UNIVERZA NA PRIMORSKEM
FAKULTETA ZA MANAGEMENT

# MAGISTRSKA NALOGA

VESNA REBEC

KOPER, 2020

2020
MAGISTRSKA NALOGA
VESNA REBEC

UNIVERZA NA PRIMORSKEM
FAKULTETA ZA MANAGEMENT

Magistrska naloga

# VARSTVO POSLOVNE SKRIVNOSTI IN TAJNIH PODATKOV V SAMOUPRAVNI LOKALNI SKUPNOSTI

Vesna Rebec

Koper, 2020

Mentorica: izr. prof. dr. Elizabeta Zirnstein

## POVZETEK

Odtekanje poslovnih skrivnosti in tajnih podatkov lahko resno ogrozi delovanje države, lokalnih skupnosti ali gospodarskih subjektov še posebej, ko gre za podatke na področju javne varnosti, obrambe, zunanjih zadev in varnostnih dejavnosti, ali podatke, ki pomenijo konkurenčno prednost. Po drugi strani pa ima javnost interes nadzirati delovanje države in lokalnih skupnosti preko instituta informacij javnega značaja ter lahko zahteva dostop do teh podatkov. V nalogi smo proučili pravno ureditev na tem področju in z analizo judikature ter z raziskavo na terenu ugotavljali, kako ta učinkuje v praksi. Ugotovili smo, da v praksi lokalne skupnosti v svojih internih aktih ne ločijo med tajnim podatkom in poslovno skrivnostjo, obseg podatkov, ki so »odvzeti« javnemu nadzoru, pa je od občine do občine zelo različen. S sintezo teoretičnega in empiričnega dela naloge smo izoblikovali priporočila za ustreznejšo normativno ureditev varovanja poslovnih skrivnosti in tajnih podatkov v lokalnih skupnostih.



*Ključne besede*: tajni podatki, poslovna skrivnost, lokalna skupnost, informacija javnega značaja, zaupni podatek.



## SUMMARY

Leaking business secrets and confidential data can seriously threaten a country’s operations, local communities, or business entities, especially when it comes to information on public safety, defense, foreign affairs, and safety activities or data with competitive advantages. On the other hand, the public is interested in monitoring the operation of the country and its local communities through the institute of significant public information, and it may also demand access to this data. In the thesis we examined this field’s legal arrangements; with jurisdiction analysis and practical studies we found how it is effective in practice. We understood that in practice local communities in their internal acts do not differentiate between classified information and business secrets; the range of data that is seized from public control is distinct from one municipality to the other. With synthesis of the theoretical and empirical parts of the thesis we formed proposals for more suitable normative arrangements for the safeguarding of business secrets and confidential information in local communities.



*Keywords*: confidential data, business secret, local community, significant public information, confidential data.

UDK: 347.4:352(043.3)

**ZAHVALA**

Pri nastajanju magistrske naloge sem hvaležna vsem, ki so mi kakorkoli pri tem pomagali. Hvala mentorici, izredni profesorici dr. Elizabeti Zirnstein, ki me je s strokovnimi nasveti vodila pri nastajanju naloge.

Iskreno zahvalo si zaslužijo moji domači in sodelavci, ki so me spodbujali in mi stali ob strani v času študija.

**VSEBINA**

**SLIKE**

## KRAJŠAVE

| | |
|---|---|
| EK | Evropska komisija |
| GD | Generalni direktorat |
| IP | Informacijski pooblaščenec |
| JKP | Javno komunalno podjetje |
| KES | Komisije Evropske skupnosti |
| KS Ljubno | Krajevna skupnost Ljubno |
| KZ | Kazenski zakonik |
| NLG | Navigazione Libera del Golfo Srl |
| Občina KG | Občina Kranjska Gora |
| OLAF | European Anti-Fraud Office (Evropski urad za boj proti goljufijam) |
| OZ | Obligacijski zakon |
| PDEU | Pogodba o delovanju Evropske unije |
| Pogodba EGS | Pogodba Evropske gospodarske skupnosti |
| RS | Republika Slovenija |
| TRIPS | Trade-Related Aspects of Intellectual Property Rights |
| UPRS | Upravno sodišče RS |
| URS | Ustava Republike Slovenije |
| VDSS | Višje delovno in socialno sodišče |
| ZBan-1 | Zakon o bančništvu |
| ZDIJZ | Zakon o dostopu do informacij javnega značaja |
| ZDR-1 | Zakon o delovnih razmerjih |
| ZGD-1 | Zakon o gospodarskih družbah |
| ZInfP | Zakon o Informacijskem pooblaščencu |
| ZJN-3 | Zakona o javnem naročanju |
| ZJU | Zakon o javnih uslužbencih |
| ZPOmK-1 | Zakon o preprečevanju omejevanja konkurence |
| ZPosS | Zakon o poslovni skrivnosti |
| ZTP | Zakon o tajnih podatkih |
| ZVDAGA | Zakon o varstvu dokumentarnega in arhivskega gradiva ter arhivih |
| ZVOP | Zakon o varstvu osebnih podatkov |

# 1 UVOD

V pogojih konkurence in globalne ekonomije je varovanje poslovnih skrivnosti in upravljanje z njimi vse bolj pomembno, saj gre za informacije, ki pomenijo konkurenčno prednost podjetja. Poslovne skrivnosti dejansko sodijo med najdragocenejša sredstva podjetja, tako kot so to odnosi s strankami ali pa naložbe v usposabljanje in izobraževanje delovne sile (Knowlton 2014, 16). Uspeh podjetja je namreč močno odvisen od konkurenčnosti informacij, ki jih podjetje ima. Dejansko je vrednost neopredmetenih sredstev podjetja, kamor spadajo poslovne skrivnosti, v primerjavi z vrednostjo fizičnih in finančnih sredstev vse od začetka osemdesetih let nenehno naraščala. Leta 2000 je bilo več kot 83 odstotkov tržne vrednosti podjetij S&P 500, (S&P je borzni indeks, ki meri uspešnost 500 velikih podjetij, ki kotirajo na borzah v Združenih državah Amerike (v nadaljevanju ZDA) sestavljenih iz neopredmetenih sredstev. Za številna znana podjetja je bil ta odstotek še višji: Johnson in Johnson (87,9 %), Proctor in Gamble (88,5 %), Merck (93,5 %), Microsoft (97,8 %) in Yahoo (98,9 %) (Mendenhall 2014, 893).

## 1.1 Teoretična izhodišča in opredelitev problema

Poslovna skrivnost sodi med pravice intelektualne lastnine, kamor spadajo tudi patent, model, blagovna znamka, avtorska pravica, inovacije, izumi in drugo (Jain 1996). Za razliko od naštetih pravic pa imetnik poslovne skrivnosti ni lastnik izključne pravice nad lastno stvaritvijo, kar nadalje pomeni, da jo lahko konkurenti odkrijejo in uporabljajo (Lampe 2014, 12). Poslovna skrivnost se namreč ne zaščiti z registracijo, pač pa tako, da se ne razkrije. Za pomembne poslovne skrivnosti ameriška podjetja vsako leto porabijo več milijard dolarjev za njihovo zaščito, zakonodaja, ki ureja varstvo poslovnih skrivnosti, pa postaja vse bolj pomembna (Mendenhall 2014, 893).

V teoriji obstaja veliko različnih opredelitev poslovne skrivnosti. Po Mendenhallu (2014, 897) je poslovna skrivnost vsaka informacija, ki je za podjetje dragocena in skrivna, daje ji konkurenčno prednost pred drugimi podjetji in bi njeno razkritje podjetju povzročilo veliko gospodarsko škodo. Takšna informacija ni omejena na tehnologijo in lahko vključuje tudi zaupne poslovne evidence ter računovodske izkaze. Poslovna skrivnost je lahko sestavljena iz katerekoli formule, vzorca, naprave ali zbiranja informacij, ki se uporabljajo pri nekem poslu, mu daje priložnost, da pridobi prednost pred konkurenti, ki je ne poznajo ali ne uporabljajo.

Po Zabojniku (2002) so poslovne skrivnosti tudi tržne strategije, procesne izboljšave, organizacijsko znanje in kapital, nabavni podatki in cene izdelkov. Zanimiva je tudi opredelitev avtorjev Pacini, Placid in Wright-Isak (2008), ki navajajo, da je poslovna skrivnost lahko vsaka informacija, ki ima neko vrednost zaradi svoje zaupnosti, ne sme pa vsebovati podatkov, ki so znani širši javnosti. Avtorji ne navajajo, definirajo točne vrednosti poslovne skrivnosti, saj menijo, da je dovolj že aktualna ali potencialna vrednost, ki bi jo poslovna skrivnost lahko imela. Podatki, ki so poslovna skrivnost, morajo biti tajni, se pravi nedostopni širši javnosti. To

pomeni, da morajo biti podatki, razumljeni kot enota − poslovna skrivnost − neznani, četudi so vsi njeni posamezni sestavni deli znani (Sousa e Silva 2014, 928).

Zirnstein (2007) razlaga, da je za poslovno skrivnost bistveno, da gre za podatek, znan določenemu in omejenemu krogu ljudi. Dober primer je inovativen, izboljšan delovni postopek, ki ga zna izvajati samo določen in omejen krog ljudi znotraj posamičnega podjetja. Podjetja poslovno skrivnost običajno opredelijo v internem splošnem pravnem aktu, v katerem tudi določajo obveznosti zaposlenih v zvezi z varovanjem poslovne skrivnosti. Obveznost varovanja poslovne skrivnosti lahko vsebuje tudi kak drugi pravni akt, kot so npr. navodila za delo, strokovna gradiva, delovna priporočila, nenazadnje pa tudi pogodba o zaposlitvi ali izjava o varovanju poslovne skrivnosti. Poslovne skrivnosti se varujejo tudi s povsem praktičnimi ukrepi, kot so gesla in kode za vstop v računalniške programe, politika čiste mize, hranjenje dokumentov v posebnih omarah ali prostorih in podobno. Nenazadnje pa obveznost varstva poslovne skrivnosti določa tudi Zakon o delovnih razmerjih (v nadaljevanju ZDR-1, Uradni list RS, št. 21/13, 78/13 – popr., 47/15 – ZZSDT, 33/16 – PZ-F, 52/16, 15/17 – odl. US in 22/19 – ZPosS). Kot poslovno skrivnost mora zaposleni varovati vsako informacijo, ki izpolnjuje zahteve za poslovno skrivnost v skladu z zakonom, ki ureja poslovne skrivnosti (ZDR-1, 38. člen, 2. odstavek).

V EU varovanje poslovne skrivnosti ureja Direktiva o varstvu nerazkritega strokovnega znanja in izkušenj ter poslovnih informacij (poslovnih skrivnosti) pred njihovo protipravno pridobitvijo, uporabo in razkritjem (v nadaljevanju Direktiva 2016/943, Uradni list EU, št. 157/1), ki je začela veljati 5. julija 2016. Države članice EU so imele dve leti časa, da določbe direktive implementirajo v nacionalno zakonodajo, torej do 9. junija 2018 (Niebel, de Martinis in Clark 2018, 445). Pri tem so lahko države članice zagotovile obsežnejše varstvo pred protipravno pridobitvijo, uporabo ali razkritjem poslovnih skrivnosti, kot ga zagotavlja Direktiva 2016/943. Slovenija je Direktivo 2016/943 implementirala s sprejemom novega Zakona o poslovni skrivnosti (v nadaljevanju ZPosS, Uradni list RS, št. 22/19). Pred sprejemom Zakona o poslovni skrivnosti je bila poslovna skrivnost opredeljena v Zakonu o gospodarskih družbah (v nadaljevanju ZGD-1, Uradni list RS, št. 65/0933/11, 91/11, 32/12, 57/12, 44/13, 82/13, 55/15, 15/17, 22/19). Slednji je za poslovno skrivnost določal subjektivni in objektivni kriterij: poleg podatka, ki je kot poslovna skrivnost označen v aktih družbe (subjektivno merilo), se je za poslovno skrivnost štel tudi podatek, za katerega je očitno, da bi nastala občutna škoda, če bi zanj izvedela nepooblaščena oseba (Zirnstein 2007). ZPosS je spremenil to definicijo in v svojem 2. členu določil, da poslovna skrivnost zajema »nerazkrito strokovno znanje, izkušnje in poslovne informacije, ki ni splošno znano ali lahko dosegljivo, ki ima tržno vrednost in za katerega je imetnik poslovne skrivnosti sprejel razumne zaščitne ukrepe pred razkritjem tretjim.« V prehodnih in končnih določbah je ZPosS vplival tudi na določbe predpisov z drugih področij, ki urejajo obveznost varstva poslovne skrivnosti, kot je to ZGD-1 ter ZDR-1, s tem, ko je v 12. in 13. členu spremenil 39. člen ZGD-ja in 38. člen ZDR-ja ter

določil, da za poslovno skrivnost štejejo informacije, ki izpolnjujejo zahteve za poslovno skrivnost v skladu z ZPosS.

Prezelj in Tarman (2015, 693) razlagata, da je pri opredelitvi poslovne skrivnosti ključno, da gre za podatek, ki je skrivnost, torej je tajen, se pravi neznan ali nedostopen širši javnosti. Prav tako ugotavljata, da je element tajnosti značilen tudi za tajne podatke. V praksi se pojmi na tem področju pogosto zamenjujejo oziroma uporabljajo kot sopomenke. To je npr. razvidno iz listin, ki vsebujejo podatke, za katere izdajatelj ali uporabnik teh listin ne želi, da dosežejo širši krog ljudi. Te so označene kot »skrivnost«, »poslovna skrivnost«, »poslovna tajna«, »poslovna tajnost«, »uradna tajnost«, »uradna skrivnost« in podobno. Vsi omenjeni izrazi se uporabljajo tako v javnem kot tudi v zasebnem sektorju. Pa vendar so tajni podatki nekaj drugega kot poslovna skrivnost. V Sloveniji je npr. varstvo tajnih podatkov urejeno v Zakonu o tajnih podatkih (v nadaljevanju ZTP, Uradni list RS, št. 50/06 – uradno prečiščeno besedilo, 9/10, 60/11 in 8/20). Glede na določila zakona je tajni podatek dejstvo ali sredstvo z delovnega področja organa, ki se nanaša na javno varnost, obrambo, zunanje zadeve ali obveščevalno in varnostno dejavnost države.

Z ZTP so določene skupne osnove enotnega sistema določanja, varovanja in dostopa do tajnih podatkov z delovnega področja državnih organov Republike Slovenije (v nadaljevanju RS), ki se nanašajo na javno varnost, obrambo, zunanje zadeve ali obveščevalno in varnostno dejavnost države ter prenehanja tajnosti takšnih podatkov. ZTP zavezuje vse državne organe, organe lokalnih skupnosti, nosilce javnih pooblastil ter druge organe, gospodarske družbe in organizacije ter posameznike v teh organih, ki pri izvajanju zakonsko določenih nalog pridobijo ali razpolagajo s takimi podatki. Po tem zakonu morajo ravnati tudi dobavitelji, izvajalci gradenj ali izvajalci storitev, ki se jim taki podatki posredujejo zaradi izvršitve naročil organa. Vsak, ki mu je bil zaupan tajni podatek ali ki se je seznanil z vsebino tajnega podatka, je odgovoren za njegovo varovanje in ohranitev njegove tajnosti.

Prezelj in Tarman (2015, 703) ugotavljata, v katerih primerih, na kakšen način in pod kakšnimi pogoji je dopustno določene podatke in informacije s področja nacionalne varnosti v sodobni liberalno-demokratični državi dati v javnost. Ugotavljata, da je v RS iz državnih varnostnih razlogov mogoče povsem legalno prikriti javnosti določene informacije oziroma podatke, ki se nanašajo na javno varnost, obrambo, zunanje zadeve ali obveščevalno in varnostno dejavnost države. V nadaljevanju še dodajata, da je v Sloveniji pri določitvi tajnosti ključni kriterij vezan na potencialno škodo v primeru razkritja. Menita še, da naj se kot tajni podatek opredeli podatek, katerega razkritje nepooblaščeni osebi povzroči »škodljive posledice za varnost države ali za njene politične ali gospodarske koristi« (Prezelj in Tarman 2015, 693). Pojasnjujeta tudi, da mora biti večina tajnih podatkov časovno omejena, zato da se lahko javnost sčasoma seznani z določenimi podatki, ki so bili v preteklosti prikriti, poleg tega pa se lahko hkrati navedejo tudi razlogi za tajnost. Avtorja opozarjata, da celostna zaščita tajnih podatkov verjetno ni mogoča nikjer, hkrati pa dodajata, da lahko s primernim sistemskim pristopom zagotovimo visoko

stopnjo zaščite in varovanja. Po drugi strani se Bakken (2013, 1) ne strinja z varovanjem tajnih podatkov in meni, da bi demokracija verjetno najbolje delovala, če bi se vsi državljani zavedali vseh vladnih operacij in informacij.

S tajnimi podatki in poslovnimi skrivnostmi se srečujejo tudi lokalne skupnosti, ki skušajo določbe predpisov na tem področju podrobneje operacionalizirati v svojih internih aktih. Na področju tajnih podatkov je namreč varovanje teh podrobneje urejeno le na nacionalni ravni, na ravni lokalnih skupnosti pa ne, čeprav jih ZTP neposredno zavezuje. Podobno situacijo srečamo na področju poslovnih skrivnosti – lokalne skupnosti skušajo tudi varovanje poslovne skrivnosti podrobneje urejati z internimi pravnimi akti. Pri tem pa morajo poleg varstva svojih interesov, interesov države ali interesov svojih poslovnih partnerjev upoštevati dejstvo, da ima javnost zaradi nadzora nad porabo javnih sredstev pravico dostopati do določenih podatkov in informacij. Javnost dela državni organov, nosilcev javnih pooblastil ter organov lokalne samouprave je namreč splošno sprejeto načelo v sleherni demokratični družbi. Zdi se, da gre na tem področju za svojevrsten paradoks: lokalna skupnost dolgoročno ne more delovati brez zaupanja javnosti, zaradi česar mora javnosti omogočiti čim širši nadzor nad lastnim delovanjem, tudi z vpogledom v določene podatke, po drugi strani pa mora v določenih primerih onemogočiti dostop do teh podatkov z naslova zagotavljanja varnosti prebivalstva, ključnih družbenih institucij in nenazadnje tudi zakonitih interesov svojih (poslovnih) partnerjev.

Izhajajoč iz zgoraj navedenih izhodišč se postavlja več zanimivih vprašanj. Prvi sklop vprašanj se nanaša na samo razumevanje pojma poslovne skrivnosti v povezavi z delovanjem lokalne skupnosti ter na razlikovanje med poslovno skrivnostjo in tajnim podatkom. Ob natančnem branju opredelitve poslovne skrivnosti v ZPosS se postavlja vprašanje, ali v lokalnih skupnostih sploh lahko govorimo o poslovni skrivnosti, ki se definira kot »nerazkrito strokovno znanje, izkušnje in poslovne informacije«, ki ima »tržno vrednost« (ZPosS, 2. člen). Zdi se, da je institut »poslovne skrivnosti« zgolj v domeni gospodarskih subjektov in ni predviden za osebe javnega sektorja. Z drugimi besedami − ali bi se ZPosS lahko nanašal tudi na javni sektor, natančneje na samoupravne lokalne skupnosti? Ali se pri slednjih lahko zgodi situacija, da »posedujejo« podatek, ki ima tržno vrednost? V povezavi z opredelitvijo tajnega podatka v ZTP kaže, da je varstvo poslovne skrivnosti bolj lastno gospodarstvu, varstvo tajnih podatkov pa javnemu sektorju. Vendar pa v praksi lokalnih skupnosti obstaja vrsta dokumentov, ki se označujejo bodisi z eno bodisi z drugo oznako, včasih celo z obema. Vsaka lokalna skupnost si pojem poslovne skrivnosti in tajnega podatka ter svoje pristojnosti v zvezi z njimi razlaga po svoje. Naj temu dodamo še označevanje dokumentov z oznakami »interna informacija«, »uradna skrivnost«, »uradna tajnost« in podobno. Skratka v lokalnih skupnostih v zvezi s tem vlada velika zmešnjava.

Drugi sklop vprašanj se nanaša na vprašanje tehtanja različnih interesov: po eni strani mora lokalna skupnost upoštevati interes javnosti in omogočati njen nadzor nad svojim delovanjem, po drugi pa mora upoštevati interese na področju državne varnosti ali interese npr. svojih

pogodbenih partnerjev (varovanje določenega podatka kot poslovno skrivnost). Ko govorimo o interesu javnosti, da nadzira delovanje lokalne skupnosti, govorimo pravzaprav o pravici dostopa do informacij javnega značaja. Kot informacije javnega značaja štejemo vse informacije, ki nastajajo pri poslovanju organa (dokumenti, zadeve, dosjeji, registri, evidence in druga gradiva), ki jim je skupno to, da so jih organi sestavili sami v sodelovanju z drugimi organi ali so jih dobili od drugih oseb (Informacijski pooblaščenec b. l.). Informacije javnega značaja ureja Zakon o dostopu do informacij javnega značaja (v nadaljevanju ZDIJZ, Uradni list RS, št. 51/06, 117/06, 23/24, 50/14, 19/15, 102/15, 7/18). Da postane določena informacija prav informacija javnega značaja, mora izpolnjevati naslednje kriterije (Informacijski pooblaščenec b. l.):

- informacija mora izhajati z delovnega področja organa,
- organ mora z omenjeno informacijo razpolagati,
- informacija mora biti v materializirani obliki.

Informacije javnega značaja se nanašajo na različne vsebine delovanja organa. Lahko so povezane s politiko poslovanja, aktivnostmi in odločitvami organa. Glede na to se postavlja dilema, ali in kdaj informacije javnega značaja prevladujejo pred poslovnimi skrivnostmi, saj ZDIJZ (4.a člen) navaja, da so informacije javnega značaja informacije o sklenjenih pravnih poslih, o izdatkih, avtorskih pogodbah, donatorjih, prejemkih, bonitetah članov poslovodnega organa, vendar določa tudi izjeme, ko se informacije javnega značaja ne smejo razkriti. Če to skušamo nekoliko bolj plastično ponazoriti, lahko zapišemo, da na eni strani obstaja interes lokalne skupnosti ali nekega zunanjega pogodbenega izvajalca o varovanju poslovnih skrivnosti, na drugi strani pa je interes javnosti, da se podatki razkrijejo kot npr. v primeru, ko gre za razkritje finančnih in poslovnih rezultatov. Kateri interes prevlada v konkretnem primeru, je eno izmed vprašanj, na katero bomo poskusili odgovoriti v magistrski nalogi.

Tretji sklop vprašanj pa se dotika povsem praktičnih aspektov določanja in varovanja poslovnih skrivnosti in tajnih podatkov v lokalni skupnosti – kako v praksi urediti sistem določanja, varovanja in dostopa do tajnih podatkov ter poslovnih skrivnosti z delovnega področja lokalne skupnosti.

### 1.2 Namen, cilji in hipoteze magistrske naloge

Namen naloge je raziskati problematiko urejanja in varstva poslovnih skrivnosti in tajnih podatkov v lokalni skupnosti in oblikovati priporočila za določanje, dostop in varovanje poslovnih skrivnosti ter tajnih podatkov z delovnega področja lokalne skupnosti.

Cilji magistrske naloge so:

- opredeliti pojem poslovne skrivnosti in tajnega podatka ter ugotoviti razliko med poslovno skrivnostjo in tajnim podatkom,
- proučiti sodno prakso z obravnavanega področja,

- ugotoviti, v katerih primerih in koliko so lokalne skupnosti zavezane k varstvu poslovnih skrivnosti,
- ugotoviti, kje je meja med varstvom tajnih podatkov oz. poslovnih skrivnosti in interesom javnosti po Zakonu do dostopu informacij javnega značaja,
- proučiti sistem odgovornosti v primeru izdaje poslovne skrivnosti (odškodninsko odgovornost, kazensko odgovornost, disciplinsko odgovornost),
- oblikovati priporočila za lokalno skupnost z internim aktom.

### 1.3 Predvidene metode raziskovanja za doseganje namena in ciljev naloge

V magistrski nalogi smo uporabili naslednje metode:
- metodo deskripcije, s katero smo definirali relevantne pojme, kot sta poslovna skrivnost in tajni podatki,
- metodo kompilacije, s katero smo povzeli navedbe in citate drugih avtorjev v zvezi z poslovno skrivnostjo in tajnimi podatki tako v zasebnem kot tudi v javnem sektorju,
- metodo komparacije, s katero smo med seboj primerjali ureditve na področju poslovne skrivnosti in tajnih podatkov v različnih državah,
- metodo analize, s katero smo analizirali slovensko zakonodajo s področja poslovnih skrivnosti in tajnih podatkov,
- metodo pravne argumentacije, s katero smo analizirali obstoječe pravne vire, sodne odločbe in oblikovali priporočila za urejanje varstva s poslovno skrivnostjo in tajnimi podatki z internim aktom občine.

### 1.4 Predvidene predpostavke in omejitve

Omejitev naloge je v tem, da je ZPosS nov, kar pomeni, da praksa v zvezi z uporabo in razlago tega zakona še ni oblikovana.

# 2 POSLOVNE SKRIVNOSTI

Poslovne skrivnosti so skupaj z odnosi s strankami in naložbami v usposabljanje in izobraževanje zaposlenih ena izmed dragocenosti vsakega poslovnega subjekta (Knowlton 2014).

Da so poslovne skrivnosti pomembne za družbo, so se ljudje zavedali že tisočletja nazaj. Že v stari Grčiji so načine ustvarjanja zlatih zlitin in njihovo obdelavo skrivali, arhitekti po celem svetu so varovali načine gradnje stolpov ali npr. na Kitajskem je bila skrivnost tehnologija izdelave izdelkov iz porcelana in izdelave svile. Na Saškem je uredba iz leta 1698 predvidevala smrtno kazen zaradi kršitve prepovedi opravljanja vajeništva tujcem ali osebam iz tujine. Takšna kazen je bila določena tudi v generalnem pruskem Landrechtu iz leta 1794 za tiste, ki so prepričali nadrejenega ali uslužbenca v tovarni, da je ta zapustil tovarno in pomagal drugemu podjetju do določenega proizvoda ali postopka pridobivanja določenega proizvoda. Takšno dejanje je bilo označeno kot razkritje poklicne skrivnosti in s tem izpostavljanje domovine nepopravljivi škodi. Poslovne skrivnosti so bile tudi fizično zaščitene. S tem je bilo onemogočeno tujcem oz. nepooblaščenim osebam, da dostopajo do zaupnih dejavnosti in postopkov, vključno s tistimi, ki so v nasprotju s poskusom preprečitve dobili tak dostop (Žakowska-Henzler 2017). Med osebami, ki so imele dostop do poslovnih skrivnosti, so vedno bili tudi uslužbenci podjetij.

Leta 2006 so trije zaposleni v družbi Coca-Cola poskušali prodati znanje o izdelku Coca-Cole konkurenčnemu podjetju PepsiCo. Namesto da bi kupili poslovne skrivnosti, je PepsiCo obvestil Coca-Colo o dejanjih zaposlenih. Poslovne skrivnosti Coca-Cole so zaradi odziva PepsiCo ostale prikrite in podjetje ni bilo oškodovano. Kljub temu pa lahko v okoliščinah, ko se poslovne skrivnosti razkrijejo nenamerno ali namerno, to dejstvo zelo škodi organizacijam, ki se zanašajo na te skrivnosti kot ključni vir konkurenčne prednosti. Da bi podjetja ohranila vrednost svojih poslovnih skrivnosti, morajo preprečiti, da bi padle v roke konkurentom. Če tega ne dosežejo, lahko nastane velika škoda za podjetje. Nedavno poročilo Pricewaterhouse Coopers in Centra za odgovorno podjetništvo in trgovino ZDA je ocenilo, da izguba poslovnih skrivnosti vsako leto stane ameriško gospodarstvo med 1 % in 3 % nacionalnega bruto domačega proizvoda (Robertson, Hannah in Lautsch 2015).

Glede na pomen varovanja poslovne skrivnosti je ključno, da organizacije in menedžerji razumejo, kako varovati svoje poslovne skrivnosti. Dejstvo je, da morajo poslovne skrivnosti na eni strani biti na razpolago zaposlenim, kadar jih potrebujejo pri svojemu delu, na drugi strani pa obstaja potencialna nevarnost, da jih razkrijejo tretjim osebam. Robertson, Hannah in Lautsch (2015) navajajo, da prav zaposleni najbolj pogosto zlorabljajo zaupanje podjetja, ko razkrijejo poslovne skrivnostih nepooblaščenim osebam bodisi proti plačilu ali iz nedolžnih razlogov, ko ne vedo, da je določena informacija poslovna skrivnost. Kot je pokazala anketa za raziskavo Monster.com iz leta 2012, ki sta jo opravila Morvillo in Farrell (2012), bi 17 % zaposlenih delilo skrivnosti družbe v zameno za nadomestilo, 8 % pa jih je to že storilo. Avtorja

ugotavljata, da naj bi vsaj 25 % zaposlenih bodisi že prodalo poslovne skrivnosti podjetja ali pa bi to storili proti plačilu. Takšni statistični podatki pojasnjujejo dejstvo, da so se v obdobju od leta 1997 do 2004 sodni spori glede razkritja poslovnih skrivnosti na zveznih sodiščih v ZDA podvojili in tak trend naj bi se nadaljeval tudi v bodoče. Podobne podatke je ugotovil tudi Almeling (2012), in sicer da so se pravdni spori glede razkritja poslovnih skrivnosti na zveznih sodiščih v ZDA v 15 letih povečali za 36 %, medtem ko so se na splošno pravni spori povečali le za 9 %.

