno ustrezno zaščititi. Zaupni podatki morajo biti shranjeni v zaklenjenih omarah, sefu, kar naj bo ognjevarno in vodotesno.

S hrambo zaupnih podatkov se zagotovi varovanje zaupnih podatkov za dalj časa, ne glede na obliko ali medij, v katerem se nahaja zaupni podatek.

Z razkritjem zaupnih podatkov se srečamo takrat, ko se zaupni podatki objavijo v javnosti z namenom, da se prikaže neko zasebno stanje. Razkritje zaupnih podatkov se za škodljivo in kaznivo izkaže, ko se zaupni podatki posredujejo osebi, ki do zaupnih podatkov ni upravičena in pooblaščen. Motivov za zlorabo in izdajo zaupnih podatkov je več. Pomembno je, da pozna organizacija čim več motivov. Organizacija ima s tem več možnosti, da prepreči takšno delovanje.

Visoko stopnjo zavarovanja zaupnih podatkov lahko zagotovi tudi organizacija z majhnim številom uslužbencev in kjer poteka poslovanje brez obiskovalcev.

Vedeti moramo, da ni sistema, ki bi bil proti razkritju ali zlorabi zaupnih podatkov popolnoma zanesljiv.

Vsaka organizacija naj bi imela izdelano politiko varovanja informacij. Politika varovanja informacij je interni akt organizacije. Ločimo tri nivoje varnostne politike: krovno varnostno politiko, varnostno politiko za posamezna področja ter operativna navodila, interni standardi in postopki za delo. Priporočljivo je, da je varnostna politika v internih aktih opredeljena kot obvezujoči akt, ki ga morajo zaposleni spoštovati.

Ker smo zgolj ljudje so nam skrivnosti bolj zanimive kot neskrivnosti. Zato je zavedanje, da se je potrebno z varovanjem zaupnih podatkov ukvarjati sistematično in celovito eden izmed temeljnih pogojev, ki jih mora družba osvojiti, da ne bo prihajalo do škodljivih primerov. Potrebno je vložiti ogromno energije in sredstev, tako za usposabljanje, tehnično in fizično obliko varovanja kot nadzorovanje s strani izkušenih profesionalcev, ki poskušajo slediti varnostnim standardom in pravilom vsake panoge.

Slovenija je z stopom v zvezo Nato in Evropsko unijo postala del držav, ki so se kot članice ene ali druge integracije obvezale, da bodo na skupnih interesnih področjih poskrbele, da bodo ta področja urejena na enak ali primerljiv način med posameznimi državami. Za vstop v obe organizacije je morala Slovenija urediti tudi področje tajnih podatkov na tak način, da so postopki in ukrepi za zagotovitev varnosti tajnih podatkov Evropske unije in zveze Nato v Sloveniji primerljivi z ukrepi, ki jih uporabljata obe organizaciji.

V Sloveniji smo (tudi zaradi vstopa v evrointegracije) dosegli primerno stopnjo razumevanja pomena zaupnih podatkov. Korak naprej k zagotavljanju ustreznega varovanja zaupnosti bo potrebno storiti še v smislu profesionalizacije varnostne dejavnosti organizacije, usposabljanje zaposlenih, opozarjanje na napake iz dnevne delovne prakse.

LITERATURA

1. BOGATAJ Jože. Podatki o fizični osebi – dolžniku v Modra knjiga o podatkih. Ljubljana, 2004.
2. ERŠTE Igor. Model varovanja podatkov za preprečevanje gospodarskega kriminala, specialistično delo. Univerza v Mariboru, Fakulteta za organizacijske vede, Kranj, 2006.
3. HAJTNIK Tatjana, Priporočilo za pripravo informacijske varnostne politike, Center Vlade RS za informatiko, Ljubljana, 2002.
4. HARTMAN Ervin. Varovanje tajnih podatkov in varnostna kultura na obrabnem področju; protiobveščevalni-varnostni vidik. Univerza v Ljubljani, Fakulteta za družbene vede, Ljubljana, 2007.
5. KOP Ivo. Varovanje in zaščita poslovnih skrivnosti, druga predelana in dopolnjena izdaja. Gospodarski vestnik, Ljubljana 1995.
6. KOROŠEC Sabina. Varnostno preverjanje v Republiki Sloveniji. Univerza v Ljubljani, Fakulteta za družbene vede, Ljubljana 2006.
7. LAVRIČ Tomaž. Zaupnost podatkov ter varstvo pravice do pridobivanja javnih informacij, magistrsko delo. Univerza v Ljubljani, Fakulteta za upravo, Ljubljana, 2006.
8. LAVRIČ Tomaž. Obravnava zaupnih podatkov. Fakulteta za upravo, študijsko gradivo, 2008.
9. LAVRIČ Tomaž. Zaupni podatki v dokumentarnem in arhivskem gradivu. Tehnični in vsebinski problemi klasičnega in elektronskega arhiviranja. Zbornik referatov z dopolnilnega izobraževanja, Maribor. 2008, str. 41-51.
10. STARE Janez, LAVRIČ Tomaž. Varovanje zaupnih podatkov. Fakulteta za upravo, študijsko gradivo, 2008.

