
B&B
VIŠJA STROKOVNA ŠOLA

Diplomsko delo višješolskega strokovnega študija
Program: Ekonomist
Modul: Organizator poslovanja

# UPORABA SLUŽBENE E-POŠTE IN VARSTVO ZASEBNOSTI

Mentor: dr. Borut Stražišar
Lektorica: Ana Peklenik, prof.

Kandidatka: Nataša Jelovčan

Kranj, december 2016

## ZAHVALA

Zahvaljujem se mentorju dr. Borutu Stražišarju za usmeritve in izkazano pomoč pri izdelavi diplomskega dela.

Zahvaljujem se tudi lektorici Ani Peklenik, ki je mojo diplomsko nalogo jezikovno in slovnično pregledala.

Posebna zahvala gre družini in prijateljem, ki so me vselej podpirali ter mi po potrebi tudi pomagali in svetovali.

**IZJAVA**

»Študentka Nataša Jelovčan izjavljam, da sem avtorica tega diplomskega dela, ki sem ga napisala pod mentorstvom dr. Boruta Stražišarja.«

»Skladno s 1. odstavkom 21. člena Zakona o avtorski in sorodnih pravicah dovoljujem objavo tega diplomskega dela na spletni strani šole.«

Dne _____ Podpis: _____

**POVZETEK**

V diplomski nalogi smo osvetlili določila zakonodajalca v povezavi z uporabo službene e-pošte ter predstavili prakso, ki se pojavlja v različnih delovnih organizacijah. V teoretičnem delu so predstavljene nekatere teoretične podlage o nadzoru zaposlenih, v empiričnem delu pa izsledki raziskave, pridobljene s spletno anketo, s katero smo ugotavljali, kako se v praksi organizacije zavedajo pomena zasebnosti pri uporabi službene pošte. Ugotovili smo, da je zakonodaja na področju zasebnosti pri uporabi službene e-pošte ustrezna, vendar jo organizacije vse premalo upoštevajo. Če bi želeli ničelno toleranco do zasebnosti na tem področju, bi bilo smiselno, da bi zakonodajalec razmislil o zakonski obveznosti uvedbe pravilnika o informacijski zasebnosti na delovnem mestu, podobno kot je urejeno področje varstva pri delu. V diplomskem delu je predstavljen tudi osnutek pravilnika o uporabi elektronske pošte, ker menimo, da bi njegova uvedba pomagala urediti medsebojna razmerja med zaposlenimi in organizacijami, povečala zavedanje o pomenu zasebnosti na delovnem mestu ter usposobila zaposlene in delodajalce za odgovorno uporabo informacijskih tehnologij.

**KLJUČNE BESEDE**

- elektronska pošta
- zasebnost
- zakonodaja
- delovna organizacija
- nadzor

**ABSTRACT**

In the theoretical section of the thesis, there is some theoretical background to employee monitoring. In the thesis, we have tried to shed light on the regulations of the employer concerning the use of work e-mail as well as the policy used in different work organisations. In the research section we have presented the results of the research, based on an internet survey that deals with how well the organisations in practice are aware of the importance of privacy in the use of work e-mail. The research shows that the legislation concerning the privacy in the use of work e-mail is sufficient but the organisations do not take it into account sufficiently. In order to achieve zero tolerance of privacy in this field it would be appropriate for the employer to consider a legal obligation concerning the regulation of data safety at the workplace in the same way it has already been regulated in the field of occupational safety. In the thesis section we have also presented a draft of the regulation when it comes to the use of e-mails because we believe that enforcing this regulation would help organize the interrelationship between employees and organisations and improve the awareness of the importance of privacy at the workplace as well as educate the employees and employers to a responsible use of information technology.

**KEYWORDS**

- e-mail
- privacy
- legislation
- work organization
- monitoring

**KAZALO**

## KAZALO SLIK



## KRATICE IN AKRONIMI

ZVOP-1: Zakon o varstvu zasebnosti
ZDR-1: Zakon o delovnih razmerjih
KZ-1: Kazenski zakonik

# 1 UVOD

## 1.1 PREDSTAVITEV PROBLEMA

Uporaba informacijske tehnologije v vsakdanjem poslovnem procesu postaja vedno bolj samoumevna. Informatizacijo tako srečujemo praktično na vsakem koraku – od popolnoma administrativnih opravil do robotizirane proizvodnje. S pojavom pametnih mobilnih telefonov in tabličnih računalnikov se je delovno okolje razširilo tudi v naše domove. Zlasti v terciarni dejavnosti pojem klasičnega delovnika izgublja pomen – zaposlenim in delodajalcem informacijska tehnologija omogoča večjo fleksibilnost delovnega časa.

Uporaba službenih sredstev informacijske tehnologije (računalnikov, pametnih telefonov ipd.) pa s seboj prinaša določene pasti. Če je bilo prej možno razlikovati med uporabo sredstev v zasebne in službene namene, tega zdaj skoraj ni več. Zaposleni dejansko informacijsko tehnologijo delodajalca uporabljajo tudi v zasebne namene. V določenih primerih delodajalci to izrecno ali molče dopuščajo, saj na ta način zaposlenim posredno povečajo plačo – gre za t. i. nefinančno motivacijo delavcev.

Dokler obstaja sporazum o takšni uporabi (lahko tudi tihi), večjih konfliktov ni. Vprašanja v zvezi z uporabo informacijske tehnologije pa se porodijo, ko dejansko pride do konflikta med delavcem in delodajalcem. V takšnem primeru želi delodajalec vpogled v uporabo takšnih sredstev tudi z namenom iskanja dokazov proti delavcu, s katerimi bi lahko še dodatno utemeljil prekinitev pogodbe o zaposlitvi.

Elektronski poštni predal (ali delavčeva e-pošta pri posameznem delodajalcu) je največkrat uporabljena storitev tudi za zasebne namene. Delavci tako poleg službene v svoj e-poštni predal prejemajo tudi zasebno pošto. Delodajalci takšne souporabe ne problematizirajo, dokler je delavec v delovnem razmerju. Do problema pa pride, če se službeni e-naslov začne uporabljati za namene blatenja delodajalca ali v primeru, ko delavcu preneha delovno razmerje (lahko iz krivdnih razlogov, lahko pa tudi zaradi smrti ali upokojitve).

Delodajalec lahko šele po daljšem času – po prenehanju delovnega razmerja ugotovi, da bi dejansko potreboval določeno e-pošto ali priponko od tam. Ker praviloma delodajalci ne nadzirajo e-pošte zaposlenih, je bistveno, da ima delodajalec vzpostavljena jasna pravila uporabe e-pošte in zlasti urejeno, kaj se zgodi s službeno e-pošto, ko delavcu preneha delovno razmerje. Ker pa na tem področju velja tudi načelo pisemske tajnosti, je treba biti pri tem zelo previden.

## 1.2 CILJI NALOGE

Cilj diplomske naloge je prikazati pravne ureditve področja e-pošte in varstva zasebnosti, da bi našli ustrezno rešitev. Ta mora na eni strani spoštovati zasebnost delavca, na drugi strani pa zagotoviti delodajalcu, da v primeru delavčevega odhoda pridobi vpogled v službeno e-pošto. Cilj naloge je tudi proučiti možnost uporabe sistema kakovosti za potrebe rešitve navedenega problema.

Rezultat naloge bo osnutek sistemskega postopka za uporabo in vpogled v e-pošto na delodajalčevem strežniku.

## 1.3 PREDSTAVITEV OKOLJA

Diplomska naloga kot osrednji problem obravnava vprašanje dostopa delodajalca v službeni e-poštni predal zaposlenih. Gre za konflikt dveh med seboj enakovrednih pravic: lastninske pravice delodajalca na e-poštnem strežniku oziroma pravice delodajalca do nadzora nad službeno dokumentacijo in pravice delavca do pisemske zasebnosti. V tem razmerju je treba upoštevati, da je delodajalčev položaj močnejši od delavčevega. Službena e-pošta je del poslovnega procesa in tako ima delodajalec neposredni pravni interes za dostop do njene vsebine.

