UNIVERZA V LJUBLJANI
FAKULTETA ZA UPRAVO

Diplomsko delo
visokošolskega programa

DOVOLJENJE ZA DOSTOP DO TAJNIH PODATKOV NA MINISTRSTVU ZA OKOLJE IN PROSTOR

Študent: Andrej Loboda
Št. indeksa: 29735

Mentor: mag. Slavko Debelak

Ljubljana, julij 2009

Povzetek

V diplomskem delu z naslovom Dovoljenje za dostop do tajnih podatkov na Ministrstvu za okolje in prostor predstavljam predpise in ureditev področja tajnih podatkov v Republiki Sloveniji in drugih državah ter Evropski uniji in Natu, poseben poudarek pa dajem raziskavi področja tajnih podatkov in dovoljenja za dostop do tajnih podatkov na Ministrstvu za okolje in prostor. V času od leta 2001 je Republika Slovenija skladno s statusom članice kandidatke za članstvo v Evropski uniji in Natu sprejela več predpisov, ki urejajo področje tajnih podatkov tako, da so le-ti skladni s predpisi v Evropski uniji in Natu. Zakonodaja je napisana natančno, pa vendar prinaša določene težave, oziroma ne določa, točno kdo v državi potrebuje dovoljenje za dostop do tajnih podatkov. Tako so državni organi sami določili delovna mesta, na katerih je kot eden od pogojev za zasedbo pridobitev dovoljenja za dostop do tajnih podatkov. Ministrstvo za okolje in prostor je ravno tako moralo določiti takšna delovna mesta. Vprašanje, s katerim se ukvarjam v diplomski nalogi, je tudi to, ali je za vsa delovna mesta potrebno dovoljenje za dostop do tajnih podatkov ali ne. Je prostor, kjer bodo ti zaposleni obravnavali ali določali tajne podatke, primeren oziroma ali sploh obstaja? Z pregledom področja pri nas in na tujem ter prakse, ki obstaja na Ministrstvu za okolje in prostor, bom poskušal odgovoriti na ta vprašanja, ki pa imajo seveda več možnih odgovorov oziroma rešitev.

Ključne besede: tajni podatki, dovoljenje za dostop do tajnih podatkov, delovna mesta z dovoljenjem za dostop do tajnih podatkov, tajni podatki Evropske unije, tajni podatki Nata, Ministrstvo za okolje in prostor.

Summary

In my diploma work entitled Authorization for access to classified information at the Ministry of Environment and Spatial Planning I am representing the field of classified information in the Republic of Slovenia and other countries, the European Union and NATO, with particular emphasis on classified information and authorization for access to classified data on the Ministry of Environment and Spatial Planning. From the year 2001, the Republic of Slovenia in accordance with the status of candidates for membership in the European Union and NATO has adopted several regulations governing the classified information so that they comply with the regulations of the European Union and NATO. The legislation is written carefully, however, entails certain problems, or does not specify exactly who in the country needs a license for access to classified information. The State public body determined the positions for which the condition for the occupation is authorization to access classified information. Ministry of Environment and Spatial Planning also needed to establish such posts, the question I am dealing with is whether this all the posts require authorization for access to classified information or not? Is the place where these employees deal with classified information, appropriate or not, is there such place at all? By reviewing this area in Slovenia and abroad, and practices that exist in the Ministry of Environment and Spatial Planning, I will try to answer some of these questions, which have of course several possible answers or solutions.

Keywords: classified information, authorization for access to classified information, jobs with the permission for access to classified information, secret informations of the European Union, NATO classified information, the Ministry of Environment and Spatial Planning.

KAZALO

1 UVOD

Tajnost ali zaupnost so besede, ki označujejo nekaj skritega, večini od nas nedostopnega in ravno zato so tajni podatki vedno bili, so in bodo zanimivi večini, ki do njih nima dostopa. Kakorkoli, nekateri so pri svojem delu vseeno primorani delati s tajnimi podatki, zato nastopi po danes veljavni zakonodaji nekaj problemov ob nastopu dela na delovnem mestu, ki zahteva dostop do tajnih podatkov določene stopnje tajnosti.

Povezanost delovnega razmerja in tajnih podatkov je v Sloveniji prisotna od sprejema Zakona o tajnih podatkih, to je od leta 2001. Danes je v veljavi nekoliko spremenjen Zakon o tajnih podatkih (UPB, Ur. l. RS št. 50/2006), največji popravki so bili v preteklosti na področju varnostnega preverjanja in varnostnih območij. Delovno razmerje in Zakon o tajnih podatkih (UPB, Ur. l. RS št. 50/2006) sta v neki določeni zvezi ves čas zaposlitve na delovnem mestu, ki zahteva dostop do tajnih podatkov določene stopnje. V prvi fazi gre za pridobitev dovoljenja za dostop do tajnih podatkov po sami zasedbi določenega delovnega mesta, v nadaljevanju delovnega razmerja. Povezanost ostaja zaradi pogoja, da mora zaposleni ohraniti dovoljenje za dostop do tajnih podatkov, dokler se na delovnem mestu zahteva dostop do tajnih podatkov, nenazadnje pa je lahko odsotnost dovoljenja za dostop do tajnih podatkov tudi razlog za prekinitev delovnega razmerja oziroma pogodbe o zaposlitvi.

Splošne pogoje za zasedbo delovnega mesta določata Zakon o delovnih razmerjih in Zakon o javnih uslužbencih. Zakon o delovnih razmerjih v našem primeru nastopa kot bolj splošen akt o pogojih za zasedbo nekega delovnega mesta, medtem ko Zakon o javnih uslužbencih predpisuje znanje uradnega jezika ter naziv, smer izobrazbe oziroma poklicne kvalifikacije, funkcionalna in specialna znanja ter sposobnosti, lahko pa tudi druge pogoje, če tako določa zakon, v našem primeru Zakon o tajnih podatkih (UPB, Ur. l. RS št. 50/2006). Ti pogoji morajo biti določeni v splošnem aktu delodajalca, torej, sistemizaciji delovnih mest, ki je podlaga za določitev nalog in pogojev za zasedbo delovnega mesta. Kot enega od pogojev za zasedbo delovnega mesta lahko torej delodajalec določi glede na naravo dela za posamezna delovna mesta tudi nacionalno dovoljenje za dostop do tajnih podatkov določene stopnje tajnosti oziroma dovoljenje za dostop do tajnih podatkov EU ali zveze Nato.

1.1 PREDMET IN CILJ RAZISKOVANJA

V diplomski nalogi bom opisal Zakon o tajnih podatkih (UPB, Ur. l. RS št. 50/2006) in podrejene predpise tega zakona, postopek zaposlitve na delovno mesto, ki zahteva dovoljenje za dostop do tajnih podatkov, in ugotovitve, kakšno pravno varstvo ima zagotovljeno oseba, pri kateri je bil ugotovljen varnostni zadržek. Področje, ki ga raziskujem, je zame zanimivo tudi zaradi dejstva, da že več kot šest let delam na obravnavanem področju, in sicer tako v postopkih, povezanih z varnostnim preverjanjem zaposlenih na Ministrstvu za okolje in prostor, varnostnimi ukrepi kot

tudi samem delu z dokumenti, ki vsebujejo tako nacionalne, EU ter Nato podatke z določeno stopnjo tajnosti.

Ugotovitve, predstavljene v diplomskem delu, bodo lahko pripomogle k boljšemu poznavanju področja tajnih podatkov in morebitni optimizaciji delovnih mest, ki imajo kot pogoj za zasedbo dovoljenje za dostop do tajnih podatkov. Diplomsko delo bo lahko pripomoček kadrovski službi Ministrstva za okolje in prostor ob sprejemanju sistemizacije oziroma njenih popravkov.

1.2 METODE DELA

Temo diplomske naloge bom obdelal s kombinacijo literature, ki obstaja, predpisi, napisanimi na temo tajnih podatkov, in delovnih razmerij, izdanih s strani zakonodajalca in Ministrstva za okolje in prostor, ter raziskavo in na koncu anketiranjem zaposlenih na Ministrstvu za okolje in prostor, ki imajo dovoljenje za dostop do tajnih podatkov.

2 PREDSTAVITEV VELJAVNE ZAKONODAJE

2.1 ZAKON O TAJNIH PODATKIH

Leta 2001 je bil sprejet krovni predpis, ki ureja varovanje tajnih podatkov, Zakon o tajnih podatkih (Ur. l. RS št. 87/2001). Zakonska ureditev področja tajnih podatkov je s tem postala primerljiva z drugimi državami članicami zveze Nato in EU. Sam zakon je prinesel kar precej novosti glede na predhodno delno urejeno področje. Že kmalu po uveljavitvi Zakona o tajnih podatkih pa se je ugotovilo, da je z zakonom predvidenih kar nekaj rešitev, za katere bi bila potrebna finančna sredstva. Sprejem zakona namreč ni predvideval nobenih finančnih posledic za njegovo uveljavitev. Po sprejetju zakona se tako nekaj časa nihče več ni ukvarjal s problemom, kako zadostiti zakonskim zahtevam. S približevanjem Republike Slovenije v zvezo Nato in EU so se določbe sprejetih predpisov vendarle pričele uresničevati v praksi. Od zveze Nato in EU smo dobili kar nekaj strokovnih usmeritev, kako mora biti organizirano področje tajnih podatkov.

Skladno z Zakonom o tajnih podatkih je bil ustanovljen Urad Vlade Republike Slovenije za varovanje tajnih podatkov (Ur. l. RS, št. 6/2002). Njegove glavne naloge so predvsem spremljanje stanja na področju določanja in varovanja tajnih podatkov, skrb za razvoj in uveljavitev fizičnih, organizacijskih in tehničnih standardov, skrb za izvrševanje sprejetih mednarodnih obveznosti, pripravljanje predlogov predpisov, dajanje mnenj o skladnosti splošnih aktov z Zakonom o tajnih podatkih, vodenje evidence izdanih dovoljenj, predlaganje ukrepov za izboljšanje varovanja tajnih podatkov in drugo. Naloga urada je bila v prvem obdobju predvsem pripravljanje predlogov predpisov, ki jih je bilo treba sprejeti na podlagi Zakona o tajnih podatkih. Urad za varovanje tajnih podatkov je akreditiran za nadzor nad delom s tajnimi podatki EU in NATO. Za nacionalne tajne podatke so za notranji nadzor odgovorni predstojniki organov.

Danes je v uporabi drugo uradno prečiščeno besedilo Zakona o tajnih podatkih – Zakon o tajnih podatkih (UPB-2, Ur. l. RS št. 50/2006).

2.2 UREDBA O VAROVANJU TAJNIH PODATKOV

Uredba o varovanju tajnih podatkov (Ur. l. RS št. 74/2005) je bila izdana z namenom zamenjave Uredbe o načinih in oblikah označevanja tajnih podatkov ter fizičnih, organizacijskih in tehničnih ukrepih ter postopkih za varovanje tajnih podatkov (Ur. l. RS, št. 70/2002). Namen izdaje nove uredbe je bil predvsem v lažjem oz. bolj izvedljivem izvajanju postopkov varovanja tajnih podatkov v praksi. Kot primer lažjega izvajanja določil uredbe lahko navedemo nekaj sprememb:

- dokumenti stopnje tajnosti Tajno ali Strogo tajno so se izven varnostnih območij prenašali le z oboroženim spremstvom, nova uredba to določilo odpravlja,

- odpravljeno je varnostno območje 3. stopnje, oz. je le-to določeno kot celotno upravno območje organa, določeno s hišnim redom,
- upravnega območja ni treba posebej označevati, kakor je to veljalo za 3. varnostno območje,
- stara uredba je prepovedovala kopiranje dokumentov s stopnjo tajnosti (z nekaj izjemami), nova uredba dovoljuje kopiranje (ob izpolnjevanju določenih pogojev), razen kopiranja dokumentov s stopnjo Strogo tajno.

2.3 UREDBA O NOTRANJEM NADZORU NAD IZVAJANJEM ZAKONA O TAJNIH PODATKIH IN PREDPISOV, IZDANIH NA NJEGOVI PODLAGI

Uredba o notranjem nadzoru nad izvajanjem zakona o tajnih podatkih in predpisov, izdanih na njegovi podlagi (Ur. l. RS, št.106/2002) bolj podrobno določa postopke notranjega nadzora nad izvajanjem zakona o tajnih podatkih oz. 41. in 42. člena Zakona o tajnih podatkih. Opredeljeni so izvajalci nadzora, oblike nadzora in vsebina nadzora.

2.4 UREDBA O IZVAJANJU INŠPEKCIJSKEGA NADZORA NA PODROČJU VAROVANJA TAJNIH PODATKOV IN VSEBINI POSEBNEGA DELA STROKOVNEGA IZPITA ZA INŠPEKTORJA

Uredba o izvajanju inšpekcijskega nadzora na področju varovanja tajnih podatkov in vsebini posebnega dela strokovnega izpita za inšpektorja (Ur. l. RS, št. 94/2006) je potrebna za nadzor nad izvrševanjem določb Zakona o tajnih podatkov in podrejenih predpisov ter mednarodnih pogodb, ki ga izvaja Inšpektorat Republike Slovenije za notranje zadeve, na obrambnem področju pa Inšpektorat Republike Slovenije za obrambo (Zakon o tajnih podatkih – UPB, Ur.l. RS št. 50/2006, 42. a člen).

2.5 UREDBA O NAČINU IN POSTOPKU VARNOSTNEGA PREVERJANJA

Uredba o načinu in postopku varnostnega preverjanja (Ur. l. RS, št. 110/2003) in Uredba o spremembah Uredbe o varnostnem preverjanju in izdaji dovoljenj za dostop do tajnih podatkov (Ur. l. RS, št. 138/2006) določa postopke varnostnega preverjanja, ki so podlaga za pridobitev dovoljenj za dostop do tajnih podatkov oz. postopke vmesnega varnostnega preverjanja. Uredba je bila sprejeta 12. 11. 2003, potem ko je bila zaradi neskladja z ustavo Republike Slovenije in večmesečnem zadržanju izvajanja Uredbe o načinu in postopku varnostnega preverjanja ter postopku izdaje in preklica dovoljenja za dostop do tajnih podatkov Ur. l. RS, št. 70/2002 nujno potrebna nova. V Uredbi o načinu in postopku varnostnega preverjanja so predpisani vsi obrazci, zaprosila, vprašalniki, ki so potrebni v postopkih nacionalnega varnostnega preverjanja, EU, in dovoljenja za dostop do tajnih podatkov zveze Nato. Z Uredbo o spremembah Uredbe o varnostnem preverjanju in

izdaji dovoljenj za dostop do tajnih podatkov so bili med drugim zamenjani varnostni vprašalniki in na novo določeni organi, ki izvajajo usposabljanje s področja tajnih podatkov. V Uredbi o načinu in postopku varnostnega preverjanja so predpisani obrazci dovoljenj za dostop do tajnih podatkov.

Slika 1: Dovoljenje za dostop do tajnih podatkov, izdano s strani Ministrstva za notranje zadeve javnemu uslužbencu


REPUBLIKA SLOVENIJA
0002607
MINISTRSTVO ZA NOTRANJE ZADEVE
Na podlagi 23. člena Zakona o tajnih podatkih (Uradni list RS, št. 87/01) izdajam
DOVOLJENJE
Številka: 60/2004
Za dostop do tajnih podatkov stopnje tajnosti: STROGO TAJNO
Ime in priimek: ANDREJ LOBODA
Datum rojstva: 08.06.1975
Dovoljenje velja od: 17.06.2004
do: 17.06.2009
Ljubljana, 17.06.2004
TP-1
Dragutin Mate
MINISTER

Vir: Arhiv Ministrstva za okolje in prostor.