Zaradi razkritja poslovnih skrivnosti imajo podjetja ogromne izgube, kot je pokazala raziskava leta 2002, ki je zajela več kot 130 podjetij. Izmed teh podjetij jih je 40 % poročalo o dejanskih in domnevnih izgubah zaradi razkritja poslovnih skrivnosti s strani zaposlenih (Hannah 2006). Še bolj odmeven je podatek, ki so ga objavili Almeling idr. (2010), ko so pregledovali 400 primerov razkritja poslovne skrivnosti, obravnavanih na zveznih sodiščih v ZDA. Ugotovili so, da je bil v več kot 85 % domnevni storilec kraje poslovne skrivnosti poslovni partner ali uslužbenec. Glede na navedeno se morajo menedžerji soočiti s težavo, kako deliti poslovne skrivnosti z zaposlenimi, hkrati pa jim preprečiti, da bi te skrivnosti razkrili zunanjim osebam. Robertson, Hannah in Lautsch (2015) navajajo, da to lahko dosežejo z ustvarjanjem pozitivnega ozračja tajnosti, s čimer pomagajo zagotoviti, da njihova podjetja pridobivajo vrednost iz skrivnosti, ne da bi jih ogrozile. Prvi korak pri ustvarjanju pozitivne kulture mora storiti menedžer in najprej oceniti, kateri podatki so poslovna skrivnost in to predstaviti vsem zaposlenim. Morvillo in Farrell (2012) menita, da ni smiselno podatke označevati z »zaupno«. Kot je ugotovilo sodišče v Kaliforniji v primeru spora, ko je delodajalec skoraj vse podatke označil za zaupne, je takšno označevanje povzročilo veliko zmede, saj zaposleni niso mogli prihajati do vseh potrebnih informacij za svoje delo. Ko podjetje resnično prepozna svoje zaupne podatke, kamor uvrščamo tudi poslovne skrivnosti, mora sprejeti dodatne korake, da se bodo zaposleni zavedali pomembnosti informacij in jih res hranili kot zaupne.

Na splošno velja, da so vsi zaupni poslovni podatki tisti, ki podjetju zagotavljajo konkurenčno prednost, zato se lahko štejejo tudi kot poslovna skrivnost. Vendar pa vsi zaupni podatki znotraj podjetja ne veljajo za poslovno skrivnost. Kot navajajo v strokovni skupini za intelektualno lastnino (Intellectual Property Expert Group b. l.), obstajajo znotraj podjetja različne ravni zaupnih informacij; poslovne skrivnosti pa so uvrščene na najvišjo raven zaupnih informacij. Poslovne skrivnosti so obenem lahko ena izmed najpomembnejših dobrin v portfelju intelektualne lastnine organizacije, kamor uvrščamo formule, prakso, postopke, oblikovanja, instrumente, vzorce, komercialne metode ali zbiranje informacij, ki jih druga podjetja na splošno ne poznajo, si pa podjetje z njimi pridobi gospodarsko prednost pred konkurenco ali kupci (Intellectual Property Expert Group b. l.).

Poslovna skrivnost je dragocen podatek za podjetja, zato poskušajo države to zakonsko urediti. Kot ugotavljajo v Intellectual Property Expert Group (b. l.), so evropska podjetja vse bolj izpostavljena razkritju poslovnih skrivnosti. Tudi zato si Evropska komisija (v nadaljevanju

EK) prizadeva, da bi bilo področje poslovnih skrivnosti v nacionalnih zakonodajah članic EU enotno ali vsaj podobno urejeno.

## 2.1 Opredelitev poslovne skrivnosti

Za označevanje poslovnih skrivnosti se v teoriji uporablja kopica različnih pojmov, kot so »nerazkrite informacije« (ang. undisclosed information), »trgovinska tajna« (ang. trade secret), zaupni podatki (ang. confidential data), poslovna skrivnost (ang. business secret). Omenjeni izrazi se v literaturi pogosto pojavljajo kot sinonimi, kljub temu da ne pomenijo nujno istega, kar je posledica konceptualnih razlik, ki glede pojma poslovne skrivnosti obstajajo med različnimi pravnimi sistemi (Zirnstein 2016, 23). Tudi v strokovni literaturi je poslovna skrivnost različno definirana. Pri večini definicij o poslovni skrivnosti je skupno, da gre za informacije, ki izhajajo iz neodvisne ekonomske, dejanske ali potencialne vrednosti ter da bi njihovo razkritje in uporaba povzročila veliko ali celo nepopravljivo škodo varovancu poslovne skrivnosti (Gleaser 2018).

Direktiva (EU) 2016/943 definira poslovno skrivnost kot informacije, ki izpolnjujejo naslednje zahteve (Direktiva 2016/943, 2. člen):

- so skrivnosti v smislu, da niso splošno znane in dostopne v krogih, kjer običajno uporabljajo te vrste informacijo,
- imajo tržno vrednost, ker so skrivnosti in
- je v danih razmerah oseba, ki ima zakonit nadzor nad informacijo, razumno ukrepala, da jo ohrani kot skrivnost.

Poslovna skrivnost so vse oblike in vrste finančnih, poslovnih, znanstvenih, tehničnih ali inženirskih informacij, vključno z vzorci, načrti, kompilacijami, programskimi napravami, dizajni, prototipi, metodami, postopki, programi ali kodami, oprijemljivimi ali neopredmetenimi in ne glede na to, ali so shranjene v fizični, elektronski obliki, grafično, fotografsko ali pisno, če je njihov lastnik sprejel razumne ukrepe za varovanje tajnosti teh podatkov in če informacije izhajajo iz neodvisne ekonomske vrednosti, dejanske ali potencialne skrivnosti (Evans 2019).

Intellectual Property Expert Group (b. l.) navaja, da je poslovna skrivnost vsak podatek, ki ni splošno znan ustreznim poslovnim krogom ali javnosti oz. so to informacije, ki niso dostopne vsakomur. Poslovna skrivnost je informacija, ki nudi nekakšno gospodarsko korist njenemu lastniku, vendar mora korist izhajati iz dejstva, da ta podatek ni na splošno znan in ima komercialno vrednost, ki je tako potencialna kot dejanska.

Med poslovne skrivnosti sodijo tudi informacije, ki vključujejo recepte (Coca-Colo Classic ali omake za piščanca KFC), formule (WD-40), proizvodne tehnike (General Electric za proizvodnjo sintetičnih diamantov), seznami strank, zbirke strank in kemičnih postopkov.

Omenjene informacije pa se lahko varujejo tudi tako, da se zavarujejo s katero od pravic intelektualne lastnine, predvsem s patentom. Za razliko od poslovne skrivnosti je ideja pravic intelektualne lastnine v tem, da imetnik takšne informacije prav to javnosti razkrije, v zameno pa dobi monopolno (izključno) pravico do proizvodnje ali prodaje izdelkov oz. storitev, ki so s to pravico zaščiteni. Pravo intelektualne lastnine s podeljevanjem izključnih (monopolnih) pravic stremi k nagrajevanju in spodbujanju »avtorjev« intelektualnih stvaritev, kot so nove tehnične rešitve tehničnih težav (ki se zaščitijo s patentom), nove oblike izdelkov (ki se zaščitijo z modelom ali avtorsko pravico), nove sorte rastlin (ki se zaščitijo z žlahtniteljsko pravico) in podobno (Zirnstein 2016). Včasih je varstvo teh stvaritev v obliki poslovne skrivnosti celo bolj primerno kot varstvo v okviru prava industrijske lastnine, predvsem to velja za patente. Pri izumih je pogoj za patentno varstvo razkritje izuma v patentni prijavi, česar podjetja zmeraj ne želijo, zato tak izum raje varujejo v obliki poslovne skrivnosti. Tu gre predvsem za tiste izume, ki se jih ne da kar tako »kopirati«. Poleg tega so s pridobitvijo patenta povezani kar precejšnji stroški, sploh če želimo pridobiti patent v več državah; v takih primerih se podjetja mnogokrat raje odločijo za varstvo v obliki poslovne skrivnosti. Nenazadnje je lahko varstvo v obliki poslovne skrivnosti dopolnilo varstvu s pravicami industrijske lastnine, na primer za varstvo izuma do njegove prijave za pridobitev patenta (Zirnstein 2016, 22). Z drugimi besedami je poslovna skrivnost lahko alternativna oblika varstva za primere, ko se izum lahko varuje s pravico intelektualne lastnine, ampak se upravičenec za takšno varstvo ne odloči. Poleg tega so patenti (kakor tudi druge pravice intelektualne lastnine) časovno omejeni in trajajo samo določeno obdobje od njihove pridobitve. Poslovne skrivnosti pa se lahko varujejo v nedogled, saj ohranijo svoj pravno zaščiten status, dokler skrivnosti ne postanejo javno znane. Zatorej podjetja lahko pri poslovni skrivnosti v nedogled izkoriščajo konkurenčno prednost, ki jo te skrivnosti ponujajo (Robertson, Hannah in Lautsch 2015).

Opredelitev poslovne skrivnosti vsebuje tudi Sporazum o trgovinskih vidikih pravic intelektualne lastnine (v nadaljevanju Sporazum TRIPS, Uradni list RS-MP, št. 10/1995), ki v 39. členu določa, da je poslovna skrivnost (i) podatek, ki ni splošno znan javnosti, (ii) ki njenemu imetniku prinaša določeno ekonomsko korist in (iii) ki je predmet naporov, da ostane nerazkrit.

V zvezi z zgoraj navedeno trditvijo Robertsona, Hannaha in Lautscha (2015), da se lahko poslovne skrivnosti varujejo v nedogled, velja izpostaviti še časovno komponento pojma poslovne skrivnosti oziroma element spremenljivosti poslovne skrivnosti v času. Poslovna skrivnost je namreč nestalna kategorija, saj lahko določeni dokumenti, informacije, podatki ipd. predstavljajo poslovno skrivnost samo v določenem časovnem obdobju. Namreč, informacije ali dokumenti, označeni kot poslovna skrivnost, s časom postanejo popolnoma neuporabni oziroma ne predstavljajo več konkurenčne prednosti (Informacijski pooblaščenec 2015). Ta (časovni) vidik poslovne skrivnosti je v teoriji in zakonodaji po našem mnenju premalo poudarjen.

## 2.2 Pravna ureditev poslovne skrivnosti v EU in Sloveniji

Ključni dokument, ki ureja poslovno skrivnost v EU, je Direktiva 2016/943 Evropskega parlamenta in Sveta, z dne 8. junija 2016, o varstvu nerazkritega strokovnega znanja in izkušenj ter poslovnih informacij (poslovnih skrivnosti) pred njihovo protipravno pridobitvijo, uporabo in razkritjem (Direktiva EU 2016/943), ki jo je tudi Slovenija vnesla v svoj pravni red. Glavni namen Direktive EU 2016/943 je bil preprečiti nezakonito pridobivanje, uporabo ali razkrivanje poslovnih skrivnosti, hkrati pa ne omejiti temeljne pravice in svoboščine ljudi.

### *2.2.1 Direktiva EU o urejanju poslovne skrivnosti*

Zaradi pomembnosti poslovnih skrivnosti in različnih ureditev nacionalnih sistemov pri varovanju poslovnih skrivnosti držav članic EU je bila leta 2016 sprejeta Direktiva EU 2016/943. Evropski parlament in Svet EU sta pri sprejemu Direktive 2016/943 izhajala iz dojemanja poslovne skrivnosti kot dragocenega strokovnega znanja ali izkušenj ter poslovnih informacij, ki jih pridobijo podjetja in nekomercialne raziskovalne ustanove na osnovi lastnega ustvarjanja in uporabe intelektualnega kapitala. Mednje uvrščamo tudi komercialne podatke, kot so informacije o odjemalcih, dobaviteljih, strategije poslovanja, poslovni načrti in tržne skrivnosti.

Kot je zapisano v uvodnem besedilu Direktive 2016/943, se inovativna podjetja pogosto srečujejo s protipravno prisvojitvijo poslovnih skrivnosti, kot npr. s kopiranjem podatkov ali vohunjenjem v EU ali zunaj nje. Evropski parlament in Svet EU sta s sprejetjem Direktive 2016/943 želela harmonizirati zakonodajo držav članic tako, da naj bi ta na notranjem trgu zagotovila zadostna in skladna civilnopravna sredstva v primerih protipravne pridobitve, uporabe ali razkritja poslovne skrivnosti. Ključne točke Direktive (EU) 2016/943 določajo ukrepe, postopke in pravna sredstva v primeru protipravnega odvzema, uporabe ali razkritja poslovne skrivnosti. Pri tem je pomembno, da so ukrepi, postopki in pravna sredstva pošteni, pravični in odvračalni ter ne smejo biti zapleteni ali dragi.

Direktiva 2016/943 je določila minimalni standard glede poslovne skrivnosti in njenega varovanja ter državam članicam prepustila, naj sprejmejo tudi strožja pravila. Tako imenovani »pristop minimalne uskladitve« (ang. minimum harmonisation approach) pomeni, da mora država članica v nacionalno pravo prenesti v direktivi predvidene zaščitne ukrepe, lahko pa jih določi tudi več – v tem primeru večjo ali strožjo zaščito poslovne skrivnosti ali obsežnejše varstvo pred protipravno pridobitvijo, uporabo ali razkritjem poslovne skrivnosti, kot je predvidena v Direktivi 2016/943. Direktiva 2016/943 (2. člen, 1. odstavek) je uvedla enotno opredelitev poslovne skrivnosti, ki zajema strokovno znanje in izkušnje, poslovne in tehnološke informacije, obstajati pa morata tudi legitimni interes, da informacije ostanejo zaupne, in legitimno pričakovanje, da se ohrani zaupnost. Poleg navedenega morajo to strokovno znanje in izkušnje ali informacije imeti tudi dejansko ali potencialno tržno vrednost. To imajo takrat,

ko je verjetno, da njihova nedovoljena pridobitev, uporaba ali razkritje škodujejo interesom osebe, ki ima nad njimi zakonit nadzor, s tem da škoduje znanstvenemu ali tehničnemu potencialu te osebe, njenim poslovnim ali finančnim interesom, strateškim pozicijam ali konkurenčni sposobnosti.

Direktiva 2016/943 loči med zakonito in protipravno pridobitvijo, uporabo in razkritjem poslovne skrivnosti. Pridobitev poslovne skrivnosti je zakonita, če se pridobi s kakršnimkoli ravnanjem, za katerim se v danih okoliščinah šteje, da je v skladu s pošteno poslovno prakso, zlasti z neodvisnim odkritjem ali s stvaritvijo, z opazovanjem, s proučevanjem, z razstavljanjem ali s preizkušanjem izdelka ali predmeta, ki je bil dan na voljo javnosti ali ga ima pridobitelj informacije zakonito v posesti (tudi obratni inženiring), z uveljavljanjem pravice zastopnikov delavcev do obveščenosti in posvetovanja v skladu s pravom EU, nacionalnim pravom in praksami. Uporaba ali razkritje poslovne skrivnosti se šteje za protipravno, če (i) poslovno skrivnost brez privolitve njenega imetnika uporabi ali razkrije oseba, ki je to poslovno skrivnost sama pridobila neupravičeno, ali pa ta oseba krši dogovorjeno zaupnost ali drugo dolžnost molčečnosti v zvezi s poslovno skrivnostjo ali (ii) če kasnejši pridobitelj v času uporabe ali razkritja ni v dobri veri ter (iii) tudi v primeru proizvodnje, ponujanja ali dajanja na trg blaga, ki je predmet kršitve, ali njegovo uvažanje, izvažanje ali skladiščenje, kadar je oseba, ki opravlja tovrstne dejavnosti, vedela ali bi v danih okoliščinah morala vedeti, da je bila poslovna skrivnost uporabljena protipravno (Direktiva 2016/943, 4. člen). Direktiva predvideva možnost uveljavljanja nadomestil (le) po civilnem (ne pa tudi po kazenskem) pravu (Direktiva 2016/943, 6. člen). V primeru neupravičene pridobitve, uporabe ali razkritja poslovne skrivnosti je Direktiva dala z načelno določbo v 6. členu državam članicam na razpolago, da same določijo potrebne ukrepe, postopke in pravna sredstva, ki pa morajo biti pošteni in pravični, učinkoviti in odvračilni ter ne smejo biti po nepotrebnem zapleteni ali dragi niti postavljati nerazumnih rokov ali povzročati neupravičenih zamud (Direktiva 2016/943, 6., 10. in 12. člen). Med splošne določbe v zvezi z ukrepi, s postopki in pravnimi sredstvi je Direktiva 2016/943 uvrstila tudi določbe za ohranitev zaupnosti poslovne skrivnosti v sodnih postopkih. Direktiva 2016/943 je v tretjem odstavku 13. člena predvidela tudi možnost plačila denarnega nadomestila (odškodnine), ki jo odredi pristojni sodni organ na zahtevo oškodovanca, in ustreza dejanski škodi, ki jo je ta utrpel zaradi protipravne pridobitve poslovne skrivnosti, njene uporabe ali razkritja. Pri določanju višine odškodnine pristojni sodni organ upošteva vse okoliščine primera, lahko pa je v ustreznih primerih odškodnina določena kot enkraten (pavšalni) znesek. Določbe Direktive 2016/943 so morale biti v nacionalne pravne rede držav članic prenesene najpozneje do 9. junija 2018.

### *2.2.2 Urejenost varstva poslovne skrivnosti v Sloveniji*

Temeljni zakon, ki ureja varovanje poslovne skrivnosti v Sloveniji, je ZPosS, sprejet leta 2019. Navedeni zakon pomeni implementacijo Direktive (EU) 2016/943. ZPosS je materialno-

procesni predpis, ki določa pojem (definicijo) poslovne skrivnosti ter hkrati postopke in ukrepe v primeru kršitev.

ZPosS določa popolnoma nov pojem poslovne skrivnosti. V drugem členu namreč definira poslovno skrivnost kot nerazkrito strokovno znanje, izkušnje in poslovne informacije, ki morajo izpolnjevati te zahteve: (i) da kot celota ali v natančni konfiguraciji in sestavi njenih komponent ni splošno znana ali lahko dosegljiva osebam v krogih, ki se običajno ukvarjajo s to vrsto informacij, (ii) ima tržno vrednost, ker je skrivnost, in da (iii) je oseba, ki ima zakoniti nadzor nad to informacijo, v danih okoliščinah razumno ukrepala, da jo ohrani kot skrivnost.

Poslovna skrivnost je lahko pridobljena zakonito in protipravno. Zakonito se poslovno skrivnost pridobi (ZPosS, 4. člen):

- z odkritjem ali ustvarjenjem informacije,
- s proučevanjem in z opazovanjem ter razstavljanjem in sestavljanjem izdelka, ki je javen ali v posesti drugega, vendar ni opredeljen kot poslovna skrivnost in
- z drugimi dejanji, ki so v skladu zakonom in s pošteno prakso.

Za protipravno pridobitev poslovne skrivnosti se šteje protipravna pridobitev informacije, ki vsebuje poslovno skrivnost in se pridobi od osebe, ki ne bi smela razkriti poslovne skrivnosti tretji osebi (ZPosS, 5. člen).

Poleg splošnih določb o uporabi pravil pravdnega postopka ter postopka izvršbe in zavarovanja ZPosS v 9. členu natančno določa tožbene zahtevke, ki jih lahko imetnik poslovne skrivnosti vloži zoper kršilca. Imetnik poslovne skrivnosti ima na voljo prepovedne ali opustitvene ukrepe, odstranitvene ali korektivne ukrepe, alternativne ukrepe in zahtevo za objavo sodbe. V primeru, da pride do razkritja poslovnih skrivnosti, lahko podjetje od osebe (pravne ali fizične), ki je razkrila, pridobila ali uporabila poslovno skrivnost, zahteva povrnitev škode po splošnih pravilih obligacijskega prava. Pravico do povrnitve odškodnine lahko imetnik poslovne skrivnosti zahteva, tudi če ni utrpel premoženjske škode, ampak je kršitev nastala namerno ali iz velike malomarnosti (ZPosS, 10. člen).

Za takojšnje prenehanje protipravnega pridobivanja, uporabe ali razkrivanja poslovne skrivnosti (tudi pri storitvah) brez čakanja na meritorno odločitev so v ZPosS določene začasne odredbe. Zakon določa pogoje za izdajo začasne odredbe, začasne ukrepe, ki jih lahko odredi sodišče, in okoliščine, ki jih mora pri tem upoštevati.

Zaradi možnosti, da bi razkritje poslovne skrivnosti med sodnim postopkom odvračalo zakonite imetnike poslovnih skrivnosti od uvedbe takih postopkov in s tem ogrožalo učinkovitost predvidenih ukrepov, 8. člen ZPosS vsebuje določbe za ohranitev zaupnosti poslovne skrivnosti v sodnih postopkih.

Zaradi zahteve Direktive 2016/943 po enotni opredelitvi poslovne skrivnosti po vsem notranjem trgu ZPosS posega v določbe ZGD-1 in ZDR-1 tako, da razveljavlja definicijo poslovne skrivnosti v navedenih dveh zakonih oziroma jo spreminja tako, da se ta dva zakona v spremenjenih določbah 38. člena (ZGD-1) oziroma 39. člena (ZDR-1) sklicujeta na uporabo definicije poslovne skrivnosti iz ZPosS. ZPosS je 39. člen ZGD-1 spremenil, in sicer tako, da je navedel, da se za poslovne skrivnosti štejejo tiste informacije, »ki izpolnjujejo zahteve za poslovno skrivnost v skladu z zakonom, ki ureja poslovne skrivnosti«. Varovanje poslovne skrivnosti v 38. člen ZDR-1 je po novem prav tako urejeno s sklicem na opredelitev v ZPosS.

Z delovno-pravnega vidika je varovanje poslovne skrivnosti ena od temeljnih obveznosti delavca in izraz lojalnosti do delodajalca (ZDR-1, 39. člen). Za javne uslužbence pa so relevantne tudi določbe Zakona o tajnih podatkih, ki določajo skupne osnove za določanje, varovanje in dostopnost tajnih podatkov na nekaterih področjih državnih organov RS.

V zvezi s kršitvijo varovanja poslovne skrivnosti ZDR-1 prepoveduje zlorabo in tudi njeno izdajo. Zloraba pomeni izkoriščanje poslovne skrivnosti za svojo osebno rabo in uporabo teh podatkov (na primer ob morebitnem ustanavljanju svojega podjetja). Drugi način kršitve varovanja poslovne skrivnosti po ZDR-1 je izdaja ali seznanjanje tretjih nepooblaščenih oseb s poslovno skrivnostjo, pri čemer ni pomembno, ali je delavcu s kršitvijo nastala premoženjska ali nepremoženjska korist ali ne. V skladu z drugim odstavkom 38. člena ZDR-1 mora delavec varovati tudi tiste podatke, ki izpolnjujejo zahteve za poslovno skrivnost po 2. členu ZPosS, tudi če jih delodajalec ni posebej označil kot poslovno skrivnost. Delavec je odgovoren, če je vedel ali bi moral vedeti za tak značaj podatkov. Pri ugotavljanju delavčeve odgovornosti ZDR-1 določa krivdno načelo, v skladu s katerim je delavec odgovoren za kršitev obveznosti varovanja poslovne skrivnosti, če je vedel ali bi moral vedeti za zaupno naravo podatkov, ki jih je zlorabil ali izdal. Njegovo védenje o tem se presoja glede na njegov položaj in delo, ki ga opravlja pri delodajalcu, njegova znanja in zmožnosti. Presoja je strožja, če delavec pri delodajalcu zaseda pomemben položaj in če ima znanja, na osnovi katerih se od njega upravičeno pričakuje, da bi moral vedeti, da gre za zaupen podatek. Kršitev določbe o varovanju poslovne skrivnosti je lahko razlog za delavčevo disciplinsko (ZDR-1, 172. člen) in odškodninsko odgovornost (ZDR-1, 177. člen) ter redno (ZDR-1, 89. člen) ali izredno (ZDR-1, 110. člen) odpoved pogodbe o zaposlitvi.

Dolžnost varovanja poslovne skrivnosti pa je po 38. členu ZGD-1 tudi vsebina korporacijsko-pravnega razmerja med družbo in njenimi družbeniki ter člani organov družb. Ob določitvi podatka, ki se šteje za poslovno skrivnost, mora gospodarska družba ali njen organ s sklepom določiti tudi način varovanja poslovne skrivnosti in odgovornost oseb, ki morajo varovati poslovno skrivnost (ZGD-1, 40. člen, 1. odstavek). Način varovanja poslovne skrivnosti je opredeljen zlasti z natančnim določanjem, katera vsebina določenega podatka je poslovna skrivnost in kako se ta podatek označuje kot poslovna skrivnost. V način varovanja poslovne skrivnosti spada tudi določitev kroga oseb, ki so lahko seznanjene s poslovno

skrivnostjo. Drugi odstavek 40. člena ZGD-1 ureja krog oseb, ki so dolžne varovati poslovno skrivnost. To so poleg zaposlenih v gospodarskem subjektu še poslovni partnerji, dobavitelji, pogodbeni izvajalci in druge osebe zunaj družbe.

Poslovne skrivnosti ureja tudi Zakon o preprečevanju omejevanja konkurence (v nadaljevanju ZPOmK-1, Uradni list RS, št. 36/08, 40/09, 26/11, 87/11, 57/12, 39/13). Slednji v 17. točki 3. člena navaja, da so poslovna skrivnost podatki, katerih razkritje bi pomenilo nastanek občutne škode in so znani omejenemu krogu oseb. Ko gre za neupravičeno izkoriščanje zaupane poslovne skrivnosti drugega podjetja, se skladno s 3. odstavkom 63.a člena ZPOmK-1 to šteje kot nelojalna konkurenca, ki je prepovedana. Tisti, ki mu je bila z dejanjem protipravne pridobitve poslovne tajnosti ali neupravičenim izkoriščanjem zaupne poslovne tajnosti storjena škoda, sme zahtevati odškodnino po pravilih obligacijskega prava (ZPOmK-1, 63.b člen, 1. odstavek). Poleg tega lahko s tožbo v pravdnem postopku zahteva prepoved nadaljnjih dejanj nelojalne konkurence, uničenje predmetov, s katerimi je bilo storjeno dejanje nelojalne konkurence, in vzpostavitev prejšnjega stanja, če je to mogoče (ZPOmK-1, 63.b člen, 2. odstavek). Zahteva lahko tudi objavo sodbe v sredstvih javnega obveščanja, če je bilo dejanje nelojalne konkurence storjeno s sredstvi javnega obveščanja ali podobno (ZPOmK-1, 63.b člen, 3. odstavek).

Neupravičena izdaja ali pridobitev poslovne skrivnosti lahko predstavlja tudi kaznivo dejanje po Kazenskem zakoniku (v nadaljevanju KZ-1, Uradni list RS, št. 50/12 – uradno prečiščeno besedilo, 6/16 – popr., 54/15, 38/16, 27/17, 23/20 in 91/20). KZ-1 v petem odstavku 236. člena določa pojem poslovne skrivnosti, ki obsega industrijsko, bančno in vsako drugo poslovno skrivnost, ki mora biti opredeljena v formalno-materialni obliki. Kaznivo dejanje se po prvem odstavku 236. člena stori s sporočanjem podatkov, ki so poslovna skrivnost. Sporočanje je lahko ustno ali pisno, neposredno ali posredno s predajo listin, ki vsebujejo take podatke, pa tudi s pridobivanjem takih podatkov, da se izročijo nepoklicani osebi, kar pomeni, da gre za neke vrste pripravljalno delo za nadaljnje sporočanje in izročanje teh podatkov. V vseh opisanih primerih se za storilca kaznivega dejanja ne zahteva, da pozna vsebino poslovne skrivnosti, mora pa vedeti, da gre za poslovno skrivnost. Pogoj za obstoj kaznivega dejanja je tudi neupravičeno ravnanje storilca, kar pomeni, da nima pravice sporočati, izročati ali pridobivati teh podatkov, česar se mora tudi zavedati. Kaznivo dejanje je prav tako podano, če storilec pride do podatkov, ki so poslovna skrivnost, na protipraven način (kot so tatvina, vlom, vdor, zatajitev, izkoriščanje priložnosti za prepis ali fotokopiranje ipd.).

### 2.3 Varovanje poslovne skrivnosti v lokalni skupnosti

Eden izmed opredelilnih elementov poslovne skrivnosti po 2. členu ZPosS je njena tržna vrednost. Lokalne skupnosti pa sodijo med osebe javnega prava, financirane so iz javnih sredstev in se ne ukvarjajo s pridobitno dejavnostjo. Iz navedenega izhaja, da lokalne skupnosti že po definiciji ne morejo biti »imetniki« poslovnih skrivnosti, kot jih določa ZPosS. To pa ne

pomeni, da zanje ne obstaja dolžnost varovanja poslovnih skrivnosti, saj pri svojem delu dostopajo do dokumentov ali podatkov, ki jih njihovi lastniki (praviloma so to poslovni subjekti) lahko označijo kot poslovno skrivnost. Pri tem gre npr. za sklepanje pogodb med lokalno skupnostjo in poslovnimi subjekti po predhodno izvedenem postopku javnega naročanja, lahko tudi za sodne postopke, v katerih nastopa občina kot tožnik, toženec ali stranski intervenient.