## 1.4 PREDPOSTAVKE IN OMEJITVE

V diplomski nalogi smo predpostavljali, da delodajalci v organizacijah praviloma ne izvajajo nadzora nad zaposlenimi pri uporabi e-pošte in ob tem spoštujejo zakonodajo Republike Slovenije.

Predpostavljamo, da lahko v organizaciji z vzpostavljenim sistemom kakovosti z ustreznim sistemskim postopkom rešimo problem delodajalčevega dostopa do službenega e-poštnega predala delavca.

V raziskovalnem delu smo se omejili na podjetja znotraj Republike Slovenije.

## 1.5 METODE DELA

Diplomska naloga je razdeljena na teoretični in raziskovalni del. V teoretičnem delu je bila uporabljena domača literatura, ki se nanaša na vprašanje varovanja zasebnosti in uporabe elektronske pošte. V teoretičnem delu so navedene opredelitve varstva zasebnosti pri uporabi elektronske pošte v delovnem razmerju, ki so najbolj problematične. V raziskovalnem delu bo s pomočjo spletenega anketiranja različnih organizacij ugotovljeno stanje in praktične izkušnje zaposlenih. Z metodo sinteze bomo pripravili osnutek sistemskega postopka za uporabo službene e-pošte.

# 2 KAJ JE ELEKTRONSKA POŠTA

Elektronska pošta je ena najbolj razširjenih storitev na internetu. Je način sestavljanja, sprejemanja in pošiljanja sporočil preko različnih elektronskih komunikacijskih sistemov. Je sredstvo za izmenjavo sporočil med posamezniki in skupinami, zato postaja glavni način sporazumevanja med posamezniki, podjetji in ustanovami. Omogoča neosebno, enostavno, hitro in najcenejšo distribucijo sporočil, omogoča tudi pripenjanje različnih prilog. Enostavno pa je tudi shranjevanje oz. arhiviranje sporočil.

Elektronska pošta prinaša posredne (finančni prihranek) in neposredne koristi (boljša informiranost), kar je eden ključnih pogojev uspešnega poslovanja. Zavedati pa se moramo, da elektronska pošta prinaša tudi nekatere pasti, kot so nezaželena pošta, preko katere lahko okužimo računalnik, našo pošto pa lahko prestrežejo drugi (ni povsem varna). Na nekaterih delovnih mestih imajo zaposleni službeni in zasebni e-poštni naslov. Službenega naj bi uporabljali izključno za službene namene, zasebnega pa naj ne bi uporabljali v službi.

Resnik (2010) navaja prednosti in slabosti elektronske pošte.

Prednosti elektronske pošte:
- stroški pošiljanja so nižji,
- sporočila se prenašajo hitro, da se prenesejo do prejemnika, je potrebnih le nekaj minut, posledično je odzivnost tako večja kot učinkovitejša, povratne informacije so hitre,
- uporablja se lahko 24 ur vsak dan,
- možno jih je pošiljati na več naslovov brez dodatnih stroškov,
- možno je pripenjati poročila ali predstavitve,
- sporočila se lahko shranjujejo, posredujejo in pregledujejo skoraj kjerkoli in kadarkoli,
- zmanjšanje administrativnega dela, nadomestilo za tiskani izvod,
- poslovanje je preglednejše;
- omogoča tudi sodelovanje na virtualnih konferencah, kar prihrani potne stroške in neprijetnosti na potovanjih.

Slabosti elektronske pošte:
- pomanjkanje zanesljivosti, varnosti in tajnosti,
- nezaupanje v novosti,
- razvitost omrežja,
- pomanjkanje znanja in strokovnega kadra,
- možnost okužbe z virusi,
- prejemanje nezaželene pošte,

- stroški nabave programske in strojne opreme,
- neosebnost,
- nezaupanje v varnost, predvsem pri posredovanju osebnih podatkov.

# 3 ZASEBNOST NA DELOVNEM MESTU

## 3.1 POJEM ZASEBNOSTI

Pravica do zasebnosti se je v pravni teoriji začela razvijati ob koncu 19. stoletja. V ZDA je leta 1890 izšel članek avtorjev SD. Warrena in L. Brandeisa Right to privacy. V njem sta prvič opredelila pravico do zasebnosti kot temeljno pravico človeka do tega, da ima pravico biti sam in da je treba varovati zasebno življenje, ki ga ogrožajo številne mehanske naprave (Waren idr., 1890). DJ Solove v knjigi Understanding privacy (Solove, 2008, str. 12–13) koncept zasebnosti opredeljuje zlasti kot:

- pravico biti sam;
- možnost omejiti drugim dostop do osebnih podatkov;
- tajnost – možnost prikriti informacije pred drugimi;
- možnost nadzora uporabe informacij s strani drugih;
- varstvo intimnih razmerij.

O pravici do zasebnosti je v Republiki Sloveniji prvi razpravljal A. Finžgar (1985), ki jo je obravnaval v sklopu osebnostnih pravic. Tako poudarja, da se z osebnostnimi pravicami izraža varstvo človekovih osebnih dobrin v razmerju med posamezniki. Kot osebnostne pravice Finžgar med drugim opredeljuje:

- pravico do časti in dobrega imena,
- pravico do lastne podobe,
- pravico do pisemske tajnosti,
- pravico do osebnega življenja,
- pravico do duševne integritete.

J. Rovšek v knjigi Zasebno in javno v medijih (Rovšek, 2005, str. 42–43) pravi, da ima pravica do zasebnosti svoj izvor v naravnem pravu. To je pravica, ki je človeku prirojena, ki jo instinktivno čuti, ne da bi jo znal natančneje definirati. Je neodtujljiva in absolutna pravica. Prizadeti jo lahko uveljavlja nasproti vsakomur: državi, fizičnim in pravnim osebam. Pravica do zasebnosti je ena od elementarnih človekovih pravic, ki jo priznavajo tako mednarodni dokumenti o varstvu človekovih pravic kakor ustave posameznih držav. V tem pogledu je pravica do zasebnosti civilnopravnega značaja in se varuje s celo vrsto mehanizmov civilnega prava. To je pravica, ki izhaja iz človekovega dostojanstva in ga varuje tako pred posegi oblasti kot pred posegi drugih posameznikov ali civilnopravnih oseb.

V knjigi Zasebnost delavcev in interesi delodajalcev Bien Karlovškova pravi (Karlovšek, 2008, str. 18), da je zasebnost vrednota, ki ščiti posameznika, mu zagotavlja samospoštovanje, občutek lastne identitete, avtonomije, zato je za mnoge teoretike tako pomembna, da iz nje izvirajo vse druge pravice. Njeno bistvo je v zagotavljanju človekove svobode in delovanja, prostega kakršnekoli prisile, tako fizične kot psihične. Zasebnost kot pravica pa je najpogosteje določena kot prepoved vmešavanja države in družbe, vendar tudi kot vrednota, ki zagotavlja in omogoča stike z drugimi – pri tem so mišljene take vezi in izmenjava informacij z drugimi, ki so posamezniku po volji.

A. Tomšič (2016) opredeljuje vrste zasebnosti po zakonu ZVOP-1:

- splošna pravica do zasebnosti, 35. člen Ustave RS (ohranja zasebnost telesa in delovanja; poseg v posameznikov prostor in delovanje),
- prostorska zasebnost 36. člen Ustave RS (preprečitev neupravičenih pregledov posameznikove lastnine, stanovanja, avtomobila),
- komunikacijska zasebnost, 37. člen Ustave RS,
- informacijska zasebnost = varstvo osebnih podatkov po 38. členu Ustave RS.