2.6 SKLEP O USTANOVITVI, NALOGAH IN ORGANIZACIJI URADA VLADE REPUBLIKE SLOVENIJE ZA VAROVANJE TAJNIH PODATKOV

Sklep o ustanovitvi, nalogah in organizaciji Urada Vlade Republike Slovenije za varovanje tajnih podatkov (Ur. l. RS, št. 6/2002) je ustanovil Urad Vlade Republike Slovenije za varovanje tajnih podatkov, ki ima v naši državi sledeče naloge:

- spremlja stanje na področju določanja in varovanja tajnih podatkov,
- predlaga Vladi Republike Slovenije v sprejem standarde za varovanje tajnih podatkov,
- sodeluje z organi Evropske unije, zveze NATO in organi drugih mednarodnih organizacij in držav in tudi spremlja distribucijo tajnih podatkov med njimi,
- za vlado in ministrstva pripravlja predloge predpisov s področja tajnih podatkov,
- podaja mnenje o skladnosti splošnih aktov o določanju, varovanju in dostopu do tajnih podatkov z zakoni,
- koordinira delovanje državnih organov, pristojnih za varnostno preverjanje, in vodi evidenco izdanih dovoljenj za dostop do tajnih podatkov,
- vodi evidenco oseb, ki so napotene na varnostno preverjanje,
- organom predlaga, svetuje in odgovarja na vprašanja glede ukrepov za izboljšanje varovanja tajnih podatkov,
- opravlja druge naloge s področja varovanja tajnih podatkov.

Urad Vlade Republike Slovenije za varovanje tajnih podatkov tudi izdaja varnostna dovoljenja Evropske unije in zveze NATO ter skrbi za organizacijo usposabljanj kurirjev za prenos zadev, ki vsebujejo tajne podatke. V tem trenutku v Sloveniji ni kurirjev (razen kurirjev v Slovenski vojski), ki so usposobljeni za prenos takšnih

podatkov, ker Urad Vlade Republike Slovenije za varovanje tajnih podatkov ni pravočasno organiziral usposabljanj.

2.7 PRAVILNIK O NAČINU IN POSTOPKU DOLOČANJA TAJNIH PODATKOV S PODROČJA OBRAMBE V GOSPODARSKIH DRUŽBAH, ZAVODIH IN ORGANIZACIJAH

V pravilniku o načinu in postopku določanja tajnih podatkov s področja obrambe v gospodarskih družbah, zavodih in organizacijah (Ur. l. RS, št. 108/2002) so formalizirana pravila za primere, ko mora gospodarska družba, zavod oziroma druga organizacija razpolagati s tajnimi podatki državnega organa, ki se nanašajo na obrambo države. Pravilnik torej velja za gospodarske družbe, zavode in organizacije, ki imajo sledeča razmerja z državno upravo:

- dejavnost je po odločitvi vlade posebnega pomena za obrambo države,
- s katerimi je sklenjena pogodba o proizvodnji in storitvah v vojnem stanju,
- proizvajajo vojaško orožje in opremo, oziroma opravljajo promet z orožjem in opremo,
- katerim se posredujejo tajni podatki s področja obrambe, če je to nujno za izvršitev nalog državnega organa.

Gospodarske družbe, zavodi in organizacije morajo izdelati oceno možnih škodljivih posledic ob morebitnem razkritju tajnega podatka nepoklicanim osebam, ki jo potrdi Ministrstvo za obrambo. Za samo določanje tajnih podatkov do največ stopnje »Tajno« so v posamezni gospodarski družbi, zavodu ali organizaciji zadolženi oziroma pooblaščeni predstojniki ali/in osebe, ki jih nadomeščajo v primeru njihove odsotnosti. Predstojniki pooblaščene osebe in delavci (ki se pri delu seznanijo s tajnimi podatki) v gospodarskih družbah, zavodih in organizacijah morajo pridobiti dovoljenje za dostop do tajnih podatkov skladno z Zakonom o tajnih podatkih. Dovoljenje za dostop do tajnih podatkov izda Ministrstvo za obrambo.

2.8 ODLOK O RAVNANJU S TAJNIMI PODATKI V DRŽAVNEM ZBORU REPUBLIKE SLOVENIJE

Odlok o ravnanju s tajnimi podatki v Državnem zboru Republike Slovenije (Ur. l. RS, št. 107/2005) določa ravnanje s tajnimi podatki v Državnem zboru Republike Slovenije, in sicer za vse poslance in zaposlene v Državnem zboru Republike Slovenije. Odlok podrobneje določa osebe, ki lahko dostopajo do tajnih podatkov (poslanci Državnega zbora) brez dovoljenja za dostop, in določa osebe, ki lahko določajo podatke s stopnjo Strogo tajno. Določeni so tudi postopki ob obravnavanju tajnih podatkov na sejah državnega zbora in podobni postopki, ki niso predpisani v Zakonu o tajnih podatkih in predpisih, sprejetih na podlagi Zakona o tajnih podatkih.

2.9 UREDBA O VAROVANJU TAJNIH PODATKOV V KOMUNIKACIJSKO INFORMACIJSKIH SISTEMIH

Uredba o varovanju tajnih podatkov v komunikacijsko informacijskih sistemih (Ur. l. RS, št. 48/2007) določa fizične, organizacijske in tehnične ukrepe in postopke varovanja tajnih podatkov v komunikacijskih in informacijskih sistemih. Po lastnem in splošnem prepričanju je ta uredba prišla precej pozno, saj smo imeli zaposleni, ki obdelujemo dokumente, ki vsebujejo tajne podatke, nemalokrat probleme ali vsaj pomisleke z zagotavljanjem varnosti tajnih podatkov ob njihovi obdelavi v informacijskih sistemih zaradi nedorečenosti zakonodaje. Osnovni namen Uredbe o varovanju tajnih podatkov v komunikacijsko informacijskih sistemih (Uradni list RS, št. 74/05) je:

- vzpostavitev minimalnih standardov, postopkov in tehničnih ukrepov, ki onemogočajo razkritje tajnih podatkov nepooblaščenim osebam,
- zagotoviti tajnost, celovitost in razpoložljivost tajnih podatkov v posameznih sistemih,
- določitev odgovorne osebe za varovanje v posameznem sistemu.

Vsak sistem, v katerem se obravnava tajne podatke stopnje Zaupno ali višje, mora pridobiti varnostno odobritev sistema od Urada Vlade Republike Slovenije za varovanje tajnih podatkov.
Uredba o varovanju tajnih podatkov v komunikacijsko informacijskih sistemih (Ur. l. RS, št. 48/2007) zelo natančno določa fizične in organizacijske ukrepe ter tehnične ukrepe varovanja tajnih podatkov v komunikacijskih in informacijskih sistemih. Uredba je tehnično zahtevna, predvsem v večjih organih, zato ima uredba rok za pridobitev mnenja o varnosti ustreznosti štiri leta, torej do 16. 06. 2011.

2.10 UREDBA O NAČINU IN POSTOPKU UGOTAVLJANJA POGOJEV ZA IZDAJO VARNOSTNEGA DOVOLJENJA ORGANIZACIJI

Uredba o načinu in postopku ugotavljanja pogojev za izdajo varnostnega dovoljenja organizaciji (Ur. l. RS, št. 70/2007) podrobneje določa način in postopek izdaje varnostnega dovoljenja dobaviteljem, izvajalcem gradenj ali storitev, ki se jim tajni podatki posredujejo zaradi izvršitve nekega naročila oziroma naročil. Sam postopek pridobitve poteka v naslednjih fazah:

- organizacija, ki varnostno dovoljenje potrebuje, da pobudo pristojnemu predlagatelju, v pobudi je navedeno naročilo (ki je razlog za potrebo po varnostnem dovoljenju), osebe v organizaciji, ki imajo dovoljenje za dostop do tajnih podatkov oziroma osebe, za katere se uvede postopek varnostnega preverjanja skupaj s soglasjem za preverjanje,
- v nadaljevanju se začne postopek za izdajo varnostnega dovoljenja organizaciji na predlog pristojnega predlagatelja,
- Urad Vlade Republike Slovenije za varovanje tajnih podatkov preveri, ali ima obravnavana organizacija že katero od varnostnih dovoljenje oziroma ali je v postopku za pridobitev varnostnega dovoljenja,

- pristojni organ nato preveri podane listine in z ogledom ugotovi, če organizacija izpolnjuje pogoje za izdajo varnostnega dovoljenja,
- pristojni organ izda ali zavrne izdajo varnostnega dovoljenja in o tem obvesti Urad Vlade Republike Slovenije za varovanje tajnih podatkov.

Organizacija, ki pridobi varnostno dovoljenje, je podvržena vmesnemu preverjanju v primeru sprememb okoliščin, ki bi lahko vplivale na izpolnjevanje pogojev Zakona o tajnih podatkih (prisilna poravnava, stečaj, likvidacija, neizpolnjevanje fizičnih, organizacijskih in tehničnih pogojev za varovanje tajnih podatkov).

2.11 UREDBA O OBLIKI IN UPORABI ZNAKA URADA VLADE REPUBLIKE SLOVENIJE ZA VAROVANJE TAJNIH PODATKOV

Uredba o obliki in uporabi znaka Urada Vlade Republike Slovenije za varovanje tajnih podatkov (Ur. l. RS, št. 1/2008) je trenutno zadnji predpis, izdan na podlagi Zakona o tajnih podatkih, in podrobneje ureja obliko in uporabo znaka Urada Republike Slovenije za varovanje tajnih podatkov.

Slika 2: Podoba znaka Urada Vlade Republike Slovenije za varovanje tajnih podatkov

Vir: Uredba o obliki in uporabi znaka Urada Vlade Republike Slovenije za varovanje tajnih podatkov (Ur. l. RS, št. 1/2008).

3 UREDITEV PODROČJA TAJNIH PODATKOV V TUJINI, EVROPSKI UNIJI IN NATU

Posamezne države v Evropi so začele uvajati varovanje tajnosti v nacionalnih zakonodajah šele konec osemdesetih let oziroma v začetku devetdesetih, medtem ko je Nato varovanje tajnosti v svoje predpise uvedla že leta 1955. S primerjavo zakonodaje s področja tajnih podatkov v Italiji, Avstriji, Nemčiji, Belgiji, Češki in Poljski sem ugotovil, da je normativna ureditev tajnosti primerljiva naši. Vse države na primer določajo stopnjo tajnosti glede na posledice, ki bi nastale, če bi bili tajni podatki razkriti nepooblaščeni osebi. Tudi v Natu in Evropski uniji enako, kar je logično glede na dejstvo, da so bila pravila glede tajnosti v Natu sprejeta že leta 1955, v časih, ko je hladna vojna toliko bolj zahtevala strogo upoštevanje predpisov Nata v zaprtem krogu članic. Po koncu hladne vojne in širjenju Nata so tudi posamezne države pripravile oziroma uzakonile nacionalno zakonodajo, ki pokriva področje tajnih podatkov, seveda nacionalna zakonodaja (vsaj v članicah Nata in kandidatkah) ni mogla biti v nasprotju s predpisi Nata, ki že sam po sebi zahteva izpolnjevanje minimalnih standardov v državah članicah. Podobno kot Nato ima varovanje tajnih podatkov urejena Evropska unija, kar je logično, saj je veliko članic Nata tudi v Evropski uniji. Razlog za poenotenje predpisov s področja Nata, Evropske unije in držav članic je v enakovrednem obravnavanju tajnih podatkov ne glede na to, v kateri državi so nastali.

3.1 SPECIFIČNA UREDITEV PODROČJA TAJNIH PODATKOV V POSAMEZNIH DRŽAVAH

V državah na področju Evropske unije se je normativno urejanje področja tajnih podatkov večinoma začelo v devetdesetih letih, ko so posamezne države ugotovile, da je treba določene podatke zaščititi pred nepooblaščenimi osebami in zagotoviti varno obravnavanje takih podatkov. Vsem ureditvam, vključno s slovensko, je skupno to, da imajo različne stopnje tajnosti za različne stopnje ogroženosti. Same označbe so v nekaterih državah različne, vendar v bistvu pomenijo določeno škodo interesom posamezne države.

3.1.1 Italija

Italija ima področje tajnih podatkov urejeno v okviru dveh predpisov. V zakonu št. 801 Ustanovitev in ureditev službe za informacije in varnost in ureditev državne tajnosti iz leta 1977 ter vladnem odloku – Nacionalni načrt za vrednotenje in varnostno potrjevanje informacijskih tehnologij s ciljem varovanja klasificiranih informacij v zvezi z notranjo in zunanjo varnostjo države iz leta 2002. Čeprav je zakon iz leta 1977, je napisan podobno kot primerljivi predpisi, ki so jih države sprejele šele v devetdesetih letih.

3.1.2 Avstrija

Avstrija ima ureditev tajnosti in varnostnega preverjanja določeno z Zakonom o varnostni policiji iz leta 1991. Določene ima tri stopnje tajnosti in možnosti dostopa oziroma obravnavanja teh podatkov. Posebnost v primerjavi s predpisi s področja tajnih podatkov drugih držav je odsotnost stopnje tajnosti Zaupno.

3.1.3 Nemčija

Nemčija ima varovanje tajnih podatkov oziroma varnostno preverjanje urejeno z Zakonom o pogojih in postopkih zveznega varnostnega preverjanja iz leta 1994. Sam zakon natančno opredeljuje varnostna preverjanja, medtem ko je bolj ohlapen pri določbah o tajnih podatkih oziroma varovanju le-teh.

3.1.4 Belgija

Belgijski zakon o klasifikaciji in dovoljenju za dostop do zaupnih podatkov iz leta 1998 vsebuje določbe o določitvi stopnje zaščite informacij, katerih neustrezna uporaba (belgijski zakon pod pojmom uporaba razume predvsem vpogled, razpolaganje, shranjevanje, uporabo, obdelavo, posredovanje, reprodukcijo, prenašanje) bi škodovala interesom, ki so določeni z zakonom ali mednarodno pogodbo (EU in Nato).

3.1.5 Češka

Republika Češka na področju tajnih podatkov uporablja Zakon o zaščiti zaupnih informacij iz leta 1998. Ta zakon določa informacije, ki jih je treba v interesu države opredeliti kot zaupne, in metodo njihove zaščite in obravnave. Republika Češka kot zaupne obravnava informacije v zvezi z ohranjanjem ustavnosti, suverenosti, ozemeljske nedotakljivosti, zagotavljanjem obrambe države in javne varnosti ter zaščite pomembnih gospodarskih in političnih interesov, pravice in svoboščine fizičnih in pravnih oseb ter življenje in zdravje prebivalstva.

3.1.6 Poljska

Poleg Češke ima še ena država bivšega vzhodnega bloka področje tajnih podatkov, predpisano z Zakonom o zaščiti tajnih podatkov iz leta 1999. Zakon določa stopnje tajnosti, načela za varovanje tajnih podatkov, načine in postopke varnostnega preverjanja in določbe o varnem obravnavanju tajnih podatkov. Zakon je pavšalno gledano podoben slovenski zakonodaji s področja tajnih podatkov.

3.2 UREDITEV TAJNOSTI V EVROPSKI UNIJI IN NATU

3.2.1 Evropska unija

Leta 2001 je Svet Evropske unije sprejel predpise o varovanju tajnosti podatkov in s tem nadomestil stare predpise, ki so se v Evropski uniji uporabljali za zagotavljanje varovanja tajnih podatkov. Določbe predpisov Sveta Evropske unije predpisujejo osnovna načela in minimalne standarde varovanja tajnih podatkov, ki jih morajo upoštevati vsi organi, članice in organizacije Evropske unije. Skladno s predpisi Sveta Evropske unije pomeni izraz »tajni podatki Evropske unije« vsak podatek, gradivo, katerega razkritje nepoklicani osebi bi lahko v določeni meri škodovalo interesom Evropske unije ali državi oziroma državam članicam Evropske unije.