Lokalna skupnost kot naročnik se v postopkih javnega naročanja srečuje tudi s poslovnimi skrivnostmi. Vendar morajo biti postopki javnih naročil pregledni (transparentni), s tem pa je povezana tudi zahteva po javnosti (publiciteti). Preglednost in javnost postopkov sta določena v javnem interesu in v interesu zainteresiranih ponudnikov. V javnem interesu je namreč, da sta razvidna namen in način porabe javnih sredstev. Vsakdo, ki želi pridobiti javno naročilo, se mora tako podrediti posebnemu načinu sklepanja pravnih poslov. Med te posebnosti sodi tudi to, da ponudniki ne morejo pričakovati popolnega varstva poslovne skrivnosti v pogodbi, sklenjeni na osnovi postopka javnega naročila (Informacijski pooblaščenec 2015).

Obveznost lokalne skupnosti, da varuje poslovne skrivnosti svojih pogodbenih partnerjev, je podrobneje opredeljena v 35. členu Zakona o javnem naročanju (v nadaljevanju ZJN-3, Uradni list RS, št. 91/15 in 14/18). Ta v prvem odstavku 35. člena določa, da naročnik ne sme razkriti informacij, ki mu jih gospodarski subjekt predloži in označi kot poslovno skrivnost, če zakon ne določa drugače. Prav tako mora naročnik zagotoviti varovanje podatkov, ki se glede na določbe zakona, ki ureja varstvo osebnih podatkov in varstvo tajnih podatkov, štejejo za osebne ali tajne podatke. Ne glede na to pa so javni vsi podatki specifikacije ponujenega blaga, storitve ali gradnje in količina iz te specifikacije, cena na enoto, vrednost posamezne postavke in skupna vrednost iz ponudbe ter vsi tisti podatki, ki so vplivali na razvrstitev ponudbe v okviru drugih meril. Po samem zakonu so torej ne glede na morebitno drugačno označbo s strani ponudnika javni tisti podatki, na osnovi katerih naročnik ponudbe ocenjuje in jih razvršča v skladu z vnaprej določenimi merili. Naročnik mora po objavi odločitve o oddaji javnega naročila omogočiti vpogled v ponudbo izbranega ponudnika vsem tistim ponudnikom, ki so oddali dopustno ponudbo, razen v tiste dele, ki predstavljajo poslovno skrivnost ali gre za tajne podatke. Tudi po pravnomočnosti odločitve o oddaji javnega naročila so vsi dokumenti v zvezi z oddajo javnega naročila javni, razen tistih delov, ki vsebujejo poslovne skrivnosti, tajne podatke ali osebne podatke (ZJN-3, 35. člen, 4. odstavek). V praksi pa se pogosto zgodi, da poslovni subjekti kot poslovno skrivnost označijo tudi podatke, ki bi po ZJN-3 (ali po ZDIJZ, več o tem v naslednjem odstavku) morali biti javni. Z označitvijo dokumentov kot poslovna skrivnost želijo zaščititi svoj know-how, metodologijo dela, osebne podatke, razne certifikate, pa čim več elementov njihove finančne konstrukcije določenega projekta ali posla (Občina Izola 2019). Vendar pa morajo subjekti javnega prava oznako »poslovna skrivnost«, zaupnost« in podobne oznake spregledati v primeru, ko so tako označeni podatki nujno potrebni za preverjanje npr. zakonitosti oddanega javnega naročila ali so nujni za izvajanje nadzora javnosti nad porabo javnih sredstev (Državna revizijska komisija za revizijo postopkov oddaje javnih

naročil 2017). V teh primerih gre za informacijo javnega značaja (več o tem v naslednjem podpoglavju).

Na tem mestu še velja omeniti, da tudi lokalne skupnosti, podobno kot poslovni subjekti, kot poslovno skrivnost označijo praviloma vse pogodbe, ki jih sklepajo v okviru izvrševanja svojih pristojnosti, in sicer navedejo, da za poslovno skrivnost štejejo dokumentacija in vsi podatki, ki se nanašajo na predmet pogodbe ali bi se na predmet pogodbe lahko nanašali. Pooblaščene osebe in drugi delavci, ki imajo dostop do te dokumentacije in podatkov, v nobenem primeru ne smejo brez izrecnega dovoljenja nadrejenega oziroma pristojne osebe o tej dokumentaciji seznanjati ali obveščati drugih oseb, razen tistih, ki morajo biti z njo seznanjeni po službeni dolžnosti, ali oseb, ki so za to pooblaščene s predpisi. Prav tako se lokalna skupnost s pogodbenimi partnerji (npr. izvajalci nekih gradbenih del) dogovori, kateri dokument bo obravnavan kot poslovna skrivnost lokalne skupnosti kot naročnika. Nato lahko lokalna skupnost s posebnim pisnim obvestilom posamezen dokument ali posamezno vrsto dokumentov izvzame iz obveznosti varovanja poslovne skrivnosti. Poslovno skrivnost lokalne skupnosti, kadar ta nastopa v vlogi naročnika, morajo poleg sopogodbenika (izvajalca) samega varovati tudi delavci izvajalca in druge osebe, ki jih bo izvajalec vključil v izvedbo dela po pogodbi. Izvajalec se pa zaveže, da bo svoje delavce in druge osebe, vključene v izvedbo dela po pogodbi, seznanil o obveznosti varovanja poslovnih skrivnosti. Poslovna skrivnost se mora varovati tudi po prenehanju veljavnosti pogodbe do preklica s strani naročnika oziroma dokler podatki, ki so poslovna skrivnost, ne postanejo javno dostopni (Občina Izola 2019). Vendar pa tukaj ne gre za poslovne skrivnosti v smislu definicije iz ZPosS (manjka element »tržna vrednost«), pač pa gre za poslovno skrivnost na osnovi odločitve pristojnega organa lokalne skupnosti. V praksi se za te skrivnosti pogosto uporablja oznaka »uradna tajnost«. Več o tem v šestem poglavju.

Ostale informacije, s katerimi razpolaga občina, kot npr. finančni rezultati, različna poročila glede zadolženosti ali likvidnosti, analize poslovanja in podobno, pa je lokalna skupnost dolžna razkriti, saj gre za informacije javnega značaja (Občina Izola 2019).).

## 2.4 Poslovna skrivnost in informacija javnega značaja

Tudi če ima lokalna skupnost podatek ali dokument, ki je označen kot poslovna skrivnost, mora takšno oznako spregledati v primeru, ko so tako označeni podatki nujno potrebni za izvajanje nadzora javnosti nad porabo javnih sredstev, saj gre v teh primerih za informacijo javnega značaja. Pravica vsakogar, da pridobi informacijo javnega značaja, je v Sloveniji urejena v 39. členu Ustave RS (v nadaljevanju URS, Uradni list RS, št. 33/91-I, 42/97 – UZS68, 66/00 – UZ80, 24/03 – UZ3a, 47, 68, 69/04 – UZ14, 69/04 – UZ43, 69/04 – UZ50, 68/06 – UZ121,140,143, 47/13 – UZ148, 47/13 – UZ90,97,99 in 75/16 – UZ70a). Ta pravica omogoča vpogled v delovanje državnih organov in s tem nadzor nad njihovim delovanjem. Obveščenost

javnosti je ključno merilo demokratičnosti določene družbe in izraža transparentno delovane oblasti (Čebulj in Žurej 2005).

Informacija javnega značaja je informacija, ki izvira s področja dela, ki ga opravlja zavezanec. Lahko je dokument, zadeva, dosje, register, evidenca ali dokumentarno gradivo (Ministrstvo za javno upravo 2020). Da lahko določeno informacijo opredelimo kot informacijo javnega značaja, mora predvsem ta obstajati, navajata Čebulj in Žurej (2005, 110), kar pomeni, da če je organ ne poseduje, je tudi ne more posredovati. Organi, ki imajo javnopravno naravo ali izvajajo javne naloge, so državni organi, organi lokalnih skupnosti, javne agencije, javni skladi, osebe javnega prava, nosilci javnih pooblastil in javnih služb ter drugih pravnih subjektov, kot so gospodarske družbe in druge pravne osebe, kjer ima država prevladujoči vpliv, občine in druge osebe javnega prava (Čebulj in Žurej 2005).

Izhodiščna dokumenta na področju ureditve dostopa do informacij javnega značaja sta Mednarodni pakt OZN o državljanskih in političnih pravicah (Uradni list SFRJ – MP, št. 7/71) in Konvencija o varstvu človekovih pravic in temeljnih svoboščin (Uradni list RS, št. 3-20/1994). Pakt sicer ne govori neposredno o informacijah javnega značaja, saj v 19. členu govori le o pravici svobodnega iskanja, sprejemanja in širjenja vsakovrstnih informacij ter idej, vendar pa v istem členu nalaga dolžnost in odgovornost pri urejanju omejitev svoboščin. Omejitve od svoboščin morajo biti urejene izključno z zakonom in vsebinsko potrebne zaradi spoštovanja pravic in ugleda drugih, zaradi zaščite nacionalne varnosti ali javnega reda, javnega zdravja ali morale.

Temeljni zakon s področja informacij javnega naročanja v Sloveniji je ZDIJZ. Sprejet je bil leta 2006, poem pa večkrat spremenjen in dopolnjen v obdobju 2014−2018. Zakon določa pravico do informacij javnega značaja, taksativno določa izjeme, zaradi katerih je možno dostop odreči, ter ureja pravno varstvo, ko organ zavrne dostop do želene informacije. Zakon kot nosilce informacij javnega značaja določa državne organe, organe lokalnih skupnosti, javne agencije, javne sklade in druge osebe javnega prava, nosilce javnih pooblastil in izvajalce javnih služb.

ZDIJZ v 5. členu določa, da so informacije javnega značaja prosto dostopne pravnim ali fizičnim osebam, kadar imajo te za dostop pravni interes. Določene informacije so izvzete in ne morejo biti javne, kot npr. zasebna zdravstvenega kartica, potni list, zasebna pošta. Izjema, ko se prosilcu lahko zavrne dostop do informacij javnega značaja, so tudi podatki, ki so opredeljeni kot tajni ali kot poslovna skrivnost; sem spadajo tudi osebni podatki, podatki, ki bi z razkritjem pomenili kršitve zaupnosti individualnih podatkov, zaupnosti davčnega postopka ali davčne tajnosti, podatki pridobljeni zaradi kazenskega pregona ali upravnega, pravdnega ali drugega sodnega postopka. Izjema so tudi podatki iz dokumenta, ki šele nastaja in bi njegovo razkritje povzročilo napačno razumevanje njegove vsebine, pa tudi podatki o naravnih in kulturnih vrednotah, ki niso dostopni javnosti zaradi varovanja naravne in kulturne dediščine (Čebulj in Žurej 2005).

Zaradi rednega seznanjanja javnosti o informacijah, do katerih ima vsakdo prost dostop, ZDIJZ vsem organom določa obveznost rednega vzdrževanja in objavljanja seznama informacij javnega značaja, s katerimi razpolaga. Vsi našteti organi morajo omogočiti dostop do teh podatkov preko spleta, prav tako pa morajo poskrbeti za ažurnost podatkov. Državni organi, lokalne skupnosti, javne agencije, javni skladi in druge osebe javnega prava morajo delovati transparentno, kar pomeni tudi vključitev javnosti za sodelovanje pri sprejemanju predpisov, hkrati javnost obveščati o porabi sredstev in si prizadevati za integriteto in preprečevanje korupcije. V primeru individualne zahteve pa je treba osebi omogočiti dostop do informacij javnega značaja (Ministrstvo za javno upravo 2020).

Prosilec lahko zahteva informacije javnega značaja pisno ali ustno, kot določata 12. in 14. člen ZDIJZ. Pisna oz. formalna oblika pomeni tudi, da se informacija javnega značaja lahko zahteva tudi v elektronski obliki po elektronski pošti tudi brez varnega elektronskega podpisa, vendar mora vsebovati vse elemente, da jo zavezanec lahko obravnava, kot to določa 17. člen ZDIJZ. Ta navaja, da se prosilec mora opredeliti, s katero informacijo se želi seznaniti in na kakšen način (le na vpogled, prepis, fotokopijo ali elektronski zapis). Da je mogoče vložiti zahtevo v elektronski obliki brez varnega elektronskega podpisa, omogoča 101. člen Uredbe o upravnem poslovanju (Uradni list RS, št. 9/18), sprejet na osnovi Zakona o splošnem upravnem postopku (ZUP, Uradni list RS, št. 24/06 – uradno prečiščeno besedilo, 105/06 – ZUS-1, 126/07. 65/08, 8/10 in 82/13).

Zahtevku o pridobitvi informacij javnega značaja se lahko ugodi, lahko pa se zahteva zavrne, če se ugotovi, da je podatek oz. dokument naveden kot izjema, ki jo določata 5.a in 6. člen ZDIJZ. Če je zahteva za dostop do informacij javnega značaja zavrnjena z odločbo, sklepom ali obvestilom, lahko prosilec vloži pritožbo k Informacijskemu pooblaščencu, ki je zadolžen za nadzor nad izvajanjem ZDIJZ.

Zakon o Informacijskem pooblaščencu (v nadaljevanju ZInfP, Uradni list RS, št. 113/05 in 51/07 – ZUstS-A), sprejet leta 2005, je ustanovil samostojni in neodvisni organ, tako imenovani Informacijski pooblaščenec, ki nudi pomoč posamezniku, ko ta meni, da mu je nekdo neupravičeno posegel v osebne podatke. Skladno z ZInfP je Informacijski pooblaščenec dolžan podati skupne praktične napotke za upravljavce zbirk osebnih podatkov. Poleg tega Informacijski pooblaščenec deluje kot pritožbeni, inšpekcijski in prekrškovni organ, odvisno od tega, na kaj se nanaša zadeva, med katere sodijo tudi kršitve pravice do dostopa oz. ponovne uporabe informacije javnega značaja (Ministrstvo za javno upravo 2020).

Za boljše razumevanje vloge Informacijskega pooblaščenca (v nadaljevanju IP) kot pritožbenega organa v nadaljevanju predstavljamo dva različna primera iz prakse, ki se nanašata na delo lokalne skupnosti.

V prvem primeru je bilo s strani IP ugodeno zahtevku prosilca, in sicer je prosilec na Krajevno skupnost Ljubno (v nadaljevanju KS Ljubno) naslovil zahtevo za dostop do informacij javnega

značaja, pri tem je navedel, da je od organa že večkrat ustno zahteval vpogled v dokumentacijo glede del, ki so bila opravljena v naselju Otoče, vendar neuspešno. Zato je od KS Ljubno zahteval, da mu omogoči vpogled v dokumentacijo oziroma mu fotokopira in dostavi dokumente ter račune v zvezi z opravljenimi deli v naselju Otoče. KS Ljubno je v postopku navajala, da dokumentacije nima, oziroma da so informacije, povezane s Cestnim podjetjem Kranj, poslovna skrivnost. Zato je bilo treba ugotoviti, ali so navedeni sporni dokumenti res poslovna tajnost. V postopku je IP res ugotovil, da določeni dokumenti ne obstajajo, saj so se ti nahajali pri podizvajalcih, medtem ko se Pogodba o izvedbi del kot del posledice sanacije peskokopa, z dne 16. 11. 2006, šteje za informacijo javnega značaja, do katere skladno s 1. odstavkom 1. člena ZDIJZ lahko dostopa vsakdo. Navedena pogodba ne sodi v izjeme, določene v (ZDIJZ, 6. člen), pa tudi je ni mogoče šteti za poslovno skrivnost skladno s 1. odstavkom 39. člena ZGD-1. Na osnovi navedenega je bila izdana odločba IP, da je KS Ljubno dolžan prosilcu posredovati fotokopijo Pogodbe, medtem ko se za ostalo dokumentacijo zahteva zavrne, ker kot informacije javnega značaja ne obstajajo (Informacijski pooblaščenec 2009).

V drugem je bila predmet spora dokumentacija, ki se je nanašala na gradbena dela. Z njo je razpolagalo Javno komunalno podjetje (v nadaljevanju JKP), ki je zavrnilo zahtevo prosilca za vpogled v omenjeno dokumentacijo iz razloga, da gre za poslovno skrivnost in s tem za izjemo od načela prostega dostopa do informacij javnega značaja. IP je najprej ugotavljal subjektivne kriterije za določitev poslovne skrivnosti in ugotovil, da se v konkretnem primeru za poslovno skrivnost ne morejo upoštevati podatki, ki so že po zakonu javni. Ker je JKP oseba javnega prava in zavezanec po ZDIJZ, sodi upravljanje z javnim bazenom med javno-pravno delovanje. Zato je menil, da zahtevani dokumenti izpolnjujejo pogoje za informacijo javnega značaja po prvem odstavku 4. člena ZDIJZ. Ker se s tem sklepom JKP ni strinjal, saj je menil, da navedena dokumentacija vsebuje tudi osebne podatke, je vložil tožbo na Upravno sodišče, ki pa je zaključilo, da je izpodbijani sklep pravilen in zakonit, zato je tožbo kot neutemeljeno zavrnilo na osnovi prvega odstavka 63. člena Zakona o upravnem sporu (ZUS-1, Uradni list RS, št. 105/06, 107/09 – odl. US, 62/10, 98/11 – odl. US, 109/12 in 10/17 – ZPP-E).

# 3 TAJNI PODATKI

V sodobni družbi smo priča številnim varnostnim tveganjem in grožnjam, zato je treba k varovanju tajnih podatkov pristopiti na sistematičen način in jim posvetiti posebno pozornost. Grožnje lahko prihajajo iz države ali pa iz zunanjih virov, pogosto obveščevalnih služb. Iz tega razloga so države razvile sisteme varovanja tajnih podatkov (Prezelj in Tarman 2015).

Varovanje tajnih podatkov Tarman (2012) razume kot splet varnostih ukrepov in postopkov, ki so potrebni za zaščito informacij z njihovim sledenjem. Tajni podatki so prisotni v vsaki demokratični državi, saj drugače država na dolgi rok ne more delovati in mora uživati zaupanje svojih državljanov. S tajnimi podatki vsaka država zagotavlja nacionalno varnost, kar pomeni suverenost ozemlja, varnost prebivalstva in drugih ključnih družbenih institucij, kot so državne institucije in kritična infrastruktura (Prezelj in Tarman 2015). Pojma tajnost in demokratičnost se uporabljata v večini demokratičnih držav, kjer pa Prezelj in Grizold (2015) v svojem prispevku opozarjata na konfliktnost navedenih pojmov. V konfliktu sta zato, ker demokracija in tajnost v teoriji ne sodita skupaj, prav tako omenjata dvojnost pojma tajnost, saj po eni strani pomeni varnost, po drugi strani pa lahko ob izgubi določenih tajnih podatkov pride do velike nevarnosti. Prav tako ugotavljata, da so mnogi raziskovalci mnenja, da se v praksi preveč podatkov označuje z besedo tajni in da je preveč tajnih podatkov označenih s previsoko stopnjo tajnosti.

Tudi Aftergood (2010) je mnenja, da je vladna tajnost na očiten način nezdružljiva z demokratičnim odločanjem. Tajnost podatkov omejuje dostop do uradnih informacij in s tem ovira sodelovanje javnosti v postopku posvetovanja ter zavira ali preprečuje odgovornost vladnih uradnikov za njihova dejanja. Vendar obstaja skoraj splošno soglasje, da je nekakšen ukrep tajnosti upravičen in potreben za zaščito nacionalne varnosti, kot so zbiranje obveščevalnih podatkov in vojaške operacije, da se omogoči zaupno razpravljanje med razvojem politike, da se zagotovi zasebnost in drugi razlogi. Uskladitev teh nasprotujočih si interesov je stalni izziv. V praksi se zdi, da so odločitve za omejevanje informacij odvisne od prevladujočih varnostnih pomislekov (tajnost je izrazitejša v času vojne), uradnih predispozicij (nekateri politični voditelji dajejo prednost tajnosti bolj kot drugi) ter stališč in pričakovanj javnosti.

Na pojav omenjene dvojnosti oziroma konfliktnosti v zvezi z varovanjem tajnih podatkov opozarjata tudi Brezovšek in Črnčec (2004), ki v svojem prispevku opozarjata na to, da demokratične države sicer morajo imeti določene tajne podatke, vendar je po njunem mnenju pri tem nujno, da je varovanje podatkov natančno pravno urejeno in da se ta ureditev v praksi tudi spoštuje.

V zadnjih letih smo priča povečanju količine tajnih podatkov kot npr. v ZDA, kjer se je količina tajnih podatkov samo v času Obamove administracije več kot potrojila. Zaskrbljenost zaradi prekomerne klasifikacije ni nova, vendar je še posebej zaskrbljujoča glede na količino zdaj

razvrščenih informacij in na število oseb, ki jih preganjajo zaradi puščanja tajnih podatkov v javnost (Taber 2015).

Zanimivo je, da se je pojem tajnosti v preteklosti in tudi danes vedno povezoval s skrivnostnostjo, čarobnostjo, z močjo in seveda varnostjo. Zavedati se moramo tudi, da če ne bi bilo potrebe oziroma zlorabe določenih podatkov, potem tajnost sploh ne bi bila potrebna (Prezelj in Grizold 2015). Tajnost se v praksi pogosto enači z besedo skrivnost, kar pa ni povsem pravilno, saj se skrivnost ne da pojasniti in opredeliti, kar pa ne velja za tajnost (Brezovšek in Črnčec 2004).

## 3.1 Opredelitev tajnih podatkov

Tajni podatek vsebuje širok spekter različnih informacij in podatkov, ki so povezani z delovanjem same države. Tajnost dokumenta ali informacije določijo za to zadolženi uslužbenci, ki določijo tudi stopnjo tajnosti glede na nevarnosti povzročitve škode, ki bi nastala pri razkritju tajnih podatkov (Razinger 2010). Za varovanje tajnih podatkov morajo poskrbeti odgovorne institucije tako na nacionalni kot tudi na lokalni ravni ne glede na to, ali gre za državne ali nedržavne organizacije. Sistem varovanja tajnih podatkov mora vsebovati kriterije, s katerimi se določi tajen podatek in zakaj ima ta določeno oznako (Prezelj in Tarman 2015). Kot navaja Pečar (2001, 3), je varovanje državnih tajnih podatkov zapleten pojav, ki nasprotuje pravici do obveščenosti in do zasebnosti ljudi.

Kot navaja Anžič (2000, 852), tajnost pomeni, da obstajajo znana dejstva »o družbenih, varnostnih, obrambnih, gospodarskih in drugih podatkih in informacijah«, ki so zaupana v uporabo in varovanje posamezniku. Zaradi različnih, pogosto nasprotujočih si interesov se tajne podatke skriva pred javnostjo načrtovano, organizirano in sistematično. Poleg tega je njihovo razkritje nevarno in škodljivo, ker so tajni dokumenti namenjeni varovanju, zaščiti državnih interesov in varovanju človekovih pravic.

Za tajne podatke je nujno, da so pravilno označeni in so z njimi seznanjeni le posamezniki, ki imajo to pravico. V Sloveniji tajne podatke opredeljuje Zakon o tajnih podatkih, po katerem je tajni podatek dejstvo ali sredstvo z delovnega področja organa, ki se nanaša na javno varnost, zunanje zadeve, obrambo države in varnostno delovanje države (ZTP, 2. člen). Do teh podatkov lahko dostopajo predsednik republike, predsednik vlade, poslanci, državni svetniki, župani in občinski svetniki, ministri in predstojniki vladnih služb, varuh človekovih pravic in njegov namestnik, guverner in njegov namestnik ter vice guverner centralne banke, član računskega sodišča, predsednik in člani državne revizijske komisije, sodniki, državni tožilci, generalni državni pravobranilci in Informacijski pooblaščenec. Vsi navedeni pridobijo dovoljenje s pričetkom funkcije oz. ko podpišejo izjavo o tajnosti.

## 3.2 Pravna ureditev varstva tajnih podatkov v RS

Označevanje, dostopanje in ravnanje s tajnimi podatki mora temeljiti na ustavnih osnovah in deklaraciji o človekovih pravicah in biti urejeno z zakonom. Za varovanje tajnih podatkov so odgovorne institucije, ki s takimi podatki operirajo (Prezelj in Tarman 2015). To področje je Slovenija uredila s sprejetjem ZTP leta 2001, ki ga je nato spreminjala in dopolnjevala leta 2003, 2006 je bil ZTP prečiščen in dopolnjen, nato še spremenjen in dopolnjen v letih 2010, 2011 in 2020.

Danes veljavni ZTP določa skupne osnove enotnega sistema določanja varovanja in dostopa do tajnih podatkov z delovnega področja državnih organov RS, ki se nanašajo na javno varnost, obrambo, zunanje zadeve ali obveščevalno in varnostno dejavnost države, ter prenehanje tajnosti takšnih podatkov. Zakon zavezuje vsako osebo, državne organe, organe lokalnih skupnosti, gospodarske družbe itd., ki se seznanijo z vsebino tajnega podatka, da so odgovorni za njegovo varovanje in ohranitev njegove tajnosti (1. člen). ZTP v 2. členu določa, da so tajni podatki opredeljeni kot dejstvo ali sredstvo z delovnega področja organa in se nanašajo na javno varnost, zunanje zadeve, obrambo države in varnostno delovanje države, zato je treba tajne podatke v skladu z določili v zakonu zavarovati pred nepooblaščenimi osebami. Pri tem gre lahko za dokumente, ki so napisani, narisani, natisnjeni, razmnoženi, posneti, fotografirani, v obliki magnetnega, optičnega ali kakšnega drugačnega zapisa. Dodaten pogoj za tajen podatek pa je, da se mora ta nanašati na (ZTP, 5. člen):

- javno varnost;
- obrambo;
- zunanje zadeve, obveščevalno in varnostno dejavnost državnih organov;
- sisteme, naprave, projekte in načrte, ki so pomembni za javno varnost obrambe;
- sisteme, naprave, projekte in načrte, pomembne za javno varnost, obrambo;
- zunanje zadeve ter obveščevalno in varnostno dejavnost državnih organov Slovenije;
- znanstvene, raziskovalne, tehnološke, gospodarske in finančne zadeve, pomembne za javno varnost, obrambo, zunanje zadeve ter obveščevalno in varnostno dejavnost državnih organov Slovenije.

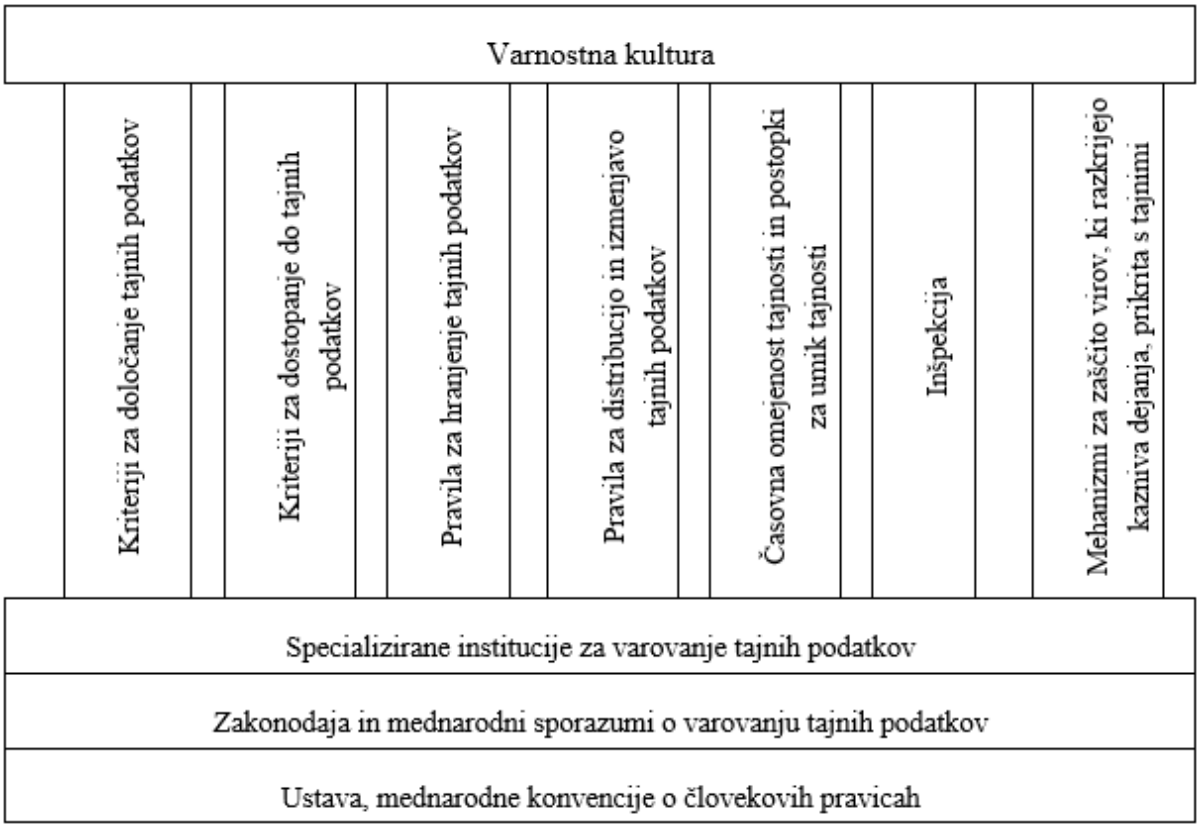
Pred sprejetjem ZTP so bili v Sloveniji tajni podatki označeni kot »vojaška skrivnost – zaupno«, na Ministrstvu za notranje zadeve pa s stopnjo tajnosti »Uradna tajnost – zaupno«. Dopolnitev ZTP leta 2011 je opredelila štiri različne ravni tajnosti glede na to, kakšne posledice lahko nastanejo ob razkritju določenih tajnih podatkov. Te štiri kategorije so:

- »strogo tajno« – razkritje ogroža vitalne interese države, škoda, ki nastane pa je nepopravljiva,
- »tajno« – razkritje hudo škoduje varnosti in interesom države,
- »zaupno« − razkritje škoduje varnosti in interesom države,
- »interno« – razkritje škoduje delovanju določenega državnega organa.