»Zakon o varstvu osebnih podatkov ZVOP-1 je sistemski zakon, ki ureja pravice, obveznosti, načela in ukrepe, s katerimi se preprečujejo neustavni, nezakoniti in neupravičeni posegi v zasebnost in dostojanstvo posameznika oziroma posameznice pri obdelavi osebnih podatkov. Povedano pomeni, da ZVOP-1 poskuša v celoti urediti področje varstva osebnih podatkov v navedenih primerih. Iz besedila omenjene določbe izhaja, da je varstvo osebnih podatkov del širšega področja varstva zasebnosti oziroma tako imenovane informacijske oziroma podatkovne zasebnosti, kar je drug naziv za varstvo osebnih podatkov« (Pirc Musar, 2007).

## 3.2 PRAVNA UREDITEV ZASEBNOSTI NA DELOVNEM MESTU V REPUBLIKI SLOVENIJI

Pri pravni ureditvi zasebnosti v Republiki Sloveniji je treba najprej izhajati iz ustreznih določb Ustave RS. Tako so za problematiko, obravnavano v tem diplomskem delu, najpomembnejše določbe 34.–38. člena.

Tako je v 34. členu določeno, da ima vsakdo pravico do osebnega dostojanstva in varnosti. Pravica do osebnega dostojanstva in varnosti pomeni, da morata biti človeško dostojanstvo in varnost zavarovana pred posegi države in tudi pred posegi posameznikov (prepoved ponižujočega ravnanja, mučenja, diskriminacije, zapoved enakosti in nedotakljivosti človeškega življenja).

Po določbi 35. člena je vsakomur zagotovljena nedotakljivost človekove telesne in duševne celovitosti, njegove zasebnosti ter osebnostnih pravic. Pravica do zasebnosti in osebnostnih pravic pomeni, da je vsakomur zagotovljena nedotakljivost človekove telesne in duševne celovitosti, njegove zasebnosti ter osebnostnih pravic.

Določba 37. člena Ustave RS zagotavlja varstvo tajnosti pisem in drugih občil. Ta člen določa, da je vsak poseg v komunikacijsko zasebnost posameznika nedopusten, v njem pa so določeni tudi pogoji, pod katerimi je lahko ta pravica omejena. S tem členom se izrazi dimenzija zasebnosti, ki se nanaša na komunikacijo. Zagotovljena je tajnost pisem in drugih občil. Samo zakon lahko predpiše, da se na podlagi odločbe sodišča za določen čas ne upošteva varstvo tajnosti pisem in drugih občil in nedotakljivost človekove zasebnosti, če je to nujno za uvedbo ali potek kazenskega postopka ali za varnost države. Kovačič (2003, str. 80–82) opozarja, da med občila štejemo telefonsko komunikacijo, elektronsko pošto, SMS-sporočila ipd., saj oblika in vsebina sporazumevanja nista pomembni. Komunikacijska zasebnost je varovana ne glede na to, ali se poročilo prenaša v zasebnih zaprtih ali v javnih telekomunikacijskih omrežjih. Poleg vsebine komunikacije so varovani tudi t. i. prometni podatki (telefonske številke, količina prenesenih podatkov, čas trajanja). Pisemska tajnost je varovana tudi v okviru 139. in 140. člena Kazenskega zakonika RS. 139. člen Kazenskega zakonika – kršitev tajnosti občil določa, da kdor neupravičeno odpre tuje pismo, tujo brzojavko ali kakšno drugo tuje zaprto pisanje ali pošiljko, se kaznuje z denarno kaznijo ali zaporom do šestih mesecev. Prav tako se z denarno kaznijo ali zaporom do enega leta kaznuje, kdor se z uporabo tehničnih ali kemičnih sredstev, ne da bi odprl tuje pismo, tujo brzojavko ali kakšno drugo tujo zaprto pošiljko, neupravičeno seznani z njihovo vsebino; kdor se z uporabo tehničnih sredstev neupravičeno seznani s sporočilom, ki se prenaša po telefonu ali s kakšnim drugim elektronskim komunikacijskim sredstvom; kdor neupravičeno odpre zaprt predmet, ki varuje sporočilo, in se neupravičeno seznani s sporočilom v njem. Enako se kaznuje, kdor s katerim od dejanj, ki so navedena v prvem in drugem odstavku tega člena, omogoči drugemu, da se neposredno seznani z vsebino sporočila ali pošiljke. Zakon v nadaljevanju določa, da se tisti, ki neupravičeno obdrži, skrije, uniči ali komu drugemu izroči tuje pismo, brzojavko ali kakšno drugo pošiljko, preden se je prejemnik seznanil z njeno vsebino, kaznuje z denarno kaznijo ali zaporom do enega leta. Zakon obenem določa, da se v primeru, da stori navedeno dejanje uradna oseba z zlorabo uradnega položaja ali uradnih pravic, poštni ali drug delavec, ki mu je zaupano prevzemanje, prenos ali predaja tujih pisem, tujih brzojavk ali kakšnih drugih pisanj ali pošiljk, tega kaznuje z zaporom od treh mesecev do petih let. 140. člen Kazenskega zakonika – nedovoljena objava zasebnih pisanj določa, da kdor brez dovoljenja pooblaščene osebe, kadar je tako dovoljenje potrebno, objavi dnevnik, pismo ali kakšno drugo zasebno pisanje, se

kaznuje z denarno kaznijo ali zaporom do enega leta (Uradni list RS, PIS, Kazenski zakonik, 2008).

Varstvo delavčeve zasebnosti je urejeno v določbah 46.–48. člena Zakona o delovnih razmerjih. Tako 46. člen ZDR-1 določa, da mora delodajalec varovati in spoštovati delavčevo osebnost ter upoštevati in ščititi delavčevo zasebnost. Po določbi 47. člena ZDR-1 je delodajalec dolžan zagotavljati takšno delovno okolje, v katerem noben delavec ne bo izpostavljen kakršnemu koli nadlegovanju ali trpinčenju s strani delodajalca, predpostavljenih ali sodelavcev. V ta namen mora delodajalec sprejeti ustrezne ukrepe za zaščito delavcev in o njih pisno obvestiti delavce. Če delavec v primeru spora navaja dejstva, ki opravičujejo domnevo, da je delodajalec ravnal v nasprotju, je dokazno breme na strani delodajalca. Določba 48. člena ZDR-1 pa je namenjena varovanju delavčevih osebnih podatkov. Osebni podatek je katerikoli podatek, ki se nanaša na posameznika, ne glede na obliko, v kateri je izražen (2. točka 6. člena ZVOP-1). Pri tem je posameznik določena ali določljiva fizična oseba, na katero se nanaša osebni podatek. Tako določa, da se osebni podatki se lahko zbirajo, uporabljajo obdelujejo in posredujejo tretjim osebam, samo če je to določeno s tem ali drugim zakonom ali če je to potrebno zaradi uresničevanja pravic in obveznosti iz delovnega razmerja ali v zvezi z delovnim razmerjem. Osebne podatke lahko zbira, obdeluje, uporablja in posreduje samo pooblaščena oseba v organizaciji. Osebni podatki, za katere ne obstaja več zakonska podlaga, se morajo takoj zbrisati in prenehati uporabljati. Te določbe se uporabljajo tudi za osebne podatke kandidatov. Seveda pa osebne podatke varuje tudi Zakon o varstvu osebnih podatkov, ki prizadetemu daje tudi možnost upravnega varstva.

Na drugi strani pa določba 67. člena ustave RS izrecno varuje lastninsko pravico posameznika (ne glede na to, ali gre za fizično ali pravno osebo). V tej določbi so opredeljeni vidiki lastnine. Zakon določa način pridobivanja in uživanja lastnine, tako da je zagotovljena njena gospodarska, socialna in ekološka funkcija. Tako ima delodajalec dejansko lastninsko pravico nad vsem, kar nastaja kot del proizvodnega procesa (in sem sodijo tudi poslovne informacije). Iz navedenega razloga v podjetjih izhaja argumentacija o popolnem varstvu delavčeve zasebnosti. Dosledno spoštovanje omenjenih načel bi namreč prepovedalo vsak delodajalčev poseg v delavčevo sfero. S tem pa je delodajalcu kršena pravica do zasebne lastnine in njegovega uživanja te. Tako se v danih okoliščinah srečamo z navzkrižjem dveh ustavnih pravic, to sta pravica do lastnine (67. člen Ustave RS) in pravica do zasebnosti. Delodajalec ima pravico do oblasti nad svojimi sredstvi, pravico do nadzora, delavec pa pričakuje zasebnost (Karlovšek, 2008, str. 27).