3.2.2 Nato

V Natu je bil že leta 1955 sprejet dokument oziroma predpis, imenovan Varnost v okviru organizacije Severnoatlantske zveze, ki določa politiko varovanja podatkov, sredstev, naprav in objektov, pomembnih za delovanje ter uresničevanje nalog Nata, in minimum varnostnih ukrepov ter postopkov, ki jih pri izpolnjevanju obveznosti, ki izhajajo iz članstva v Natu, morajo izvajati države članice in organi Nata. Novi predpisi, ki predstavljajo celoto varnostnih standardov, ki veljajo v Natu, so bili s strani Odbora zveze Nato za varnost sprejeti šele leta 2002. Razvrstitve tajnosti so primerljive s stopnjami v Evropski uniji in državah članicah.

4 ČLOVEKOVE PRAVICE IN VARSTVO ZASEBNOSTI V DELOVNIH RAZMERJIH

4.1 SPLOŠNO

Ustava Republike Slovenije je pri določanju in varovanju človekovih pravic in temeljnih svoboščin zelo jasna. Natančno opredeljuje človekove pravice in temeljne svoboščine, ki jih lahko delimo na politične, ekonomske, kulturne, socialne in druge. Tudi varovanje človekovih pravic je v naši ustavi opredeljeno. Bolj natančno so glede na naravo posamezne svoboščine skladno s 15. in 87. členom ustave lahko urejene z zakonom. Po določbah ustave se samo način in uresničevanje človekovih pravic in temeljnih svoboščin lahko predpišeta z zakonom, in sicer v primerih, kadar tako določa ustava, ali pa če je to nujno zaradi same narave posamezne svoboščine oziroma pravice. Skladno s 3. odstavkom 15. člena Ustave Republike Slovenije so človekove pravice in temeljne svoboščine omejene samo s pravicami drugih in v primerih, ki jih določa sama ustava. Torej je po ustavni določbi mogoče človekove pravice in temeljne svoboščine omejevati le z zakonom. Zakoni določajo pogoje in način uresničevanja pravic, vendar moramo vedeti, da z zakonom ne določamo pogojev in načina omejevanja pravic, temveč določamo način in pogoje uresničevanja pravic.

4.2 PRAVICA DO ZASEBNOSTI

Varstvo zasebnosti in osebnostnih pravic je že uveljavljena kategorija in stalnica v našem življenju. Zlasti izrazito je varstvo zasebnosti in osebnostnih pravic postalo z uveljavitvijo slovenske ustave leta 1991, ki je namenila tej problematiki celo drugo poglavje. Vedno več je govora o varstvu osebnostnih pravic, zasebnosti, a vseeno se o varstvu zasebnosti in osebnostnih pravic v delovnem razmerju oziroma delovnem pravu ni govorilo veliko. Ta tema v zadnjih letih vseeno počasi prihaja na površje. Jasno je, da se o varstvu zasebnosti in osebnostnih pravic ni govorilo v času drugačnih družbenoekonomskih odnosov, ko je delovno razmerje imelo drugačne temelje. Seveda ne moremo trditi, da varovanje zasebnosti v asociativnih delovnih razmerjih ni bilo pomembno. Vendar pa je bil v preteklosti drugačen zlasti odnos države in posameznikov, torej delodajalcev in zaposlenih, do varovanja zasebnosti v delovnih razmerjih. Moje prepričanje je, da je takšno mnenje izhajalo iz družbenoekonomskih odnosov v času pred osamosvojitvijo naše države. Glede na to, da so odnosi temeljili na družbeni lastnini, vsaj za področje takratnega družbenega sektorja ne moremo govoriti o klasičnih delodajalcih in zaposlenih. Z vidika družbene lastnine lahko govorimo o delavcih na vodilnih ter vodstvenih funkcijah ter ostalih delavcih, v obeh kategorijah naj bi bil edini glavni interes plačilo. In čeprav je bilo varovanje zasebnosti in osebnosti v asociativnem razmerju enako pomembno kot danes, je bil odnos do kršitev pravice zasebnosti in osebnostnih pravic drugačen. Po

vzpostavitvi lastninskih razmerij se je ta odnos spremenil, dopolnjeval in razvijal, tudi z določili Zakona o delovnih razmerjih, kljub dejstvu, da je pomen varovanja zasebnosti in osebnostnih pravic do danes ostal isti. Civilno pravo pozna nekatere osebne in nepremoženjske pravice, ki pripadajo človeku. Vežejo se na njegovo osebo in njegova osebna razmerja. Te pravice opredeljujemo kot osebnostne pravice, saj varujejo človeka in njegovo osebnost. Osebnostne pravice so ene tistih pravic, katerih obseg in pomen se pogosto spreminja in dopolnjuje, ker so zelo odvisne od družbenega razvoja. Najbolj pa lahko mednje prištevamo pravice, kot so:

- pravica do življenja, zdravja in telesne inetgritete,
- pravica do zasebnosti,
- pravica do osebnega življenja,
- pravica do pisemske tajnosti,
- pravica do časti in dobrega imena,
- pravica do osebne identitete,
- pravica do prostosti.

Zato ker osebnostne pravice temeljijo na vprašanjih, ki so povezana z naravo osebnosti, problemi bivanja, socialnim povezovanjem, je zaradi družbenega razvoja te pravice težko naštevati in dokončno vsebinsko opredeliti. Različni avtorji uporabljajo, oziroma so v preteklosti uporabljali različne termine kot na primer »pravice na lastni osebi« ali »individualne pravice«. Ne glede na izrazoslovje pa je bit vsebine te pravice v tem, da vsak poseg v tako pravico pomeni nezakonitost, proti kateri je posameznik zaščiten v celoti in proti vsakomur (seveda pod pogojem, da pravna država deluje v celoti). Zaradi teh dejstev te pravice imenujemo absolutne. Ena pomembnih osebnostnih pravic z vsemi lastnostmi takšne pravice je pravica do zasebnosti. V njej se združuje vrsta pravic v zvezi s človekovo osebnostjo in njegovimi osebnimi razmerji.

4.3 DEFINICIJA ZASEBNOSTI

Popolna definicija zasebnosti je težavna, po besedah nekaterih teoretikov pa tudi nepotrebna. Kaj vse zajema pravica do zasebnosti, ni možno točno opredeliti, tako kot je to težko pri definiranju osebnostnih pravic. Tudi v evropski pravni literaturi ne zasledimo splošne definicije zasebnosti. Zasebnost je velikokrat razumljena kot varstvo osebe v njenem bivalnem prostoru, kjer je absolutno varna pred posegi javnosti in tretjih oseb, čeravno takšna opredelitev ni popolnoma ustrezna, saj je prostorsko varstvo kot takšno sicer pomembno, vendar pa v smislu varovanja zasebnosti preohlapno. Vplive na zasebno okolje je tako možno združiti v štiri pomembne kategorije:

- prepoved nasilnih komunikacij z vdorom v zasebno sfero,
- svoboda pri izbiranju lastnih komunikacijskih partnerjev,
- svoboda pred izsiljenimi komunikacijskimi udeležbami,
- prepoved izoliranja od informacij iz komunikacijskega omrežja.

Svet Evrope oziroma evropski parlament je poskušal z resolucijo št. 428 iz leta 1970 podati definicijo pravice do zasebnosti, ki naj bi obsegala pravico živeti lastno

življenje s čim manj vplivi od zunaj. Vsebuje pravico do osebnega življenja, pravico do družine in doma, pravico do fizične in psihične nedotakljivosti, pravico do časti in ugleda, pravico do prepovedi prikazovanja v napačni luči, pravico do prepovedi razkrivanja za posameznika nepomembnih in neprijetnih dejstev, prepoved objave zasebnih fotografij in pravico do varstva zaupno pridobljenih podatkov. Že prej pa je predlagano definicijo zasebnosti oziroma njenega varovanja razširila Nordijska konferenca pravnikov. Definiciji zasebnosti je dodala še prepoved uporabe oziroma zlorabe osebnega imena, prepoved ugotavljanja ali fotografiranja brez soglasja, prepoved vohunjenja za osebo, spoštovanje pisem in prepoved razkrinkanja uradnih informacij. Po splošni deklaraciji o človekovih pravicah je pravica do zasebnosti povezana še s pravico do svobodnega izražanja pod predpostavko, da jo pravica do zasebnosti vsebuje kot pogoj za vzpostavitev in ohranitev medčloveških odnosov. Med pravice do zasebnosti, ki so pomembne v delovnem razmerju, pa je treba uvrstiti tudi posameznikove osebne podatke, osebne razmere, osebna stanja, človekove dejavnosti in njegov videz. Na podlagi takšne opredelitve človekovih pravic in temeljnih svoboščin, ob definiranju t. i. negativnega statusa posameznika v razmerju do državne oblasti in osebnostnih pravic in svoboščin z vidika varovanja telesne celovitosti in osebnostnih pravic lahko ugotovimo, da so področja, ki jih kot zasebne varuje ustava, široka, in sicer je zasebnost varovana tako prostorsko kot osebno. Ob tem seveda ostaja vprašanje, v katerih primerih pa se dejansko posega v človekovo pravico do zasebnosti. Ali je to le v primeru domovanja (v najširšem smislu) ali tudi v drugih okoljih, na primer na delovnem mestu? Pričakovanje zasebnosti, četudi glede službenih telekomunikacij, mora biti utemeljeno. Dodati je treba, da je posameznikova zasebnost varovana povsod, kjer jo lahko upravičeno pričakuje, ne glede na to, ali je bil s posegom v zasebnost hkrati izvršen tudi poseg v lastninsko pravico. Zgleden primer za takšno obrazložitev je primer, ki je potekal na francoskem kasacijskem sodišču, ter se nanaša na prejemanje zasebne pošte na službenem računalniku. Omenjeno sodišče je v svoji odločitvi zavrnilo odpustitev delavca na podlagi njegove hude napake, ki naj bi bila storjena tako, da je delavec na svoj službeni elektronski naslov sprejemal in pošiljal zasebna sporočila, ki so bila namenjena njegovi vzporedni dejavnosti. Po tej odločitvi ima zaposleni tudi na delovnem mestu in med delovnim časom pravico do spoštovanja intimnosti zasebnega življenja, ki še posebej zajema tajnost pošte in pogovorov. Iz tega izhaja, da se delodajalec brez kršitve temeljne pravice in svoboščine ne more seznaniti z osebnimi sporočili, ki jih delavec sprejel in poslal s pomočjo informacijske opreme, ki mu je bila dana na razpolago za opravljanje njegovega dela. To velja tudi v primeru, če bi delodajalec prepovedal neprofesionalno rabo računalnika.

4.3.1 Delovno razmerje

Z razvojem pogodbenosti delovnega razmerja, torej odnosa med delodajalcem kot močnejšo in delavcem kot šibkejšo stranko, ta tema prihaja na površje ne le na teoretični ravni, temveč tudi v praktičnih dejanjih. Delovno razmerje je poseben odnos med delavcem in delodajalcem, v katerem je še posebej izraženo načelo zaupanja in lojalnosti. Delodajalec na eni strani si zagotavlja ohranjanje ali večanje kapitala, delavec pa si zagotavlja vsaj socialno varnost. Zaradi tega je obseg delavčeve zasebnosti v delovnem pravu odvisen od nasprotnega interesa delodajalca.

Kljub navedenemu tudi v delovnem razmerju velja, da je zasebnost pomemben sestavni del tega razmerja, predvsem za delavca, saj mora človek za svoje uspešno delo ohraniti del zasebnosti. Treba je vedeti, da so človekove pravice, med katere spada tudi pravica do zasebnosti, najstarejše pravice, ki jih država ne more podeljevati ali pogojevati, ker pripadajo človeku že samo zaradi dejstva, da je človek. Gre za osebno in nepremoženjsko pravico, ki učinkuje proti vsakemu. Ta pravica izvira iz naravnega prava in na njem temeljijo sodobni pravni akti. Človekove pravice so absolutne pravice, ki so lahko omejene samo z istovrstnimi pravicami drugega. Tiste sodobne družbe, ki so utemeljene kot socialne države, glede varovanja zasebnosti spoštujejo podobne standarde, čeprav ima vsaka država določene lastne rešitve. Upošteva se načelo, da je vsakemu zagotovljena pravica do spoštovanja njegovega zasebnega življenja in tudi družinskega življenja, doma in dopisovanja. Razlike obstajajo pri vmešavanju oblasti v uresničevanje te pravice, predvsem z vidika državne ali javne varnosti, ljudske blaginje in družbene morale. Zasebnost je torej tehtanje med zasebnim in javnim interesom.

4.3.2 Mednarodni pravni viri

Pravica do zasebnosti je zagotovljena v mednarodnih pravnih virih in v slovenskem pravu. Gre za pravico posameznika, da se avtonomno odloči, kdaj, kako in koliko se v to pravico lahko posega, saj je vsak poseg brez njegove svobodne odločitve prepovedan. Splošna deklaracija o človekovih pravicah v 12. členu določa, da nikogar ni dovoljeno nadlegovati s samovoljnim vmešavanjem v njegovo zasebno življenje, njegovo družino, v njegovo stanovanje, njegovo dopisovanje ali z napadi na njegovo čast in ugled. Podobno določilo vsebuje tudi Mednarodni pakt o državljanskih in političnih pravicah, ki v 17. členu določa, da se nihče nikomur ne sme samovoljno in nezakonito vmešavati v zasebno življenje, družino, stanovanje ali dopisovanje in ga tudi ne sme nezakonito žaliti ali škodovati njegovemu ugledu. Proti takšnemu vmešavanju, žalitvam ali škodovanju ima vsakdo pravico do zakonitega varstva. Evropska konvencija o človekovih pravicah v prvem odstavku 8. člena določa, da ima vsakdo pravico do spoštovanja njegovega zasebnega in družinskega življenja, doma in dopisovanja. Ta pravica je sicer omejena z interesi drugih in z javnim interesom, pri čemer je zmeraj treba upoštevati težo interesov prizadetih partnerjev oziroma načelo sorazmernosti. Pravica do zasebnosti je varovana pred posegom v pravico, pa tudi kasneje, ko je že bila kršena. Pred posegom jo varujejo mednarodni akti, ustava, zakoni, po kršitvi pa je možno kazenskopravno ali civilnopravno varstvo.

4.3.3 Delovno pravo

Tudi v delovnem pravu je zasebnost težko definirati. Stalno spreminjanje življenjskih razmer in tehničnih sredstev, s katerimi vplivamo na življenje posameznikov, spreminjajo obseg in pomen zasebnosti, še posebej v delovnem pravu. Tem dejstvom navkljub lahko rečemo, da sta zasebnost in varstvo zasebnosti tudi v delovnem pravu splošna in vseobsegajoča pravica posameznika, da dovoli ali ne dovoli posega v svoje zasebno področje, področje njegove osebnosti in njegovega dostojanstva. To pomeni, da bo delavec v delovnem razmerju tisti, ki bo določil,

katero ravnanje v zvezi s posegi v zasebnost bo dopustil in ga s tem izvzel iz varovanja ter kdo je tisti, ki mu je to dovoljeno. Praviloma je v delovnem pravu pravica do zasebnosti tista pravica, ki združuje več pravic v zvezi z delavčevo osebo in njegovimi osebnimi razmerji. Gre torej za osebno in ne premoženjsko pravico, ki učinkuje proti vsakomur in mora biti kot taka varovana. V delavčevo zasebnost lahko vštevamo delavčevo osebo v najširšem smislu (njegov dom, družino ter dokumente v zvezi s tem). Varstvo zasebnosti v delovnem pravu je lahko zagotovljeno proti posegom in zlorabam katere od naštetih kategorij s predpisi delovnega prava ali splošnimi predpisi.