Na osnovi ZTP so bile sprejete različne uredbe:

- leta 2005 − Uredba o varovanju tajnih podatkov (Uradni list RS, št. 74/05, 7/11 in 24/11 – popr.), ki je konkretneje določala sistem fizičnih, organizacijskih in tehničnih postopkov in drugih ukrepov pri varovanju tajnih podatkov;
- leta 2006 − Uredba o varnostnem preverjanju in izdaji dovoljenj za dostop do tajnih podatkov (Uradni list RS, št. 71/06 in 138/06), ki:
  - natančneje določa obliko in postopek varnostnega preverjanja oseb, ki morajo zaradi določenih funkcij na delovnih mestih v določeni organizaciji pridobiti dovoljenje za dostop do tajnih podatkov,
  - natančno določa obliko in postopek izdaje in tudi preklica dovoljenja fizičnim osebam za dostop do tujih tajnih podatkov,
  - predpisuje obliko in potek usposabljanja oseb za obravnavo in varovanje tajnih podatkov stopnje tajnosti ZAUPNO in višje;
- leta 2007 − Uredba o varovanju tajnih podatkov v informacijsko-komunikacijskih sistemih (Uradni list RS, št. 48/07 in 86/11), ki določa področje varovanja tajnih podatkov v informacijsko-komunikacijski tehnologiji. Navedena uredba je vzpostavila sistem minimalnih fizičnih, organizacijskih in tehničnih standardov, postopkov in ukrepov za varovanje tajnih podatkov.

S spremembo Zakona o tajnih podatkih leta 2006 so bile v Uredbo o varovanju tajnih podatkov v informacijsko-komunikacijskih sistemih vnesene določbe, ki vzpostavljajo pravne okvire za sodelovanje javne uprave z zasebnim sektorjem. Kot je že v preteklosti pokazala praksa s področja varovanja tajnih podatkov, je treba z njimi ravnati odgovorno in jih predvsem zaščititi, kar je tudi odvisno od varnostne kulture organizacije. Kako naj bi izgledal sodobni sistem varovanja tajnih podatkov, prikazuje Slika 1.




**Slika 1: Sodobni sistem varovanja tajnih podatkov**

Vir: Prezelj in Tarman 2015, 690.

Na Sliki 1 so navedeni le ključni splošni elementi varovanja tajnih podatkov (Prezelj in Tarman 2015, 690). Da bi zagotovili varstvo človekovih pravic, je nujno, da država sitem določanja tajnosti uredi s pravnim redom (Anžič 2001, 48). Izvajanje določil ZTP in mednarodnih predpisov v Sloveniji spremlja Urad Vlade za varovanje tajnih podatkov. Poleg tega usklajuje stanje varovanja tajnih podatkov, predlaga ukrepe za izboljšanje njihovega varovanja, usklajuje delovanje organov, ki so pristojni za varnostno preverjanje itd. (ZTP, 43.a člen).

Za dostop do tajnih podatkov obstajajo različni kriteriji. Kot prvi kriterij za dostop do tajnih podatkov naj bi bila potreba po védenju, ki določi osebo, odgovorno za določeni tajni podatek in njegovo distribucijo (Shulsky in Schmitt 2002, po Prezelj in Tarman 2015, 695), drugi kriterij pa je preverjanje osebe, odgovorne za varnost tajnih podatkov.

Skladno z ZTP morajo vse osebe, ki so zadolžene za varovanje podatkov, biti zanesljive in verodostojne, pri čemer se ugotavlja tudi osebni značaj in okoliščine, ki bi vplivale na varnostno težavo. Pri varovanju tajnih podatkov je namreč ključna vloga človeškega vira in njegovega neodgovornega delovanja (Prezelj in Tarman 2015). Dolžnost varovanja tajnih podatkov ne preneha, ko te osebe prenehajo z delom ali funkcijo (ZTP, 8. člen).

Kot določa ZTP v četrtem odstavku 1. člena, je vsakdo, ki mu je bil zaupan tajni podatek ali je z njim bil seznanjen, odgovoren za njegovo varovanje in ohranjanje varnosti. Kdaj gre za

zlorabo tajnih podatkov, urejata 35. in 36. člen Uredbe o varovanju tajnih podatkov. Skladno s 35. členom navedene uredbe se za zlorabo šteje vsak nepooblaščen dostop, uničenje, odtujitev ali kakršenkoli drugi dogodek, ki ima znake zlorabe. Takoj, ko pride do takega dogodka, je treba obvestiti pristojno osebo ali pooblaščen organ. Če gre za nacionalno varnost, je treba obvestiti nacionalni organ, v primeru kaznivega dejanja pa tudi policijo. Kazenske določbe za prekrške o razkritju ali izgubi tajnih podatkov vsebuje ZTP v VI. poglavju, medtem kot 260. člen Kazenskega zakonika opredeljuje kaznivo dejanje izdaje tajnih podatkov. Skladno s tem je zaporna kazen do treh let predpisana za uradno osebo ali drugo osebo, ki v nasprotju s svojimi dolžnostmi varovanja tajnih podatkov sporoči ali izroči komu tajne podatke ali mu kako drugače omogoči, da pride do njih, ali zbira take podatke, zato da jih izroči nepoklicani osebi. Enako se kaznuje, kdor protipravno pride do tajnih podatkov, da bi jih neupravičeno uporabil, in kdor take podatke brez dovoljenja javno objavi.

Skladno s 1. členom ZTP morajo poleg državnih organov, nosilcev javnih pooblastil in drugih organov, gospodarskih družb in organizacij tajne podatke ščititi tudi v lokalnih skupnostih. Lokalna skupnost je dolžna tako kot druge državne institucije varovati svoje podatke. Skladno z zakonskimi in podzakonskimi predpisi so lokalne skupnosti dolžne izdelati načrt varovanja tajnih podatkov, ki zajema fizične, organizacijske in tehnične postopke ter ukrepe varovanja tajnih podatkov. Ker tajni podatki nimajo neskončne dobe zaupnosti, jih je treba ves čas dopolnjevati oz. vsaj enkrat letno pregledati in preveriti (Inštitut za ekonomijo, pravo in informatiko 2019).

### 3.3 Varovanje tajnih podatkov v lokalnih skupnostih

Vsak tajni podatek ima določen življenjski cikel, zato mora označevanje takega podatka kot tajnega potekati po točno določenih pravilih. Sistem varovanja tajnih podatkov zajema čas njihovega nastanka, uporabo in prenehanje stopnje tajnosti (Prezelj in Tarman 2015).

Na lokalni ravni tajnih podatkov skorajda ni oz. je teh zelo malo. Včasih so oznako tajnosti imeli obrambni načrti in načrti civilne zaščite, sedaj pa teh dokumentov lokalne občine nimajo več. Najpogostejši pravni akt, s katerim se v lokalni skupnosti zapišejo postopki o ravnanju s tajnimi podatki, je pravilnik s tega področja. Župan je kot predstojnik lokalne skupnosti pooblaščen za določitev »lastnosti« tajnega podatka. Poleg njega imajo takšno pristojnost tudi druge osebe, ki jih župan za to pisno pooblasti, ker je to pomembno za njihovo nemoteno opravljanje dela kot to določa 10. člen ZTP. To pooblastilo je neprenosljivo. ZTP v 38. členu navaja določbe, ki jih mora vsebovati Pravilnik o ravnanju in načinih varovanja s tajnimi podatki (v nadaljevanju Pravilnik).

V Pravilniku se določijo osebe, katerih dolžnost je tudi varovanje tajnih podatkov (javni funkcionarji in uslužbenci, člani delovnih komisij, odborov, občinski svetniki). Zaposleni morajo že pred zaposlitvijo predložiti izjavo o nekaznovanosti, ob zaposlitvi pa s podpisom

posebne izjave potrditi, da so seznanjeni s tovrstnim Pravilnikom ter da se zavedajo svoje odgovornosti (disciplinske, kazenske, materialne) v primeru razkritja tajnih podatkov. Za nadzor nad izvajanjem Pravilnika je odgovoren župan, ki mora delo organizirati tako, da bodo zaposleni seznanjeni, kdo je zadolžen za varovanje tajnih podatkov. Pooblaščene osebe, ki dostopajo do tajnih dokumentov, morajo zaklepati omare ali prostor, v katerih se ti podatki hranijo. Vsakemu zaposlenemu, ki dostopa do tajnih podatkov, se določi geslo. V primeru, da zaposleni ugotovijo razkritje tajnih podatkov, so dolžni o tem takoj obvestiti župana, ki mora takoj ukrepati. Pri oznakah zaupno se uporabljajo določbe ZTP. Za izboljšanje varovanja poslovne skrivnosti ali tajnih podatkov morajo v to biti vključeni vsi zaposleni in zunanji sodelavci, ki opravljajo delo po pogodbi.

V primeru, da zaposleni ali drugi sodelavci (zunanji) odkrijejo kakšne pomanjkljivosti pri varovanju podatkov ali ugotovijo namerne ali nenamerne varnostne kršitve, opazijo nepravilno ali sumljivo delovanje informacijskih sistemov oz. njegovo nedelovanje, so dolžni takoj prijaviti incident (Nacionalni inštitut za javno zdravje 2016).

Naj omenimo še en zakon, ki je pomemben pri varovanju tajnih podatkov v lokalni skupini, in sicer je to Zakon o varstvu dokumentarnega in arhivskega gradiva ter arhivih (v nadaljevanju ZVDAGA, Uradni list RS, št. 30/06 in 51/14,), ko gre za arhiviranje tajnih podatkov.

# 4 OBVEZNOSTI IN ODGOVORNOSTI ZAPOSLENIH PRI VAROVANJU POSLOVNIH SKRIVNOSTI IN TAJNIH PODATKOV V LOKALNI SKUPNOSTI

Varovanje podatkov ni pomembno le za državo, ampak se tega pomena vedno bolj zavedajo tudi v organizacijah, kjer pa gre za zaupne podatke, ki pomembno vplivajo na delovanje organizacije. Varovanje zaupnih podatkov je povezano s stroški glede na to, da živimo v času digitalne tehnologije, kjer gre tudi za drago opremo. Zato se v praksi organizacije odločajo med tveganji in stroški, ki so potrebni za sistem varovanja komunikacij in informacij. V primeru, da so podatki pravilno shranjeni in zaščiteni, pridobijo organizacije večje zaupanje s strani partnerjev, zagotavljajo korektno poslovanje, skladno z veljavno zakonodajo in pravili, hkrati pa zmanjšujejo tveganja pri poslovanju (Kralj in Starček 2012).

## 4.1 Uvod

Raziskava, ki jo je leta 2010 prvič izvedlo podjetje Price Waterhouse Coopers (2010) med 539 malimi, srednjimi in velikimi podjetji iz različnih industrijskih sektorjev različnih držav po svetu, je pokazala, kateri so faktorji, ki lahko ogrožajo varnost informacijskih podatkov. Raziskava je pokazala, da so v 62 % največje težave pri varovanju podatkov človeški faktor, nepoštenost in slabi nameni. Največjo grožnjo (82 %) pri varovanju podatkov organizaciji predstavljajo zaposleni, ko preko pametnih telefonov in tabličnih računalnikov dostopajo do poslovnih podatkov organizacij. V letu 2012 je 47 % zaposlenih razkrilo zaupne informacije podjetja (Price Waterhouse Coopers 2012), v letu 2014 je 81 % velikih podjetij poročalo, da so utrpele škodo zaradi razkrivanja varnosti, v letu 2015 pa se je ta odstotek še zvišal na 90 %. Večina anketiranih podjetij pričakuje, da se bo število kršitev glede varovanja podatkov v prihodnjih letih še povečalo (Price Waterhouse Coopers 2015). Glede na to je nujno zagotoviti čim bolj učinkovito varovanje podatkov tako iz organizacijskega, tehničnega, kadrovskega in varnostnega vidika, da bi se obvladovale notranje in zunanje grožnje.

Delovno razmerje je razmerje med delavcem in delodajalcem, ki ima zaradi svoje pravne narave in (običajno) daljšega trajanja določene posebnosti − med njimi so tudi potreba po medsebojnem zaupanju in lojalnosti. Obveznost varovanja poslovnih skrivnosti določa 38. člen ZDR-1, po katerem »delavec ne sme izkoriščati za svojo osebno uporabo ali izdati tretjemu delodajalčevih poslovnih skrivnosti, ki jih kot take določi delodajalec in ki so bile delavcu zaupane ali s katerimi je bil seznanjen na drug način«.

Pri vzpostavitvi delovnega razmerja se med delodajalcem in delavcem sklene pogodba o zaposliti. Pogodba o zaposlitvi vsebuje pravice in obveznosti obeh strank (delavca in delodajalca), s čimer postaneta obe stranki odgovorni za ravnanja, specifična za delovno-pravni odnos. Obe stranki odgovarjata tako disciplinsko, odškodninsko in kazensko, skladno z ZDR-1, kazenskim in obligacijskim zakonikom (Turk 2019). Ena izmed kršitev, ko delavec lahko

disciplinsko, odškodninsko in kazensko odgovarja, je tudi razkritje poslovnih skrivnosti in tajnih podatkov.

### 4.2 Delovno-pravni vidik

V primeru, če bi zaposleni razkril tajne podatke in poslovne skrivnosti, krši svoje delovne obveznosti. Delavec je odgovoren tudi, če pri razkritju poslovne skrivnosti ni nastala nikakršna premoženjska škoda. Delavec je odgovoren za kršitev, če je vedel ali bi moral vedeti za tak značaj podatkov. Če delavec to svojo obveznost krši, lahko od njega delodajalec zahteva odškodnino (tudi pavšalno) ali plačilo pogodbene kazni (če je ta določena v kolektivni pogodbi, ki zavezuje delodajalca, ali v pogodbi o zaposlitvi med delavcem in delodajalcem), prav tako lahko zoper delavca vodi disciplinski postopek in mu izreče disciplinske ukrepe ali pa mu (redno ali izredno) odpove pogodbo o zaposlitvi, če so za to podani z zakonom predpisani pogoji. Ob tem je treba opozoriti še na kazensko odgovornost po KZ-1, ki med kaznivimi dejanji določa tudi neupravičeno zlorabo poklicne skrivnosti v 142. členu ter izdajo in neupravičeno pridobitev poslovne skrivnosti v 236. členu.

V zvezi z varovanjem tajnih podatkov in poslovnih skrivnosti je pomemben tudi 12. člen Zakona o javnih uslužbencih (v nadaljevanju ZJU, Uradni list RS, št. št. 63/07 – uradno prečiščeno besedilo, 65/08, 69/08 – ZTFI-A, 69/08 – ZZavar-E in 40/12 – ZUJF), ki določa, da je javni uslužbenec dolžan varovati tajne podatke in poslovne skrivnosti tako med trajanjem kot po prenehanju delovnega razmerja. Obveznost varovanja tajnih podatkov velja toliko časa, dokler delodajalec javnega uslužbenca te dolžnosti ne razreši, pri čemer ni pomembno, ali se je javni uslužbenec s podatki seznanil pri opravljanju svojih nalog ali kako drugače.

V izogib nejasnosti, kaj so to poslovne skrivnosti in tajni podatki, so organizacije, kamor uvrščamo tudi lokalne skupnosti, dolžne to področje urediti v svojih internih aktih. Poleg tega mora biti iz akta jasno razvidno, kdo lahko dostopa do poslovnih skrivnosti in tajnih podatkov. Cilj lokalne skupnosti je, da v okviru svojega sistema zaščiti podatke, da jih ne bi protipravno pridobila in uporabljala oseba, ki do njih ni upravičena. Bistvo je, da se delavec v okviru svoje narave dela vzdrži vseh ravnanj, ki bi materialno ali moralno škodovala poslovnim interesom delodajalca.

V primerih kršitve varovanja poslovne skrivnosti je kot temeljno treba dokazati, da nek podatek šteje za poslovno skrivnost. Delavec je odgovoren za kršitev le v primeru, če je vedel ali bi moral vedeti za tak značaj podatkov, kar je prav tako treba dokazovati, v primeru odškodninske odgovornosti delavca pa je treba dokazati vse predpostavke odškodninske odgovornosti po Obligacijskem zakoniku (v nadaljevanju OZ, Uradni list RS, št. 97/07 – uradno prečiščeno besedilo, 64/16 – odl. US in 20/18 – OROZ631). Ob tem je treba upoštevati tudi, da je izredna odpoved pogodbe o zaposlitvi lahko zakonita le v primeru, če nadaljevanje delovnega razmerja ni mogoče niti do izteka odpovednega roka (ZDR-1, 109. člen).

V zvezi z varovanjem poslovnih skrivnosti je treba omeniti še nekatere primere iz sodne prakse. Slednji se sicer ne nanašajo na lokalno skupnost, vsebujejo pa pomembne odgovore na vprašanje, do kod sega obveznost delavca varovati poslovne skrivnosti delodajalca oziroma kaj se šteje za kršitev prepovedi škodljivega ravnanja.

Začenjamo s primerom Vrhovnega sodišče RS, št. VIII Ips 211/2012 (Vrhovno sodišče RS 2013a), kjer je bilo relevantno dejansko stanje v osnovi naslednje: tožnik, delavec in nekdanji član uprave tožene stranke (delodajalca) je za slovenski dnevnik dal intervju in kasneje še objavil pismo bralca, pri čemer je navajal določene podatke, s katerimi se je seznanil pri opravljanju svojega dela za toženo stranko, ta pa mu je izredno odpovedala pogodbo o zaposlitvi, ker je štela, da je huje kršil pravila komuniciranja z mediji, dolžnost varovanja poslovne skrivnosti in dolžnost varovanja ugleda tožene stranke, njegova kršitev pa naj bi imela tudi znake kaznivega dejanja izdaje in neupravičene pridobitve poslovne skrivnosti po prvem odstavku 236. člena Kazenskega zakonika (kršitev iz 1. in 2. alineje prvega odstavka 111. člena tedaj veljavnega Zakona o delovnih razmerjih, v sedaj veljavnem ZDR-1 temu ustrezata določbi 1. in 2. alineje prvega odstavka 110. člena). Sodišča so kot bistveno za odločitev ugotavljala, ali so podatki, ki jih je tožnik razkril v intervjuju in v pismu, v resnici takšni, da predstavljajo za toženo stranko poslovno skrivnost.

Vrhovno sodišče je s sodbo, opr. št. VIII Ips 211/2012 (Vrhovno sodišče RS 2013a), ugotovilo, da so bili podatki, ki jih je tožena stranka označila za zaupne (namen širjenja ponudbe storitev z bolnišnicami, domovi za ostarele itd.), javnosti znani že pred objavo spornega intervjuja. Revizijsko sodišče je soglašalo s stališčem nižjih sodišč, da samo ime O. ne more predstavljati poslovne skrivnosti. Vprašanje pa je, ali je z razkritjem cene za posamezno nepremičnino in cene celotnega projekta tožnik kršil svojo dolžnost varovanja poslovne skrivnosti po prvem odstavku 2. člena Pravilnika o poslovni skrivnosti (interni akt delodajalca), ki določa, da za poslovno skrivnost veljajo vsi podatki, informacije ali dokumenti, za katere je očitno, da bi nastala občutna škoda, če bi zanje izvedela nepooblaščena oseba. Pri odgovoru na to vprašanje se je sodišče najprej osredotočilo na to, ali ta podatek za toženo stranko pomeni konkurenčno prednost. Če je odgovor na to vprašanje pritrdilen, je očitno, da bi z razkritjem takega podatka nastala občutna škoda. Revizijsko sodišče je soglašalo s stališčem sodišča druge stopnje, da ti podatki za toženo stranko v razmerju do njenih konkurentov niso mogli predstavljati nikakršne konkurenčne prednosti in zato ne predstavljajo poslovne skrivnosti.

Drugi sodni primer se je nanašal na zadevo št. VIII Ips 52/2012 (Vrhovno sodišče RS 2013b). S sodbo in sklepom je Vrhovno sodišče odločalo o reviziji zoper sodbo Pdp 996/2011, z dne 6. 12. 2011, Višjega delovnega in socialnega sodišča, ko je tožena stranka kot delodajalec podala tožniku izredno odpoved pogodbe o zaposlitvi zaradi tega, ker je razkril podatke o proizvodnji ter o gospodarskih načrtih družbe in realizaciji nepooblaščenim osebam, tako da je sestavil in posredoval dopis »stanje proizvodnje v P. od 1. 1. do 1. 5. 2007« ter ga posredoval poslancu Državnega zbora Republike Slovenije. Iz izredne odpovedi pogodbe o zaposlitvi izhaja, da se

je tožena stranka pri opredelitvi poslovne skrivnosti družbe in s tem glede ravnanja tožnika oprla predvsem na Pravilnik o varovanju osebnih podatkov in poslovnih tajnostih in na tej podlagi zavrnila tožnikov zagovor, da gre za podatke javnega značaja, navedla pa je tudi, da pri izredni odpovedi ni mogoče prezreti dejstva, da delavec opravlja naloge ožjega poslovodstva in da bi se glede na naravo dela moral vzdržati ravnanj, ki morda škodujejo ali bi lahko škodovala njenim poslovnim interesom. Med strankama je bilo tako sporno, ali imajo posredovani podatki v dopisu tožnika naravo zaupnih podatkov oziroma ali predstavljajo poslovno skrivnost družbe ter ali tožnikovo razkritje teh podatkov pomeni hujšo kršitev, storjeno naklepno ali iz hude malomarnosti.

Vrhovno sodišče je ugotovilo, da tožnik s pošiljanjem dopisa poslancu ni kršil svoje obveznosti varovanja poslovne skrivnosti, ker ne morejo vsi na kakršenkoli način dostopni podatki o poslovanju družbe predstavljati poslovne tajnosti družbe. Da gre za poslovno skrivnost, mora biti točno določeno, kateri so ti podatki, pri tem pa ni pomembno, ali gre za podatke, katerih posredovanje je zapisano v delokrogu določenega delavca ali ne, saj dejstvo delokroga ni razlikovalni kriterij poslovne skrivnosti. V predmetni zadevi se je izkazalo tudi, da niso poslovna skrivnost podatki, ki se kumulativno pojavljajo v letnem in polletnem poročilu tožene stranke. S posredovanjem teh podatkov ni nastala za toženo stranka občutna škoda, kar je potrdil tudi izvedenec, ki je govoril le o potencialni škodi brez konkretnejših pojasnil, kaj bi bilo ob sporočenih podatkih lahko bistvenega pomena za konkurenco. Upoštevati pa je bilo treba tudi, da je tožnik dopis posredoval le poslancu državnega zbora, pa še to v zvezi s pogovori tožene stranke in dveh njenih največjih lastnikov (Kapitalske družbe in Slovenske odškodninske družbe).

Naslednja sodba se nanaša na zaupne informacije, ki naj bi jih delavec razkril. V sodbi VIII Ips 138/2016 z dne 11. 10. 2016 (Vrhovno sodišče RS 2016a) v povezavi s sodbo Višjega delovnega in socialnega sodišča št. Pdp 941/2015 z dne 18. 2. 2016 (Višje delovno in socialno sodišče RS 2016) je bilo med drugim sporno, ali je tožnica brez ustreznega soglasja poslovnemu partnerju sporočila izjemno občutljivo in zaupno informacijo, ki je ni dovoljeno in dopustno izdajati nepooblaščenim osebam. V podani izredni odpovedi se ji je namreč med drugim očitalo, da je po sporočilu direktorja tožene stranke, da odhaja (pri čemer je bilo delavcem pojasnjeno, da te informacije ni dopustno sporočiti nepooblaščenim osebam), čez nekaj ur to sporočila poslovnemu partnerju delodajalca v zvezi s pripravo pogodbe o dobavi. Sodišče je ugotovilo, da je s tem tujemu partnerju brez utemeljenega razloga posredovala informacijo, ki jo je tožena stranka štela za zaupno, kot neutemeljene pa je zavrnilo tožničine navedbe, da gre za informacijo javnega značaja. Ko je informacija o spremembi direktorja objavljena v sodnem oziroma poslovnem registru, je seveda to javna informacija. Vendar pa gre lahko pred tem za poslovno odločitev tožene stranke, kdaj poslovnim partnerjem oziroma javnosti ta podatek sporoči, oziroma kdaj je to zanjo najbolj primerno. V tem smislu pa gre za zaupno informacijo, ki je tožnica ni smela posredovati osebam, oziroma je s svojim ravnanjem postopala v nasprotju z jasnimi navodili tožene stranke v smislu 34. člena ZDR-1. Sodišče je presodilo, da je izredna

odpoved zakonita, vendar pa je bila ta tožnici podana še zaradi drugih kršitev, zato je težko odgovoriti na vprašanje, ali bi sodišče zgolj in samo zaradi navedene kršitve presodilo, da je podan temeljni pogoj za zakonitost izredne odpovedi pogodbe o zaposlitvi, to je, da ni mogoče nadaljevati delovnega razmerja niti do izteka odpovednega roka (ZDR-1, 109. člen, 1. odstavek).

Tudi na osnovi zadeve VIII Ips 200/2012 (sodba z dne 19. 2. 2013) (Vrhovno sodišče RS 2013c) v povezavi s sodbo Višjega delovnega in socialnega sodišča št. Pdp 6/2012, z dne 25. 4. 2012, ni mogoče postaviti jasne ločnice, kdaj kljub izdaji poslovne skrivnosti s strani delavca izredna odpoved ni zakonita zaradi neobstoja drugega pogoja za zakonitost izredne odpovedi pogodbe o zaposlitvi (ZDR-1, 109. člen, 1. odstavek). Gre namreč za poseben primer, ko je tožnica za dokaz v sporu predložila zaupno listino, ki se je nanašala na delovno razmerje njenega sodelavca z njegovimi osebnimi podatki, čeprav do tega ni imela dostopa. Sodišče je poudarilo, da v postopku pred sodišči obstajajo procesne možnosti za zaščito tajnih oziroma osebnih podatkov, da jih je tožnica predložila v zaščito svojih pravic iz delovnega razmerja in da je postopek potekal med strankama tega spora. Za bojazen, da bo tožnica tudi v bodoče razkrivala poslovne skrivnosti tožene stranke glede na razlog, zaradi katerega jih je v spornem primeru razkrila, in način, na katerega je to storila, po ugotovitvah sodišča ni bilo realne podlage, kakor tudi ne za zatrjevano izgubo zaupanja v tožničino lojalnost.

Kot smo navedli v uvodu tega poglavja, lahko delodajalec v razmerju do delavca, ki krši obveznost varovanja poslovne skrivnosti, uveljavlja tudi odškodninsko odgovornost. V zadevi Pdp 1132/2013 (sodba z dne 10. 4. 2014) (Višje delovno in socialno sodišče RS 2014) je Višje delovno in socialno sodišče presojalo, ali je tak zahtevek utemeljen v razmerju do delavca, za katerega se je ugotovilo, da je na svojem službenem računalniku hranil dokumente, ki jih na njem ne bi smel imeti (ugodnejša ponudba druge gospodarske družbe poslovnemu partnerju delodajalca), ni pa bilo dokazano, da je poslovno skrivnost delodajalca izdal tretjemu ali jo izkoristil za svojo osebno uporabo. Ugotovljeno je bilo, da sama hramba dokumentov, ki jih delavec ne bi smel imeti na svojem računalniku, ni kršitev varovanja poslovne skrivnosti, prav tako ne gola navedba, da bi nepooblaščene osebe lahko vdrle v sistem stranke delodajalca. Sodišče ni pritrdilo navedbam delodajalca, da že samo dejstvo, da je delavec to listino imel na svojem službenem računalniku, dokazuje njegov namen po osebni uporabi teh podatkov. Za druge podatke pa je sodišče ugotovilo, da bi moral delodajalec konkretno navesti, kateri podatki iz pogodbe predstavljajo poslovno skrivnost, hkrati pa bi moral v postopku dokazati, da je delavec te podatke izkoristil za osebno rabo oziroma posredoval tretji osebi. Pavšalna opredelitev, da poslovno skrivnost predstavlja vse v zvezi z izvedbo te pogodbe, ni zadostna.