Ustava RS v 38. členu zagotavlja varstvo osebnih podatkov. Z namenom zaščite informacij, ki se nanašajo na posameznika, ustava zagotavlja varstvo osebnih podatkov na naslednji način: prepovedana je uporaba osebnih podatkov v nasprotju

z namenom njihovega zbiranja. Zbiranje, obdelovanje, namen uporabe, nadzor in varstvo tajnosti osebnih podatkov določa zakon. Vsakdo ima pravico seznaniti se z zbranimi osebnimi podatki, ki se nanašajo nanj, in pravico do sodnega varstva ob njihovi zlorabi.

## 3.3 ZASEBNOST NA DELOVNEM MESTU

Meje zasebnosti na delovnem mestu so začrtane z razmerjem med delavcem in delodajalcem in s tem z razmerjem, ki tradicionalno velja za razmerje med dvema neenakovrednima akterjema: med izrazito šibkim delavcem in izrazito močnim delodajalcem. Delodajalčeva moč se ne kaže le v ekonomski premoči, temveč tudi na občutljivem področju posameznikove svobode kot tiste dobrine, ki zasebnost varuje. Hiter tehnološki razvoj, predvsem interneta in informacijske tehnologije, pomeni novo grožnjo zasebnosti kljub številnim prednostim v delovnem procesu. Nove tehnične možnosti namreč potencialno omogočajo doslej neznane možnosti posega v zasebnost, delodajalci pa jih pogosto nekritično sprejemajo, ker bi pripomogle k boljšemu izkoristku delavca, k večji storilnosti in produktivnosti, varovale naj bi delavčevo lastnino in prispevale k boljši kakovosti dela (Karlovšek, 2008, str. 18–19).

Na delovnem mestu se nad zaposlenimi izvajajo naslednje oblike nadzora (Cerar, 2006):

- osebnostno in psihološko testiranje in raziskovanje osebnih lastnosti,
- nadzor nad prihodom in odhodom z delovnega mesta,
- splošni video nadzor,
- nadzor nad telefonskimi klici,
- snemanje pogovorov na sestankih ali v določenih prostorih,
- nadzor nad uporabo interneta,
- nadzor nad e-pošto,
- nadzor nad uporabo računalniške tipkovnice,
- nadzor nad lokacijo oziroma gibanjem delavca znotraj službenih prostorov,
- nadzor nad lokacijo delavca pri uporabi službenega avtomobila,
- nadzor nad delavčevo prehrano in morebitnimi odvisnostmi,
- nadzor nad oblačenjem, vedenjem in druženjem delavcev.

Precejšnji del navedenih oblik nadzora se v praksi pri nas ne uporablja, zaposlene je treba nadzirati do neke mere, kajti popoln nadzor je lahko nekakšno totalitarno nasilje nad posameznikom.

Velja prepričanje, da je do neke mere delavcu treba dopustiti oziroma tolerirati zasebnost, če to ne vodi v poslabšanje kakovosti dela ali v prevelike dodatne stroške. Delavca določena dopustna mera zasebnih ravnanj lahko spravijo v zadovoljstvo ali sprostitev, kar lahko pozitivno oziroma stimulativno vpliva na

njegovo kakovost in učinkovitost. Pameten delodajalec bo delavcem vedno dopustil toliko svobode, zasebnosti in osebnega dostojanstva, da se bo delavec počutil človeško (Cerar, 2006).

Zasebnost v pravu delimo na pet področij (Karlovšek, 2008, str. 20):

- informacijska zasebnost, ki se nanaša na osebne podatke in informacije o posamezniku;
- zasebnost človeškega telesa, ki ščiti pred nedovoljenimi posegi v posameznikovo telo;
- zasebnost človeške osebnosti, ki ščiti njegove nazore, opredelitve, način izražanja;
- komunikacijska zasebnost, ki ščiti komunikacijo in z njo povezane podatke;
- prostorska zasebnost, ki varuje posameznika v vseh prostorih, kjer pričakuje zasebnost.

## 3.4 E-POŠTA IN ZASEBNOST NA DELOVNEM MESTU

Elektronska pošta v današnji informacijsko-komunikacijski družbi predstavlja eno najhitrejših komunikacijskih sredstev. Pri poslovanju podjetja je najpomembnejša, ker omogoča obveščanje zaposlenih na najhitrejši način v katerem koli času. Ker je preprosta za uporabo, se je v praksi zelo dobro uveljavila. Podjetja z njo pošiljajo razna obvestila, gradiva za sestanke, račune kupcem, razne poslovne dokumente ipd. S tem se prihranijo stroški za tiskanje, stroški pošiljanja, predvsem pa čas. Z vse hitrejšim razvojem različnih tehnologij je tako postal tudi nadzor nad zaposlenimi enostavnejši, vendar je pri tem treba upoštevati zakonska določila.

Številne možnosti nadzora pripeljejo do konflikta med delavci, delodajalci in tretjimi osebami. Največ vprašanj, ki zadevajo korporativne interese in pravice posameznika do zasebnosti, se poraja v zvezi z e-pošto. Oprema in službeni elektronski naslov sta namreč last delodajalca, zaposleni pa imajo zgolj pravico do uporabe, zato lahko delodajalec omejuje dostop do službene e-pošte, saj je včasih težko ločiti zasebna sporočila od službenih. Dodatno težavo predstavljajo tudi sporočila tretjih oseb, ki so lahko službene ali zasebne narave, saj se z nadzorom komunikacij delavca nadzoruje tudi komunikacija njegovih zunanjih partnerjev (Hvaliček, 2012).

V našem pravnem prostoru je koncept zasebnosti uveljavljen in močan. Odmaknjen je od t. i. lastninskega koncepta, po katerem ima delodajalec številne pravice, ker poseduje poslovne prostore, ker upravlja in vzdržuje delovna sredstva (telefone, računalnike, internet ipd.) (Karlovšek, 2008, str. 21). Zasebnost zagotavlja že Ustava RS v 37. členu, ki govori, da samo zakon lahko predpiše, da se na podlagi odločbe sodišča za določen čas ne upošteva varstvo tajnosti pisem in drugih občil ter nedotakljivost človekove zasebnosti, če je to nujno za uvedbo ali potek

kazenskega postopka ali varnost države. To pomeni, da delodajalec brez dovoljenja pošiljatelja in prejemnika ne sme prebirati elektronskih sporočil.

Delovnopravna zakonodaja narekuje delavcu, da opravlja delo po navodilih in ob nadzoru delodajalca. Tako so delodajalci upravičeni do nadzora nad delavci, vendar morajo biti delavci vnaprej seznanjeni s pravili. Delavci se morajo s nadzorom strinjati prostovoljno in brez prisile. Delodajalec si lahko legalno pomaga z nastavitvami poštnega strežnika, kar pomeni, da lahko uporabo e-pošte in interneta omeji, tako da delavcem omogoči dostop samo do tistih spletnih strani, ki jih potrebujejo za delo, oz. blokira dostop do določenih spletnih strani, blokira določeno e-pošto na strežniku ipd. (Hvaliček, 2012).