4.3.4 Zakon o delovnih razmerjih

Zakon o delovnih razmerjih navkljub z ustavno zagotovljeno pravico do zasebnosti lahko pridobi določene podatke, ki so v neposredni zvezi z delovnim razmerjem. Delodajalec pri tem ne sme pogojevati sklenitve pogodbe o zaposlitvi s pridobitvijo podatkov, ki niso v skladu z 26. členom Zakona o delovnih razmerjih.Tudi preizkus znanja oziroma zdravstvene sposobnosti se ne smejo nanašati na okoliščine, ki niso v neposredni zvezi z delovnim mestom, za katerega se sklepa pogodba o zaposlitvi. Naslednja določba, ki se nanaša na varovanje delavčeve zasebnosti, je v 27. členu Zakona o delovnih razmerjih in določa, da kandidat ni dolžan odgovarjati na vprašanja, ki niso v neposredni zvezi z delovnim razmerjem. Zakon o delovnih razmerjih delodajalcu torej nalaga varovanje delavčeve osebnosti. Izrecno je določeno, da mora delodajalec varovati in spoštovati delavčevo osebnost in upoštevati ter varovati delavčevo zasebnost. Prizadevati si mora, da noben delavec ni žrtev spolnega nadlegovanja in da nihče ni žrtev nadlegovanja zaradi tega, ker se je pritožil proti razlikovanju med spoloma. Določbe Zakona o delovnih razmerjih so povsem v skladu z zakonskimi in pogodbenimi določbami, še bolj pa s prakso v delovnih razmerjih večine gospodarsko razvitih evropskih držav in pomenijo za nas velik korak naprej pri varovanju delavčeve zasebnosti. V državah, kjer imajo dobro urejeno varstvo delavčeve zasebnosti, gre za dolgoletno demokratično tradicijo z izoblikovanim delavskim razredom. Socialistični družbeni sistem je sicer oblikoval delavski razred, zaradi duha kolektivizma pa je bil ravnodušen do problema zasebnosti. Instituta zasebnosti kot takega ni poznal niti ustavni red, čeprav je poznal druge človekove pravice in svoboščine, ki so se po vsebini približevale tudi pravici do zasebnosti, zato se niti v družbi niti v delovnih razmerjih ni razvijal.

4.4 VARSTVO OSEBNIH PODATKOV V DELOVNIH RAZMERJIH

Določeno je, da se osebni podatki lahko zbirajo, obdelujejo, uporabljajo in dostavljajo le, če je to določeno z zakonom, oziroma je v zvezi z delovnim razmerjem. S podatki lahko razpolaga delodajalec ali delavec, ki ga je zato pooblastil delodajalec. V Sloveniji je varstvo osebnih podatkov postala ustavno varovana pravica že v letu 1989, ko so bili sprejeti amandmaji k tedanji republiški ustavi iz leta 1974. Tudi sedaj je varstvo osebnih podatkov umeščeno v poglavje o človekovih pravicah in temeljnih svoboščinah, in sicer med osebnostne pravice, ki varujejo človekovo dostojanstvo.

Ustava Republike Slovenije tako v 38. členu določa, da je zagotovljeno varstvo osebnih podatkov ter prepovedana uporaba osebnih podatkov v nasprotju z namenom njihovega zbiranja. Zbiranje, obdelovanje, namen uporabe, nadzor in varstvo tajnosti osebnih podatkov določa Zakon o varstvu osebnih podatkov. Pomembna je tudi pravica posameznika, da se seznani z zbranimi podatki, ki se nanašajo nanj, in pravica sodnega varstva ob njihovi zlorabi. Ustavna ureditev varstva osebnih podatkov se opira zlasti na načela varstva osebnih podatkov, ki so vsebovana v Konvenciji o varstvu posameznika glede na avtomatsko obdelavo podatkov, ki je bila sprejeta v okviru Sveta Evrope in je bila sprejeta oziroma ratificirana v Republiki Sloveniji leta 1994. Cilj varstva osebnih podatkov ni varstvo osebnih podatkov kot takih, temveč varstvo posameznika, na katerega se le-ti nanašajo.

4.5 VARNOSTNO PREVERJANJE – POSEG V ZASEBNOST ZAPOSLENEGA

Posegi v človekove pravice in temeljne svoboščine, tako dovoljeni kot nedovoljeni, so številni. Nekatere posege v okviru opravljanja svoje dejavnosti in na podlagi izrecnega zakonskega pooblastila izvajajo državni organi v okviru obveščevalne in varnostne dejavnosti. V tej nalogi bodo obravnavani posegi v varstvo osebnih podatkov na področju varnostnega preverjanja kot oblike obveščevalne in varnostne dejavnosti. Področje varnostnega preverjanja sicer ni nova kategorija. Preverjanje v najširšem smislu je staro najmanj toliko časa, kolikor se ljudje zavedajo svojega obstoja. Preverjanje se tako ali drugače pojavlja v vsakodnevnem življenju, saj mnogokrat preverjamo določene podatke, pa se tega sploh ne zavedamo.Tako nas zanimajo določeni podatki o naših sosedih, sogovornikih, sodelavcih in podobno. Prav tako so različni tudi razlogi za preverjanje (nekdo nam je všeč ali ne, drugi od nas kaj hoče). To so seveda preverjanja za našo osebno uporabo in vanje ne vlagamo veliko napora. Varnostno preverjanje, potrebno za izdajo dovoljenja za dostop do tajnih podatkov, izdajajo na podlagi zakona Ministrstvo za notranje zadeve, Ministrstvo za zunanje zadeve in Slovenska obveščevalno varnostna agencija. Zakon o tajnih podatkih (UPB, Ur.l. RS št. 50/2006) določa, da se lahko določeno osebo, ki bo imela dostop do tajnih podatkov, varnostno preveri z njenim soglasjem. Posameznik, ki bo potreboval dovoljenje za dostop do tajnih podatkov, bo torej moral po sklenitvi delovnega razmerja izpolniti več vprašalnikov z različnimi osebnimi podatki. Vendar varnostno preverjanje ni le zbiranje osebnih podatkov, temveč gre za širši poseg v zasebnost, kot je to opredeljeno v 35. členu Ustave Republike Slovenije. Na podlagi tega lahko ugotovimo, da ni izrecne opredelitve zasebne in intimne sfere, je pa pojem zasebnosti vsebovan v več ustavnih pravicah in svoboščinah.

4.6 SKLEPNO O ČLOVEKOVIH PRAVICAH IN VARSTVU ZASEBNOSTI

Na različnih področjih življenja in dela prihaja do nasprotij med pravico do zasebnosti, določeno v ustavi, in posegov oziroma omejitev te pravice, kar prav tako določa ustava. Do posegov v zasebnost potemtakem prihaja tudi v delovnih

razmerjih. Ugotovimo lahko, da je bil odnos države in posameznikov do varovanja zasebnosti v delovnih razmerjih v preteklosti drugačen, kot je danes. To izhaja iz družbene ureditve, ki je vladala takrat še skupni državi. Vse skupaj je temeljilo na družbeni lastnini, klasičnih delodajalcev in delavcev je bilo malo. Tudi varnostno preverjanje zaradi pridobitve dovoljenja za dostop do tajnih podatkov, kot ga poznamo danes, pomeni omejevanje zasebnosti, zlasti na področju osebnih podatkov, kjer je zelo pomembno upoštevanje načela sorazmernosti med varovano dobrino (v našem primeru tajnim podatkom) in pravico posameznika do zasebnosti. Verjetno bomo v prihodnosti zaradi groženj, ki jih danes še ne poznamo, še bolj podvrženi raznim varnostnim preverjanjem, ki jih človek osebno ne bo obravnaval, vse dokler jih ne bo izvrgel nek informacijski sistem, ki bo zbiral vse podatke o nas in naši družbi. Tudi varnostno preverjanje za potrebe pridobitve dovoljenja za dostop do tajnih podatkov je le naša odločitev, pa čeprav mogoče odločitev, da na naši karierni poti ne bomo mogli stopiti po vseh poteh, ki vodijo do našega cilja.

5 VAROVANJE TAJNIH PODATKOV

Slovenija je od leta 2004 polnopravna članica Evropske unije in zveze Nato. Obdobje od osamosvojitve do polnopravnega članstva v obeh organizacijah je zaznamovalo intenzivno delo vseh vej državne oblasti pri vzpostavitvi organiziranosti države, ki ima danes usklajeno zakonodajo tako z EU kot tudi z zvezo Nato. Na zakonodajnem področju so bili sprejeti številni predpisi, nekateri so v osmih letih tudi že delno ali v celoti ukinjeni, oziroma so prenehali učinkovati. Na področju tajnih podatkov so se izoblikovali predpisi, ki sedaj urejajo organiziranost varovanja tajnih podatkov tako na nacionalnem kot na nadnacionalnem nivoju.

Dostop do podatkov, informacij in dokumentov, ki nastajajo pri javnih osebah v Republiki Sloveniji po letu 1991, določajo Zakon o varstvu osebnih podatkov, Zakon o tajnih podatkih (UPB, Ur.l. RS št. 50/2006), Zakon o avtorskih in sorodnih pravicah ter Zakon o dostopu do informacij javnega značaja. Navedeni predpisi so večinoma usklajeni z navodili Sveta Evrope in direktivami Evropske unije. Varstvo poslovne tajnosti ureja Zakon o gospodarskih družbah. Postopke uporabe dokumentov urejajo tudi Zakon o splošnem upravnem postopku, sodni red ter številni področni predpisi, zelo na splošno pa tudi Uredba o poslovanju organov javne uprave z dokumentarnim gradivom.

V zakonodaji je temeljnega pomena, kako se razume pojem tajnosti. Kako je zakonsko definirana tajnost, je najbolj pomembno pri razumevanju vsebine, ki jo predstavlja tajni podatek oziroma tajni dokument. Glede na to, kako na nek tajni podatek gledamo in kakšen pomen mu pripisujemo, pa mu na tej osnovi določimo težo v družbi s tem, da ga ovrednotimo z določeno stopnjo tajnosti. V nekdanji SFRJ so bili tajni dokumenti poleg stopnje tajnosti označeni še z vrsto tajnosti glede na to, ali je šlo za državno ali vojaško tajnost. Ta razdelitev se je obdržala v naši zakonodaji vse do sprejetja Zakona o tajnih podatkih leta 2001.

5.1 NOSILCI VAROVANJA

Subjekti, ki se morajo ravnati po Zakonu o tajnih podatkih (UPB, Ur. l. RS št. 50/2006), so vsi državni organi, organi lokalnih skupnosti, nosilci javnih pooblastil ter drugi organi, gospodarske družbe in organizacije ter posamezniki v teh organih. Prav tako se morajo po zakonu ravnati dobavitelji, izvajalci gradenj ali storitev. Zavezanci so torej vsi, ki kakorkoli pridejo v stik s tajnimi podatki. Glede na to, da imajo tajni podatki poseben status, jih je treba celovito varovati.

Ključnega pomena pri varovanju tajnih podatkov je, da podatki ostanejo tajni. Ko enkrat pride do njihovega razkritja, niso več tajni. Z namenom zagotovitve ustreznega izdelovanja, označevanja, prenašanja in hranjenja je bila sprejeta Uredba o varovanju tajnih podatkov (Uradni list RS, št. 74/05). V uredbi so določeni načini in oblike označevanja tajnih dokumentov ter osnovni organizacijski, fizični in tehnični

ukrepi za varovanje tajnih podatkov. Namen vseh teh ukrepov je učinkovita zaščita tajnih podatkov na njihovi poti od nastanka do arhiviranja oziroma uničenja.

Po posameznih segmentih lahko razdelimo ukrepe varovanja tajnih podatkov na:

- organizacijske, kamor sodi sama priprava in izdelava tajnega dokumenta, njegov prenos in hranjenje oziroma uničenje;
- fizični ukrepi se nanašajo predvsem na neposredno fizično varovanje tajnih podatkov ter varovanje prostorov in objektov;
- tehnični ukrepi pa se nanašajo na varovanje tajnih podatkov in prostorov s tehničnimi sredstvi.

Za ustrezno izvajanje navedenih ukrepov so odgovorni posamezni našteti organi in posamezniki v teh organih. Za izvedbo vseh nalog morajo izdelati ustrezne načrte z vsebino, ki je navedena v prejšnjem poglavju.

Varovanje tajnih podatkov je prav tako pomembno za podjetja, ki bi želela pridobiti projekt tajne narave. Podjetja, ki bodo želela konkurirati na razpisih za pridobitev te vrste projektov, bodo morala izpolnjevati vse zahtevane pogoje za delo s tajnimi podatki. Pridobitev projekta s tajno vsebino ni omejena samo na področje Slovenije; v primeru EU in Nata bodo organizacije pogodbo lahko sklenile samo ob predhodni ugotovitvi, da izpolnjujejo vse zahteve po ustrezni zaščiti tajnih podatkov v skladu s standardi Nata in EU. Ti kriteriji so naslednji:

- izpolnjevanje vseh organizacijskih, fizičnih in tehničnih pogojev;
- vse osebe, ki bodo sodelovale pri posameznem projektu, bodo morale biti ustrezno varnostno preverjene, najmanj do stopnje tajnosti, do katere bo označen projekt;
- prav tako bodo morale osebe podpisati izjavo o seznanjenosti, ki pomeni, da vedo, kako je treba ravnati s tajnimi podatki;
- izbrano podjetje bo moralo zagotoviti, da bo dovolilo vpogled samo osebam, ki bodo imele potrebo po vedenju (need to know); v praksi to pomeni, da oseba v podjetju, kjer je preverjena in sodeluje v projektu, kljub vsem izpolnjenim kriterijem ne more avtomatično imeti vpogleda v vse dokumente.

Organizacija, ki želi skleniti posel tajne narave, mora zainteresiranim izvajalcem v začetku pogajanj posredovati dokumentacijo, iz katere je razvidna identiteta in zahtevana stopnja dostopa do tajnih podatkov za vse izvajalce in podizvajalce, ki bodo sodelovali v projektu, za posameznike pa mora biti razvidno, do katere ravni in s katero količino tajnih podatkov se bodo seznanjali pri izpolnjevanju pogodbene storitve. Pred posredovanjem tajnih podatkov mora organ pozvati odgovorno osebo izvajalca, da predloži podatke, iz katerih je mogoče ugotoviti uresničevanje ukrepov za varovanje tajnih podatkov, določenih v pogodbi med naročnikom in organizacijo, ki bo izvajala storitev.

Pooblaščeni državni organ bo po izpolnitvi vseh pogojev izvedel nadzor v podjetju in izdal varnostno potrdilo. Veljavno varnostno potrdilo je pogoj za pridobitev posla. Za akreditacijo o ustreznosti prostorov v skladu s standardi Nata in EU je pristojen Urad za varovanje tajnih podatkov.

5.2 VARNOSTNI NAČRT

Varnostni načrti so opredeljeni v Uredbi o varovanju tajnih podatkov, vsebina varnostnega načrta je deljena na splošni in posebni del. Splošni del načrta varovanja vsebuje zlasti:

- oceno ogroženosti;
- opis glavnega in pomožnih objektov (lega, vhodi, izhodi, zasilni izhodi, skica oziroma fotografije objekta, glavne in pomožne poti do objekta ter podatki o varnostnotehnični opremi);
- podatke o nosilcu varnostnega načrta;
- zaščitne ukrepe za osebe, ki imajo dostop do tajnih podatkov.
- Posebni del načrta varovanja vsebuje zlasti:
- ukrepe fizičnega varovanja (zunanje in notranje fizično varovanje, varnostne točke z opisi nalog izvajalcev);
- ukrepe tehničnega varovanja (zunanje in notranje tehnično varovanje, nadzor nad vstopom in izstopom, alarmni sistem in postopki ob sprožitvah posameznih stopenj alarmov, dokumentiranje);
- postopke ob nasilnem vstopu in nepredvidenem dogodku: požaru, potresu, povodnji in drugih naravnih nesrečah;
- postopke in ukrepe ob izgubi, razkritju ali odtujitvi tajnega podatka;
- ukrepe in postopke pri opravljanju vzdrževalnih in drugih del v varnostnih območjih.