Sodobna tehnologija lahko za poslovne subjekte predstavlja povečano stopnjo tveganja za izdajo poslovnih skrivnosti s strani zaposlenih. V zadevi št. Pdp 774/2015 (sodba z dne 21. 1. 2016) (Vrhovno sodišče RS 2016b) je Višje delovno in socialno sodišče presojalo zakonitost izredne odpovedi, ki jo je tožena stranka tožniku podala zaradi očitka, da se je v času bolniškega

staleža prek oddaljenega dostopa prijavil v računalnik tožene stranke z uporabniškim imenom in geslom druge delavke in z informacijskega sistema tožene stranke prenesel celotno vsebino map, v katerih so bile datoteke z osebnimi podatki zaposlenih in študentov ter zaupni podatki o poslovanju tožene stranke, kar se vse šteje za poslovno skrivnost. Ugotovilo je, da očitane kršitve predstavljajo utemeljen razlog za izredno odpoved pogodbe o zaposlitvi po 1. in 2. alineji prvega odstavka 110. člena ZDR-1, saj je delavec izpolnil znake kaznivih dejanj zlorabe osebnih podatkov (KZ-1, 143. člen, 2. odstavek) in napada na informacijski sistem (KZ-1, 221. člen, 1. in 2. odstavek) ter da je podan tudi pogoj nemožnosti nadaljevanja delovnega razmerja niti do izteka odpovednega roka (ZDR-1, 109. člen, 1. odstavek), saj je bila kršitev zelo huda, ker je šlo za prenos osebnih podatkov na nepooblaščeno mesto, v konkretnem primeru pa dodatno težo daje še dejstvo, da je bil tožnik pri toženi stranki zaposlen kot sistemski inženir. Na oddaljeno mesto je prenesel večjo količino podatkov, ki so predstavljali poslovno skrivnost tožene stranke (šlo je tudi za osebne podatke študentov doktorskega študija). Tožena stranka je tako utemeljeno izgubila zaupanje v tožnika in nadaljevanje delovnega razmerja do izteka odpovednega roka ni bilo mogoče.

### 4.3 Civilno-pravni vidik (odškodninska odgovornost)

Zaposleni v organih lokalne skupnosti so javni uslužbenci, zato je odškodninska odgovornost povzročena na delu ali v zvezi z delom opredeljena z ZJU in ZDR-1. Izhajajoč iz tega je pomembno, da se v nadaljevanju osredotočimo tudi na omenjena zakona.

Osnovno pravilo odškodninskega prava je načelo, da za povzročeno škodo drugemu odgovarja njen povzročitelj. Navedeno pravilo pa pozna tudi nekatere izjeme. Med njimi je tudi odgovornost delodajalca za škodo, ki jo povzročijo pri njem zaposleni delavci. Ureditev odgovornosti delodajalca za delavce vsebuje 147. člen OZ, ki določa, da je za škodo, ki jo povzroči delavec na delu ali v zvezi z delom tretji osebi, odgovoren delodajalec. *Ratio* te ureditve je v tem, da je delavec pravzaprav podaljšana roka delodajalca, namen prenosa odgovornosti pa v zagotovitvi primerne samoiniciativnosti delavcev (Bizjak 2014, 74). Slednji se lahko odgovornosti razbremeni, če dokaže, da je delavec v danih okoliščinah ravnal tako, kot je bilo treba. Če delavec povzroči škodo namenoma, pa ima oškodovanec pravico zahtevati povrnitev škode neposredno od delavca. Če to »prevedemo« na raven lokalne skupnosti, ugotovimo, da je za škodo tretjim osebam, ki jo povzroči zaposleni v lokalni skupnosti, odgovorna lokalna skupnost (občina) kot delodajalec. Ker pa so zaposleni v lokalni skupnosti javni uslužbenci, je zanje pomemben predvsem ZJU, ki je glede na ZDR-1 *lex specialis*.

ZJU v 135. členu določa, da je za škodo, ki jo na delu ali v zvezi z delom protipravno povzroči javni uslužbenec tretji osebi, odškodninsko odgovoren delodajalec. Neposredna odgovornost javnega uslužbenca pa pride v poštev, če je škoda povzročena naklepno, vendar gre v tem primeru za solidarno odgovornost obeh, javnega uslužbenca in njegovega delodajalca (ZJU, 135. člen, 3. odstavek). Namen razbremenitve neposredne odgovornosti javnih uslužbencev je

v spodbujanju njihove samoiniciativnosti oziroma samostojnosti pri delu. Javni uslužbenec pa je državi – svojemu delodajalcu – regresno zavezan: če država izplača oškodovancu odškodnino, lahko v primeru, da je bila škoda povzročena namenoma ali s hudo malomarnostjo, zahteva povrnitev škode od javnega uslužbenca (OZ, 139. člen). Vsi, ki ravnajo v imenu države oziroma izvršujejo javna pooblastila, pa ne sodijo med javne uslužbence. To velja predvsem za funkcionarje v državnih organih ali organih lokalnih skupnosti. Kot poudarja Možina (2013), je Vrhovno sodišče navedlo, da je treba od delavcev v javnem sektorju razlikovati člane državnih organov. Medtem ko je za prve upravičena uporaba pravil o odškodninski odgovornosti za ravnanje drugega, za ravnanje državnih organov neposredno odgovarja država.

### 4.4 Kazensko-pravni vidik

Poslovna skrivnost je varovana z 236. členom KZ-1 (Izdaja in neupravičena pridobitev poslovne skrivnosti). 142. člen KZ-1 pa varuje zasebne informacije posameznikov, s katerimi se seznanijo osebe pri opravljanju svojega poklica, razkritje teh informacij pa bi občutno poseglo v posameznikovo ustavno pravico do zasebnosti.

Kazniva je le izdaja tistih skrivnosti, ki so bile ugotovljene pri opravljanju storilčevega poklica. Kaznivo dejanje po 142. členu KZ-1 ni podano, če storilec izve za skrivnost v zasebni sferi ali po naključju. Skrivnost se lahko nanaša na katerokoli osebo, o kateri storilec pridobi zasebne informacije med opravljanjem poklica. Ne zahteva se torej, da se storilec seznani s skrivnostjo neposredno od osebe, na katero se skrivnost nanaša. Storilec se lahko s skrivnostjo seznani neposredno ustno, prek listin, slik ali drugega gradiva, ki storilcu razkrije neko zasebno informacijo o posamezniku. Če je poklicna oseba vedela določeno informacijo o posamezniku, pa se s to ni seznanila v okviru svojega poklica, še preden ji je to informacijo vnovič nekdo sporočil pri opravljanju poklica, potem izdaja take skrivnosti ni kaznivo dejanje po 142. členu KZ-1. Izdaja poklicne skrivnosti mora biti neupravičena in (s tem) protipravna. Izdaja ni protipravna, če posamezen predpis poklicni osebi zapoveduje določeno ravnanje. Oseba, na katero se podatki, ki pomenijo skrivnost, nanašajo, ima nad njimi neomejeno razpolagalno sposobnost vsaj v smeri sproščanja omejitev pri varovanju: drugo osebo sme odvezati molčečnosti in jo s tem polno pravno veljavno pooblastiti za izdajo teh podatkov. V tem primeru gre za osrednjo dobrino inkriminacije, navaja Možina (2013).

# 5 ANALIZA SODNE PRAKSE NA PODROČJU VARSTVA POSLOVNIH SKRIVNOSTI IN TAJNIH PODATKOV

Vsaka organizacija izvaja svojo politiko zaščite in dostopa do tajnih informacij, poslovnih skrivnosti in informacij javnega značaja, ki morajo biti skladni z določili ZTP in drugimi predpisi, ki so bili izdani na njegovi podlagi (Nacionalni inštitut za javno zdravje 2016). ZTP je »sistemski postopkovni zakon« (Višje delovno in socialno sodišče, v nadaljevanju VDSS 2012), ki ureja dostop do tajnih podatkov, hkrati pa omogoča, da se v sodnih postopkih s tajnimi podatki seznani stranka ali njen pooblaščenec, kar je pokazala sodna praksa v tožbah (VDSS 2012), kjer je sodišče dolžno spoštovati temeljne pravice vseh strank. Pri sporu ne obstaja nikakršna hierarhija, ampak mora sodišče odločiti, kateri stranki bo dodelila pravico in zakaj. V primeru, da bi se v postopku morali razkriti tajni podatki, ki bi lahko ogrozili ustavno ureditev države in splošne človeške vrednote, mora sodišče konflikt rešiti na tak način, da nihče ne bo prikrajšan za bistveno in varovano vsebino, ki bi vplivala na njegovo odločitev (Demšar-Potočnik 2015).

## 5.1 Primeri iz sodne prakse v Republiki Sloveniji

V podatkovni bazi sodne prakse, ki se vodi pri Vrhovnem sodišču RS, so zanimivi nekateri primeri odločb o varovanju tajnih podatkov in poslovnih skrivnostih, ki jih podrobneje povzemamo v nadaljevanju.

### *5.1.1 Zadeva I U 1911/2012*

Bistvo: obveznosti o varovanju zaupnih podatkov ne veljajo, če se v določenem primeru uporablja drugi zakon, in sicer ZJN-3 in ZDIJZ.

Dejansko stanje: primer iz sodne prakse, ko gre za razkrivanje poslovne skrivnosti, se nanaša na dostop do informacij javnega značaja. Upravno sodišče RS (v nadaljevanju UPRS 2013) je 23. 12. 2013 izdalo sodbo št. I U 1911/2012, s katero ni ugodilo zahtevi tožeče stranke po razkritju poslovne skrivnosti banke drugi osebi, in sicer Podjetju A., d. o. o., ki je sodelovalo v postopku javnega naročanja. Zato je ta podala zahtevo, da dostopa do informacij javnega značaja, in sicer do kopije ponudbe in celotne korespondence med tožečo stranko v tem upravnem sporu in družbo B., d. d. Tožeča stranka podjetju A., d. o. o., tega ni omogočila, saj je menila, da obstaja možnost, da so takšni podatki zaupni, saj gre za osebne podatke, bančno tajnost, zaupne podatke revizorja, skladne z 2. in 4. točko 6. člena ZDIJZ.

Predmet spora: družba A., d. o. o., je podala zahtevo za dostop do informacij javnega značaja, in sicer je zahtevala kopijo ponudbe in celotno korespondenco med tožečo stranko v tem upravnem sporu in družbo B., d. d., v postopku oddaje javnega naročila (sodba št. I U 1911/2012).

UPRS (2013) je v obrazložitvi navedlo, da dokumenti v postopkih javnega naročanja rekonstrukcij izvirajo z delovnega področja organa. »Ponudba B., d. d., in korespondenca med naročnikom ter B., d. d., zato predstavlja informacijo, ki izvira z delovnega področja organa, in se nahaja v obliki dokumentov, kjer pa je te dokumente organ pridobil od drugih oseb oziroma jih je izdelal sam« (sodba št. I U 1911/2012).

»Ker je organ na osnovi lastnih izkušenj ugotovil, da obstaja možnost, da so nekateri podatki znotraj ponudbene dokumentacije poslovna skrivnost, osebni podatek, bančna tajnost, zaupni podatki revizorja oziroma zaupni individualni podatki o poročevalskih enotah, je predvsem presojal, ali je podana izjema po 2. točki 6. člena ZDIJZ (torej poslovna skrivnost), 3. točki 6. člena ZDIJZ (torej osebni podatek) in 4. točki 6. člena ZDIJZ (torej zaupnost individualnih podatkov o poročevalskih enotah), izjema tajnosti bančnih podatkov in izjema zaupnosti revizorjevih poročil. Skladno z 2. odstavkom 22. člena ZJN so »javni podatki količina iz specifikacije, cena na enoto, vrednost posamezne postavke in skupna vrednost iz ponudbe, v primeru merila ekonomsko najugodnejše ponudbe pa tisti podatki, ki so vplivali na razvrstitev ponudbe v okviru drugih meril«. Tej odločitvi ni potrdilo UPRS (2013), ki v svoji obrazložitvi navaja, da se postopek do informacij javnega značaja sploh ne more pričeti, če ni pravnomočno končan postopek javnega naročanja. Sedmi odstavek 22. člena ZJN-3 navaja, da mora naročnik javne ponudbe dovoliti vpogled v druge ponudbe in ostalo dokumentacijo, razen če gre za poslovne ali tajne dokumente. Poleg tega je UPRS (2013), ugotovilo, da je zmotno razmišljanje, da se določila ZDIJZ lahko uporabijo šele ko je pravnomočen sklep o javnem naročanju, ampak je to možno takoj, ko se odda javno naročilo. Tožeča stranka lahko zavrne dostop do informacij javnega značaja, če obstajajo zakonske podlage, nikakor pa to ne more storiti, če ji razkritje naloži pravnomočna odločba Informacijskega pooblaščenca. Ko se je tožeča stranka odločila za oddajo javnega naročila, ne more določiti, komu bo dovolila vpogled v bančne izpiske in komu ne. V samem postopku javnega naročila tudi ni navedla, da so podatki poslovna skrivnost in bi z njihovim razkritjem nastala škoda skladno s drugim odstavkom 39. člena Zakona o gospodarskih družbah.

Glede poslovne skrivnosti banke bi ta morala podati oznako na dokumentih, da gre za zaupne podatke skladno z določili 214, 215 in 216. člena Zakon o bančništvu (Uradni list RS, št. 99/2010), kar pa ni bilo storjeno. Tudi obveznosti o varovanju zaupnih podatkov ne veljajo, če se v določenem primeru uporablja drugi zakon, in sicer ZJN-3 in ZDIJZ. Skladno po določilu drugega odstavka 22. člena ZJN-3 morajo javni podatki in poslovne skrivnosti biti dostopni tudi drugim strankam, ki sodelujejo v ponudbah javnega naročanja. Glede na navedeno je UPRS (2013) odločilo, da ne obstajajo dokazi, da dokumenti niso javni oz. da jih ne bi stranka A., d. o. o., tudi pridobila.

### *5.1.2 Zadeva Sodba I U 900/2016-44*

Bistvo: prvi odstavek 5. člena ZDIJZ omogoča dostop do informacij javnega značaja, če ne sodijo podatki med zakonsko določene izjeme. Če bi podatki, ki so bili predmet spora, sodili med te izjeme, bi bili tudi ustrezno zaščiteni in do njih ne bi dostopal nihče razen pooblaščenih oseb.

Dejansko stanje: sodba I U 900/2016-44, ki jo je izdalo UPRS, dne 3. 10. 2018, se prav tako nanaša na informacije javnega značaja, ki pa izvirajo z delovnega področja. Toženka je bila v zadevi dolžna po odločbi št. 9000-4/2015-7, z dne 23. 4. 2015 (UPRS 2016), tožencu razkriti osebne podatke posameznikov, ki so se nanašali na izplačila avtorskih in podjemnih pogodb za obdobje od 1. 1. 2005 do 10. 3. 2015, vendar tega ni storila. Za mnenje se je obrnila na mnenje Informacijskega pooblaščenca, ki je pritožbi delno ugodilo ter postopek vrnilo v ponovno odločanje toženi stranki, in sicer Fakulteti za upravo Ljubljana.

Predmet spora: v konkretnem primeru je sporno, ali informacije, ki jih je zahtevala prizadeta stranka, ne izvirajo z delovnega področja organa in zato ne gre za informacije javnega značaja.

V obrazložitvi sodbe I U 900/2016-44 sodišče ugotavlja, da so v konkretnem primeru bili izpolnjeni pogoji, določeni v tretjem odstavku 6. člena ZDIJZ, zato bi toženka morala dopustiti razkritje osebnih podatkov profesorjev, ki so se nanašali na opravljeno delo skladno z avtorskimi in podjemnimi pogodbami, saj se ti nanašajo na porabo javnih sredstev. Poleg tega so zahtevani podatki pomembni, saj gre za osebe, ki so bile hkrati tudi v delovnem razmerju. S temi ugotovitvami se toženka ni strinjala, saj je menila, da ne gre za porabo javnih sredstev in tudi ni povezave z opravljanjem javne funkcije ali delovnim razmerjem javnega uslužbenca.

UPRS (2016) je v postopku ugotovilo, da je tožničina navedba nepravilna, ko navaja, da ni zavezanka po ZDIJZ, saj ta zakon vsakemu omogoči prost dostop do informacij javnega značaja skladno s prvim odstavkom 1. člena. Poleg tega prvi odstavek 5. člena ZDIJZ omogoča dostop do informacij javnega značaja, če ne sodijo podatki med zakonsko določene izjeme. Če bi podatki, ki so bili predmet spora, sodili med te izjeme, bi bili tudi ustrezno zaščiteni in ne bi do njih dostopal nihče razen pooblaščenih oseb, pa tudi če je podatek pomemben za varstvo pravic in pravne koristi. Zato UPRS(2016) tožeči stranki ni ugodilo.

### *5.1.3 Zadeva VDSS sklep Pdp 727/2012 z dnem 30. 11. 2012*

Bistvo: dostop do tajnih podatkov je omejen in mogoč na način in ob pogojih, določenih z ZTP in s predpisi, izdanimi na njegovi podlagi ter na način in ob pogojih, določenimi z drugimi sistemskimi postopkovnimi zakoni ali mednarodnimi pogodbami, ki jih je sklenila RS.

Dejansko stanje: v individualnem delovnem sporu VDSS sklep Pdp 727/2012, z dnem 30. 11. 2012, je VDSS (2012) odločalo o dostopu do tajnih podatkov stranke in njenem pooblaščencu.

Prvostopenjsko sodišče je namreč odločilo, da pooblaščeni zastopnik (odvetnik) ne more zastopati stranke, dokler ne predloži dovoljenja, da lahko dostopa do tajnih podatkov, ki ga izdaja pristojno ministrstvo, kar naj bi bilo skladno z 22. členom ZTP. Tožena stranka se je na to odločitev prvostopenjskega sodišča pritožila, saj naj bi ji bila kršena določila Ustave RS. Pri tem se je sklicevala na 22. člen. Ustave RS, ki določa pravico do enake obravnave in enakega varstva pravic.

Predmet spora: v konkretni zadevi je sporno, ali pooblaščenec toženih strank, odvetnik A. A., v zadevi ne more zastopati toženih strank, dokler v skladu z 22. členom Zakona o tajnih podatkih ne predloži dovoljenja za dostop do tajnih podatkov stopnje tajno.

Pri odločitvi je sodišče sledilo sodni praksi Evropskega sodišča za človekove pravice v zadevi Matyjek v. Poland application No. 38184/03 ter na odločitev nekdanjega Zveznega ustavnega sodišča SFRJ v zvezi s pravico odvetnikov in do zastopanja v kazenskem postopku, v katerem so bili obravnavani tajni podatki (VDSS sklep Pdp 727/2012 z dnem 30. 11. 2012)

### *5.1.4 Odločbi U I 93/05 z dnem 24. 5. 2017*

Bistvo: omejitve pridobivanja tajnih podatkov ne smejo pomeniti takšne kvalitativne neenakosti med strankama postopka glede možnosti učinkovitega uveljavljanja njunih pravic, da bi šlo za kršenje ustavne pravice, določene v 22. členu Ustave RS.

Dejansko stanje: VDSS (2017) je pritožbi tožene stranke ugodilo, s tem da je sledilo mnenju Ustavnega sodišča, navedenega v odločbi U I 93/05, z dnem 24. 5. 2017. To je namreč odločilo, da je dostop do tajnih podatkov sicer omejen, ampak le po pogojih, ki jih določa ZTP ter drugi predpisi, ki so določeni s sistemskimi postopkovnimi zakoni ali mednarodnimi pogodbami. Sistemski postopkovni zakon, ki ureja dostop do tajnih podatkov, je ZPP, vendar ta ne prepoveduje, da bi se stranka oz. njen pooblaščenec lahko seznanila s tajnimi podatki. Poleg tega je VDSS (2017) navedlo, da omejitve pridobivanja tajnih podatkov ne smejo pomeniti takšne kvalitativne neenakosti med strankama postopka glede možnosti učinkovitega uveljavljanja njunih pravic, da bi šlo za kršenje ustavne pravice, določene v 22. členu Ustave RS. Sodišče je tako ugodilo pritožbi in razveljavilo izpodbijani sklep ter določilo, da ima odvetnik, ki je poklic vrednega zaupanja, pravico do pridobitve do tajnih podatkov. Dejstvo je, da 1. člen 4. odstavka ZTP določa, da je vsak, ki mu je zaupan tajni podatek, odgovoren za njegovo varovanje in ohranjanje tajnosti, kar velja tudi za odvetnika tožene stranke.

Predmet spora: pobudnica izpodbija Zakon o pravdnem postopku (ZPP) in Zakon o tajnih podatkih (v nadaljevanju ZTP). Navaja, da je tožnica v delovnem sporu, v katerem je sodišče na njeno pobudo od tožene stranke zahtevalo predložitev posameznih listin v dokazne namene. Tožena stranka naj bi te listine sodišču sicer predložila, vendar zgolj v enem izvodu, pri čemer naj bi se sklicevala na to, da gre za listine zaupne narave, s katerimi se ima pobudnica možnost

seznaniti le na sodišču v prisotnosti pooblaščene osebe in ob predhodnem podpisu izjave o varovanju tajnosti, njihovo kopiranje pa ji ni dovoljeno. Meni, da ji je na takšen način zagotovljen samo formalen dostop do sodišča in da ji v postopku niso zagotovljene enake možnosti kot toženi stranki. Hkrati navaja, da ZTP in ZPP sploh ne urejata vprašanj v zvezi z možnostjo dostopa pravdnih strank do listin s tajno vsebino oziroma vprašanj v zvezi z dopustnostjo uporabe takšnih listin v sodnih postopkih. ZTP še očita, da omogoča arbitrarno odločanje o tem, kateri podatki se lahko opredelijo kot tajni. Zatrjuje neskladje izpodbijane ureditve z načeli pravne države (URS, 2. člen) z načelom enakosti pred zakonom (URS, 14. člen, 2. odstavek) in s pravico do enakega varstva pravic (URS, 22. člen).

### *5.1.5 Zadeva Sklep I Cpg 977/2017*

Bistvo: že sama objava tajnih podatkov je prepovedana, izdaja tajnih podatkov pa je tudi kaznivo dejanje. Tako ravnanje je tako protipravno.

Dejansko stanje: Višje sodišče v Ljubljani je 19. 12. 2017 izdalo Sklep I Cpg 977/2017 (Višje sodišče v Ljubljani, Gospodarski oddelek 2017), s katerim je potrdilo sklep sodišča prve stopnje, s katerim je bilo določeno, da mora dolžnik takoj prenehati z objavo listin iz sodnega spisa II K 38943/2010 in z navajanjem vsebine teh listin tudi na njegovi spletni strani. Ker se stranka s sklepom prvostopenjskega sodišča ni strinjala, se je pravočasno pritožila na višje sodišče, ki pa je njeno pritožbo zavrnilo. Dejstvo je, da je objava tajnih podatkov prepovedana, njena izdaja pa kazniva. Tudi ravnanje s tajnimi podatki je protipravno ne glede na to, ali je dolžnik zavestno tako ravnal ali ne. Najbolj pomembno je, da se tajne podatke zavaruje in se jih ne posreduje javnosti, razen če za to obstaja utemeljen primer (Višje sodišče v Ljubljani, Gospodarski oddelek 2017).

Predmet spora: v konkretnem primeru je sporno, ali je ravnanje s tajnimi podatki protipravno ne glede na to, ali je dolžnik zavestno tako ravnal ali ne.

Da bi se zagotovila učinkovita in enotna uporaba zakonodaje EU in da bi se izognili vsakršnemu odstopanju, se lahko nacionalni sodniki obrnejo − včasih se morajo − na Sodišče EU s predlogom za razjasnitev kakega vidika razlage prava EU (predhodno vprašanje), da bi lahko na primer preverili skladnost svoje nacionalne zakonodaje s tem pravom. Predlog za sprejetje predhodne odločbe je lahko namenjen tudi nadzoru veljavnosti pravnih aktov EU. Sodišče ne odgovori le s preprostim mnenjem, ampak s sodbo ali z obrazloženim sklepom. Nacionalno sodišče je kot naslovnik odločbe pri obravnavanju spora vezano na dano razlago. Vendar gre povedati, da so sodbe sodišča EU zavezujoče tudi za druga nacionalna sodišča, ki bi odločala o enaki težavi.

## 5.2 Primeri iz sodne prakse v Evropski uniji

Sodna praksa EU, ki bo v nadaljevanju predstavljena, sicer ne vsebuje primera, kjer je bilo postavljeno predhodno vprašanje, so pa predstavljeni primeri, ko so bili sproženi postopki proti institucijam EU zaradi ničnosti in zaradi opustitve ukrepanja, predvsem postopki zoper EK. Predstavljeni so predvsem primeri, ko tožnik zahteva, da se ukrep, ki naj bi bil v nasprotju s pravom EU, razglasi za ničnega skladno z 263. členom Pogodbe o delovanju Evropske unije (PDEU, Ur. l. EU C 326, 2012), ali v primeru kršitve prava EU, ko institucija, organ, urad ali agencija opustijo ukrepanje (PDEU, 265. člen). Postopke lahko sprožijo države članice, same institucije oziroma vsaka fizična ali pravna oseba, če se nanašajo na ukrep (zlasti uredbo, direktivo ali sklep), ki ga sprejmejo institucija, organ, urad ali agencija in je naslovljen nanje. Sodišče akt razglasi za ničnega ali ugotovi, da je bilo opuščeno ukrepanje, skladno s 266. člen PDEU. Ta navaja, da mora odgovorna institucija sprejeti ukrepe, ki so potrebni za izvršitev sodbe Sodišča EU. Skrb Sodišča EU je, da bi si vse države EU enako razlagale pravo EU. Naloga Sodišča EU je še reševanje pravnih sporov, ki bi nastali med državami članicami in institucijami EU, pa tudi tožb, ko jih vložijo posamezniki, podjetja in druge organizacij proti instituciji EU v primeru kršenja njihovih pravic (Sodišče Evropske unije 2020).

Dejstvo je, da nacionalna sodišča držav EU morajo skrbeti za pravilno uporabo prava EU, vendar se lahko zgodi, da ga v različnih državah različno razlagajo. Če je nacionalno sodišče v dvomih glede razlage ali veljavnosti zakonodaje EU, lahko zaprosi za pojasnilo Sodišče EU. Po enaki poti lahko tudi preveri, ali je nacionalni predpis ali praksa v skladu s pravom EU. Na sodišču EU nastaja sodna praksa, ki je poleg primarne in sekundarne zakonodaje vir pravnega reda EU.

Sodišče EU pri svojem delu sodeluje z drugimi sodišči iz držav članic EU, ki so pristojna za delo s področja prava EU. Ker je pomembno zagotavljati učinkovitost in enotnost uporabe evropske zakonodaje ter v izogib kakršnimkoli odstopanjem, se lahko oz. se včasih tudi morajo, nacionalni sodniki obrniti na Sodišče EU za pomoč zaradi razjasnitve kakšnega vidika pravne razlage EU. Na tak način nacionalni sodniki preverijo skladnost svoje zakonodaje s evropskim pravom. Sodišče EU nacionalnemu sodišču odgovori s sodbo ali z obrazloženim sklepom, kar mora nacionalno sodišče upoštevati v primerih, ki so vezana na podano obrazložitev sklepa. Takšen sklep je zavezujoč tudi »za druga nacionalna sodišča, ki bi odločala o enakem problemu« (Evropsko sodišče 2020).

### *5.2.1 Zadeva C-3/88*

Bistvo: Italija kot država članica EU mora omogočiti enako obravnavo vsem podjetjem ne glede na to, iz katere države članice prihajajo. Po drugi strani je treba opozoriti, da je mogoče obdelovanje zaupnih podatkov in varovanje tajnosti zaščititi, ne da bi bilo treba omejiti svobodo enake obravnave.

Dejansko stanje: izdana sodba Evropskega sodišča, z dne 5. 12. 1989 v zvezi z odločitvijo Komisije Evropske skupnosti (KES, 1989) proti Italiji, se nanaša na kršitev načela enake obravnave, 52. in 59. člena Pogodbe Evropske gospodarske skupnosti (Pogodba EGS) (Evropska gospodarska skupnost 1957) in Direktive Sveta 77/62 / EGS, z dnem 21. decembra 1976, o usklajevalnih postopkih za oddajo javnih naročil blaga (1977, Ur.1. EU 1, L 13, str. 1). Skladno s sodno prakso je KES (1989) poudarila, da 52. in 59. člen Pogodbe EGS prepoveduje diskriminacijo, zato je Italijo opozorila, da ne smejo sprejeti zakoni in uredbe biti v korist le italijanskim podjetjem, ampak tudi drugim podjetjem izven meja Italije. Italijanska vlada je navajala, da gre pri tem za razkrivanje zaupnih podatkov, zato naj bi pogodbe bile sklenjene le s tistimi podjetji, ki uživajo njihovo zaupanje, predvsem ker gre za vzpostavitev delovanja informacijskega sistema. S takšno ugotovitvijo se KES (1989) ni strinjala, saj se zadeve nanašajo na oblikovanje, opredelitev programov in upravljanje informacijskih sistemov, kar pomeni, da je tehnične narave in niso povezani z izvajanjem javnih pooblastil. Italija kot država članica EU mora omogočiti enako obravnavo vsem podjetjem ne glede na to, iz katere države članice prihajajo. Po drugi strani je treba opozoriti, da je mogoče obdelovanje zaupnih podatkov in varovanje tajnosti zaščititi, ne da bi bilo treba omejiti svobodo enake obravnave. Poleg tega je javno naročilo možno tudi ločiti, na eni strani je to lahko nakup opreme, ki je potrebna za oblikovanje informacijskega sistema, na drugi strani pa njegovo načrtovanje in upravljanje.