## 3.5 VPOGLED V ELEKTRONSKO POŠTO ZAPOSLENEGA

Delodajalčevo preverjanje elektronske pošte zaposlenega je dopustno, le če vnaprej opredeli namene, primere, okoliščine, zaradi katerih je potrebna obdelava elektronskih sporočil, naslovljenih na delavca. Primeri, v kateri bi bilo to dopustno, so grozeča poslovna škoda, dolgotrajna odsotnost, nezmožnost pridobitve osebne privolitve za vpogled. Vsebino same pošiljke bi delodajalec lahko pogledal samo na podlagi privolitve zaposlenega. Določilo v pogodbi o zaposlitvi, da lahko delodajalec gleda elektronsko pošto zaposlenega, ne pomeni generalnega pooblastila za delodajalca, da lahko pregleduje pošto. Pomeni lahko le seznanitev z možnostjo pregleda v primerih, ki morajo biti vnaprej določeni in zapisani v internem aktu podjetja. Če bi delodajalec sumil, da delavec preko elektronske pošte opravlja kaznivo dejanje, je dolžan obvestiti pristojne organe. Delodajalec pa lahko omeji uporabo službenega elektronskega naslova, če se izkaže, da ta ni uporabljen v skladu s politiko delodajalca glede uporabe službenih sredstev (povečano število virusov, počasno delovanje sistema, odziv tretjih oseb ipd.) (Pirc Musar, 2010).

Zastavlja se vprašanje, kako je z vpogledom ali preusmeritvijo elektronske pošte bivšega zaposlenega v podjetju. To elektronsko pošto se občasno potrebuje za delo. V podjetju imajo nastavljen samodejni odgovor, da osebe ni več v podjetju, vendar je treba zagotoviti nemoten delovni proces. Ali je dovoljen vpogled oziroma preusmeritev stare pošte? Pooblaščenec odgovarja, da zastopa stališče, da je zaposlenemu pred prekinitvijo dana možnost, da še zadnjič vpogleda v svojo elektronski predal in pošto, ki se nanaša na njegovo osebnost, zbriše oz. shrani na drug medij, hkrati pa obvesti svoje kontakte, da njegov naslov ni več dostopen. To je najbolje storiti ob prisotnosti komisije, da ne bi zbrisal še podatkov, ki so pomembni za podjetje. Ob koncu se napiše zapisnik. V to pošto bivšega zaposlenega bi lahko dostopali samo na podlagi odločbe sodišča. Vsaka oblika nadzora, ki pomeni poseg v zasebnost, mora biti vnaprej utemeljena v internih aktih podjetja in mora imeti zakonsko podlago. Pregled e-pošte s strani delodajalca mora biti določen vnaprej.

Ena od rešitev tega problema bi bilo oblikovanje skupnega službenega elektronskega predala z neosebnim imenom (Prelesnik, 2015).

Če delodajalec pregleduje elektronsko pošto, ko je delavcu delovno razmerje prenehalo oz. še dela, če delavec ni predhodno seznanjen in določilo ni vpisano v internem aktu podjetja, je to kaznivo dejanje. Za pregon kaznivega dejanja pa je pristojno državno tožilstvo. V primeru prenehanja delovnega razmerja je delodajalec dolžan blokirati elektronski naslov in zbrisati e-pošto bivšega zaposlenega.

## 3.6 MOŽNE REŠITVE

Kot je bilo omenjeno, službeno e-pošto zaposleni uporabljajo tako za zasebne kot tudi za službene namene. Ker so možnosti vpogleda v e-pošto zaposlenih s strani delodajalca zelo omejene, je torej treba vzpostaviti sistem, ki bo ščitil tako delavčevo zasebnost kot tudi delodajalčevo pravico do službene dokumentacije (ki je last delodajalca in ne last delavca). Gre torej za konflikt med lastninsko pravico delodajalca na službeni dokumentaciji (kamor med drugim sodijo tudi komunikacija s strankami, interna korespondenca v zvezi s službenimi problemi ipd.) ter pravico delavca do zasebnosti in pisemske tajnosti (kamor uvrščamo tudi e-pošto). Pristop delodajalca k temu problemu mora biti tako večstopenjski in posledično jasno urejen z notranjimi akti.

Prva naloga delodajalca je jasna opredelitev, kaj je službena dokumentacija. Pri tem se lahko uporablja kombinacija objektivnih (ni določen s sklepom, je pa očitno, da bo nastala občutna škoda, če bi zanj izvedela nepooblaščena oseba) in subjektivnih (določeno s pisnim sklepom) kriterijev. Tako so lahko kot službena dokumentacija opredeljena vsa sporočila posredovana ali prejeta od poslovnih partnerjev oz. njihovih zaposlenih (npr. sporočila, ki vsebujejo poštni naslov partnerja). Na drugi strani pa so lahko podani naslednji objektivni kriteriji:

- sporočilo vsebuje sklicevanje na določen poslovni dopis;
- sporočilo je vezano na reševanje določene reklamacije ali spora med poslovnima partnerjema;
- sporočilo vsebuje informacije, vezane na notranji proizvodni proces delodajalca;
- sporočilo vsebuje priponke, ki so del poslovne dokumentacije delodajalca (npr. ponudba, račun, predračun, zapisnik, osnutki internih aktov, pogodb ipd.);
- vsebina sporočila pomeni izvršitev delavčeve obveznosti (npr. obvestilo o nastopu bolniškega dopusta, poročilo o službeni poti ipd.).

Drugo stopnjo v procesu predstavlja vzpostavitev sledljivosti dokumentacije (kar velja tudi za e-pošto). To pomeni, da mora delavec pošto, ki se nanaša na isto

zadevo ali poslovne dogodke, sam razvrščati v ustrezne podmape znotraj poštnega predala ali pa, da se mora vzpostavljati znotraj samega sistema odgovarjanja nepretrgana veriga sporočil. Dodatno k sledljivosti prispevajo tudi pravila o označevanju zadeve v meta podatkih (so podatki, ki opisujejo druge podatke in s tem dajejo dodatno informacijo o pomenu in lastnostih) e-pošte ali pa uporaba dodatnega polja znotraj samega e-poštnega sporočila, ki vsebuje ključne deskriptorje. Dejstvo je, da e-pošta praviloma pomeni zgolj »vrečo« praviloma neorganiziranih sporočil. Če ima podjetje vzpostavljen elektronski sistem obvladovanja dokumentacije, se lahko tudi službena pošta z izvozom ustrezno obdeluje znotraj takšnega sistema. V takšnem primeru je potreba delodajalca po vpogledu v e-pošto delavca bistveno zmanjšana. V tem delu procesa je treba vzpostaviti tudi jasno pravilo, da mora delavec znotraj e-pošte vzpostaviti posebno mapo za zasebno e-pošto in da mora vsa takšna sporočila iz predala s prispelo pošto prenašati v takšno podmapo. Torej gre za delavčevo pravico in obveznost, da sam poskrbi za varovanje svoje zasebnosti in pisemske tajnosti.

Tretjo stopnjo predstavlja izdelava in sprejem notranjega akta ali sistemskega postopka, ki vzpostavi sistem uporabe službene e-pošte tako za službene kot tudi za zasebne namene. Priporočljivo je, da delodajalec takšen akt pred sprejemom da v javno obravnavo in zaposlenim (oz. njihovim predstavnikom) omogoči tudi rešitve, ki so vezane na določeno lokalno okolje (oz. za utečeno stanje).

Zadnjo stopnjo predstavlja seznanjanje vseh zaposlenih s sprejetimi pravili na področju upravljanja s službenim e-poštnim predalom. Tudi ta stopnja naj se izvaja postopoma s sprotnim in dnevnim informiranjem o novosti ter pomočjo zaposlenim pri razreševanju zatečenega stanja. Zavedati se je treba, da sprememb ni možno doseči čez noč. Spremembe namreč zahtevajo tako prilagoditev obnašanja zaposlenih kot tudi prilagoditev njihovih osebnih vrednot.

# 4 RAZISKAVA UPORABE SLUŽBENE ELEKTRONSKE POŠTE IN VARSTVO ZASEBNOSTI

V današnjem času globalizacije in vse hitrejšega razvoja, ko vse več poslovnih aktivnosti poteka preko računalniške tehnologije, kot so pametni telefoni in tablični ter prenosni računalniki, in se delo ne opravlja zgolj na sedežu podjetja in ne zgolj ob določenem delovnem času, ampak se opravlja od doma, na daljavo ipd., je uporaba službene pošte težko ločljiva od zasebnosti. Zato smo se odločili raziskati, kakšen je nadzor na delovnem mestu in zasebnost glede uporabe elektronske pošte v nekaterih slovenskih podjetjih in ustanovah. Naključno smo izbrali predstavnike različnih podjetij, ki se ukvarjajo z gospodarsko dejavnostjo, javna podjetja, zdravstvene ustanove, šole, vrtce, kulturne ustanove, ministrstva.