5.3 USTREZNA MATERIALNO-TEHNIČNA PODPORA

Za zagotovitev pogojev za delo s tajnimi podatki je nujno potrebna ustrezna logistična podpora. Ureditev prostorov urejajo Merila za ureditev poslovnih prostorov za potrebe državne uprave – MUPP in Uredbo o varovanju tajnih podatkov v komunikacijsko informacijskih sistemih (Ur. l. RS 48/2007).

Slika 3: Napisna tabla, ki opozarja na varnostno območje

Vir: Uredba o varovanju tajnih podatkov (Ur. l. RS št. 74/2005).

Prostori za obdelavo in hrambo tajnih podatkov morajo biti zgrajeni tako, da omogočajo operativno obdelavo in pripravo dokumentov ter omogočajo njihovo obravnavo na sestankih. V teh prostorih je treba zagotoviti prostor za namestitev

kriptotelefonov in kriptofaksov ter računalniško opremo, ki ni priklopljena na javno ali interno omrežje. Prostori, v katerih je strežniška računalniška oprema (sistemski prostor), morajo biti okvirno velikosti 8 do 12 m2 z nadzorovanim dostopom. Talne obloge morajo biti iz antistatičnih materialov z ustrezno ozemljitvijo. Za prostore, ki so namenjeni hranjenju tajnih podatkov, morajo biti zagotovljeni: klimatizacija, protipožarno javljanje in protivlomno varovanje. V prostoru se mora zagotoviti vzdrževanje temperature med 18 in 26 stopinj Celzija z relativno zračno vlago 40 do 60 %. Sistemski prostor, namenjen prenosu, obdelavi in hranjenju obrambnih podatkov, mora ustrezati zahtevam, ki jih določi Ministrstvo za obrambo. Prostori, namenjeni prenosu, obdelavi in hranjenju tajnih podatkov zveze Nato in EU, pa morajo ustrezati zahtevam teh dveh organizacij.

Video nadzor se zagotovi na vhodih in glavnih komunkacijskih točkah ter v prostoru za hrambo tajnih podatkov in obrambno načrtovanje. Video sistem je centralno voden. Priporočena je digitalna tehnologija kamer, za katero se zagotovi ustrezna razsvetljava ponoči. Prav tako je obvezen za potrebe državne uprave in s tem za prostore s tajnimi podatki sistem neprekinjenega napajanja (UPS). Na UPS se smejo priklopiti računalniki, tiskalniki in ostale računalniške naprave, alarmni sistemi, sistem video nadzora ter drugi sistemi interne komunikacije. Prav tako je v prostorih za hranjenje tajnih podatkov obvezen domofon.

Varnostne omare za hranjenje tajnih podatkov morajo imeti predpisane certifikate. Način zaklepanja se določi glede na stopnjo tajnosti. Velikost in število varnostnih omar se določi glede na obseg dokumentacije in vrsto poslovanja po posameznem organu, pri čemer je treba zagotoviti ustrezno talno nosilnost. Velikost prostorov za hrambo tajnih podatkov in obrambno načrtovanje se deli na prostore za dokumente, prostore za varnostne omare in prostore za serverje, velikost prostorov pa se predvidi v posameznem projektu.

5.4 USTREZNOST KADRA

S tajnimi podatki lahko delajo osebe na podlagi veljavnega dovoljenja za dostop do tajnih podatkov in potrebo po vedenju. Dostop je omejen in je mogoč le na način in ob pogojih, določenih z Zakonom o tajnih podatkih (UPB, Ur. l. RS št. 50/2006) in njegovimi podzakonskimi predpisi, z drugim zakonom ali z mednarodnimi pogodbami. Pravico dostopa do tajnih podatkov imajo samo tiste osebe, ki imajo dovoljenje in se morajo s temi podatki seznaniti zaradi opravljanja funkcije ali delovnih nalog. Dostop imajo samo do tajnih podatkov stopnje tajnosti, določene v dovoljenju, in ob predpostavki, da obstaja potreba po vedenju.

Nekatere osebe lahko dostopajo do tajnih podatkov tudi brez takega dovoljenja. Dostop brez dovoljenja imajo vse osebe, ki opravljajo funkcijo ali delajo v organu, vendar samo do stopnje tajnosti interno. Za to stopnjo tajnosti tudi ni potrebno varnostno preverjanje, ampak osebe dobijo dovoljenje z začetkom funkcije oziroma nastopom dela, ko podpišejo izjavo, da so seznanjene s predpisi, ki urejajo varovanje

tajnih podatkov. S podpisom izjave se zavezujejo, da bodo s tajnimi podatki ravnale v skladu z veljavnimi predpisi.

Do tajnih podatkov vseh stopenj lahko dostopa brez dovoljenja večina funkcionarjev, kot so predsednik republike, predsednik vlade, poslanci, ministri, župani, občinski svetniki, funkcionarji na sodiščih in v banki Slovenije, varuh človekovih pravic itd. Vsi našteti imajo dostop do nacionalnih tajnih podatkov, ne pa tudi do podatkov EU. Zveza Nato ima skladno z direktivo AC/35-D/2000 – REV3 z dne 6. 7. 2007 v 34. členu opredeljeno možnost dostopa do tajnih podatkov zveze Nato za predsednika države in vlade, ministre, člane parlamenta in sodnike na podlagi določil nacionalne zakonodaje, kar pomeni, da ne potrebujejo dovoljenj za dostop do tajnih podatkov. Glede na to, da je delo predstavnikov oblasti zaradi vključenosti v EU zelo povezano tudi s temi podatki, lahko zaradi tega pride do težav, ko morajo predstavniki sodelovati z navedenima institucijama. Smiselno je, da se preverjanje opravi tudi za navedene kategorije oseb.

Vsi ostali, ki nimajo tega privilegija, so podvrženi varnostnemu preverjanju. Postopek preverjanja se prične na pisni predlog predlagatelja, ki mora vsebovati podatke o osebi, ki jo je treba varnostno preveriti, in stopnjo tajnosti, do katere se bo oseba imela možnost seznanjati s tajnimi podatki. Varnostna preverjanja opravljajo Ministrstvo za notranje zadeve, Policija, Ministrstvo za obrambo in Slovenska obveščevalno varnostna agencija.

5.5 POSTOPKI OB RAZKRITJU TAJNEGA PODATKA

Tajni podatki lahko nastanejo na različnih področjih, največ pa jih je vseeno povezanih z obrambnim področjem. Tajni podatki gredo skozi različne cikluse od nastanka, uporabe, hranjenja in do uničenja na koncu. Tajni podatek lahko za tajnega določijo samo določene osebe na podlagi pisne ocene. Po določitvi stopnje tajnosti je treba dokumente označiti s predpisanimi označbami, ki se razlikujejo glede na stopnjo tajnosti. Pri določanju stopenj tajnosti je treba izbrati najnižjo stopnjo tajnosti, ki bo še zagotavljala, da bo podatek ustrezno zaščiten. Distribuiranje tajnih podatkov lahko poteka preko pošte, s pomočjo kurirjev ali s pomočjo informacijsko-komunikacijskih sredstev. Nacionalni tajni podatki so večinoma še vedno zapisani na papirju in se samo v manjšem obsegu prenašajo po računalniških omrežjih ali preko zaščitenih telefonskih zvez. Ne glede na to, v kateri fazi svojega življenja je tajni podatek, moramo skladno z Zakonom o tajnih podatkih (UPB, Ur. l. RS št. 50/2006) upoštevati naslednja določila v zvezi z zlorabo tajnih podatkov:

- Z vsakim nepooblaščenim dostopom do tajnih podatkov, njihovim uničenjem, odtujitvijo ali kakršnimkoli drugim dogodkom, ki kaže na zlorabo tajnih podatkov (v nadaljnjem besedilu: zloraba tajnega podatka), je treba takoj seznaniti predstojnika organa oziroma osebo, ki jo pooblasti, in mora se zagotoviti vse ukrepe za preprečitev nadaljnje zlorabe tajnega podatka in izsleditev odtujenih tajnih podatkov.

- Če zloraba tajnega podatka kaže na sum storitve kaznivega dejanja, mora predstojnik organa s tem seznaniti policijo ali drug pristojen organ.
- Predstojnik organa, v katerem je bil zlorabljen tajni podatek, mora o tem obvestiti organ, ki je določil tajni podatek.
- Odgovorna oseba organizacije mora o zlorabi tajnega podatka takoj obvestiti naročnika.
- Če je tajnost podatka določil drug organ ali organizacija, ga je o zlorabi tajnega podatka in sprejetih ukrepih treba nemudoma obvestiti.
- O vsaki zlorabi tajnega podatka je treba obvestiti nacionalni varnostni organ.
- Vsak organ mora ob zlorabi tajnega podatka predpisati podrobne postopke in ukrepe.

5.6 LOJALNOST JAVNEGA USLUŽBENCA

Za javnega uslužbenca velja, da mora svoje delo opravljati v skladu Zakonom o javnih uslužbencih. Iz tega izhaja, da mora javni uslužbenec varovati tajne podatke ne glede na način, kako je do njih prišel, oziroma jih izvedel. Ta dolžnost ne preneha veljati tudi po prenehanju delovnega razmerja, oziroma velja do takrat, ko delodajalec javnega uslužbenca te dolžnosti ne razreši.

5.7 POGODBA O ZAPOSLITVI PO ZAKONU O JAVNIH USLUŽBENCIH

Že pred začetkom sprejemanja in kasneje veljavnosti ter uporabe Zakona o javnih uslužbencih je bil v Sloveniji zgrajen uslužbenski sistem v javni upravi, urejen z Zakonom o delavcih v državnih organih, ki je urejal zaposlovanje, sklenitev delovnega razmerja, imenovanje in razrešitev, napredovanje, razporejanje, opravljanje dela ter pravice in dolžnosti delavcev v državnih organih in organih lokalne skupnosti. Zakon o javnih uslužbencih torej ni povsem nov zakon, gre za dograjen, dopolnjen oziroma izboljšan predpis, ki je uvedel tudi pogodbo o zaposlitvi, ki je sicer v sistemu delovnega prava že uveljavljena s splošno delavsko zakonodajo.

Delovno razmerje sklene torej javni uslužbenec s pogodbo o zaposlitvi. Za sestavine pogodbe o zaposlitvi se uporabljajo določbe Zakona o javnih uslužbencih (Ur. l. RS št. 63/2007, s spremembami). Pogodba o zaposlitvi vsebuje navedbo pogodbenih strank, navedbo organa, v katerem bo javni uslužbenec opravljal delo, čas trajanja delovnega razmerja, navedbo delovnega mesta oziroma položaja, na katerem bo javni uslužbenec opravljal delo, podatke o vrsti dela s kratkim opisom dela. Nadalje mora pogodba o zaposlitvi vsebovati podatke o datumu začetka opravljanja del, o kraju opravljanja dela ter določilo o tem, ali se delo opravlja s polnim ali skrajšanim delovnim časom. Pogodba o zaposlitvi mora vsebovati tudi druge podatke, ki jih določa Zakon o javnih uslužbencih, ali drugi področni predpis, ki ureja položaj javnih uslužbencev v organih, ter določilo o osnovni plači in morebitnih dodatkih, vezanih na osnovno plačo. Glede določil o letnem dopustu, delovnem času in odpovednem roku se pogodba o zaposlitvi sklicuje na veljavne predpise, kolektivne pogodbe za

negospodarstvo oziroma splošne akte delodajalca. V pogodbi o zaposlitvi mora biti navedeno tudi, da lahko posamezne sestavine pogodbe delodajalec enostransko spreminja, seveda v skladu z veljavnimi predpisi.

5.8 PROBLEM ZAPOSLITVE NA DELOVNO MESTO, KI ZAHTEVA DOSTOP DO TAJNIH PODATKOV

Ko zaposlimo delavca, ki skladno s sistemizacijo potrebuje dovoljenje za dostop do tajnih podatkov in le-ta še nima dovoljenja, se začne na predlog predstojnika organa postopek preverjanja, ki poteka po Zakonu o upravnem poslovanju. Sam postopek v večini primerov traja do 50 dni, kar predstavlja problem za zaposlenega oziroma organizacijo, saj zaposleni ne sme imeti stika s tajnimi podatki. V primeru, da ima delavec pretežen del delovnega časa kontakt z dokumenti, ki vsebujejo tajne podatke, moramo vedeti, da približno 50 dni za delavca ne bo veliko dela.

5.9 ODPOVED POGODBE O ZAPOSLITVI ZARADI ODVZEMA DOVOLJENJA ZA DOSTOP DO TAJNIH PODATKOV

Zaradi kršitev določb predpisov, ki se nanašajo na varovanje tajnih podatkov, bi lahko bil eden od razlogov za odpoved pogodbe o zaposlitvi po Zakonu o javnih uslužbencih kršitev varovanja tajnih podatkov skladno z Zakonom o tajnih podatkih (UPB, Ur. l. RS št. 50/2006) in podrejenimi predpisi in bi bil zaradi tega predlagan disciplinski postopek, v nadaljevanju pa dokazana odgovornost in nazadnje izrečen disciplinski ukrep odpovedi pogodbe o zaposlitvi.

Drugi razlog odpovedi pogodbe o zaposlitvi zaradi kršitve predpisov o tajnih podatkih pa je določen v 28. a členu Zakona o tajnih podatkih. Na podlagi te določbe lahko delodajalec pri javnemu uslužbencu, ki ne izpolnjuje pogojev za zasedbo delovnega mesta, ker mu je bilo dovoljenje za dostop do tajnih podatkov zavrnjeno oziroma preklicano, uporabi določbe Zakona o javnih uslužbencih.

Delodajalec lahko redno odpove pogodbo o zaposlitvi, če je delavec spoznan za disciplinsko odgovornega in mu je bil izrečen ukrep odpovedi pogodbe o zaposlitvi. Javnih uslužbencev na kršitve pogodbe o zaposlitvi tudi ni treba pisno opozarjati in je možno pogodbo o zaposlitvi odpovedati skladno z razlogi, naštetimi v 159. členu Zakona o javnih uslužbencih. Zakon o javnih uslužbencih med razlogi za prenehanje delovnega razmerja določa tudi odpoved pogodbe o zaposlitvi s strani delodajalca in prenehanje delovnega razmerja na drug način, če tako določa drug področni zakon. Delodajalec lahko odpove pogodbo o zaposlitvi, če je postalo delo javnega uslužbenca nepotrebno iz poslovnega razloga in ga ni mogoče premestiti v skladu z zakonom. Prav tako je mogoče javnemu uslužbencu odpovedati pogodbo o zaposlitvi, če je v posebnem postopku ugotovljeno, da je javni uslužbenec nesposoben za svoje delovno mesto in ga ni mogoče premestiti skladno z zakonom.

Ker Zakon o javnih uslužbencih v 3. odstavku 154. člena določa, da lahko delovno razmerje javnega uslužbenca preneha tudi na drug način, gre torej za odpoved delovnega razmerja iz poslovnih razlogov, ki ga ureja drug zakon, v našem primeru Zakon o tajnih podatkih (UPB, Ur. l. RS št. 50/2006). V primeru odpovedi pogodbe o zaposlitvi javnemu uslužbencu se izda pisni sklep, ki mora biti obrazložen. V sklepu se obvezno določi datum prenehanja delovnega razmerja ter pravice in obveznosti v zvezi s prenehanjem tega razmerja. Pisna odpoved se izda najkasneje v petih dneh od ugotovitve razloga za odpoved. Zoper sklep o odpovedi pogodbe o zaposlitvi je dovoljena pritožba. O pritožbah zoper odločitve o pravicah ali obveznostih iz delovnega razmerja in o drugih vprašanjih, kadar zakon tako določa, pa odloča pristojna komisija za pritožbe iz delovnega razmerja.