VIRI

1. Bančni kodeks in Združenja Bank Slovenije.
Dosegljivo na: <http://www.zbs-giz.si/zdruzenje-bank.asp?StructureId=381> (2. 9. 2009).
2. ČALETA Denis. Varovanje tajnih podatkov v zvezi NATO. Bilten slovenske vojske, let. 6, str. 59-81. 2004.
3. ČRNČEC Damir. Dostop do tajnih podatkov in varnostno preverjanje oseb. Varstvoslovje, 2004, let. 6, št. 1. 47-58.
4. Kazenski zakonik. Ur. list RS, št. 55/2008.
5. KOVAČ Polona, Pravna praksa, 5. 6. 2008, str. 11-13.
6. Merilo za ureditev poslovnih prostorov državne uprave. Ministrstvo za javno upravo 2007. Dosegljivo na:

http://www.mju.gov.si/fileadmin/mju.gov.si/pageuploads/mju_dokumenti/pdf/Merila_POSLOVNI_PROSTORI_DUO.pdf (10. 10. 2009).

7. Odvetniška Zbornica Slovenije. Kodeks odvetniške poklicne etike.
Dosegljivo na: <http://www.odv-zb.si/default.aspx?cid=2&aid=12> (9. 9. 2009).
8. Pravilnik o varovanju zaupnih ter osebnih podatkih ter varovanja dokumentarnega gradiva.
9. Predlog zakona o spremembah in dopolnitvi ZTP.
10. Slovar Slovenskega knjižnega jezika CD-rom.
11. Zakon o bančništvu. Ur. list RS, št. 131/2006.
12. Zakon o bankah in hranilnicah. Ur. list RS, št. 1/1991.
13. Zakonu o davčnem postopku. Ur. list RS, št. 117/2006.
14. Zakon o dostopu informacij javnega značaja. Ur. list RS, št. 51/2006.
15. Zakon o gospodarskih družbah. Ur. list RS, št. 65/2009.
16. Zakon o industrijski lastnini. Ur. list RS, št. 51/2006.
17. Zakon o policiji. Ur. list RS, št. 66/2009.
18. Zakon o poklicnem in strokovnem izobraževanju. Ur. list, št. 79/2006.
19. Zakona o Slovenski obveščevalni-varnostni agenciji. Ur. list RS, št. 81/2006.
20. Zakon o tajnih podatkih. Ur. list RS, št. 135/2003.
21. Zakon o varstvu osebnih podatkov. Uradni list RS, št. 94/2007.
22. Zakon o zasebnem varovanju. Uradni list RS, št. 126/2003.
23. Ustava Republike Slovenije. Ur. list RS, št. 33/1991.
24. Sindikalnik območne organizacije ZSSS.
Dosegljivo na: <http://sindikalnik.blog.siol.net/2008/02/29/surs-29-2-2008/> (2. 9. 2009).
25. Wikipedia The Free Encyclopedia. Zaupnost.
Dosegljivo na: <http://en.wikipedia.org/wiki/Confidentiality> (11. 10. 2009).

PRILOGA

ANKETNI VPRAŠALNIK

Lepo pozdravljeni!

Moje ime je Katja Mavhar in sem študentka Univerze v Ljubljani, Fakultete za upravo. Pod mentorstvom doc. dr. Janeza Stareta delam diplomsko delo, katerega tema je Ravnanje z zaupnimi podatki.

Prosim vas za sodelovanje v kratki anketi, ki mi bo pomagala pri raziskavi, ki je sestavni del diplomskega dela. Anketa je neobvezna, anonimna in ne vsebuje osebnih podatkov, pridobljeni rezultati pa bodo namenjeni zgolj izdelavi diplomskega dela.

Za sodelovanje se vam lepo zahvaljujem.

Katja Mavhar

1. Spol

- a) moški
- b) ženski

2. Starost

- a) manj kot 20 let
- b) 20–30 let
- c) 30–40 let
- d) 40–50 let
- e) več kot 50 let

3. Stopnja izobrazbe

- a) srednja
- b) poklicna
- c) višja
- d) visoka
- e) magisterij
- f) doktorat

4. Delovna doba

- a) manj kot 5 let
- b) 5–10 let
- c) 10–20 let
- d) 20–30 let
- e) 30–40 let
- f) več kot 30 let

5. Menite, da ste dovolj seznanjeni s predpisi, ki urejajo zaupne podatke?

- a) da, poznam predpise zelo dobro
- b) dobro
- c) samo okvirno
- d) ne poznam predpisov

6. Kako ste v vaši organizaciji seznanjeni z dolžnostmi varovanja zaupnih podatkov?

- a) preko priročnika za zaposlene, preko brošure o varovanju informaciji ali internega pravilnika (akta)
- b) v pogodbi o zaposlitvi
- c) z izobraževanjem
- d) drugo_____
- _____.

7. Zaupni podatki se morajo ustrezno obdelovati in hraniti. Ali imate v vaši organizaciji varno zaščitene prostore in opremo, kjer hranite zaupne podatke?

- a) da, zelo dobro
- b) dobro
- c) slabo
- d) ne vem

8. Ali ima vaša organizacija napisano politiko o varovanju informacij (varnostno politiko)?

- a) da
- b) ne
- c) v pripravi
- d) ne vem

9. Je že prišlo v vaši organizaciji do kakšnega razkritja, zlorabe zaupnih podatkov s strani zaposlenih.

- a) da
- b) ne
- c) ne vem

Če ste odgovorili z da, kakšne so bile sankcije za uslužbenca?

11. Zaupni podatki so danes zelo ogroženi, zakaj? (Izpostavite po vašem mnenju dva najpomembnejša vzroka.)

- a) okužba z računalniškim virusom
- b) zloraba interneta s strani zaposlenih
- c) zunanji vdor v prostore, kjer se hranijo zaupni podatki
- d) kraja računalniške opreme
- e) poškodba podatkov