Zaradi najlažjega in najenostavnejšega dostopa in obdelave podatkov smo se odločili, da opravimo spletno anketo, ki je bila izdelana in opravljena s pomočjo aplikacije Moja anketa.si. Anketiranje je potekalo od 4. do vključno 9. oktobra 2016, tako da je bila povezava do spletne ankete poslana vsem izbranim osebam po elektronski pošti.

Namen in cilj anketnega vprašalnika, ki je sestavljen iz 14 vprašanj, je pridobiti informacije o tem, ali podjetja opravljajo nadzor na delovnem mestu, kakšne so oblike nadzora, ali anketiranci menijo, da je nadzor na delovnem mestu potreben, kakšna je zasebnost na delovnem mestu, še posebej pa nas je zanimala zasebnost pri uporabi elektronske pošte v nekaterih slovenskih podjetjih in organizacijah.

## 4.1 REZULTATI RAZISKAVE

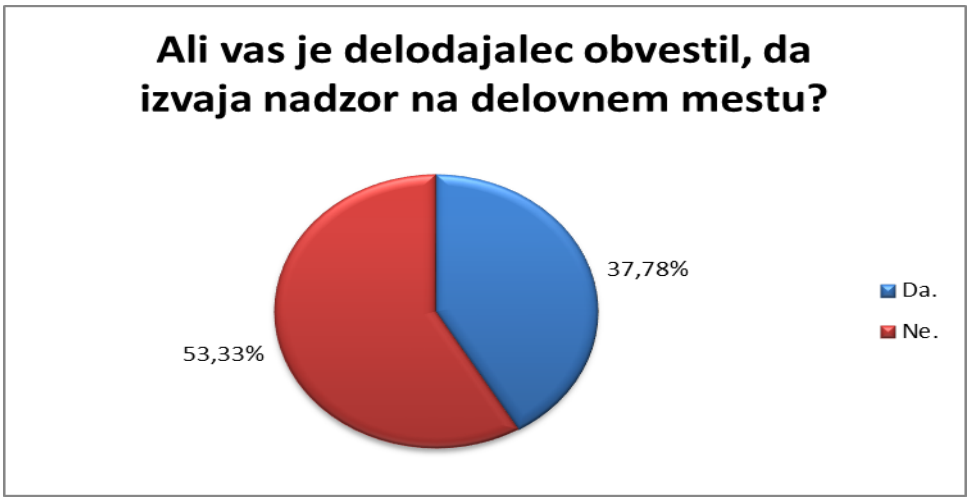
Kot je bilo že omenjeno, so anketo izpolnjevali predstavniki različnih slovenskih podjetij preko spletnega vprašalnika. V času anketiranja smo zbrali 45 izpolnjenih anket. Anketiranje je bilo anonimno.


*Slika 1: Število zaposlenih*
(Lastni vir)

Najprej smo vprašali, koliko zaposlenih je v njihovem podjetju. Velika večina anketirancev, kar 73,33 %, opravlja delo v večjih organizacijah. Razlika med majhnimi, srednjimi in velikimi podjetji naj bi se kazala predvsem v zavedanju informacijske varnosti, kadrovskih, organizacijskih zmožnostih njenega organiziranja. Manjša podjetja so največrat tudi v družinski lasti, ne posvečajo dovolj pozornosti informacijski varnosti in se ne zavedajo zahtev zakonodaje na tem področju. Iz grafa je razvidno, da so odgovarjali v največjem deležu zaposleni iz večjih podjetij, kjer bi morali imeti področje informacijske varnosti urejeno.


*Slika 2: Nadzor na delovnem mestu*
(Lastni vir)

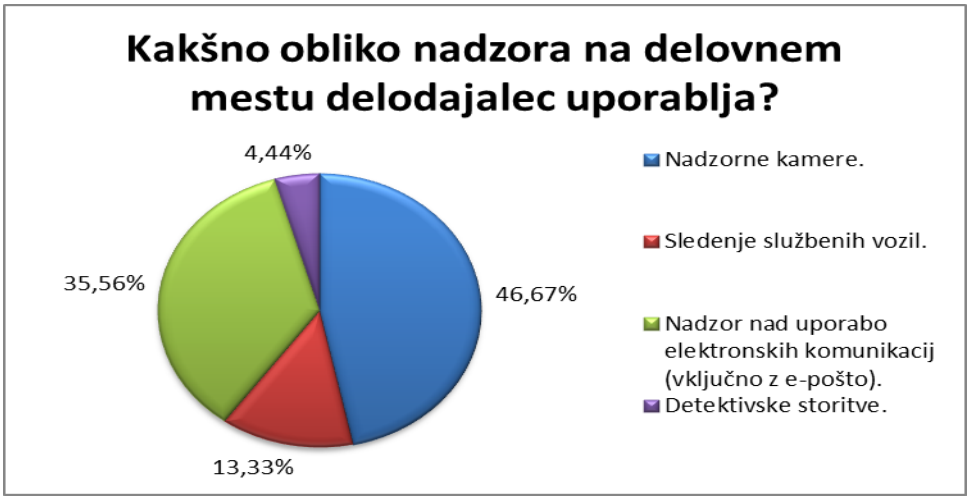
Iz grafikona na sliki 2 je razvidno, da se pri dobri polovici, kar 51,11 % anketirancih, izvaja nadzor na delovnem mestu. 33,33 % anketirancem to ni znano, pri 15,56 % anketiranih pa se to ne dogaja. Rezultat je zanimiv, saj se v večini primerov nadzor na delovnem mestu dogaja, smiselno pa je ugotavljati, ali se izvaja skladno z zakonskimi določili ali prihaja do nezavednih ali celo zavednih kršitev zakonodaje.




*Slika 3: Obvestilo o nadzoru na delovnem mestu*
(Lastni vir)

Zaskrbljujoče je, da kar 53,33 % zaposlenih ni bilo obveščenih o nadzoru na delovnem mestu, kar si delno lahko razlagamo s korelacijo z drugim vprašanjem, pri katerem 15,56 % organizacij ne izvaja nadzora na delovnem mestu, vendar je razkorak vseeno prevelik. V anketi so sodelujoči odgovarjali, da je obveščanje odvisno od vrste nadzora: preko oglasne deske, pisnih navodil zaposlenim ali preko nenapovedanih pregledov. Vse oblike, navedene v odgovorih, so lahko sporne, saj

mora imeti organizacija izdelan notranji pravilnik za izvajanje nadzora na delovnem mestu, ki je usklajen z zakonodajo in največkrat tudi s sindikatom podjetja.