5.10 UGOTOVITVE, DOBLJENE PRI DELU NA MINISTRSTVU ZA OKOLJE IN PROSTOR

Ob stikih s sodelavci, ki imajo ali pa morajo pridobiti dovoljenje za dostop do tajnih podatkov, prevladuje mnenje, da so vsi problemi, ki izhajajo iz rokovanja s tajnimi podatki, zajeti v zakonodaji, vezani na Zakon o tajnih podatkih (UPB, Ur. l. RS št. 50/2006), s čimer se seveda ne moremo strinjati, oziroma ni res. Zakon o tajnih podatkih (UPB, Ur. l. RS št. 50/2006) se ukvarja s tajnimi podatki, ki izhajajo iz področja javne varnosti, obrambe, zunanjih zadev ali obveščevalno varnostne dejavnosti Republike Slovenije, dejansko pa opravljanje kakršnekoli dejavnosti zahteva stalno varovanje nekaterih podatkov kot na primer varstvo osebnih podatkov, poslovne in druge tajnosti. Posledično iz teh dejstev izhaja, da je treba »pomembne« podatke varovati tudi, če niso obravnavani v Zakonu o tajnih podatkih. V primeru Ministrstva za okolje in prostor je treba definirati varovanje takšnih podatkov v Pravilniku o notranji organizaciji in sistemizaciji delovnih mest. Ta način bi bil primerljiv s statuti gospodarskih družb, društev ipd. Ob tem je treba posebno pozornost posvetiti odnosom med tajnimi podatki po Zakonu o tajnih podatkih, osebnih podatkih, ki se zbirajo in hranijo skladno z določili Zakona o varstvu osebnih podatkov, ter drugimi podatki, ki se jih mora varovati zaradi interesov organizacije, v kateri so nastali. Skladno z Zakonom o tajnih podatkih lahko rečemo, da imamo moto: »Kar ni tajno, še ne pomeni, da je javno.« Seveda, če tak podatek ni urejen z Zakonom o dostopu do informacij javnega značaja (UPB – Ur. l. RS, št. 51/2006).

6 TAJNI PODATKI NA MINISTRSTVU ZA OKOLJE IN PROSTOR

Ministrstvo za okolje in prostor na prvi pogled oziroma iz zornega kota nepoznavalca obrambnega sistema v Republiki Sloveniji nima delovnega področja, ki bi imelo kaj dosti skupnega s tajnimi podatki. V času, kot je danes, in nam Ocena ogroženosti države ne napoveduje neposrednih groženj z vojaško silo, vseeno prihaja do ocen, da je možnost asimetričnih groženj realna. Ministrstvo za okolje in prostor v Direktoratu za prostor skupaj z Ministrstvom za obrambo določa območja, ki so posebnega pomena za obrambo države. Uprava Republike Slovenije za jedrsko varnost ima podatke o skladiščih nevarnega jedrskega odpada, ki ga je mogoče uporabiti za umazane bombe, in druge občutljive podatke. Upravitelj obrambnega načrta skrbi za obrambni načrt in v teh dokumentih so podatki, ki se v nekaterih primerih označijo kot tajni. V primeru večje ogroženosti države bi stopnjo tajnosti verjetno dobili tudi podatki o vodnih virih in distribucijskih sistemih vode, ki so verjetno eden od najbolj potrebnih in hkrati tudi zelo ogroženih delov naše države.

6.1 PRAVILNIK O RAVNANJU Z DOKUMENTARNIM GRADIVOM MINISTRSTVA ZA OKOLJE IN PROSTOR, KI VSEBUJE TAJNE PODATKE

Pravilnik ureja sistem postopkov in ukrepov varovanja tajnih podatkov v Ministrstvu za okolje in prostor ter v organih v njegovi sestavi, ki ustrezajo določeni stopnji tajnosti podatkov, in onemogoča njihovo razkritje nepoklicanim osebam. Postopki in ukrepi varovanja tajnih podatkov v ministrstvu obsegajo:

- splošne varnostne ukrepe in varovanje oseb, ki imajo dostop do tajnih podatkov;
- varovanje prostorov;
- sprejem in evidentiranje pošte, ki vsebuje tajne podatke;
- odpiranje pošte, ki vsebuje tajne podatke;
- ravnanje s tajnimi podatki in zagotovitev tajnosti podatkov;
- pristojnosti za določanje tajnih podatkov;
- označevanje tajnih podatkov;
- prenos tajnih podatkov.

6.1.1 Odgovornost za izvajanje predpisov in nadzora nad tajnimi podatki

Za izvajanje predpisov, ki urejajo ravnanje s tajnimi podatki, je primarno odgovoren predstojnik, za izvajanje postopkov in ukrepov varovanja tajnih podatkov pa so odgovorni tudi vodja glavne pisarne oziroma vložišča ter vsi zaposleni, ki imajo dostop do tajnih podatkov. Notranji nadzor nad izvajanjem zakona o tajnih podatkih in predpisov, izdanih na njegovi podlagi, v Ministrstvu za okolje in prostor opravlja organizacijska enota, ki jo s sklepom določi minister, in sicer je to Služba za notranjo revizijo.

6.1.2 Dostop in dovoljenje za dostop do tajnih podatkov

Vse osebe, ki opravljajo funkcijo ali delajo v ministrstvu, imajo dostop do tajnih podatkov stopnje Interno. Dovoljenje pridobijo po opravljenem osnovnem usposabljanju s področja obravnavanja in varovanja tajnih podatkov ter podpisom izjave, da so seznanjene z zakonom o tajnih podatkih in drugimi predpisi, ki urejajo varovanje tajnih podatkov, in da se zavezujejo s tajnimi podatki ravnati v skladu s temi predpisi. Vsebina izjave je objavljena v Uredbi o varnostnem preverjanju izdaji dovoljenj za dostop do tajnih podatkov, podpisan izvod izjave pa se hrani v kadrovski mapi zaposlenega. Napotitev na osnovno usposabljanje s področja obravnavanja in varovanja tajnih podatkov izvaja kadrovska služba ministrstva. Usposabljanje izvaja Urad Republike Slovenije za varovanje tajnih podatkov ali organizacijska enota oziroma oseba, ki jo pooblasti minister. Osebe, ki zaradi opravljanja funkcij ali izvajanja nalog na delovnih mestih, za katera je v sistemizaciji delovnih mest kot pogoj za zasedbo delovnega mesta zahtevano dovoljenje za dostop do tajnih podatkov stopenj Zaupno, Tajno ali Strogo tajno, morajo pridobiti dovoljenje za dostop do tajnih podatkov ustrezne stopnje tajnosti. Za osebo, ki potrebuje dovoljenje za dostop do tajnih podatkov, minister na Ministrstvu za okolje in prostor predlaga postopek varnostnega preverjanja za izdajo dovoljenja za dostop do tajnih podatkov. Osebe, ki zaradi opravljanja funkcij ali izvajanja nalog na delovnih mestih, za katera je v sistemizaciji delovnih mest kot poseben pogoj zahtevano dovoljenje za dostop do tajnih podatkov NATO ali EU, pridobijo dovoljenje za dostop do teh podatkov po pridobitvi nacionalnega dovoljenja za dostop do tajnih podatkov ustrezne stopnje po postopku in na način, določen z Zakonom o tajnih podatkih.

6.1.3 Obravnava in hranjenje tajnih podatkov

Tajni podatki z delovnega področja ministrstva se lahko obdelujejo in hranijo samo v prostorih ministrstva. Tajni podatki stopnje tajnosti Interno se lahko obravnavajo v upravnem območju. Upravno območje določi minister oziroma predstojnik organa v sestavi s sklepom, in sicer je tak sklep na Ministrstvu za okolje in prostor sprejet za vse objekte ministrstva. Tajni podatki stopnje tajnosti Zaupno ali višje stopnje tajnosti se lahko obravnavajo le v varnostnem območju, ki se vzpostavi znotraj upravnega območja. Vzpostavitev varnostnega območja določi minister ali predstojnik organa v sestavi s sklepom, ki v konkretnem primeru določa eno varnostno območje. Z načrtom varovanja tajnih podatkov se glede na stopnjo tajnosti podatkov in oceno ogroženosti določijo fizični, organizacijski in tehnični ukrepi ter postopki za varovanje tajnih podatkov v varnostnem območju. Minister določi odgovorno osebo za izdelavo načrta varovanja tajnih podatkov s sklepom.

6.1.4 Evidentiranje dokumentov, ki vsebujejo tajne podatke

Za evidentiranje dokumentov, ki vsebujejo tajne podatke, se uporabljajo določbe Uredbe o varovanju tajnih podatkov (Ur. l. RS št. 74/05) in predpisov, ki urejajo poslovanje organov javne uprave z dokumentarnim gradivom, ter drugih predpisov, ki urejajo poslovanje z dokumentarnim gradivom. Za evidentiranje dokumentov v

ministrstvu uporabljamo aplikacijo SPIS 4. Pri evidentiranju dokumentov, ki vsebujejo tajne podatke, je treba zagotoviti, da se iz posameznih vpisov, ki jih vsebuje evidenca, ne da razbrati vsebine tajnega podatka. Dokumentov, ki vsebujejo tajne podatke, ni dovoljeno skenirati, je pa v opombe treba navesti, da dokument vsebuje tajne podatke ter stopnjo tajnosti. Evidentiranje dokumentov v aplikacijo SPIS 4 (uvrstitev dokumenta v zadevo oziroma odprtje nove zadeve), ki vsebujejo tajne podatke stopnje tajnosti Interno, opravi glavna pisarna, evidentiranje dokumentov, ki vsebujejo tajne podatke stopnje tajnosti Zaupno ali višjo stopnjo tajnosti, pa glavna pisarna na zahtevo osebe, ki je prejemnik dokumenta ali prejemnik dokumenta sam. V primeru, ko zunanji dostavljavec vroči dokument, ki vsebuje tajne podatke neposredno naslovniku, je naslovnik dolžan o tem obvestiti glavno pisarno oziroma odgovorno osebo v varnostnem območju ter poskrbeti, da se opravi evidentiranje. Vhodna pošta, ki vsebuje tajne podatke stopnje Interno, se sprejema v glavni pisarni ministrstva ali organa v sestavi. Glavna pisarna dokument, ki vsebuje tajne podatke stopnje Interno, dostavi naslovniku z notranjo kurirsko službo. Za ta namen se uporablja kurirska knjiga za dostavo tajnih podatkov stopnje Interno. V kurirsko knjigo se vpiše:

- zaporedna številka vpisa,
- datum vpisa,
- podatki o prejemniku,
- datum prejema ter podpis prejemnika.

Če ime in priimek naslovnika nista razvidna, glavna pisarna glede na vsebino dokumenta dostavi dokument v obravnavo pristojni organizacijski enoti ali odgovornemu delavcu, ki vodi zadevo. Za dokumente, ki vsebujejo tajne podatke stopnje tajnosti Interno, lahko podpis naslovnika v dostavni knjigi nadomesti vročilnica, podpisana s strani prejemnika. Izpolnjene in s strani prejemnika podpisane vročilnice se hranijo v glavni pisarni, v kurirski knjigi pa se označi, da je bil dokument vročen z vročilnico. Vhodno pošto, ki vsebuje tajne podatke stopnje tajnosti Zaupno ali višjo stopnjo, sprejema odgovorna oseba v varnostnem območju, ki jo s sklepom določi minister. Prejeta pošta se vpiše v evidenco tajnih podatkov stopnje Zaupno ali višje stopnje. Evidenca vsebuje podatke o:

- zaporedni številka vpisa,
- datum prejema,
- podatke o pošiljatelju,
- številko in datum nastanka dokumenta,
- podatke o naslovniku,
- stopnji tajnosti,
- številki izvoda,
- datumu in uri vročitve naslovniku,
- podpis naslovnika.

Oseba v varnostnem območju, ki je sprejela pošto, ki vsebuje tajne podatke stopnje Zaupno ali višje stopnje, nemudoma obvesti naslovnika, da je zanj prispela pošta, ki vsebuje stopnjo tajnosti Zaupno ali višje stopnje, ter ga pozove, da prevzame pošto v varnostnem območju. Pri dokumentu, ki vsebuje tajne podatke stopnje tajnosti Tajno ali Strogo tajno, naslovnik izpolni pripet obrazec Seznam vpogledov v dokument. Če k dokumentu obrazec Seznam vpogledov v dokument ni pripet, obrazec izpolni in

pripne k dokumentu. V primeru, da prejemnik oceni, da je potrebno tajni podatek stopnje tajnosti Zaupno ali višje stopnje tajnosti zaradi točno določene naloge obravnavati zunaj varnostnega območja, je treba ravnati skladno z določili prvega, drugega in tretjega odstavka 16. člena Uredbe o varovanju tajnih podatkov. Podatki o iznosu dokumenta iz varnostnega območja se hranijo kot priloga evidenci tajnih podatkov stopnje Zaupno ali višje stopnje. Pošto, ki vsebuje tajne podatke, odpira naslovnik, ki ima dovoljenje za dostop do tajnih podatkov. Pošto, ki vsebuje tajne podatke, naslovljeno na ministrstvo, odpre minister, državni sekretar ali generalni sekretar, v organih v sestavi pa predstojnik organa v sestavi oziroma osebe, ki imajo dovoljenje za dostop do tajnih podatkov ustrezne stopnje tajnosti in ki jih s sklepom pooblasti minister ali predstojnik organa v sestavi. V primeru daljše odsotnosti naslovnika, na katerega je naslovljena pošta, ki vsebuje tajne podatke, v ministrstvu odpira minister, državni sekretar ali generalni sekretar oziroma predstojnik organa v sestavi ali od njega pooblaščena oseba, ki ima dovoljenje za dostop do tajnih podatkov ustrezne stopnje tajnosti.

6.1.5 Ravnanje s tajnimi podatki

S tajnimi podatki je treba ravnati tako, da nepooblaščenim osebam ni omogočen vpogled v njihovo vsebino. Oseba, ki se je v okviru svojega dela ali opravljanja funkcije seznanila s tajnimi podatki, teh ne sme uporabljati za druge namene kot za izvajanje delovnih nalog ali opravljanje funkcije. Vsaka seznanitev s tajnimi podatki stopnje Tajno in Strogo tajno se zabeleži v obrazec Seznam vpogledov, ki je pripet dokumentu. Tajni podatek stopnje tajnosti Strogo tajno se ne sme razmnoževati, kopirati ali prepisovati. Dodatne izvode zapisa tega tajnega dokumenta sme izdelati le pooblaščena oseba organa, v katerem mu je bila določena stopnja tajnosti. Tajni podatek stopnje tajnosti Interno, Zaupno ali Tajno se lahko kopira v ustreznem varnostnem območju le na podlagi pisarniške odredbe predstojnika ali osebe, ki jo za to pooblasti predstojnik. Pisarniška odredba mora vsebovati podatke o naslovu, številki in datumu dokumenta, število kopij in prejemnikih kopij. Iz vsake kopije tajnega podatka mora biti razvidno, iz katerega zapisa ali dela zapisa izhaja kopija (številka in datum dokumenta). Pisarniška odredba za kopiranje dokumenta, ki vsebuje tajni podatek, se hrani pri originalu dokumenta, ki je bil kopiran.

6.1.6 Določanje stopnje tajnosti

Podatkom lahko stopnjo tajnosti določajo minister, predstojniki organov v sestavi in osebe, ki jih za to skladno z določili 10. člena Zakona o tajnih podatkih s sklepom pooblasti minister. V sklepu o pooblastilu za določanje tajnih podatkov se določi tudi stopnja tajnosti, do katere ima oseba pooblastilo za določanje stopnje tajnosti. Oseba, ki je pristojna, oziroma ima pooblastilo za določanje stopnje tajnosti, podatkom določi stopnjo tajnosti pod pogoji in na način, ki so določeni v zakonu o tajnih podatkih.