### *5.2.2 Zadeva T-334/94 je Sarrió SA*

Bistvo: izmenjava posameznih poslovnih informacij je že sama po sebi pomenila kršitev 85. člena 1. odstavka Pogodbe Evropske gospodarske skupnosti (Pogodba ES, 2012), tudi prihodnja prepoved take izmenjave informacij izpolnjuje pogoje, ki se zahtevajo za uporabo 3. člena 1. odstavka Uredbe sveta št. 17 (UL 13).

Dejansko stanje: v zadevi T-334/94 je Sarrió SA, družba španskega prava, s sedežem v Pamploni, Španija, sprožila predlog proti Komisiji Evropske skupnosti, da ugotovi ničnost Odločbe Komisije Evropske skupnosti št. 94/601 (Odločba Komisije), z dnem 13. julija 1994 zaradi kršitve 85. člena Pogodbe ES (IV/C/33.833 – Carton) (UL L 243, str. 1). Sodišče je delno ugodilo tožeči stranki. Odločilo je, da se določbe točk a, b., in c. prvega odstavka 2. člena Odločbe Komisije podrobneje nanašajo na prepovedi prihodnjih izmenjav poslovnih informacij. Določila iz točke a prvega odstavka 2. člena, ki v prihodnje prepoveduje kakršnokoli izmenjavo poslovnih informacij, iz katerih bi lahko udeleženci posredno ali neposredno pridobili posamezne podatke o konkurenčnih družbah, predpostavlja, da je Komisija v Odločbi ugotovila nezakonitost izmenjave takih informacij glede na prvi odstavek 85. člena Pogodbe (Sodišče prve stopnje Evropskih skupnosti 1998).

### *5.2.3 Zadeva T-109/05 in T-444/05*

Bistvo: pri presoji zaupnosti informacije je treba tehtati med legitimnimi interesi, ki nasprotujejo njenemu razkritju, in splošnim interesom, ki zahtevajo, da dejavnosti institucij Skupnosti potekajo čim bolj javno.

Dejansko stanje: v združenih zadevah T-109/05 in T-444/05 je potekal postopek med Navigazione Libera del Golfo Srl (v nadaljevanju NLG), prej Navigazione Libera del Golfo SpA, s sedežem v Neaplju (Italija), proti Evropski komisiji. Njen predlog se je nanašal na razglasitev ničnosti odločb Komisije Evropske skupnosti (2005) 997, z dnem 3. februarja 2005, in D(2005) 9766, z dnem 12. oktobra 2005. Tožeči stranki je bil zavrnjen dostop do nekaterih podatkov, ki jih je navajala Odločba Komisije, z dnem 16. marca 2004, o državni pomoči, ki jo je Italija izplačila ladjarskim podjetjem Adriatica, Caremar, Siremar, Saremar in Toremar (skupina Tirrenia) (2005/163/ES) (Sodišče prve stopnje Evropskih skupnosti 2005). V tem primeru je šlo razkritje poslovne skrivnosti, zato je Komisija EU pritožbo NLG zavrnila. Komisija EU je odločila, da gre za informacije, ki so poslovna skrivnost in bi njihovo razkritje javnosti ali zgolj njihovo posredovanje drugemu pravnemu subjektu, ki teh informacij ni zagotovil, lahko resno škodilo interesom osebe, ki je te informacije dala. Nujno je, da so interesi, ki jim razkritje informacije lahko povzroči škodo, objektivno vredni zaščite. Pri presoji zaupnosti informacije je treba tehtati med legitimnimi interesi, ki nasprotujejo njenemu razkritju, in splošnimi interesi, ki zahtevajo, da dejavnosti institucij Skupnosti potekajo čim bolj javno.

Z izpodbijanjem te odločbe NLG meni, da je bila Komisija v hudi pravni zmoti, saj je očitno spregledala določbe, ki so navedene v njenem sporočilu K(2003) 4582, z dnem 1. decembra 2003, o poslovni skrivnosti v odločbah na področju državnih pomoči, ki v točki 17 izrecno določajo transparentnost in javnost podatkov ter informacij o stroških javnih služb, če se ti ne štejejo za zaupne in krite s poslovno skrivnostjo. Vendar so take informacije lahko poslovna skrivnost, če se nanašajo na poslovanje, imajo dejansko ali potencialno tržno vrednost, njihovo razkritje ali uporaba pa bi prinesla tržne koristi drugim podjetjem (Splošno sodišče Evropske unije 2011).

### *5.2.4 Zadeva T-48/05*

Bistvo: dejstvo, da je bil del zaupnega spisa preiskave verjetno nezakonito poslan tisku, samo po sebi ne upravičuje odstopanja od zaupnosti tega spisa in od preiskave, ki jo vodi Evropski urad za boj proti goljufijam (ang. European Anti-Fraud Office, v nadaljevanju OLAF), v korist domnevno prizadetega uradnika.

Dejansko stanje: zadeva T-48/05 se nanaša na tožbo Yvesa Francheta in Daniela Byka proti Komisiji Evropskih skupnosti (vloženo 28. januarja 2005), ki sta sodišču predlagala, da določi

plačilo škode v višini enega milijona evrov, saj naj bi bil OLAF kriv za kazniva dejanja glede ravnanja z določenimi spisi o Evrostatu. OLAF naj bi posredoval spise o obdolžitvi francoskemu in luksemburškim sodnim organom, pri tem pa naj ne bi obvestil niti tožeče stranke niti Komisije in s tem razkril zaupne podatke skladno z 9. členom Uredbe 1073 o načelu dobre uprave (Sodišče prve stopnje Evropske unije 2005).

V skladu s 5. odstavkom 6. čl. Uredbe št. 1073/1999 Evropskega parlamenta in Sveta z dne 25. maja 1999 o preiskavah, ki jih izvaja Evropski urad za boj proti goljufijam (OLAF) (Uradni list L 136) mora biti trajanje preiskave sorazmerno okoliščinam in kompleksnosti prime. Nadaljnje 8. čl. iste Uredbe v prvem odstavku določa, da se podatki, v kakršnikoli obliki, pridobljeni med zunanjo preiskavo, varujejo v skladu z ustreznimi določbami, medtem ko drugi odst. istega člena določa, da se podatki v kakršnikoli obliki poslani ali dobljeni med notranjimi preiskavami, obravnavajo kot poslovna skrivnost in se varujejo v skladu z določbami, ki veljajo za institucije Evropskih skupnosti.

Poslovne skrivnosti ureja tudi Uredba EU št. 575/2013 Evropskega parlamenta in Sveta (z dnem 26. junija 2013) o bonitetnih zahtevah za kreditne institucije in investicijska podjetja ter o spremembi Uredbe Evropskega parlamenta in sveta o bonitetnih zadevah za kreditne institucije in investicijska podjetja ter o spremembi Uredbe št. 648/2012 Evropskega parlamenta in Sveta, z dne 4. julija 2012 o izvedenih finančnih instrumentih OTC, centralnih nasprotnih strankah in repozitoriji sklenjenih poslov , kjer 431. člen določa področje uporabe zahtev glede razkritja, medtem ko 2. odstavek 432. člen navaja pod nekaterimi pogoji je dovoljena opustitev razkritja podatkov, ki so poslovna skrivnost ali so zaupni.

Tudi Direktiva 2003/98/ES Evropskega parlamenta in Sveta (2003), z dnem 17. novembra 2003, o ponovni uporabi informacij javnega sektorja opredeljuje poslovno skrivnost. V prvem delu (1. člen in 2.c člen, tretja alineja) dopušča neomejen (absoluten) dostop do vseh podatkov iz avtorskih in svetovalnih pogodb, tudi če so te pogodbe opredeljene kot poslovna skrivnost. Predložitveno sodišče navaja, da ta zakonska določba velja le za subjekte pod prevladujočim vplivom države. Drugi del vprašanja se nanaša na to, ali na razlago Direktive vpliva Uredba št. 575/2013.

V skladu s to določbo se Direktiva 2003/98/ES ne uporablja za dokumente, do katerih ni dostopa na temelju nacionalne zakonodaje. Razlog za to je prav dejstvo, da je ponovna uporaba (na osnovi Direktive) mogoča le, kadar je do dokumentov mogoče dostopati (na osnovi nacionalne zakonodaje). Torej bi dejstvo, da so v 1. členu 2. odstavka, c točke, tretja alineja, te direktive „poslovne tajnosti (npr. poslovne ali poklicne skrivnosti oziroma skrivnosti podjetja)“ navedene kot eden od primerov.

### *5.2.5 Zadeva C/517/75*

V zadevi C/517/75 so družbe P-R AGC Glass Europe sprožile postopek proti Evropski komisiji, da bi se razveljavila sodba Splošnega sodišča EU (tretji senat, 2015), z dnem 15. julija 2015, (T-465/12), s katero je bila zavrnjena tožba za razglasitev ničnosti Sklepa Komisije C(2012) 5719, z dnem 6. avgusta 2012, ter hkrati tudi izdana začasna odredba na osnovi Pogodbe EGS (278. in 279. člen), s katero bi tožeče stranke dosegle odložitev izvršitve izpodbijanje sodbe in spornega sklepa (Sodišče Evropske unije 2016). Iz potrjene sodbe Splošnega sodišča v zadevi T-465/12 z dne 15. 7. 2015 izhaja, da je Generalni direktorat (v nadaljevanju: GD) Komisije za konkurenco po korespondenci s tožečimi strankami AGC Glass, decembra 2011 sprejel nezaupno različico odločbe o avtomobilskih steklih, ki se bo objavila na spletnem mestu Komisije. Iz zadevne korespondence je razvidno, da GD za konkurenco ni ugodil predlogom tožečih strank naj prekrije informacije v 246 točkah obrazložitve in 122 opombah odločbe o avtomobilskih steklih. GD za konkurenco meni, da je mogoče te informacije razdeliti v tri kategorije. Prva zajema imena strank in opis zadevnih proizvodov ter vsako informacijo, na podlagi katere bi bilo mogoče prepoznati stranko (informacije I. kategorije). druga zajema količine dobavljenih delov, dodelitev kvot vsakemu proizvajalcu avtomobilov, sporazume o cenah, njihov izračun in razlike ter nenazadnje številke in odstotke, povezane z dodelitvami strank med udeleženci kartela (informacije II. kategorije). Tretja zajema popolnoma administrativne informacije, ki napotujejo na dokumente v spisu (informacije III. kategorije). Pooblaščenec za zaslišanje je o predlogu tožečih strank odločil z Odločbo Komisije C(2012) 5719 final z dne 6. 8. 2012 o zavrnitvi prošnje za zaupno obravnavanje, ki so jo vložile tožeče stranke. V uvodu je pooblaščenec za zaslišanje navedel, da Obvestilo Komisije o imuniteti pred globami in znižanju glob v kartelnih zadevah pri tožečih strankah ne ustvarja legitimnih pričakovanj, ki bi Komisiji preprečevale objavo informacij, ki niso poklicna skrivnost. Nadaljnje je pooblaščenec navedel, da so informacije I. kategorije, ki zajemajo imena strank in opis zadevnih proizvodov, zaradi svoje narave in ob upoštevanju posebnosti trga avtomobilskih stekel znane tudi drugim osebam poleg tožečih strank, da so zastarele ter da so povezane s samim bistvom kršitve, njihovo razkritje pa narekujejo interesi oškodovanih oseb (Splošno Sodišče – šesti senat, 2017).

Ob taki objavi naj bi namreč lahko do teh informacij dostopale in jih uporabljale tretje osebe, zlasti tako, da bi iz njih izpeljale druge poslovne podatke, kot so izračuni cen, spremembe cen in druge finančne informacije, katerih anonimnost potem ne bi bila več zagotovljena. Zato naj bi ta objava pritožnicam povzročila resno in nepopravljivo škodo, ki je dovolj predvidljiva in verjetna. V smislu Direktive EU 2016/943 Evropskega parlamenta in Sveta z dne 8. junija 2016 o varstvu nerazkritega strokovnega znanja in izkušenj ter poslovnih informacij (poslovnih skrivnosti) pred njihovo protipravno pridobitvijo, uporabo in razkritjem pomeni, da nedovoljena pridobitev, uporaba ali razkritje strokovnega znanja in izkušenj škoduje interesom imetniku teh znanj, prav tako pa tudi njegovim znanstvenim in tehničnim potencialom, konkurenčni sposobnosti, strateški poziciji kot tudi poslovnim interesom.

Predmet spora: v primeru škode, ki jo je povzročilo podjetje zaradi storitve kršitve pravil Unije o konkurenci, Komisija pa je v okviru preganjanja te kršitve razkrila nekatere informacije o imenih strank in opisu zadevnih proizvodov, odločilni vzrok za škodo, ki je bila povzročena tretjim osebam in katere povrnitev se zahteva z odškodninskimi tožbami, ni razkritje informacij s strani Komisije, ampak kršitev konkurenčnega prava, ki jo je storilo kaznovano podjetje. Čeprav te informacije dejansko lahko olajšajo predložitev dokaza tožečim strankam, ki zahtevajo odškodnino od kaznovanega podjetja, če te informacije navedenim tožečim strankam zagotavljajo dokaze, na katere se sicer ne bi mogle sklicevati, taka okoliščina Komisiji vseeno ne prepoveduje razkritja informacij zgolj zato, ker bi te lahko pomenile take dokaze in posledično škodile položaju kaznovanega podjetja. To bi namreč pomenilo, da bi se od Komisije zahtevalo, naj ohrani informacije zaupne zgolj z namenom zaščititi interes, ki ga imajo naslovniki odločbe, s katero je ugotovljen obstoj kršitve pravil konkurenčnega prava Unije, za onemogočenje dostopa do zadevnih dokazov tožečim strankam, ki bi zahtevale odškodnino. Čeprav se v pravu Unije priznava pomen tega interesa, zlasti v okviru pravice do obrambe v tovrstnih tožbah, ostaja dejstvo, da se po eni strani Komisiji z nobenim pravilom prava Unije ne nalaga, naj zaščiti tak interes z ohranjanjem zaupnosti informacij, kot so zadevne informacije, v nasprotju z obveznostjo preglednosti, ki ji je naložena s členom 15 PEU (2012), natančneje v obravnavanem primeru s 30. členom Uredbe Sveta (ES) št. 1/2003 z dne 16. december 2002 o izvajanju pravil konkurence iz členov 81. in 82. Pogodbe o delovanju Evropek unije (2012). Po drugi strani 5. člen 5. odstavka Direktive 2014/104 o nekaterih pravilih, ki urejajo odškodninske tožbe po nacionalnem pravu za kršitve določb konkurenčnega prava držav članic in Evropske unije, izrecno določa, da interes podjetij, da se po kršitvi konkurenčnega prava izognejo odškodninskim tožbam, ne predstavlja interesa, ki bi ga bilo treba zaščititi.

### *5.2.6 Zadeva T 15/02*

Bistvo: poslovna skrivnost in načelo učinkovitega upravljanja.

Predmet spora: ali sodita značaj in višina predlagane sankcije v postopkih, v katerih se lahko izreče globa, v okvir poslovne skrivnosti, dokler sankcija ni dokončno potrjena in razglašena?

Dejansko stanje: zadeva T 15/02 se nanaša na tožbo BASF AG s sedežem v Ludwigshafenu (Nemčija) proti Komisiji Evropskih skupnosti. Tožeča stranka opozarja na to, da je Sodišče prve stopnje v sodbi, z dnem 6. julija 2000, v zadevi Volkswagen proti Komisiji (T-62/98, Recueil, str. II-2707, točka 281) razsodilo, da sodita značaj in višina predlagane sankcije v postopkih, v katerih se lahko izreče globa, v okvir poslovne skrivnosti, dokler sankcija ni dokončno potrjena in razglašena. Dodaja, da v smislu navedene sodbe to načelo izhaja zlasti iz potrebe po spoštovanju ugleda in dostojanstva zainteresirane osebe, dokler ni bila obsojena, ter ne ustreza samo dolžnosti spoštovanja poklicne tajnosti, ampak tudi dolžnosti učinkovitega upravljanja (Sodišče prve stopnje Evropskih skupnosti 2003).

### *5.2.7 Zadeva T-341/12*

Predmet spora: v kakšnem obsegu so informacije poslovne skrivnosti ali bi morale biti obravnavane zaupno na kaki drugi podlagi; sporne informacije so poslovna skrivnost ali vsaj zaupne poslovne informacije.

Dejansko stanje: v zadevi T-341/12 je tožnik Evonik Degussa GmbH s sedežem v Essnu (Nemčija) vložil tožbo proti EK za razglasitev ničnosti Sklepa Komisije C(2012) 3534, z dnem 24. maja 2012, o zavrnitvi prošnje za zaupno obravnavanje. Svojo tožbo je utemeljil s petimi razlogi, med katere je tudi navedel kršitve poslovnih skrivnosti in zaupnih informacij. Sodišče je tožbo v celoti zavrnilo, saj je menilo, da v konkretnem primeru ni šlo za razkritje poslovnih skrivnosti. Dejstvo je, da mora pooblaščenec za zaslišanje delovati kot neodvisen arbiter, ko poskuša »razrešiti vprašanja, ki negativno vplivajo na učinkovito uveljavljanje procesnih pravic zadevnih strank, drugih udeleženih strank, pritožnikov ali zainteresiranih tretjih oseb, kadar jih ni bilo mogoče razrešiti v predhodnih stikih s službami Komisije, odgovornimi za vodenje postopkov o konkurenci, ki morajo spoštovati te procesne pravice.« (Sodišče Evropske unije 2011), kot to določa 8. člen Sklepa predsednika Evropske komisije z dne 13. oktobra 2011 o funkciji in mandatu pooblaščenca za zaslišanje v nekaterih postopkih o konkurenci (2011/695/EU). Glede na navedeno pooblaščenec sam sprejme sklep, katere informacije so poslovna skrivnost ali zaupne narave. Pooblaščenec je dolžan, poleg tega, da prouči dokumente, ki so zaupne narave, proučiti tudi druge informacije, katerih se ne sme razkriti, skladno z načeli EU, ki jih določa Uredba Sveta (ES) št. 1/2003 z dne 16. decembra 2002 (o izvajanju pravil konkurence iz členov 81 in 82 Pogodbe o gospodarski skupnosti (2012), saj lahko gre za dokumente, ki so poslovna skrivnost.

# 6 RAZISKAVA UREJENOSTI PS/TP Z INTERNIM AKTOM LOKALNIH SKUPNOSTI/OBČINE

Za analizo pravne urejenosti poslovnih skrivnosti in zaupnih tajnih podatkov v lokalni skupnosti so predstavljene tri lokalne skupnosti, ki so sprejele interni pravilnik s tega področja, in sicer so to občine Kranjska Gora, Šentjernej in Preddvor. Od Občine Kranjska Gora je navedeni pravilnik bil pridobljen po elektronski pošti, medtem ko sta ga občini Šentjernej in Preddvor objavili na svoji spletni strani.

## 6.1 Analiza urejenosti PS/TP v treh občinah

Področje varovanja poslovnih skrivnosti in uradne tajnosti je *Občina Kranjska Gora* (v nadaljevanju Občina KG) uredila s Pravilnikom o varstvu osebnih in zaupnih podatkov. Pri tem je dokumente razdelila v dve kategoriji, in sicer kot »uradna tajnost« in »poslovna tajnost«.

Za uradno in poslovno tajnost je Občina KG določila vse listine in podatke, ki so z zakonom ali drugimi splošnimi akti ter s sklepom župana tako pomembni, da bi njihovo razkritje lahko imelo hujše posledice za Občino KG. Stopnjo zaupnosti pri uradni in poslovni tajnosti določa župan. Podatki, ki imajo oznako uradna tajnost, se nanašajo na štiri področja, in sicer na delovanje civilne zaščite, delovanje nadzornega odbora občine, notranjo kontrolo in revizijo ter prenesenih pristojnosti opravljanja nalog na lokalno skupnost (Občina Kranjska Gora 2005).

Podatki, ki so določeni za poslovno tajnost, se nanašajo na listine in poslovne podatke, ki so določeni z zakonom ali drugim splošnim aktom občine ter imajo oznako »zaupno«. Stopnjo zaupnosti določi župan. Kot poslovna tajnost so to lahko strokovna navodila za opravljanje delovnih nalog, delovni materiali za predpise iz pristojnosti občine in delovna gradiva za občinski svet in odbore pri občinskem svetu (Občina Kranjska Gora 2005).

*Občina Šentjernej* (2010) je področje tajnih zaupnih podatkov uredila v Pravilniku o določitvi, ravnanju in varovanju zaupnih podatkov, ki je bil nazadnje sprejet 1. 2. 2010. V njem je Občina Šentjernej (2010) podatke razdelila v tri kategorije, ki so:

- »zaupen podatek«, kamor so uvrščeni dokumenti z delovnega področja občine in bi njihovo razkritje predstavljalo škodljive posledice zanje. To so dokumenti, ki so bili bodisi napisani, narisani, natisnjeni, razmnoženi, posneti ali fotografirani, lahko pa so tudi optičen ali kakšen drugačen zapis;
- »tajen podatek« se nanašajo na javno varnost, obrambo, zunanje zadeve, obveščevalne in varnostne dejavnosti države, ki so varovani skladno z ZTP. Oznako tajen podatek določi za to pooblaščena oseba, saj je dokumente treba zavarovati pred nepoklicanimi osebami;
- »poslovna skrivnost«, kamor so uvrščeni vsi materializirani (zapisi, načrti, sheme, diagrami, ipd.) in nematerializirani (vsako ustno seznanjanje s podatki, idejami, razgovori ipd.) podatki, informacije in stvaritve, določene z veljavno zakonodajo, s pravilnikom in z

drugimi akti občine ali s sklepom uprave oz. z dokumenti, ki jih pooblaščena oseba razglasi za poslovno skrivnost in so pomembni za Občino Šentjernej.

Med zaupne podatke je Občina Šentjernej (2010) uvrstila tudi osebne podatke zaposlenih, poslovne ali interesne podatke partnerjev in pogodbenih strank ter drugih oseb, za katere občina zbira podatke. Poleg tega so kot zaupni podatki označeni tudi dokumenti s področja varovanja in zaščite ter vsi ostali podatki, ki jih s sklepom določi Občina Šentjernej.

Podatki, ki imajo oznako poslovna skrivnost, so dokumenti, ki jih določa pravni red (zakoni, pravilniki) in še drugi, ki se nanašajo na uspešno delo občine. Med te je Občina Šentjernej (2010) uvrstila strateške odločitve poslovanja občine, finančne in denarne tokove ter likvidnost in solventnost občine, poslovne pogodbe in vsebine poslovnih razgovorov do sklenitve poslovne pogodbe, aktivnosti, ki se vodijo po Zakonu o javnem naročanju, ponudbe za naročila ali licitacije, dokler ni javno objavljen izid naročanja, načrtovanje in izvajanje razvojnih, raziskovalnih, projektnih, analitskih aktivnosti in njihove rezultate, gesla in kode za vstop v računalniške programe ter šifriranje, podatke v zvezi s poslovanjem in zaposlenostjo pogodbenih strank ter druge podatke, ki jih kot poslovno skrivnost določi župan, občinska uprava ali pooblaščena oseba.

*Občina Preddvor* (2002) je področje varovanja tajnih podatkov in poslovnih skrivnosti tako kot preostali dve občini uredila s Pravilnikom o varovanju zaupnih in osebnih podatkov ter o varovanju dokumentarnega gradiva v občinski upravi Občine Preddvor leta 2002 (2002). Navedeni pravilnik je sicer prenehal veljati 30. 9. 2009, vendar smo ga kljub temu uporabili pri analizi urejenosti poslovnih skrivnosti in tajnih podatkov, saj nov še ni objavljen. V navedenem pravilniku je Občina Preddvor (2002) področje poslovnih skrivnosti in tajnih podatkov uredila na naslednji način:

- z oznako »zaupen podatek« se označijo tisti podatki, katerih razkritje bi imelo škodljive posledice za delovanje občinske uprave;
- »osebni podatek« je tisti, ki se nanaša na posameznika ne glede na to, kako je podatek izražen;
- »zbirka podatkov« zajema zbirko, kjer so zajeti zaupni in osebni podatki in se vodijo bodisi s sredstvi za avtomatsko obdelavo podatkov ali na klasičen način ter so pomembni pri izvajanju nalog občinske uprave;
- »tajni podatki«, ki zajemajo:
  - »državno tajnost«, kjer pa ne gre za podatke skladne z ZTP. Kljub temu so podatki tako pomembni, da bi z njihovim razkritjem nastale škodljive posledice za varnost države ali njene politične ali gospodarske korist;
  - »uradno tajnost« − zajemajo pomembne dokumente za Občino Preddvor. Če bi prišlo do njihovega razkritja, bi s tem lahko nastala veliko škoda za delovanje in delo organov občine. Podatkom, ki so uradna tajnost, določijo tudi stopnje zaupnosti, kot so:

- »strogo zaupno«, kamor Občina Preddvor uvršča načrte nalog, ukrepov zavarovanja in varnostnih ukrepov v primeru vojne nevarnosti in tudi evidence gesel uporabnikov in gesla supervizorjev;
- »zaupno« so označeni različni dokumenti, kot so gradiva in zapisniki kolegija, kadrovske in zdravstvene dokumentacije vsakega zaposlenega na Občini Preddvor, nato še vsa dokumentacija o preizkusu strokovnega znanja delavcev občine, letni programi dela in letna poročila posameznih delavcev občine, evidenca disciplinskih ukrepov delavcev občine in izvorni zapis programske opreme, ki je izdelana za lastne potrebe;
- »interno« gradivo – tako se označijo strokovna navodila za opravljanje delovnih nalog, navodila za uporabo zbirk zaupnih podatkov, delovni materiali za odloke in druge predpise, ki jih pripravlja občina, analitična, statistična in druga gradiva o delu oziroma težavah in pojavih, ki so namenjeni internemu informiranju in interni imeniki;
- »osebni podatki«, ki se obdelujejo le skladno z zakoni ali če to pisno privoli posameznik. Z osebnimi podatki morajo zaposleni ravnati enako kot s podatki, ki imajo »uradno tajnost«, kjer je treba ločiti med strogo zaupne dokumente, zaupne ali interno. Kakšna je stopnja zaupnosti zbirke osebnih podatkov, določi tajnik občine, vendar se te varujejo s stopnjo zaupnosti, ki ima enako težo kot »uradna tajnost − zaupno«.

## 6.2 Razprava

Na osnovi analize pravilnikov treh lokalnih skupnosti ugotavljamo, da na tem področju velja velika zmeda, saj se pri vseh mešajo pojmi in pomen tako poslovnih skrivnosti kot tajnih oz. zaupnih podatkov. Skupno pri vseh treh občinah je, da je varovanje poslovnih skrivnosti in tajnih podatkov urejeno z internimi pravilniki. Enotno pri vseh treh pravilnikih je njihov naslov, ki omenja varovanje osebnih in zaupnih podatkov. Prav tako vse tri lokalne skupnosti v pravilnikih navajajo poslovne skrivnosti in tajne podatke, vendar jih je vsaka poimenovala drugače, in sicer Občina KG navaja le uradno tajnost in poslovno tajnost, Občina Šentjernej je podatke razdelila na zaupne, tajne podatke in poslovno skrivnost, medtem ko jih je Občina Preddvor razdelila na zaupne, osebne, zbirke podatkov in tajne zaupne podatke, ki jih je dodatno razdelila na državno tajnost, uradno tajnost, uradno tajnost – strogo zaupno, uradno tajnost – zaupno, uradno tajnost – interno in osebne podatke. Enotno pri pravilnikih je to, da med tajne podatke uvrščajo dokumente, ki se nanašajo na javno varnost, obrambo občine (civilno zaščito), obveščevalne in varnostne dejavnosti delovanja državnih organov, kar je skladno z ZTP. Na splošno pa smo ugotovili velike pomanjkljivosti v vseh treh pravilnikih, kar podrobneje pojasnjujemo v nadaljevanju.

Med dokumente, ki se nanašajo na poslovno skrivnost, občine uvrščajo varovanje osebnih podatkov, kar ni pravilno. Osebni podatek namreč nima tržne vrednosti, poleg tega zanje velja čisto druga pravna podlaga, in sicer Zakon o varstvu osebnih podatkov (Uradni list RS, št. 94/07,v nadaljevanju ZVOP-1 (ne pa ZPosS). Tudi ne držijo navedbe, da so poslovna skrivnost delovni materiali, predpisi iz pristojnosti občin, delovna gradiva občinskega sveta in njegovih odborov, strategije odločitev poslovanja, finančni in denarni tokovi, aktivnosti okoli javnega naročanja, ker je to v nasprotju z opredelitvijo poslovnih skrivnosti.

V omenjenih pravilnikih zasledimo podatek, da so kot poslovna skrivnosti označena delovna gradiva in zapisniki občinskega sveta ter njihovih odborov. Ti dokumenti so v občinah informacije javnega značaja, ki ga ureja ZDIJZ. Po ZDIJZ so informacije javnega značaja dostopne vsakomur, zato ne morejo biti poslovna skrivnost. Tudi ponovna uporaba informacij javnega značaja je zagotovljena vsakomur ne glede na to, ali informacijo potrebuje v pridobitne ali nepridobitne namene, kot to določa tretji odstavek 5. člena ZDIJZ. Pravilniki kot poslovno skrivnost navajajo še različna gesla zaposlenih za vstop v računalniške programe in šifriranja, kjer pa gre za zaupne podatke in ne poslovne skrivnosti.