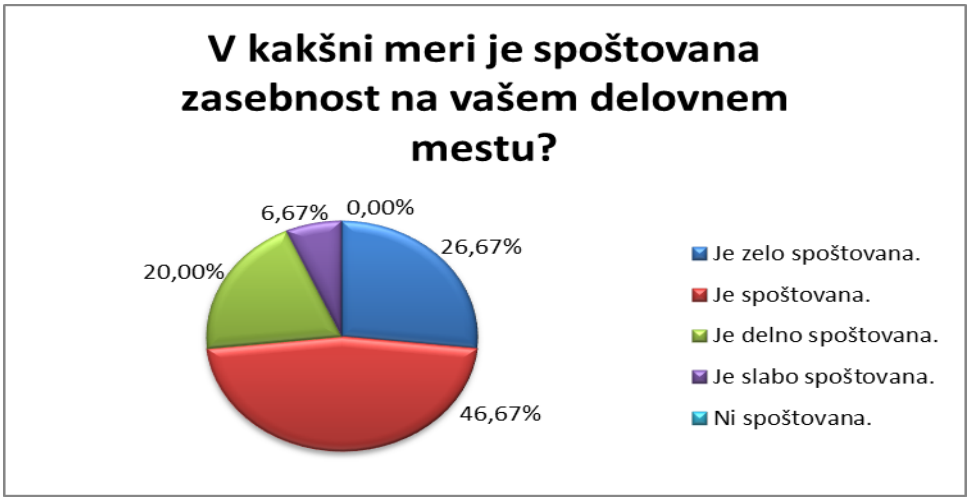

*Slika 4: Oblike nadzora na delovnem mestu*
(Lastni vir)

Odvisno od panoge organizacije uporabljajo različne oblike nadzora, kot je nadzor nad uporabo elektronskih komunikacij, nadzorne kamere, sledenje vozilom, detektivske storitve. Vsaka od naštetih oblik nadzora je načeloma dovoljena, vendar je zakonodajalec predvidel številne omejitve pri uporabi teh metod, kar mora biti v podjetju natančno določeno z notranjim pravilnikom. V podjetjih se verjetno uporabljajo tudi drugi načini nadzora, vendar so zgoraj opisani najpogostejši. V vsakem primeru pa mora biti nadzor reguliran, usklajen z zakonodajo in zaposlenimi.


*Slika 5: Mnenje o nadzoru na delovnem mestu*
(Lastni vir)

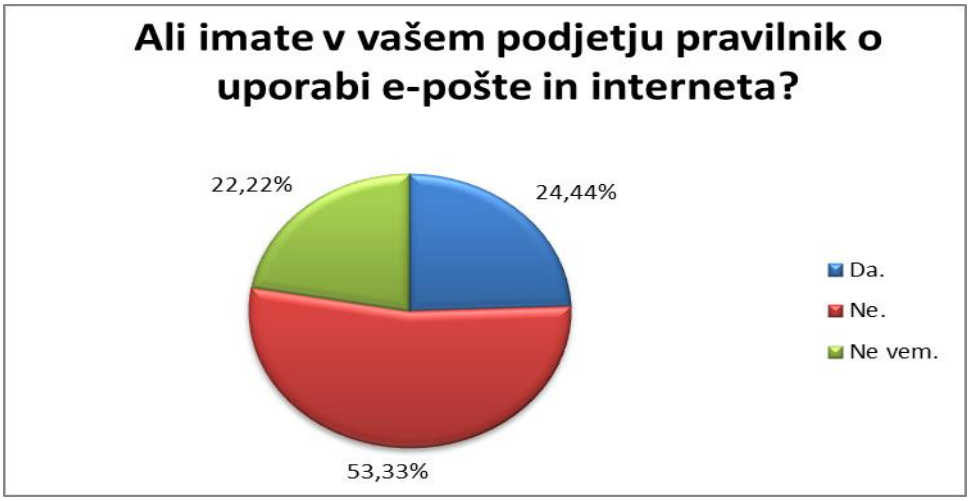
Zanimiv je izid ankete, ki kaže, da kar 66,67 % zaposlenih čuti, da je nadzor na delovnem mestu potreben. To kaže, da večina zaposlenih razume potrebo po

nadzoru, predvsem z varnostnega vidika, kot npr. trgovke v varovanih območjih trgovin, bančni uslužbenci, zaposleni v transportu. 33,33 % zaposlenih pa meni, da nadzor ni potreben in ga povezujejo z zlorabami novih tehnologij, nadzorom nad učinkovitostjo dela ali celo mobingom na delovnem mestu. V vsakem primeru ima nadzor veliko prednosti, če se uporablja za pravi namen. Če pa pride do zlorab, so lahko posledice zelo neprijetne za udeležence, kar znova kaže pomembnost ureditve področja v organizaciji na sistematičen in z zakonom usklajen način.



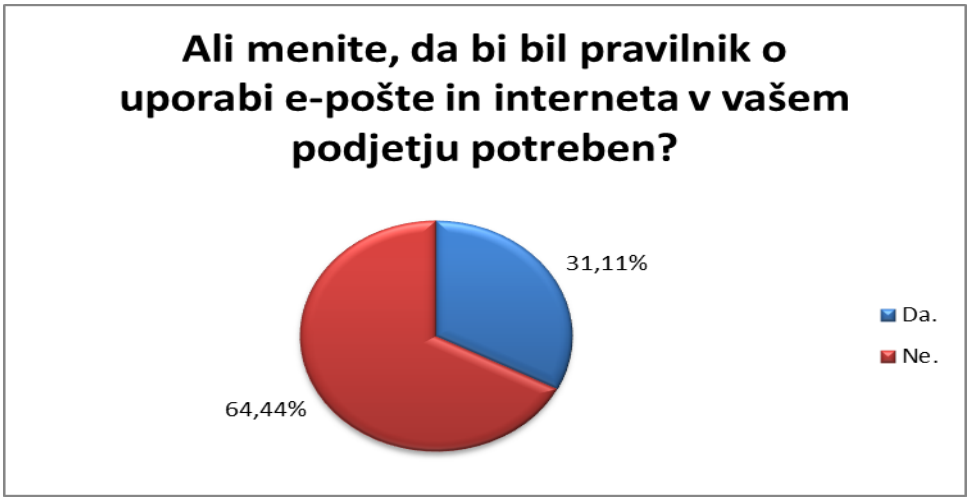

*Slika 6: Mnenja o spoštovanju na delovnem mestu*
(Lastni vir)

Ohrabrujoč je podatek, da je delež prvih treh kategorij, kjer je zasebnost na delovnem mestu od zelo do zadovoljivo spoštovana, kar 93,33-odstoten. Popolne ignorance do spoštovanja do zasebnosti na delovnem mestu v anketi ni zaznati, 6,67 % organizacij pa ima to področje slabo urejeno in bi bile izboljšave nujne. Iz rezultatov lahko sklepamo, da je kljub majhnemu deležu organizacij s slabo urejeno zasebnostjo na delovnem mestu, ta še vedno znatno previsok in bi bilo nujno zagotoviti večjo osveščenost o omenjeni problematiki.




*Slika 7: Pravilnik o uporabi e-pošte in interneta*
Vir: lasten

Velik delež organizacij, kar 53,33 %, nima pravilnika o uporabi e-pošte ali interneta, kar pa ne pomeni, da kršijo zakonska določila, vendar bi bilo vseeno smiselno to urediti. Velik je tudi delež organizacij, v katerih anketiranci ne vedo, ali obstaja pravilnik. To lahko kaže, da tega področja nimajo urejenega ali pa proces organizacije pretoka informacij znotraj organizacije ni optimalen. V vsakem primeru menimo, da bi morali skupaj z uvedbo pravilnika o tem seznaniti in usposobiti vse zaposlene v organizaciji z namenom, da se zavedo svojih obveznosti in pravic, ki izhajajo iz pravilnika.




*Slika 8: Nujnost pravilnika v podjetju*
(Lastni vir)

64,44 % anketirancev ocenjuje, da pravilnik o uporabi e-pošte in interneta v organizaciji ni potreben. To verjetno izhaja iz subjektivnega ali objektivnega občutka, da je njihova zasebnost na tem področju spoštovana. Tisti, ki so odgovorili, da bi bil potreben, so to utemeljevali, da je prav, da se opredelijo pravila in meje nadzora.

Kljub subjektvnemu mnenju anketirancev menimo, da bi bilo smiselno v vsaki organizaciji to področje urediti.


*Slika 9: Uporaba službene e-pošte v zasebne namene*
(Lastni vir)

Delež anketirancev, ki uporabljajo službeno e-pošto v zasebne namene, je 33,33 %, kar je precej velik delež. Na tem področju še zagotovo nekaj sivega prostora, saj je v človeški naravi, da službeno e-pošto včasih uporabimo tudi v zasebne namene, vendar tudi če verjamemo rezultatom ankete, menimo, da bi moralo biti to področje regulirano in dogovorjeno med zaposlenimi in organizacijo v obliki pravilnika.