6.1.7 Označevanje in prenašanje tajnih podatkov

Tajni podatki morajo biti označeni skladno z določili Uredbe o varovanju tajnih podatkov. Tajni podatki stopnje tajnosti Interno se lahko prenašajo v zaprti ovojnici po lastni prenosni mreži z vročilnico ali po priporočeni pošti s povratnico. Tajni podatki stopnje tajnosti Zaupno ali višje stopnje tajnosti se prenašajo v dveh ovojnicah. Zunanja ovojnica je iz trdega, neprosojnega in nepropustnega materiala, na njej pa morajo biti podatki o naslovniku, pošiljatelju in številka dokumenta. Iz oznak na zunanji ovojnici ne sme biti razvidno, da vsebuje tajni podatek. Notranja ovojnica mora imeti oznako stopnje tajnosti, številko dokumenta, podatke o naslovniku in pošiljatelju ter druge podatke, pomembne za varnost. Tajne podatke stopnje tajnosti Zaupno ali višje stopnje tajnosti prenašajo kurirji pod pogoji in na način, določen v četrtem poglavju uredbe o varovanju tajnih podatkov.

6.2 DELOVNA MESTA NA MINISTRSTVU ZA OKOLJE IN PROSTOR Z DOVOLJENJEM ZA DOSTOP DO TAJNIH PODATKOV

Ministrstvo za okolje in prostor ima skupaj z organi v sestavi 1488 zaposlenih, posamezni organi ministrstva imajo sledeče število zaposlenih in delovnih mest, ki imajo kot pogoj za zasedbo delovnega mesta določeno tudi dovoljenje za dostop do tajnih podatkov (nacionalni, EU in Nato):

Tabela 1: Število dovoljenj na Ministrstvu za okolje in prostor

	ST	T	Z	EU-ST	EU-T	EU-Z	N-ST	N-T	N-Z
MOP	13	37	0	0	3	1	0	3	0
ARSO	0	2	0	0	2	0	0	2	0
IRSOP	0	1	0	0	0	0	0	0	0
GURS	0	2	0	0	0	0	0	0	0
URSJV	1	15	1	1	11	1	1	11	0

Vir: Evidence Ministrstva za okolje in prostor.

Podatki o izdanih dovoljenjih za dostop do tajnih podatkov se zbirajo centralno na Ministrstvu za okolje in prostor, ki jih po potrebi posreduje Uradu Republike Slovenije za varovanje tajnih podatkov. Večina dovoljenj za dostop do tajnih podatkov je izdana vodjem direktoratov, predstojnikom organov, vodjem sektorjev in služb ter strokovno tehničnim delavcem ministrstva, ki opravljajo dela v Glavni in sprejemni pisarni Ministrstva za okolje in prostor. Drugače je v Direktoratu za prostor in na Upravi za jedrsko varnost, kjer imajo podatki, s katerimi delajo zaposleni večkrat kot na ostalem delu Ministrstva za okolje in prostor, določeno stopnjo tajnosti in zato pogoj, da je na določenem delovnem mestu potrebno dovoljenje za dostop do tajnih podatkov, ni vezan le na vodstveno funkcijo.

6.2.1 Količina dokumentov, ki vsebujejo tajne podatke na Ministrstvu za okolje in prostor

V času pred uveljavitvijo zakonodaje, kot jo poznamo danes, so zaposleni dokumente označevali velikokrat po lastni presoji, ni bilo evidenc o številu dokumentov s tajnimi podatki in nasploh je bilo stanje nepregledno. Ob pregledu evidenc danes vidimo, da od leta 2006 naprej Ministrstvo za okolje in prostor ni prejelo ali določilo nobenega dokumenta, ki bi vsebovalo tajne podatke stopnje Zaupno ali višje. Pridobljenih je bilo le nekaj dokumentov s tajnimi podatki Nata, ki vsebujejo podatke stopnje Zaupno ali višje, ostali dokumenti, ki jih je malo manj kot 40, pa imajo določeno stopnjo tajnosti Interno. Če pogledamo pred leto 2006, vidimo, da je stanje precej drugačno, prejeto ali določeno je bilo več kot 50 dokumentov, ki vsebujejo stopnjo tajnosti Zaupno ali višje, med njimi pa so tudi dokumenti stopnje Strogo tajno. Ob vseh teh dokumentih je seveda še nekaj neevidentiranih dokumentov, ki pridejo na Ministrstvo za okolje in prostor nenamensko in so vrnjeni izdajatelju v najkrajšem možnem času (gre predvsem za poročila Sove, ki so predstavljena oziroma razdeljena na sejah vlade).

6.2.2 Posebni primeri

Ob sprejetju Zakona o tajnih podatkih in določitvi delovnih mest, ki zahtevajo dovoljenje za dostop do tajnih podatkov, je seveda prišlo tudi do nestrinjanja glede takšne odločitve kadrovske službe, saj je bilo določeno število zaposlenih mnenja, da nikoli ne dostopajo oziroma ne bodo dostopali do tajnih podatkov in v zvezi s tem ne pustijo določenega vdora v svojo zasebnost z izpolnjevanjem varnostnih vprašalnikov, morebitnim preverjanjem navedenih podatkov, zaslišanjem ipd. V večini primerov je vseeno prišlo do varnostnega preverjanja, če ne drugače, tudi z opozorilom, da lahko zavrnitev varnostnega preverjanja vodi tudi do odpustitve zaposlenega. Le v enem primeru je ministrstvo zaradi »upora« zaposlenega popustilo in spremenilo sistemizacijo delovnih mest tako, da dovoljenje za dostop do tajnih podatkov ni bilo več pogoj za zasedbo delovnega mesta. Seveda je primer specifičen zato, ker je Ministrstvo za okolje in prostor zaradi slabe možnosti nadomestitve delavca spregledalo lastno odločitev o potrebi po dovoljenju za dostop do tajnih podatkov na določenem delovnem mestu.

6.2.3 Delovni prostori Ministrstva za okolje in prostor

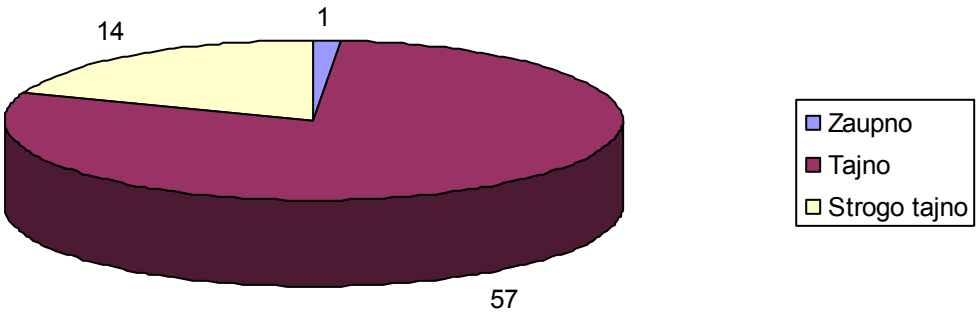
V vseh prostorih, ki jih uporablja Ministrstvo za okolje in prostor, je s sklepom ministra določeno upravno območje. To pomeni, da lahko zaposleni na Ministrstvu za okolje in prostor, ki so bili na osnovnem usposabljanju s področja obravnavanja in varovanja tajnih podatkov, ter podpisom izjave, da so seznanjeni z zakonom o tajnih podatkih in drugimi predpisi, ki urejajo varovanje tajnih podatkov, in da se zavezujejo s tajnimi podatki ravnati v skladu s temi predpisi, na celotnem upravnem območju rokujejo s tajnimi podatki do stopnje tajnosti Interno. S tajnimi podatki

stopnje tajnosti Zaupno ali višje stopnje lahko zaposleni z dovoljenjem za dostop do tajnih podatkov in ugotovljeno potrebo po vedenju rokujejo le v varnostnem območju, ki je vzpostavljeno na Ministrstvu za okolje in prostor.

6.3 PODATKI O IN ANKETA ZAPOSLENIH NA MINISTRSTVU ZA OKOLJE IN PROSTOR, KI IMAJO DOVOLJENJE ZA DOSTOP DO TAJNIH PODATKOV

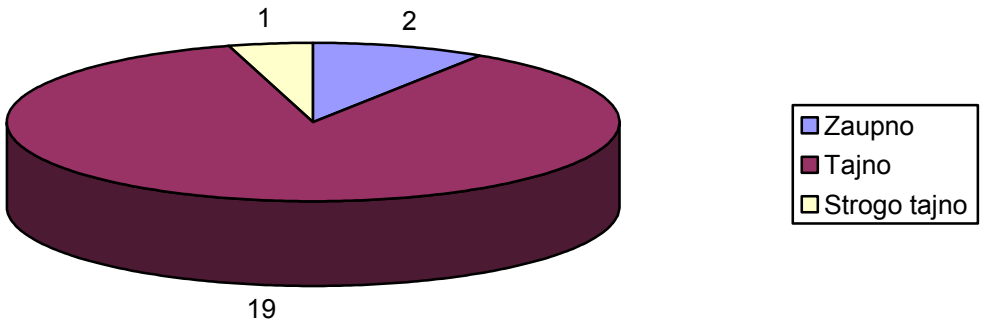
6.3.1 Podatki o zaposlenih na Ministrstvu za okolje in prostor, ki imajo dovoljenje za dostop do tajnih podatkov

Grafikon 1: Dovoljenje za dostop do tajnih podatkov na Ministrstvu za okolje in prostor z vsemi organi v sestavi glede na stopnjo tajnosti:



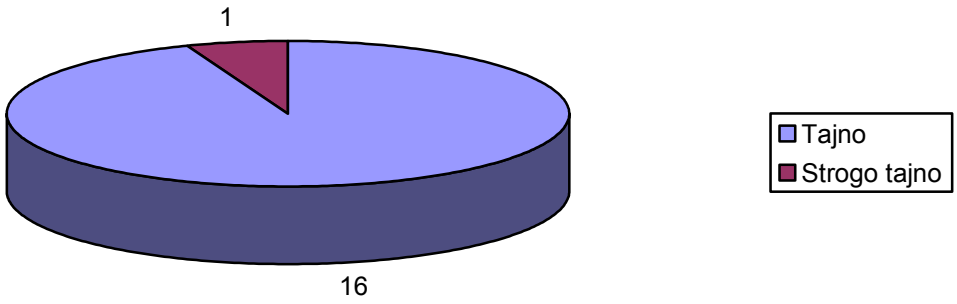
Vir: Evidence Ministrstva za okolje in prostor.

Grafikon 2: EU dovoljenje za dostop do tajnih podatkov na Ministrstvu za okolje in prostor z vsemi organi v sestavi glede na stopnjo tajnosti:



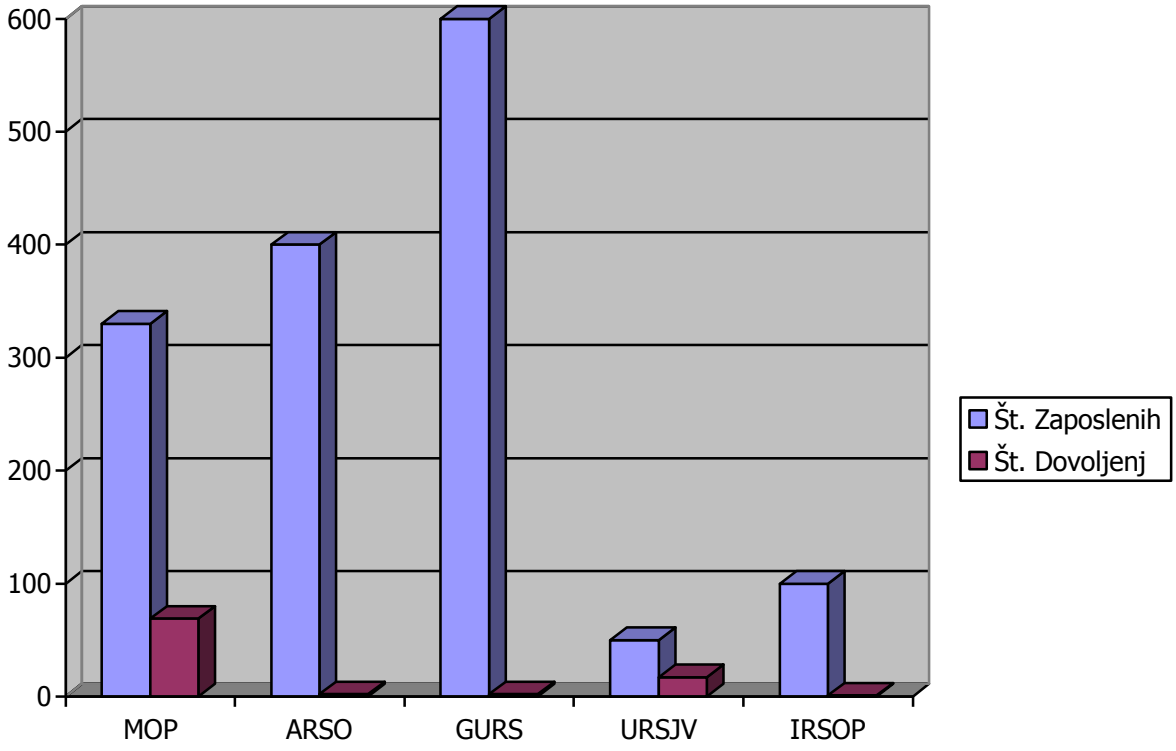
Vir: Evidence Ministrstva za okolje in prostor.

Grafikon 3: Nato dovoljenje za dostop do tajnih podatkov na Ministrstvu za okolje in prostor z vsemi organi v sestavi glede na stopnjo tajnosti:



Vir: Evidence Ministrstva za okolje in prostor.

Grafikon 4: Število zaposlenih z dovoljenjem za dostop do tajnih podatkov in število zaposlenih po posameznem organu Ministrstva za okolje in prostor:

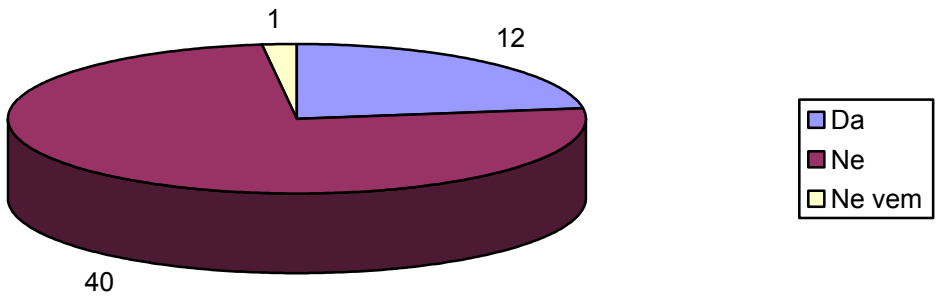


Vir: Evidence Ministrstva za okolje in prostor.

6.3.2 Anketa med zaposlenimi na Ministrstvu za okolje in prostor

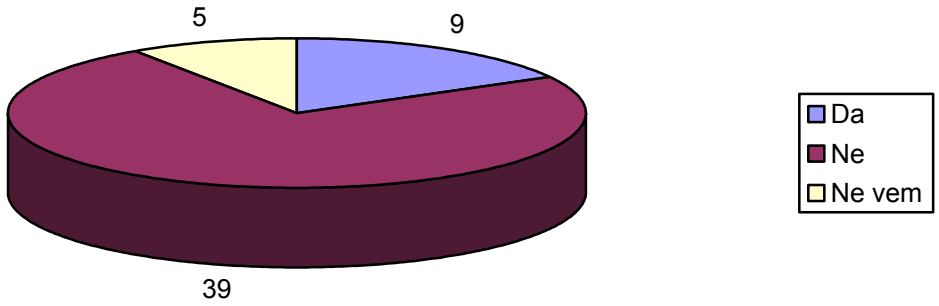
Anketa je izvedena na vzorcu 53 od skupno 72 zaposlenih na Ministrstvu za okolje in prostor, ki imajo dovoljenje za dostop do tajnih podatkov stopnje Zaupno ali višje in so sodelovali oziroma oddali pravilno izpolnjeno anketo.