Lokalne skupnosti so pri ravnanju s tajnimi podatki dolžne spoštovati 38. člen ZTP, ki zavezuje lokalne skupnosti, da skladno s sprejetimi predpisi vzpostavijo sistem postopkov in ukrepov varovanja tajnih podatkov. ZTP natančno določa, kaj bi morali pravilniki vsebovati, in sicer splošne varnostne ukrepe, varovanje oseb, ki imajo dostop do tajnih podatkov, varovanje prostora, dokumentov, medije, ki vsebujejo tajne podatke, komunikacijske kanale, kjer se prenašajo tajni podatki, načine označevanja, varovanje opreme, kjer so tajni podatki shranjeni, pa tudi načine, kako se uporabnike seznani s tajnimi podatki, ter postopke njihovega varovanja. Poleg tega ZTP določa še kontrolo in evidentiranje dostopov, pošiljanje in distribucijo tajnih podatkov.

ZTP tudi določa, da je predstojnik organa oz. župan pooblaščen, da določenemu podatku opredeli status tajnega podatka. To navedbo je v svojem pravilniku zapisala le Občina KG, ostali dve občini tega ne omenjata. Noben od analiziranih pravilnikov ne določa, kje se hranijo tajni podatki, kako je treba z njimi ravnati, kakšne obveznosti ima tisti, ki razpolaga s tajnimi podatki, in kdo, kdaj in na kakšen način se lahko podatki uničijo. Vse to je nujno potrebno, saj se na tak način zmanjša nevarnost arbitriranja ob sporih. Bistveno je, da morajo biti vse omejitve točno zapisane, s tem da se ne sme omejevati človekovih pravic (Anžič 2000, 853).

Poleg navedenega smo ugotovili, da vsi trije pravilniki nimajo strukture akta in niso usklajeni z veljavno zakonodajo, zato v nadaljevanju podajamo priporočila, ki naj bi jih občine vnesle v Pravilnike o ravnanju s tajnimi podatki ter o načinu varovanja tajnih podatkov.

# 7 PRIPOROČILA ZA UREJANJE VARSTVA TAJNIH PODATKOV IN POSLOVNIH SKRIVNOSTI Z INTERNIM AKTOM OBČINE

Lokalne skupnosti morajo pri varovanju tajnih podatkov upoštevati ZTP, ki določa varovanje in dostop do tajnih podatkov z delovnega področja državnih organov. Lokalne skupnosti bi morale imeti varovanje tajnih podatkov podrobneje urejeno v svojih internih aktih. Ti podatki se nanašajo na javno varnost, obrambo, zunanje zadeve ali obveščevalne in varnostne dejavnosti. Načini varovanja tajnih podatkov so zapisani v 39. členu ZTP, ki navaja, da morajo tajni podatki biti dostopni samo osebam, ki imajo dovoljenje za njihovo uporabo. Nadalje določa tudi načine v primerih, ko se podatke pošilja izven prostorov lokalne skupnosti.

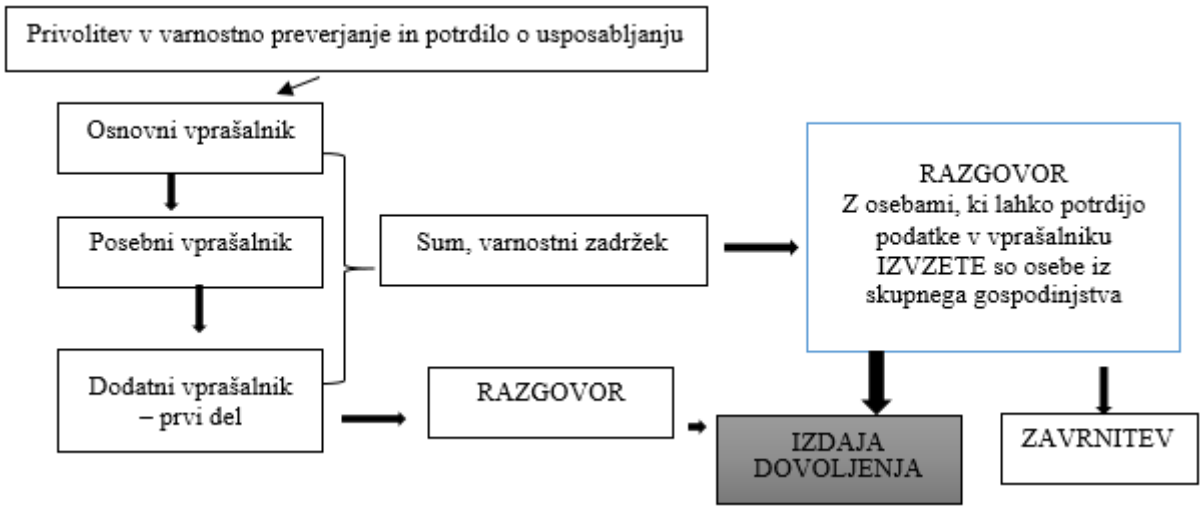
Lokalne skupnosti sicer nimajo poslovnih skrivnosti skladno z ZPosS, ampak so kljub temu dolžne varovati poslovne skrivnosti svojih pogodbenih partnerjev skladno s 35. členom ZJN. Med poslovne skrivnosti lahko upoštevamo tudi podatke, do katerih je lokalna skupnost sama prišla in se nanašajo na procese in strategije delovanja lokalne skupnosti. Govorimo o intelektualni lastnini, ko zaposleni v okviru svojega dela in nalog oz. pogodbe o zaposlitvi izumijo, inovirajo določene postopke, s katerimi si zaposleni olajšajo delo, kot npr. če njihov računalničar razvije aplikacijo za hitrejšo izdelavo odločb pri izračunu taks, plač ali ko gre za posebno strategijo komunikacije, s katero lokalno skupnost pridobi konkurenčno prednost pred drugimi lokalnimi skupnostmi in bi njihovo razkritje imelo škodljive posledice zanjo. Glede na navedeno imajo lokalne skupnosti predvsem označene le tajne oz. zaupne podatke, kamor so uvrščeni osebni podatki zaposlenih, vendar se za njihovo varovanje uporablja ZVOP.

Na osnovi tega podajamo naslednja priporočila lokalnim skupnostim pri varovanju tajnih in zaupnih podatkov ter poslovnih skrivnosti. Smiselno je, da bi lokalne skupnosti sprejele pravilnik, v katerem bi uredili varovanje tajnih podatkov po ZTP, kakor tudi druge podatke, ki po ZTP niso tajni, vendar bi njihovo razkritje lahko povzročilo lokalni skupnosti škodo pri izvedbi določenih postopkov oz. delovnih procesov. Skladno z navedenim morajo lokalne skupnosti sprejeti Pravilnik o varovanju tajnih in zaupnih podatkov ter poslovnih skrivnosti (v nadaljevanju Pravilnik o varovanju TP, ZP ter PS ), ki naj bo sestavljen iz splošnega in posebnega dela ter tehničnih ukrepov pri varovanju tajnih podatkov ter poslovnih skrivnosti.

## 7.1 Priporočila za splošni del Pravilnika o varovanju TP, ZP ter PS

V splošnem delu Pravilnika o varovanju TP, ZP ter PS je najprej treba definirati, kaj so to poslovne skrivnosti in tajni podatki, kjer se pri opredelitvi poslovnih skrivnostih sklicujemo na ZPosS iz leta 2019, pri tajnih podatkih pa na ZTP (2006). Nadalje je treba opredeliti namen Pravilnika o varovanju TP, ZP ter PS, kaj ureja in za koga velja, opredeliti stopnje tajnosti ter določiti pristojnosti in odgovornosti zaposlenih.

V Pravilniku o varovanju TP, ZP ter PS je treba navesti osebe, zadolžene za varovanje tajnih podatkov, nato predvideti tudi, da osebe ob zaposlitvi v lokalni skupnosti (občini) ob podpisu pogodbe o zaposlitvi podpišejo še Izjavo o zaupnosti, s katero se zavežejo, da bodo varovale tajne podatke lokalne skupnosti in da so seznanjene s Pravilnikom o varovanju TP, ZP ter PS. Omenjeno izjavo podpišejo tudi druge osebe, ki sodelujejo z občino. Za osebe, ki naj bi imele dostop do tajnih podatkov po ZTP, se določi postopek varnostnega preverjanja. V postopku preverjanja se ugotovi lojalnost osebe, zanesljivost in verodostojnost, pa tudi osebnostni značaj in okoliščine, ki bi lahko ogrozile varovanje tajnih podatkov skladno s 25. členom ZTP. Primer varnostnega preverjanja za osebe, ki so jim zaupane strogo tajne zadeve, prikazuje Slika 2.




**Slika 2: Primer varnostnega preverjanja z varnostnim poizvedovanjem**

Vir: Urad vlade RS za varovanje tajnih podatkov 2020

Za celostno izvajanje postopkov in ukrepov varovanja internih in zaupnih podatkov po definiciji ZTP z določitvijo osebe, odgovorne za varovanje podatkov ter informiranjem zaposlenih o tem, je odgovoren župan.

V Pravilniku o varovanju TP, ZP ter PS je treba jasno določiti, da so se zaposleni v okviru svojega dela dolžni seznaniti z internimi in zaupnimi podatki lokalne skupnosti, vendar jih lahko uporabljajo izključno pri svojem delu. Poleg tega se o njih ne sme govoriti ali dajati na vpogled nepooblaščenim osebam ali jih odnašati izven prostorov, razen če to določi odgovorna oseba, ki je običajno župan občine. Zaposlenim mora biti prepovedano izdajati, zlorabljati, posredovati zaupne podatke nepooblaščenim osebam, prav tako jih morajo skrbno varovati, da ne pride do izgube ali uničenja. Tudi ko zaposlenemu preneha delovno razmerje, je ta še vedno dolžan skrbeti za varovanje podatkov, s čimer se zaveže s podpisom Izjave ob nastopu delovnega razmerja. V Pravilniku je treba prav tako zapisati, da so zaposleni v primeru kršitev varovanja tajnih podatkov disciplinsko, odškodninsko, kazensko in delovno-pravno odgovorni (menimo, da je treba tovrstno kršitev določiti kot hujšo kršitev delovnih obveznosti, zaradi katere je mogoče uporabiti tudi izredno odpoved pogodbe o zaposlitvi).

V Pravilniku o varovanju TP, ZP ter PS je treba določiti tudi stopnjo tajnosti dokumentov in čas, ko ti ne smejo biti razkriti. Na vsakem dokumentu mora biti jasno zapisano in vidno, ali gre za zaupne podatke in čas varovanja teh podatkov. Zaupne podatke je treba hraniti na tak način, da niso dostopni nepooblaščenim osebam. Župan določi, kateri dokumenti imajo stopnjo tajnih podatkov oz. ali gre za interno, zaupno, tajno in strogo tajno. Kakšno stopnjo tajnosti ima dokument, je predvsem odvisno od tega, kakšne posledice bi njegovo razkritje pomenilo za lokalno skupnost. V večini premerov Pravilniki o varovanju TP, ZP ter PS te podatke ločijo zgolj v dve skupini: na interne in zaupne podatke po definiciji ZTP. Pri dokumentih z oznako »interno« so mišljeni dokumenti, katerih razkritje nepoklicanim osebam bi lahko škodovalo delovanju in izvajanju nalog lokalne skupnosti. Pod interno so to lahko dokumenti različnih zapisnikov delovnih skupin, osnutki odločitev o določenih zadevah, lahko so to študije, raziskave, ki so namenjene strategiji delovanja občine in ne širši javnosti, različna gradiva (dopisi, organizacijske sheme, lastni izračuni, kadrovska evidenca, interna glasila itd.) in deli gradiv, ki jih lokalna skupnost prejme iz drugih virov, če oceni, da bi razkritje teh gradiv lahko lokalni skupnosti povzročilo škodo. Z oznako interno župan določi tudi druga gradiva in informacije, ki bi lahko škodovale delovanju občine, če bi prišlo do njihovega razkritja. Pri oznakah zaupno se uporabljajo stopnje tajnosti, ki jih določa ZTP, kamor uvrščamo uradne listine in podatke s področja delovanja civilne zaščite, nadzornega odbora občine, notranjih kontrol in revizij ter drugih poslovnih tajnosti, ki jih določi župan.

Za celostno izvajanje postopkov in ukrepov varovanja internih in zaupnih podatkov po definiciji ZTP podatkov z določitvijo osebe, odgovorne za varovanje podatkov ter informiranjem zaposlenih o tem, je odgovoren župan. Slednji je odgovoren tudi za izvajanje rednega notranjega nadzora na tem področju.

### 7.2 Priporočila za posebni del Pravilnika o varovanju TP, ZP ter PS

V posebnem delu Pravilnika o varovanju TP, ZP ter PS je treba natančneje določiti čisto konkretni, praktični ukrep varovanja tajnih podatkov, zaupnih podatkov in poslovnih skrivnosti. Tukaj gre tako za ukrepe v zvezi z varovanjem prostorov, prenosom podatkov, hrambo podatkov, sledljivostjo podatkov in podobno. S Pravilnikom o varovanju TP, ZP ter PS je treba opredeliti enoten sistem določanja in označevanja internih in zaupnih podatkov po definiciji ZTP, njihov prenos, razmnoževanje, evidentiranje, uničevanje in arhiviranje ter postopek ob zlorabi tajnega podatka. Varnost navedenih se prepleta s fizičnimi in tehničnimi ukrepi, vse z namenom, da do njih ne dostopajo nepooblaščene osebe, zato je pomembna njihova sledljivost skozi celoten čas življenjske dobe.

Interne in zaupne podatke po definiciji ZTP lahko lokalna skupnost hrani v železnih omarah oz. v protivlomnih omarah. Njihovo kopiranje ni dovoljeno, razen če to dovoli župan. Ko podatki niso več tajni, se jih lahko uniči, da niso več prepoznavni, npr. z rezalnim strojem. Tajni podatki morajo biti shranjeni skladno z Uredbo o varovanju tajnih podatkov, kot to določa 10. člen

navedene uredbe. Ta določa območje, kje se lahko obravnava tajne podatke. Tajni podatki z oznako »interno« se obravnavajo v upravnem območju, medtem ko se podatke s stopnjo »zaupno« ali višjo obravnava, hrani le za to določen prostor, imenovan varnostno območje. Že sam dostop do varnostnega območja ni dostopen vsakomur, ampak se izvajajo posebni varnosti ukrepi, ki zagotavljajo popolni nadzor pri vstopu in izstopu v območje. Vsak, ki želi vstopiti na varnostno območje, mora imeti ustrezno dovoljenje. Pred vstopom v varnostno območje se osebo seznani z razvidom tajnih podatkov. Ob vstopu oseba ne sme imeti nikakršnih mehanskih, elektronskih ali podobnih naprav, ki bi ji omogočile posneti ali prenesti tajne podatke. Ves čas se opravlja tudi fizična prisotnost oz. se mora zagotoviti popoln nadzor nad varnostnim območjem iz nadzornega centra (Prezelj in Tarman 2015, 697).

Koliko oseb lahko pozna kombinacije elektronskih ali mehanskih ključavnic na varnostnih omarah s tajnimi podatki, je odvisno od vsake lokalne skupnosti posebej, vendar pa naj bi bilo to število čim manjše, o čemer govori 20. člen Uredbe o varovanju tajnih podatkov. Za večjo varnost naj bi se kombinacije elektronskih in mehanskih ključavnic zamenjale ob namestitvi vsakih šest mesecev s prenehanjem opravljanja nalog glede tajnih podatkov in ko o tem odloči predstojnik organa. Ključi za dostop do varnostnega območja se morajo hraniti v posebnem prostoru, kjer je onemogočen dostop nepooblaščenim osebam. Strojno in programsko opremo, namenjeno obravnavi tajnih podatkov, se uporablja izključno za opravljanje nalog, povezanih z lokalno skupnostjo.

Posebno varovanje je namenjeno digitalnim dokumentom, zato morajo biti prenosni računalniki, preko katerih zaposleni v občini dostopajo do tajnih dokumentov, zaklenjeni v za to določenem prostoru oz. omari. Pomembno je, da do strojne računalniške opreme dostopajo le pooblaščeni serviserji in vzdrževalci, ki imajo sklenjeno pogodbo z lokalno skupnostjo (občino), ter zaposleni, vendar le do tistih podatkov, ki jim jih odobri župan. Celotno računalniško omrežje, kjer so shranjeni tajni podatki, mora biti varovano pred nepooblaščenimi osebami s protivirusno opremo. Prav tako se teh podatkov ne sme pošiljati po nezaščitenih komunikacijskih sredstvih. Boljša rešitev so lastne prenosne mreže, v primeru fizičnih prenosov (pošiljk) pa lastne kurirske službe ali zaprte neprosojne ovojnice, kjer se označi stopnja tajnosti.

Pravilnika o varovanju TP, ZP ter PS mora urejati tudi varovanje prostorov, kjer se hranijo tajni oz. zaupni podatki, to so v večini primerov prostori lokalne skupnosti. Lokalne skupnosti naj bi omejile gibanje po občini s hišnim redom, z navodili in akti, ki jih sprejme lokalna skupnost. Tajni oz. zaupni podatki se morajo tudi tehnično varovati, kar pomeni, da do njih ni mogoče dostopati brez elektronskih kartic in alarmnih sistemov. Če je možno, lahko lokalne skupnosti zagotovijo tudi fizično prisotnost varnostnika. Poleg tega morajo vsi zaposleni po končanem delu shraniti tajne podatke v omare, ki se morajo zaklepati, ključe pa shraniti v prostore, ki je dostopen le s šifro, računalnike obvezno izključiti. V primeru, da zaposleni odnašajo tajne podatke iz prostorov lokalne skupnosti, jih tam ne smejo puščati brez nadzora. Enaka pravila veljajo tudi pri prenosnih računalnikih. Računalnike lahko vzdržuje in popravlja le za to

določena oseba; kadar je to zunanji izvajalec, naj ima lokalna skupnost sklenjeno ustrezno pogodbo, s katero se ta izvajalec zaveže upoštevati celotno varnostno politiko lokalne skupnosti, kar pomeni, da osebnih in internih informacij ne bo posredoval drugim osebam, temveč jih bo varoval tako, da ne bo prišlo do njihovega razkritja oz. jih ne bo uporabljal na drugačen način, kot je dogovorjeno s sklenjeno pogodbo in z drugimi predpisi, ki urejajo to področje.

Poleg vsega zgoraj navedenega se dostop do tajnih dokumentov varuje tudi z identifikacijo uporabnika. Vsak uporabnik mora imeti svoje geslo, s katerim dostopa do tajnih dokumentov, ki se hranijo v zapečatenih kuvertah in na za to določenih zavarovanih mestih. Na kuverto je treba napisati ime sistema oz. aplikacije in datum, ko je geslo bilo zadnjič spremenjeno (to naj bi se spreminjala vsaj štirikrat letno, vsake tri mesece), nato pa zaprto kuverto s podpisom uporabnika gesla in imena shraniti. V primeru, da je treba zaprto kuverto odpreti, je treba to evidentirati (kdo in kdaj je dostopal do gesla). Dejstvo je, da je geslo uporabnika informacijskega sistema izključno namenjeno le njegovemu lastniku, zato je ta tudi odgovoren za vse, kar bi se zgodilo z uporabo njegove identitete. Izhajajoč iz tega se gesla ne smejo razkrivati ali posoditi nobeni drugi osebi. V primeru, da zaposleni zasluti neodgovorno ravnanje z gesli, je dolžan o tem takoj obvestiti nadrejenega, geslo pa nemudoma spremeniti. Gesla se lahko določijo tudi kot začasna, vendar jih je treba uporabniku sporočiti na varen način, ki je lahko tudi ustno sporočilo.

Računalniško omrežje je treba zavarovati s protivirusno opremo. Govorimo o politiki fizične zaščite do informacijskega sistema lokalne skupnosti. S pravili in postopki omogočimo dostop do informacijskega sistema le pooblaščenim osebam. Nepooblaščeni dostop lahko razkrije podatke lokalne skupnosti, kamor uvrščamo osebne podatke ali tiste, ki so okvalificirani kot interni. Na območjih javnega dostopa, kot je npr. hodnik, se osebni podatki ne hranijo ali obdelujejo, ampak le v tistih prostorih, kjer se nahajajo zaposleni. To so pisarne vodstva, finančnih služb, splošnih služb, kjer mora dostop biti urejen s kontrolo dostopa (ali s ključem, brezkontaktno kartico, slepo kljuko).

Posebni del Pravilnika o varovanju TP, ZP ter PS mora vsebovati tudi načine, kako uporabnike seznaniti s postopki varovanja tajnih podatkov. Na splošno se ukrepi zaščite pričnejo že ob sklenitvi delovnega razmerja, ko je vsak novo zaposleni javni uslužbenec dolžan podpisati izjavo o varovanju tajnih podatkov. Poleg tega naj vsak zaposleni zaklepa pisalne mize, pisarno, predvsem takrat, ko se v njej nahajajo tajni podatki. Ko se v pisarni nahajajo nepooblaščene osebe, morajo zaposleni poskrbeti, da ne more nihče pogledati v tajne dokumente. Govorimo o politiki praznega računalniškega zaslona, ki onemogoči vpogled nanje. V posameznih primerih lahko vpogled na računalniški zaslon dovoli le zaposleni, če gre za obdelavo podatkov o uporabniku storitev in ta mora pogledati v svoje osebne podatke. Ob vključitvi računalnika se mora uporabiti geslo, ob odhodu domov pa se zaposleni odjavi iz sistema, vključi ohranjevalnik zaslona in zaklene računalnik. Če zaposleni zapusti delovno mesto za več kot pet minut, mora

poskrbeti, da se ohranjevalnik zaslona avtomatsko vključi in se zaklene. S tem se prepreči dostop do podatkov nepooblaščenim osebam. Če zaposleni ugotovijo, da je prišlo do izgube ali razkritja tajnih podatkov nepooblaščenim osebam, so o tem takoj dolžni obvestiti župana, ki mora nemudoma ukrepati, da ne prišlo do škodljivih posledic.

Glede na to, da je treba zaupne podatke pošiljati tudi izven občine, je pri tem treba biti še posebno pozoren. Zagotoviti je treba, da bo podatke prejela le oseba, ki so ji namenjeni, zato se jih ne sme pošiljati po nezaščitenih komunikacijskih kanalih. Zaupni podatki se prenašajo v zaprtih neprosojnih ovojnicah po pošti priporočeno s povratnico ali po kurirski službi (ta je obvezna, ko gre za zaupne podatke) in se hranijo izključno v zaklenjenih železnih omarah. Lahko se jih kopira, vendar le v primeru, če to določi župan. V primeru, da ni dovoljeno kopiranje tajnega dokumenta, je to treba posebej označiti na dokumentu.

Pravilnik o varovanju TP, ZP ter PS ureja tudi postopek uničenja in arhiviranja zaupnih podatkov. Podatki se morajo uničiti na takšen način, da niso več prepoznavni. O tem, kdaj je treba zaupen podatek uničiti, odloča veččlanska komisija, imenovana s strani župana. Komisija za uničevanje tajnih podatkov o svojem delu vodi zapisnik, ki vsebuje vse relevantno v zvezi z uničenim podatkom oziroma dokumentom (vsaj razlog, datum in stopnjo tajnosti uničenega podatka).

Zaupne podatke je treba tudi arhivirati, kjer pa morajo zaposleni upoštevati predpise s področja arhiviranja dokumentov, predvsem ZVDAGA. Nepravilna hramba in arhiviranje kopij podatkov, ki so klasificirane z oznako »interno« ali »zaupno«, lahko predstavlja možnost za zlorabo podatkov, zato se je treba temu izogniti. Na kakšen način se bodo podatki hranili in arhivirali, naj bo usklajeno z varnostnimi zahtevami. Priporočljivo je, da se dokumente pregleduje in prilagaja spremembam procesov in občutljivosti podatkov. Podatki morajo biti arhivirani toliko časa, kot to določa veljavna zakonodaja, nikakor pa ne smejo biti uničeni pred potekom obdobja, določenega za hrambo. Nekateri se hranijo nekaj let, nekateri pa tudi trajno.

Pravilnik o varovanju TP, ZP ter PS se zaključi s prehodnimi in končnimi določbami, kjer se navede datum, od kdaj se uporablja, ter s podpisom župana.

Poleg navedenega priporočamo lokalnim skupnostim, da v svoj interni akt o varovanju podatkov vključijo tudi poglavje o usposabljanju zaposlenih na tem področju. Zato naj bi se zaposleni udeležili Usposabljanj s področja varovanja osebnih in tajnih podatkov, ki jih izvaja Ministrstvo za obrambo in Urad Vlade RS za varovanje tajnih podatkov in ki potekajo v obliki e-izobraževanja (Urad vlade RS za varovanje tajnih podatkov 2020) ter navsezadnje tudi usposabljanje za arhiviranje dokumentarnega gradiva skladno s Pravilnikom o strokovni usposobljenosti za delo z dokumentarnim gradivom (Uradni list RS, št. 66/16). Skladno z drugim odstavkom 3. člena navedenega pravilnika so zaposleni dolžni obnavljati strokovno znanje vsake tri leta, da se seznanijo z novostmi s tega področja.

# 8 SKLEPNE UGOTOVITVE

Varovanje poslovnih skrivnosti in tajnih podatkov je široko in kompleksno področje. V raziskavi smo ugotovili, da med poslovno skrivnostjo in tajnimi podatki obstajajo razlike. Opredelitve poslovnih skrivnosti so v strokovni literaturi različne, enotno pa je, da gre za podatke, ki so dostopni le določenim osebam, imajo tržno vrednost in njihovo razkritje pomeni nepopravljivo škodo. Med poslovne skrivnosti spadajo različni dokumenti, kot npr. znanstvene, tehnične in inženirske informacije, poslovni načrti, strategije poslovanja, lahko so to tudi programske naprave, dizajn, prototipi, metode dela, postopki, recepti, formule, proizvodne tehnike, izumi in podobno. Varovanje poslovnih skrivnosti, s čimer podjetja ohranijo svojo konkurenčno prednost, je lahko za razliko od varovanja prav teh s pravicami intelektualne lastnine neomejeno dolgo. Poslovna skrivnost se tudi sicer uvršča v pravice intelektualne lastnine. V nasprotju s poslovno skrivnostjo pa so tajni podatki tisti podatki, ki se nanašajo na javno varnost, obrambo, zunanje zadeve ali obveščevalno in varnostno dejavnost države. Varovanje tajnih podatkov pa določa Zakon o tajnih podatkih, po katerem je tajni podatek vsak podatek s področja delovanja organa, ki se nanaša na javno varnost, obrambo, zunanje zadeve ali obveščevalno in varnostno dejavnost države, ki ga je treba zavarovati pred nepoklicanimi osebami in je označen kot tajen.

Poslovne skrivnosti v Sloveniji ureja Zakon o poslovni skrivnosti (ZPosS) iz leta 2019, s katerim je bila v slovenski pravni red implementirana Direktiva EU 2016/943. Pred sprejetjem ZPosS je bilo področje varovanja poslovne skrivnosti urejeno v 39. členu Zakona o gospodarskih družbah, ki je poslovno skrivnost tudi definiral. Tajne podatke pa ureja Zakon o tajnih podatkih (ZTP).

S tajnimi podatki in poslovnimi skrivnostmi se srečujejo tudi lokalne skupnosti, ki skušajo določbe predpisov na tem področju podrobneje operacionalizirati v svojih internih aktih. Na področju tajnih podatkov je namreč varovanje teh podrobneje urejeno le na nacionalni ravni, na ravni lokalnih skupnosti pa ne, čeprav jih ZTP neposredno zavezuje. Podobno situacijo srečamo na področju poslovnih skrivnosti – lokalne skupnosti skušajo tudi varovanje poslovne skrivnosti podrobneje urejati z internimi pravnimi akti.

V magistrski nalogi smo si uvodoma zastavili več vprašanj glede urejanja varovanja poslovne skrivnosti in tajnih podatkov v lokalni skupnosti, na katere smo poskušali tudi odgovoriti tekom celotnega besedila. Prvo vprašanje se je nanašalo na dilemo obstoja poslovnih skrivnosti v zvezi z delom lokalne skupnosti, saj so poslovne skrivnosti že po definiciji samo tiste, ki vsebujejo tržno vrednost. V zvezi s tem smo ugotovili, da so lokalne skupnosti osebe javnega prava, katerih namen ni pridobivanje dobička, zato ne morejo posedovati podatka, ki ima tržno vrednost. Pri izvajanju svojih pristojnosti pa lahko imajo opravka s poslovnimi skrivnostmi drugih recimo pogodbenih partnerjev.