Grafikon 5: Ali ste kdaj rokovali z dokumenti, ki vsebujejo tajne podatke?



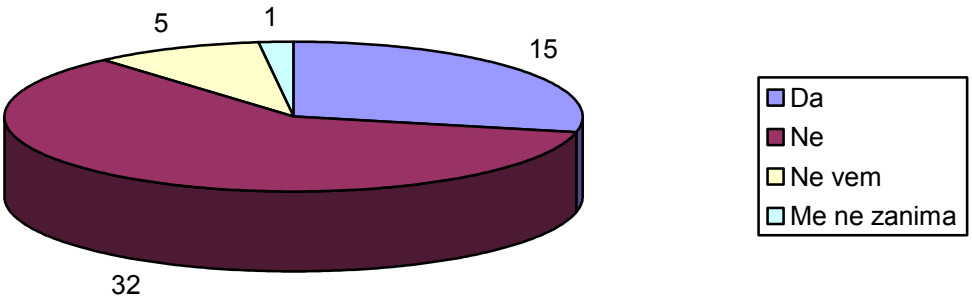
Vir: Anketa, izvedena na Ministrstvu za okolje in prostor.

Grafikon 6: Ali menite, da za opravljanje delovnih nalog ali funkcije na vašem delovnem mestu potrebujete dovoljenje za dostop do tajnih podatkov?



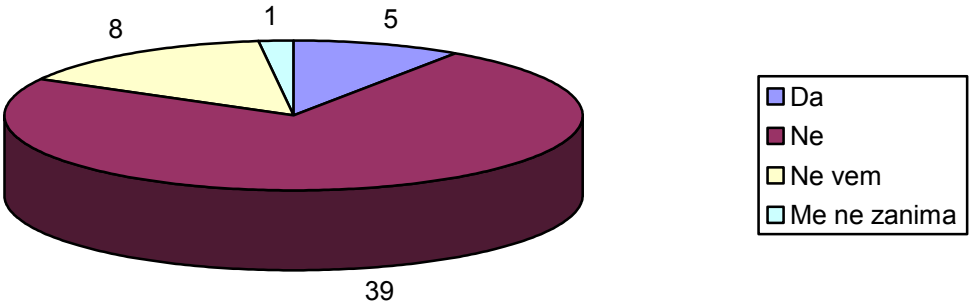
Vir: Anketa, izvedena na Ministrstvu za okolje in prostor.

Grafikon 7: Ali mislite, da ste dovolj usposobljeni za rokovanje s tajnimi podatki?



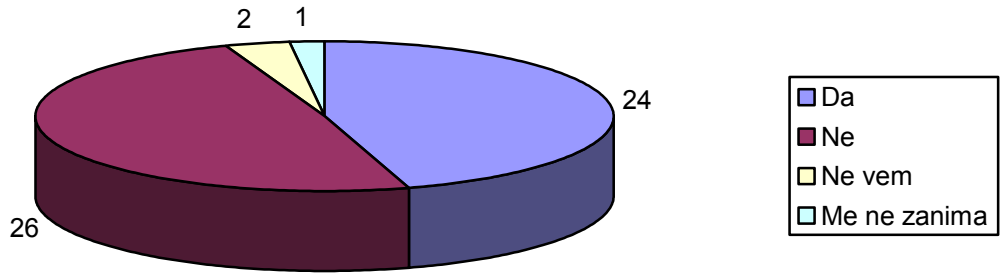
Vir: Anketa, izvedena na Ministrstvu za okolje in prostor.

Grafikon 8: Ali je vaše delovno mesto primerno opremljeno oziroma primerno za rokovanje s tajnimi podatki?



Vir: Anketa, izvedena na Ministrstvu za okolje in prostor.

Grafikon 9: Ali vam je znan izraz »potreba po vedenju«?



Vir: Anketa, izvedena na Ministrstvu za okolje in prostor.

7 ZAKLJUČEK

Za področje delovnih razmerij lahko rečemo, da ima javna uprava izkušnje in tradicijo na področju tajnih podatkov, vendar pa pred letom 2001 v Republiki Sloveniji zakonodaje, ki bi bila usklajena z zakonodajo EU in Nata, ni bilo. Zato smo v Republiki Slovenije leta 2001 sprejeli Zakon o tajnih podatkih (UPB, Ur. l. RS št. 50/2006), ki sicer velja le za tajne podatke Republike Slovenije, vendar se določbe Zakona o tajnih podatkih (UPB, Ur. l. RS št. 50/2006) uporabljajo tudi za podatke držav članic EU in Nato. Je pa poznavanje naše zakonodaje s področja tajnih podatkov in nacionalno varnostno preverjanje potrebno za zaposlene v javni upravi, ki se pri svojem delu srečujejo s tajnimi podatki EU ali Nata.

Obravnavano področje zajema veliko skupino predpisov, ki so v nekaterih delih zelo zahtevni oz. restriktivni. Ko ima organ enkrat vzpostavljeno varnostno območje, osebe, zaposlene v njem, pa so varnostno preverjene, lahko pomislimo, da smo tajne podatke zavarovali pred zlorabami ali razkritji, vendar kmalu ugotovimo, da je samo varovanje tajnih podatkov bolj enostavno kot pa na primer določitev nekega podatka za tajnega. Takrat se vprašamo, ali bo podatek, ki mu določimo stopnjo tajnosti na primer »Tajno«, ob morebitni zlorabi oz. razkritju nepoklicani osebi res hudo škodoval varnosti ali interesom Republike Slovenije, in ugotovimo, da tega verjetno nikoli ne bomo izvedeli. Upamo tudi lahko, da ne bo prišlo do zlorab na način, kot ga opisuje 6. člen Zakona o tajnih podatkih (UPB, Ur. l. RS št. 50/2006), ki govori, da podatek, ki je določen za tajnega z namenom, da bi se prikrilo storjeno kaznivo dejanje, ni tajen, kajti ko je enkrat podatek določen za tajnega, se bo lahko hitro izgubil v množici dokumentov in le težko ga bo našel na primer obrambni inšpektor, ki bo pregledoval stanje na področju tajnih podatkov. Verjetno je največja garancija pred zlorabami tajnih podatkov postavitev odgovornih oseb na delovna mesta, kjer se uporablja tajne podatke, kajti samo varnostno preverjanje ne more zagotoviti nerazkritja oz. zlorabe tajnih podatkov v določenem trenutku, zagotovo pa velja, da je treba določati stopnjo tajnosti določenih podatkov čim bolj racionalno oz. v smislu, da lokacija na primer enega tanka še ni tajen podatek, kakor je bila praksa v času skupne države, vsaj ne v času, v katerem živimo.

Pogodba o zaposlitvi in dovoljenje za dostop do tajnih podatkov Republike Slovenije, EU ali Nata so povezani, nekateri javni uslužbenci ga potrebujemo in imamo z obstojem dovoljenja za dostop do tajnih podatkov izpolnjene pogoje, vezane na naše delovno mesto.

Na Ministrstvu za okolje in prostor ima dovoljenje za dostop do tajnih podatkov v aktu o sistemizaciji delovnih mest 50 zaposlenih od skupno 331 zaposlenih oseb na ministrstvu. V organih v sestavi Ministrstva za okolje in prostor je zaposlenih 1190 oseb, dovoljenje za dostop do tajnih podatkov pa ima 22 zaposlenih. Kot je razvidno iz anketnih vprašanj, večina zaposlenih nikoli ni rokovala s tajnimi podatki, in se tudi zaveda, da niso najbolje usposobljeni za rokovanje s takšnimi podatki.

Ob pregledu evidenc dokumentov tajnih podatkov ugotavljam, da je le 15 zaposlenih na Ministrstvu za okolje in prostor dejansko imelo vpogled, oziroma je delalo z dokumenti, ki vsebujejo tajne podatke. Do vpogleda do dokumentov s tajnimi podatki je seveda lahko prišlo tudi na drugi lokaciji oziroma v tujini, vendar ocena na podlagi poznavanja dela Ministrstva za okolje in prostor govori o zanemarljivem številu zaposlenih, ki so imeli dejanski kontakt s tajnimi podatki.

Samo dovoljenje za dostop do tajnih podatkov še ne dovoljuje vpogleda v dokument s tajnim podatkom, treba je tudi imeti potrebo po vedenju. Kaj je to, anketiranim zaposlenim na Ministrstvu za okolje in prostor tudi ni preveč jasno. Ob neformalnem pogovoru z nekaj sodelavci Ministrstva za okolje in prostor, ki imajo dovoljenje za dostop do tajnih podatkov, sem kot sogovornik hitro doumel, da je dovoljenje za večino vse, kar potrebujejo za dostopanje do tajnih podatkov. K sreči, v večini primerov zaposleni na Ministrstvu za okolje in prostor niso imeli opravka s tajnimi podatki. Se pa postavlja vprašanje, kdo vse bi dejansko potreboval dovoljenje za dostop do tajnih podatkov. Ali so to praktično vsi vodje sektorjev, služb oziroma oddelkov, kot je to na Ministrstvu za okolje in prostor (z nekaj izjemami) urejeno danes, ali pa bi bila potrebna temeljita analiza, ki bi ugotovila, kdo zares potrebuje, oziroma bo potreboval dovoljenje za dostop do tajnih podatkov v primeru krize, poslabšanja varnostnih razmer v Sloveniji ali svetu ipd. V preteklosti sem sam sodeloval pri nastajanju pravilnikov v zvezi z varovanjem tajnih podatkov in urejanju varnostnega območja, ni pa bilo jasno, kako določiti delovna mesta z zahtevo po dovoljenju za dostop do tajnih podatkov, zato so bila na moj predlog kot koordinatorja določena na področju varovanja tajnih podatkov (približno 15 delovnih mest), ostala delovna mesta pa so tak pogoj dobila brez premisleka. Moj predlog je, da Ministrstvo za okolje in prostor na podlagi analize evidenc prejetih dokumentov, ki vsebujejo tajne podatke v zadnjih letih (od uveljavitve trenutne zakonodaje s področja tajnih podatkov), na novo določi delovna mesta, ki imajo kot enega od pogojev za zasedbo tudi pridobitev dovoljenja za dostop do tajnih podatkov, saj s tem ne bi po nepotrebnem obremenjevali ali mogoče strašili zaposlenih, ki morajo pridobiti dovoljenje za dostop do tajnih podatkov. Racionalizacija oziroma zmanjšanje števila dovoljenj je logična tudi zaradi vse manjšega števila dokumentov, ki vsebujejo tajne podatke.

LITERATURA

1. Čaleta, Denis. Ustrezen sistem varovanja tajnih podatkov – nujnost v Slovenski vojski, Bilten Slovenske vojske št. 2, Ministrstvo za obrambo, Ljubljana, 2003.
2. Deklaracija o človekovih pravicah, A/RES/217A (III), Generalna skupščina Združenih narodov, 12/1948.
3. Evropska konvencija o človekovih pravicah, Uradni list RS (13. 6. 1994) MP, št.7-41/1994 (RS 33/1994).
4. Kolektivna pogodba za javni sektor, Uradni list RS, št. 57/2008.
5. Konvencija o varstvu posameznika, Uradni list RS(28. 2. 1994)-MP, št. 3-18/1994 (RS 11/1994).
6. Mednarodni pakt o državljanskih in političnih pravicah, Resolucija št. 2200, Generalna skupščina Združenih narodov 12/1966.
7. Merila za ureditev poslovnih prostorov za potrebe državne uprave. Vlada Republike Slovenije, šif. 361-00/2001-8 z dne 04. 11. 2004.
8. Odlok o ravnanju s tajnimi podatki v Državnem zboru Republike Slovenije (OdRTP), Ur.l. RS, št. 107/2005.
9. Pravilnik o hišnem redu v objektih Ministrstva za okolje in prostor, Ministrstvo za okolje in prostor, 11. 11. 2008.
10. Pravilnik o načinu in postopku določanja tajnih podatkov s področja obrambe v gospodarskih družbah, zavodih in organizacijah, Ur. l. RS, št. 108/2002.
11. Pravilnik o notranji sistemizaciji in organizaciji delovnih mest na Ministrstvu za okolje in prostor, št. 125/2004 in spremembe sistemizacijskega akta.
12. Pravilnik o ravnanju z dokumentarnim gradivom Ministrstva za okolje in prostor, ki vsebuje tajne podatke, z dne 4. 4. 2005.
13. Sklep o ustanovitvi, nalogah in organizaciji Urada Vlade RS za varovanje tajnih podatkov Uradni list RS, 6/2002.
14. Uredba o izvajanju inšpekcijskega nadzora na področju varovanja tajnih podatkov in vsebini posebnega dela strokovnega izpita za inšpektorja, Ur. l. RS, št. 94/2006.
15. Uredba o načinu in postopku varnostnega preverjanja Uradni list RS, št. 110/2003.
16. Uredba o notranjem nadzoru nad izvajanjem zakona o tajnih podatkih in predpisov, izdanih na njegovi podlagi Uradni list RS, 106/2002.
17. Uredba o spremembah Uredbe o varnostnem preverjanju in izdaji dovoljenj za dostop do tajnih podatkov, Ur. l. RS, št. 138/2006.
18. Uredba o ugotavljanju izpolnjevanja pogojev za posredovanje tajnih podatkov drugi organizaciji Uradni list RS, 106/2000.
19. Uredba o varnostnem preverjanju in izdaji dovoljenj za dostop do tajnih podatkov, Ur. l. RS, št. 71/2006.
20. Uredba o varovanju tajnih podatkov v komunikacijsko informacijskih sistemih, Ur. l. RS, št. 48/2007.
21. Uredba o varovanju tajnih podatkov, Uradni list RS 74/2005.
22. Ustava Republike Slovenije, Uradni list, RS, št. 33I/1991-I.
23. Zakon o delovnih razmerjih, Uradni list RS, št. 42/2002.

24. Zakon o dostopu do informacij javnega značaja (Uradno prečiščeno besedilo) Uradni list RS, št. 61/2005.
25. Zakon o javnih uslužbencih (uradno prečiščeno besedilo), Uradni list RS, št. 73/2007.
26. Zakon o tajnih podatkih, (uradno prečiščeno besedilo), Uradni list RS, 50/2006.
27. Zakon o varstvu osebnih podatkov.

SEZNAM SLIK IN TABEL

SEZNAM UPORABLJENIH KRATIC

EU – Evropska unija
Nato – North Atlantic Threaty Organisation – Severnoatlantska zveza
MOP – Ministrstvo za okolje in prostor
ARSO - Ministrstvo za okolje in prostor – Agencija Republike Slovenije za okolje
GURS - Ministrstvo za okolje in prostor – Geodetska uprava Republike Slovenije
URSJV - Ministrstvo za okolje in prostor – Uprava Republike Slovenije za jedrsko varnost
IRSOP - Ministrstvo za okolje in prostor – Inšpektorat Republike Slovenije za okolje in prostor
ST – Stopnja tajnosti Strogo tajno
T – Stopnja tajnosti Tajno
Z – Stopnja tajnosti Zaupno
EU - ST – Evropska stopnja tajnosti Strogo tajno
EU - T – Evropska stopnja tajnosti Tajno
EU - Z – Evropska stopnja a tajnosti Zaupno
N - ST – Nato stopnja tajnosti Strogo tajno
N - T – Nato stopnja tajnosti Tajno
N - Z – Nato stopnja a tajnosti Zaupno
Sova – Slovenska obveščevalno varnostna agencija

IZJAVA O AVTORSTVU IN NAVEDBA LEKTORJA

Izjavljam, da je diplomsko delo z naslovom Dovoljenje za dostop do tajnih podatkov na Ministrstvu za okolje in prostor moje avtorsko delo.

Andrej Loboda

Diplomsko delo z naslovom Dovoljenje za dostop do tajnih podatkov na Ministrstvu za okolje in prostor je lektorirala Vesna Muhič, profesorica slovenščine.