Ker so lokalne skupnosti po ZDIJZ dolžne omogočiti dostop do informacij javnega značaja, se je drugo vprašanje nanašalo na tehtanje različnih interesov. Na eni strani mora lokalna skupnost upoštevati interes javnosti, po drugi strani pa interese na področju državne varnosti ali interese drugih, kot npr. svojih pogodbenih in poslovnih strank. Kateri interes prevlada v konkretnem primeru, je eno od vprašanj, na katero smo poskusili odgovoriti v magistrski nalogi. Na eni strani je Slovenija demokratična država, zato imajo njeni državljani skladno s 39. členom Ustave RS zagotovljeno pravico pridobiti informacije javnega značaja, kar pa ne velja za državno varnost, ko gre za dokumente oz. tajne podatke, do katerih lahko dostopajo le določene osebe, kot npr. predsednik države, predsednik vlade, poslanci, župani. V lokalni skupnosti je najbolj pomembno, da lokalna skupnost označi, kateri podatki so zaupne narave, kar pomeni dostopnost le določenim pooblaščenim osebam in z rokom trajanja zaupnosti, in kateri so dokumenti javnega značaja. Pri tem mora lokalna skupnost točno določiti ravnovesje med tveganji in sistemsko zaščito, saj bo s tem zmanjšala nevarnost samovoljnemu odločanju sodišča ob morebitnih sporih, kot smo ugotovili skozi analizirano sodno prakso.

Zaposleni, ki bi razkril tajne in zaupne podatke ali poslovne skrivnosti nepooblaščenim osebam, lahko odgovarja disciplinsko, odškodninsko in kazensko. ZDR-1 določa disciplinsko odgovornost zaposlenega, ko se mu lahko izreče tudi najstrožji ukrep odpovedi delovnega razmerja, ZJU navaja, da zaposleni odgovarja za škodo, ki jo je povzročil lokalni skupnosti, medtem ko KZ govori o kaznivem dejanju, za katerega je določena tudi zaporna kazen do treh let, če se ugotovi, da je zaposleni neupravičeno sporočil drugemu poslovne skrivnosti ali omogočil, da do njih pride nepoklicana oseba.

Namen magistrske naloge je bil, da na podlagi analize internih aktov o varovanju tajnih podatkov treh lokalnih skupnosti Občine Kranjska Gora, Občine Šentjernej in Preddvor oblikujemo priporočila, ki bi pomagala lokalni skupnosti pri varovanju tajnih podatkov. V raziskavi je bilo ugotovljeno, da noben Pravilnik o varovanju tajnih podatkov navedenih lokalnih skupnosti ni v skladu s sprejeto zakonodajo in da glede terminov »zaupno«, »uradno«, »tajno«, »interno« v praksi vlada velika zmeda. Glede na to smo podali priporočila lokalnim skupnostim za urejanje tega področja. Predvsem je pomembno, da lokalna skupnost v takem aktu jasno razlikuje med podatki, ki so tajni zaradi varovanja obrambnih in varnostnih interesov države, od tistih, ki se varujejo pred razkritjem zaradi interesov lokalne skupnosti, in nenazadnje od tistih, kjer gre za poslovne skrivnosti.

Lokalni skupnosti priporočamo, da sprejmejo Pravilnik o varovanju TP, ZP ter PS. Res je, da lokalne skupnosti na eni strani nimajo poslovnih skrivnosti, kot to določa ZPosS in naj tega pojma ne bi uporabljale, vendar na drugi strani so dolžne varovati poslovne skrivnosti poslovnih partnerjev skladno z ZJN-3. Poleg tega obstajajo tudi podatki povezani z intelektualno lastnino zaposlenih v lokalni skupnosti, s katerimi si zaposleni olajšajo delo in so skrbno varovana skrivnost. Glede na navedeno lokalnimi skupnosti priporočamo, da v Pravilniku o varovanju TP, ZP ter PS točno določijo, kateri podatki so poslovna skrivnosti, kateri so interni, kateri

zaupni, kakšno stopnjo imajo zaupni podatki, kolikšna je njihova življenjska doba ter kdo lahko dostopa do njih. Poleg tega naj navedeni pravilnik vsebuje disciplinsko, odškodninsko in kazensko odgovornost zaposlenega, ki bi neupravičeno razkril ali posredoval podatke drugim, nepooblaščenim osebam. Poleg tega so lokalne skupnosti dolžne sprejeti še pravila o hranjenju tajnih podatkov in njihovo obravnavo ter razpošiljanje. Ko so pravila sprejeta, obstaja manjše tveganje, da bodo podatke prejele nepooblaščene osebe. Lokalne skupnosti morajo imenovati komisijo, ki bo skrbela za uničenje tajnih podatkov. Vsemu temu je treba posvetiti pozornost, če bo lokalna komisija želela varovati tajne podatke in s tem olajšati delo svojim zaposlenim, pa tudi ustrezno ukrepati v primeru njihovega razkritja. Vsekakor bodo lokalne skupnosti morale to storiti, da bodo vsi, tako župan kot zaposleni, točno vedeli, kaj lahko in česa ne smejo razkriti.

Ker smo danes priča velikim spremembam, se tudi spreminjajo stopnje tajnih podatkov, zato je treba poskrbeti za stalno osveščanje, izobraževanje in usposabljanje pooblaščenih oseb, ki bodo preverjale stopnje tajnosti podatkov in po potrebi oznako tudi odstranile. Glede na to je pomembno, da se zaposleni zavedajo lojalnosti do delodajalca, saj menimo, da zgolj zakonodaja ni dovolj učinkovita za varovanje poslovnih skrivnosti in tajnih podatkov v praksi, marveč je tukaj zelo pomembna tudi individualna varnostna kultura.

## LITERATURA


Aftergood, Steven. 2010. National security secrecy: how the limits change. *Social Research* 77 (3): 839–852.

Almeling, David S. 2012. Seven reasons why trade secrets are increasingly important. *Berkeley Technology Law Journal* 27 (2): 1091–1118.

Almeling, David S., Darin W. Snyder, Michael Sapoznikow, Whitney E. McCollum in Jill Weader. 2010. A statistical analysis of trade secret litigation in federal courts. *Gonzaga Law Review* 45 (2): 291–334.

Anžič, Andrej. 2000. Tajnost: vrednota in zlo. *Teorija in praksa* 37 (5): 849–863.

Anžič, Andrej. 2001. Tajnost kot družbeni fenomen – varnostni vidik. V *Javna predstavitev mnenj o predlogu Zakona o tajnih podatkih,* ur. Igor Belić, 43–54. Ljubljana: Ministrstvo za notranje zadeve Republike Slovenije.

Bakken, Tim. 2013. The prosecution of newspapers, reporters, and sources for disclosing classified information: the government's softening of the first amendment. *University Of Toledo Law Review* 45: 1–29.

Bizjak, Domen. 2014. Odškodninska odgovornost države za škodo, ki izvira iz protipravnega delovanja inšpektorjev. *Uprava=Administration* 7 (1): 63–84.

Brezovšek, Brane in Damir Črnčec. 2004. Tajnost v demokraciji. *Teorija in praksa* 41 (3/4): 506–523.

Čebulj, Tomaž in Jurij Žurej. 2005. *Varstvo osebnih podatkov in informacije javnega značaja*. Ljubljana: Nebra.

Demšar-Potočnik, Ivanka. 2015. Razkritje tajnih podatkov v pravdnem postopku. *Pravnik* 70 (11/12): 807–837.

Državna revizijska komisija za revizijo postopkov oddaje javnih naročil. 2017. *Sklep 018-048/2017-6.* Http://www.dkom.si/odlocitve_DKOM/2017041010422224/ (7. 7. 2020).

Evans, Michelle. 2019. Trade secret status for business customer lists under the defend trade secrets act. *Tulane Journal of Technology and Intellectual Property* 21: 21–33.

Evropska gospodarska skupnost. 1957. *Pogodba o ustanovitvi Evropske gospodarske skupnosti*. Https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:11957E/TXT&from=EN (7. 1. 2020).

Evropski parlament in Svet. 2003. *Direktiva 2003/98/ES Evropskega parlamenta in Sveta z dne 17. novembra 2003 o ponovni uporabi informacij javnega sektorja*. Https://eur-lex.europa.eu/legal-content/SL/TXT/?uri=celex%3A32003L0098 (12. 1. 2020).

Evropsko sodišče. 2020. *Predstavitev*. Https://curia.europa.eu/jcms/jcms/Jo2_7024/sl/ (23. 7. 2020).

Gleaser, Stephen. 2018. The effects of proprietary information on corporate disclosure and transparency: Evidence from trade secrets. *Journal of Accounting and Economics* 66 (1): 163–193.

Hannah, David R. 2006. Keeping trade secrets secret. *Sloan Management Review* 47 (3): 17–20.

Informacijski pooblaščenec. 2009. *Odločba št. 090-57/2009/9*. Https://www.ip-rs.si/ijz/prosilec-krajevna-skupnost-ljubno-984/ (17. 6. 2020).

Informacijski pooblaščenec. 2015. *Odločba št. 090-32/2015*. Https://www.ip-rs.si/ijz/telemach-doo-obcina-pivka-2601/ (7. 7. 2020).

Informacijski pooblaščenec. B. l. *Kaj so informacije javnega značaja?* Https://www.ip-rs.si/informacije-javnega-znacaja/ijz-pri-organih/kaj-so-informacije-javnega-znacaja/ (10. 10. 2019).

Inštitut za ekonomijo, pravo in informatiko. 2019. *Varstvo tajnih podatkov*. Http://www.ipri-zavod.si/ostalo/varstvo-tajnih-podatkov/ (2. 1. 2020).

Intellectual Property Expert Group. B. l. *Trade secrets*. Https://www.ipeg.com/trade-secrets/ (5. 1. 2020).

Jain, Subhash C. 1996. Problems in international protection of intellectual property rights. *Journal of International Marketing* 4 (1): 9–32.

Knowlton, William R. 2014. Implementing noncompete agreements in Utah: protecting business trade secrets, goodwilt, and investment in employees. *Utah Bar Journal* 27 (3): 16–19.

Komisija Evropske skupnosti (KES). 1989. *Zadeva C-3/88 Komisija Evropske skupnosti Italijanski republiki ECLI:EU:C:1989:606.* Https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:61988CJ0003&from=SL (5. 1. 2020).

Kralj, Tomaž in Simon Starček. 2012. Pomen izvedbenih politik pri uvajanju sistema upravljanja informacijske varnosti. *Uprava=Administration* 10 (4): 91–104.

Lampe, Rok. 2014. Pravna ureditev poslovne skrivnosti: nasveti za kadrovsko politiko. *HRM: Strokovna revija za ravnanje z ljudmi pri delu* 12 (58): 12–17.

Mendenhall, Kyle J. 2014. Can you keep a secret? The court's role in protecting trade secrets and other confidential business information from disclosure in litigation. *Drake Law Review* 62 (3): 885–917.

Ministrstvo za javno upravo. 2020. *Informacije javnega značaja*. Https://www.gov.si/teme/informacije-javnega-znacaja/ (4. 2. 2020).

Morvillo, Christopher J. in Megan E. Farell. 2012. *Speaking confidentially: tips for protecting trade secrets and other confidential business information*. Https://ccbjournal.com/articles/speaking-confidentially-tips-protecting-trade-secrets-and-other-confidential-business (13. 6. 2020).

Možina, Damjan. 2013. *Odškodninska odgovornost države*. Https://www.ic-geoss.si/wp-content/uploads/2018/12/5-%C4%8Clanek-Od%C5%A1kodninska-odgovornost-dr%C5%BEave-Mozina.pdf (7. 7. 2020).

Nacionalni inštitut za javno zdravje. 2016. *Krovna in področne politike varovanja informacij*. Interno gradivo, Nacionalni inštitut za javno zdravje.

Niebel, Rembert, Lorenzo de Martinis in Birgit Clark. 2018. The EU trade secrets directive: all change for trade secret protection in Europe? *Journal of Intellectual Property Law & Practice* 13 (6): 445–457.

Občina Izola. 2019. *Notranja navodila o vsebini in krogotoku pogodb*. Interno gradivo, Občina Izola.

Občina Kranjska Gora. 2005. *Pravilnik o varstvu osebnih in zaupnih podatkov*. Interno gradivo, Občina Kranjska Gora.

Občina Preddvor. 2002. *Pravilnik o varovanju zaupnih in osebnih podatkov ter o varovanju dokumentarnega gradiva v občinski upravi Občine Preddvor in področja tajnih podatkov in poslovnih skrivnosti*. Interno gradivo, Občina Preddvor.

Občina Šentjernej. 2010. *Pravilniku o določitvi, ravnanju in varovanju zaupnih podatkov*. Interno gradivo, Občina Šentjernej.

Pacini, Carl J., Raymond Placid in Christine Wright-Isak. 2008. Fighting economic espionage with state trade secret laws. *International Journal of Law and Management* 50 (3): 121–135.

Pečar, Janez. 2001. Javnost ali tajnost državnih podatkov. *Revija za kriminalistiko in kriminologijo* 52 (1): 3–10.

Prezelj, Iztok in Anton Grizold. 2015. Razmerje med tajnostjo in javnostjo nacionalno varnostnih podatkov v sodobni demokratični državi. *Teorija in praksa* 52 (4): 670–685.

Prezelj, Iztok in Milan Tarman. 2015. Sistem varovanja tajnih podatkov v republiki Sloveniji v luči demokratičnega zagotavljanja nacionalne varnosti. *Teorija in praksa* 52 (4): 687–706.

Price Waterhouse Coopers. 2010. *Information security breaches survey 2010. Technical report*. Https://pwc.blogs.com/files/isbs-2010-report final.pdf (5. 1. 2020).

Price Waterhouse Coopers. 2012. *Information security breaches survey 2012. Technical report*. Https://www.pwc.co.uk/assets/pdf/olpapp/uk-information-security-breaches-survey-technical-report.pdf (5. 1. 2020).

Price Waterhouse Coopers. 2015. *Information security breaches survey 2015. Technical report*. Https://www.pwc.co.uk/assets/pdf/2015-isbs-technical-report-blue-digital.pdf (5. 1. 2020).

Razinger, Damjan. 2010. *Tajni podatki in industrijska varnost*. Magistrsko delo, Fakulteta za državne in evropske študije.

Robertson, Kirsten M., David R. Hannah in Brenda A. Lautsch. 2015. The secret to protecting trade secrets: How to create positive secrecy climates in organizations. *Business Horizons* 58 (6): 669–677.

Shulsky, Abram in Gary Schmitt. 2002. *Silent warfare: Uniderstanding the world of intelligence.* Lincoln: Potomac Books.

Sousa e Silva, Nuno. 2014. What exactly is a trade secret under the proposed directive? *Journal of Intellectual Property Law & Practice* 9 (11): 923–932.

Sodišče Evropske unije. 2020. *Pregled***.** Https://europa.eu/european-union/about-eu/institutions-bodies/court-justice_sl (23. 7. 2020).

Taber, Alexander M. 2015. Information control: making secrets and keeping them safe. *Arizona Law Review* 57 (2): 582–607.

Tarman, Milan. 2012. Obvladovanje informacij – korelacija varovanja tajnih podatkov in poslovnih skrivnosti. *Korporativna varnost* (1): 19–22.

Turk, Boštjan J. 2019. *Kazenska, odškodninska in disciplinska odgovornost delodajalca in delavca. Na kaj še posebej paziti?* Https://www.findinfo.si/medijsko-sredisce/v-srediscu/250830 (13. 7. 2020).

Urad vlade RS za varovanje tajnih podatkov. 2020. *Usposabljanja s področja varovanja tajnih podatkov*. Https://www.gov.si/dogodki/usposabljanje-s-podrocja-tajnih-podatkov-2/ (7. 2. 2020).

Zabojnik, Jan. 2002. A theory of trade secrets in firms. *International Economic Review* 43 (3): 831–855.

Zirnstein, Elizabeta. 2007. *Patentno varstvo v Evropi: razvoj in perspektive*. Koper: Univerza na Primorskem, Fakulteta za management.

Zirnstein, Elizabeta. 2016. *Izumi, avtorska dela in drugi rezultati ustvarjalnosti in inovativnosti v delovnem razmerju*. Koper: Univerza na Primorskem, Fakulteta za management.

Žakowska-Henzler, Helena. 2017. Confidential business information - definition and legal character of protection. *Wyższej Szkoły Finansów i Prawa w Bielsku-Białej* (4): 60–79.

## PRAVNI VIRI

Evropska skupnost (1994). Odločba Komisije 94/601/ES z dne 13. julija 1994. Https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A31994D0601 (13. 1. 2020).

Evropsko sodišče za človekove pravice (IV. oddelek). Tadeusza Matyjeka proti Poljski. Vloga št. 38184/03, 30. 5. 2003.

Sodišče Evropske unije. 2011. *Sklep predsednika Evropske komisije z dne 13. oktobra 2011 o funkciji in mandatu pooblaščenca za zaslišanje v nekaterih postopkih o konkurenci (2011/695/EU)*. Https://eur-lex.europa.eu/legal-content/SL/TXT/?uri=CELEX%3A32011D0695 (21. 7. 2020).

Sodišče Evropske unije. 2016. *Sklep podpredsednika Sodišča z dne 14. januarja 2016, AGC Glass Europe in drugi proti Evropski komisiji, ... Zadeva C-517/15 P-R.* Https://eur-lex.europa.eu/legal-content/SL/TXT/?uri=CELEX:62015CO0517 (13. 1. 2020).

Sodišče prve stopnje Evropske unije. 2005. *Zadeva T -48/05: Tožba Yvesa Francheta in Daniela Byka proti Komisiji Evropskih skupnosti, vložena dne 28. januarja 2005.* Https://op.europa.eu/en/publication-detail/-/publication/dd6baace-3224-471d-989c-705165f445fb/language-sl/format-PDF (12. 1. 2020).

Sodišče prve stopnje Evropskih skupnosti. 1998. *Sodba Sodišča prve stopnje (tretji razširjeni senat) z dne 14. maja 1998, Sarrió SA proti Komisiji Evropskih skupnosti, Konkurenca - Globa – Obrazložitev, Zadeva T-334/94, ECLI identifier: ECLI:EU:T:1998:97.* Https://eur-lex.europa.eu/legal-content/SL/TXT/?uri=CELEX%3A61994TJ0334 (11. 1. 2020).

Sodišče prve stopnje Evropskih skupnosti. 2003. *Sklep Sodišča prve stopnje (četrti senat) z dne 25. februarja 2003, Zadeva T-15/02, BASF AG proti Komisiji Evropskih skupnosti, Intervencija, Zadeva T-15/02, ECLI identifier: ECLI:EU:T:2003:38.* Https://eur-lex.europa.eu/legal-content/SL/ALL/?uri=CELEX:62002TO0015 (13. 1. 2020).

Sodišče prve stopnje Evropskih skupnosti. 2005. *Tožba Stradeblu s.r.l. proti Komisiji Evropskih skupnosti, vložena dne 6. maja 2005*. Https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2005:155:0031:0032:SL:PDF (9. 1. 2020).

Splošno sodišče Evropske unije (šesti senat). 2017. *Sodba Sodišča (šesti senat) z dne 26. julija 2017. AGC GLass Europe proti Evropski Komisiji - C 517/15P. Https://eur-lex.europa.eu/legal-content/SL/TXT/?uri=CELEX:62015CJ0517* (25. 7. 2020).

Splošno sodišče Evropske unije (tretji senat). 2015. *Sodba Splošnega sodišča (tretji senat) z dne 15. julija 2015. AGC GLass Europe proti Evropski Komisiji - T 465/12. Https://eur-lex.europa.eu/legal-content/SL/TXT/?uri=CELEX:62012TJ0465* (25. 7. 2020).

Splošno sodišče Evropske unije. 2011. *Sodba Splošnega sodišča (četrti senat) z dne 24. maja 2011, Navigazione Libera del Golfo Srl (NLG) proti Evropski komisiji ... Združeni zadevi T-109/05 in T-444/05, European Court Reports 2011 II-02479, ECLI identifier: ECLI:EU:T:2011:235.* Https://eur-lex.europa.eu/legal-content/SL/TXT/?uri=CELEX:62005TJ0109 (12. 1. 2020).

Upravno sodišče RS. 2013. *Sodba I U 1911/2012 z dne 23. 12. 2013.* Http://sodisce.si/usrs/odlocitve/2012032113074552/ (6. 1. 2020).

Upravno sodišče RS. 2016. *Sodba I U 900/2016-44 z dne 3. 10. 2018.* Http://www.sodisce.si/usrs/odlocitve/2015081111425841/ (7. 1. 2020).

Višje delovno in socialno sodišče RS (VDSS). 2012. *Sodba VDSS sklep Pdp 727/2012 z dne 30. 11. 2012.* Http://www.sodnapraksa.si/?q=id:2012032113054467&database[SOVS]=SOVS&database[IESP]=IESP&database[VDSS]=VDSS&database[UPRS]=UPRS&_submit=i%C5%A1%C4%8Di&page=0&id=2012032113054467 (5. 1. 2020).

Višje delovno in socialno sodišče RS. 2014. *Sodba Pdp 1132/2013 z dne 10. 4. 2014*. Http://www.sodisce.si/vdss/odlocitve/2012032113069112/ (5. 1. 2020).

Višje delovno in socialno sodišče RS. 2016. *Sodba Pdp 941/2015 z dne 18. 2. 2016*. Http://www.sodisce.si/vdss/odlocitve/2015081111398712/ (5. 1. 2020).

Višje sodišče v Ljubljani, Gospodarski oddelek. 2017. *VSL Sklep I Cpg 977/2017 ECLI:SI:VSLJ:2017:I.CPG.977.2017.* Http://www.sodnapraksa.si/?q=id:2015081111415957&database[SOVS]=SOVS&database[IESP]=IESP&database[VDSS]=VDSS&database[UPRS]=UPRS&_submit=i%C5%A1%C4%8Di&order=code&direction=desc&rowsPerPage=20&page=0&id=2015081111415957 (12. 1. 2020).

Vrhovno sodišče RS. 2013a. *Sodba VIII Ips 211/2012 z dne 2. 9. 2013.* Http://www.sodisce.si/znanje/sodna_praksa/vrhovno_sodisce_rs/2012032113058395/ (7. 1. 2020).

Vrhovno sodišče RS. 2013b. *Sodba in sklep VIII Ips 52/2012 z dne 16. 4. 2013*. Http://www.sodisce.si/vsrs/odlocitve/2012032113054487/ (8. 1. 2020).

Vrhovno sodišče RS. 2013c. *Sodba VIII Ips 200/2012 z dne 19. 2. 2013*. Http://sodisce.si/vsrs/odlocitve/2012032113053411/ (8. 1. 2020).

Vrhovno sodišče RS. 2016a. *Sodba in sklep VIII Ips 138/2016 z dne 11. 10. 2016*. Http://www.sodisce.si/vsrs/odlocitve/2015081111400156/ (8. 1. 2020).

Vrhovno sodišče RS. 2016b. *Sodba in sklep Pdp 774/2015 z dne 21. 1. 2016*. Http://www.sodisce.si/vdss/odlocitve/2015081111397259/ (9. 1. 2020).

Direktiva (EU) 77/62 EEC z dne 21. december 1976. Coordinating procedures for the award of public supply contracts. Https://op.europa.eu/en/publication-detail/-/publication/d56d7442-c46b-4126-84dc-170b896a9d4a/language-en (9. 1. 2020).

Direktiva (EU) 2016/943 Evropskega parlamenta in Sveta z dne 8. junija 2016 o varstvu nerazkritega strokovnega znanja in izkušenj ter poslovnih informacij (poslovnih skrivnosti) pred njihovo protipravno pridobitvijo, uporabo in razkritjem. *Uradni list EU*, št. L 157/1.

Mednarodni pakt o ekonomskih, socialnih in kulturnih pravicah OZN. *Uradni list SFRJ – MP*, št. 7/71Konvencija o varstvu človekovih pravic in temeljnih svoboščin. *Uradni list RS*, št. 3-20/1994.

Pogodba o delovanju Evropske unije (2012). *Uradni list EU*, št. C 326/47. Https://www.iusinfo.si/Priloge/EUII/12012E_TXT-SI.pdf (10. 1. 2020).

Pravilnik o strokovni usposobljenosti za delo z dokumentarnim gradivom. *Uradni list RS*, št. 66/16.

Sporazum o trgovinskih vidikih pravic intelektualne lastnine (Sporazum TRIPS). *Uradni list RS-MP*, št. 10/1995.

Uredba (EU) št. 648/2012 Evropskega parlamenta in Sveta z dne 4. julija 2012 o izvedenih finančnih instrumentih OTC, centralnih nasprotnih strankah in repozitorijih sklenjenih poslov. Https://eur-lex.europa.eu/legal-content/sl/TXT/?uri=celex%3A32012R0648 (28. 7. 2020).

Uredba Evropskega parlamenta in sveta o bonitetnih zahtevah za kreditne institucije in investicijska podjetja ter o spremembi Uredbe (EU) št. 648/2012. *Uradni list EU*, št. L 176/2013.

Uredba o upravnem poslovanju. *Uradni list RS*, št. 9/18.

Uredba o varnostnem preverjanju in izdaji dovoljenj za dostop do tajnih podatkov. *Uradni list RS*, št. 71/06 in 138/06.

Uredba o varovanju tajnih podatkov v komunikacijsko informacijskih sistemih. *Uradni list RS*, št. 48/07 in 86/11.

Uredba o varovanju tajnih podatkov. *Uradni list RS*, št. 74/05, 7/11 in 24/11 – popr.

Uredba Sveta (ES) št. 1/2003 z dne 16. decembra 2002 o izvajanju pravil konkurence iz členov 81 in 82 Pogodbe. *Uradni list EU*, št. L 1. Https://op.europa.eu/en/publication-detail/-/publication/509603ca-b929-4acf-8e11-765cd0079c06/language-sl (21. 7. 2020).

Uredba Sveta (ES) št. 1073/1999 Evropskega parlamenta in Sveta z dne 25. maja 1999 o preiskavah, ki jih izvaja Evropski urad za boj proti goljufijam. *Uradni list EU*, št. L 136. Https://eur-lex.europa. eu/eli/reg/1999/1073/oj?locale=sl (31. 7. 2020).

Ustava Republike Slovenije (URS). *Uradni list RS*, št. 33/91-I, 42/97 – UZS68, 66/00 – UZ80, 24/03 – UZ3a, 47, 68, 69/04 – UZ14, 69/04 – UZ43, 69/04 – UZ50, 68/06 – UZ121,140,143, 47/13 – UZ148, 47/13 – UZ90,97,99 in 75/16 – UZ70a.

Kazenski zakonik (KZ-1). *Uradni list RS*, št. 50/12 – uradno prečiščeno besedilo, 6/16 – popr., 54/15, 38/16, 27/17, 23/20 in 91/20.

Obligacijski zakonik (OZ). *Uradni list RS*, št. 97/07 – uradno prečiščeno besedilo, 64/16 – odl. US in 20/18 – OROZ631.

Zakon o bančništvu (ZBan-1). *Uradni list RS*, št. 99/2010.

Zakon o delovnih razmerjih (ZDR-1). *Uradni list RS*, št. 21/13, 78/13 – popr., 47/15 – ZZSDT, 33/16 – PZ-F, 52/16, 15/17 – odl. US in 22/19 – ZPosS.

Zakon o dostopu do informacij javnega značaja (ZDIJZ). *Uradni list RS*, št. 51/06, 117/06, 23/24, 50/14, 19/15, 102/15, 7/18.

Zakon o gospodarskih družbah (ZGD-1). *Uradni list RS*, št. 65/09, 33/11, 91/11, 32/12, 57/12, 44/13, 82/13, 55/15, 15/17, 22/19.

Zakon o Informacijskem pooblaščencu (ZInfP). *Uradni list RS*, št. 113/05 in 51/07 – ZUstS-A.

Zakon o javnem naročanju (ZJN-3). *Uradni list RS*, št. 91/15 in 14/18.

Zakon o javnih uslužbencih (ZJU). *Uradni list RS*, št. 63/07 – uradno prečiščeno besedilo, 65/08, 69/08 – ZTFI-A, 69/08 – ZZavar-E in 40/12 – ZUJF.

Zakon o poslovni skrivnosti (ZPosS). *Uradni list RS*, št. 22/19.

Zakon o pravdnem postopku (ZPP). *Uradni list RS*, št. 73/07 – uradno prečiščeno besedilo, 45/08 – ZArbit, 45/08, 111/08 – odl. US, 57/09 – odl. US, 12/10 – odl. US, 50/10 – odl. US, 107/10 – odl. US, 75/12 – odl. US, 40/13 – odl. US, 92/13 – odl. US, 10/14 – odl. US, 48/15 – odl. US, 6/17 – odl. US, 10/17, 16/19 – ZNP-1 in 70/19 – odl. US.

Zakon o preprečevanju omejevanja konkurence (ZPOmK-1). *Uradni list RS*, št. 36/08, 40/09, 26/11, 87/11, 57/12, 39/13.

Zakon o splošnem upravnem postopku (ZUP). *Uradni list RS*, št. 24/06 – uradno prečiščeno besedilo, 105/06 – ZUS-1, 126/07. 65/08, 8/10 in 82/13.

Zakon o tajnih podatkih (ZTP). *Uradni list RS*, št. 50/06 – uradno prečiščeno besedilo, 9/10, 60/11 in 8/20.

Zakon o upravnem sporu (ZUS-1). *Uradni list RS*, št. 105/06, 107/09 – odl. US, 62/10, 98/11 – odl. US, 109/12 in 10/17 – ZPP-E.

Zakon o varstvu dokumentarnega in arhivskega gradiva ter arhivih (ZVDAGA). *Uradni list RS*, št. 30/06 in 51/14.

Zakon o varstvu osebnih podatkov (ZVOP-1). *Uradni list RS*, št. 94/07 – uradno prečiščeno besedilo.