*Slika 10: Dostopanje do zasebne pošte v službenem času*
(Lastni vir)

Tudi zadnje vprašanje se dotika dogovora med organizacijo in zaposlenimi. Smiselno je, da delodajalec omogoči zaposlenim, da tudi v službenem času dostopajo do zasebne pošte preko svojih poštnih strežnikov, če to ne ovira delovnega procesa, prav tako pa lahko pripomore k zadovoljstvu zaposlenih. V vsakem primeru pa je to področje smiselno urediti s pravilnikom.

## 4.2 ZAKLJUČKI RAZISKAVE

Raziskava pravne ureditve področja e-pošte in zasebnosti je bila opravljena z metodo anketiranja, pri čemer operiramo z manjšim vzorcem zaposlenih iz 45 različnih naključno izbranih delovnih organizacij. V raziskavo so zajete tako manjše kakor tudi večje delovne organizacije, kar je razvidno iz odgovorov na prvo anketno vprašanje. Ker gre za manjši vzorec, rezultatov ne moremo posploševati na celotno populacijo v Republiki Sloveniji, vendar nam da grobo sliko, iz katere lahko povzamemo določene zaključke.

Delež zaposlenih, ki se srečujejo z nadzorom na delovnem mestu, je relativno visok, kar pa nas ob napredku tehnologije in potrebnostjo njene uporabe pri sodobnem poslovanju ne bi smelo presenetiti. Kot smo že ugotovili, rezultata ne smemo problematizirati, vendar nam nadaljevanje ankete pokaže, da zaposleni problematiko nadzora pri svojem delu zaznavajo.

Vprašanje o zavedanju zaposlenih po potrebnosti nadzora na delovnem mestu je pokazalo, da se večina zaposlenih strinja, da je določen nadzor potreben, še vedno velik delež zaposlenih pa prav tako meni, da nadzor ni potreben. Verjetno bi bil rezultat precej drugačen, če bi bili zaposleni ozaveščeni o pravicah do zasebnosti, ki izhajajo iz zakonodaje, in če bi organizacije striktno upoštevale zakonska določila. Organizacije v večji meri spoštujejo zasebnost na delovnem mestu, ob predpostavki, da imamo ničelno toleranco do kršenja zasebnosti na delovnem mestu, je delež odgovorov, ki kaže, da je zasebnost na delovnem mestu slabo spoštovana, še vedno zelo visok.

Anketa kaže tudi deleže različnih najpogostejših oblik nadzora na delovnem mestu, pri čemer moramo poudariti, da so posamezne oblike nadzora v veliki meri odvisne od dejavnosti, s katero se podjetje ukvarja. Normalno je, da se v trgovski dejavnosti, bankah, zdravstvenih ustanovah uporablja videonadzor že zaradi same varnosti zaposlenih, podobno je v transportnih podjetjih, kjer se iz istega razloga uporablja sledenje vozilom. Organizacija pa se mora kljub temu odreči skušnjavi, da bi nadzor uporabljala za namene nadzora učinkovitosti zaposlenih, za kar obstajajo druge metode in ta oblika ni primerna. Prvenstveno pa je cilj ugotoviti, koliko se na delovnem mestu izvaja nadzor nad e-pošto v primerjavi z drugimi oblikami nadzora.

Rezultat, ki se nanaša na obveščanje o nadzoru na delovnem mestu, je dokaj zanimiv, tako pri odgovorih tistih, ki so bili opozorjeni na nadzor na delovnem mestu, saj oblike obveščanja največkrat niso ustrezne in skladne z zakonskimi določili, največ odgovorov pa kaže, da delodajalci niso uredili tega področja ali vsaj zaposleni tega ne vedo.

Organizacije v večji meri spoštujejo zasebnost na delovnem mestu, ob predpostavki, da imamo ničelno toleranco do kršenja zasebnosti na delovnem mestu, je delež

odgovorov, ki kaže, da je zasebnost na delovnem mestu slabo spoštovana, še vedno zelo visok.

Urejenost področja zasebnosti e-pošte najbolj elegantno rešimo s pravilnikom o uporabi e-pošte v organizaciji, ki je usklajen z zaposlenimi ali njihovim sindikatom ter ustrezno predstavljen zaposlenim. Rezultat kaže, da ta način uporablja znatno premajhen delež podjetij. Presenetljivo pa je, da majhen delež, tretjina zaposlenih čuti potrebo po pravilniku, ki bi urejal to področje. To si lahko razlagamo s slabo ozaveščenostjo in slabim poznavanje zakonskih določil.

Odgovori pa kažejo tudi stanje uporabe službene pošte tako v poslovne kakor tudi zasebne namene. V nalogi zagovarjamo stališče, da je ta možnost, ki jo organizacija zaposlenim ponudi, lahko prispevek k zadovoljstvu zaposlenih, če le ne moti delovnega procesa. Delež zaposlenih, ki uporabljajo službeno e-pošto v zasebne namene, ni zanemarljiv in ta pojav se bo vedno dogajal, zato ni smiselno, da bi organizacija zasebna sporočila preganjala, smiselna pa je ureditev tega področja s pravilnikom.

## 4.3 SISTEMSKI POSTOPKI

Sistemski postopki v različnih organizacijah, tako v zasebnem, državnem lastništvu kakor tudi v javni upravi, je večinoma sinhronizirano z zahtevani standardov ISO 9001, zadnja verzija standarda ISO 9001:2015 v poglavju 7.1.3 opredeljuje okolje za delovanje procesov, pri čemer je pomembno, da organizacija opredeli, zagotovi in vzdržuje potrebno okolje za delovanje svojih procesov. V točki 4.2 standarda ISO 9001:2015 so opredeljena razmerja in pričakovanja zainteresiranih strani, kjer so pomembna zainteresirana stran za sistem vodenja tudi zaposleni. Prav tako je zelo pomembna zainteresirana stran v podjetju tudi država s svojimi zakonskimi in podzakonskimi akti, ki jih moramo v organizaciji tako v skladu s pričakovanji standarda ISO 9001:2015, kakor tudi prejšnjih veljavnih verzij standarda strogo spoštovati.

Procesna orientiranost organizacije določa tudi prepoznavanje notranjih procesov, med katere spada tudi obvladovanje in prepoznavanje zakonskih določil, torej tudi zasebnost pri uporabi e-pošte. Organizacija mora prav tako zagotavljati kompetentnost, opisano v točki 7.2 zgoraj navedenega standarda, kjer je potrebno zagotoviti osebje, ki v okviru konteksta organizacije obvladuje prepoznane procese.

Sistemska dokumentacija obvladovanja vodenja definira interno dokumentacijo tako na nivoju poslovnika kakovosti, operativnih postopkov kakor tudi na podlagi internih delovnih navodil, imenovanih tudi interni akti, ki nam pomagajo obvladovati dokumente in podatke organizacije, kot so:

- nadrejena sistemska dokumentacija,
- tehnično-tehnološka dokumentacija,
- neveljavna, arhivirana dokumentacija.

Za izdelavo sistemske dokumentacije je odgovoren pooblaščenec za sistem vodenja kakovosti (v novem standardu ISO 9001:2015 ni zahtevan) in skrbnik posameznega procesa, kar potrdi direktor ali najvišje vodstvo organizacije. Organizacije morajo pri svojem poslovanju v skladu s točko 4.2 standarda ISO 9001:2015 sprejeti predpisane notranje akte, ki jih določa zakonodaja. Priporočljivo pa je, da sprejmejo še dodatne interne akte, da bi izboljšali uspešnost, organiziranje in varnost podjetja.

Glede na kontekst posamezne organizacije so največkrat obvezni:

- akt o sistematizaciji delovnih mest (obvezen je za organizacije z 10 ali več zaposlenimi. Vsebuje opis delovnih mest in organizacijsko strukturo);
- pravilnik o varnem in zdravem okolju (delodajalec je delavcu dolžan zagotoviti varno in zdravo okolje);
- pravilnik o varstvu osebnih podatkov (delodajalec v skladu s določili ZDR predpiše postopke in ukrepe ter določi odgovorne osebe, obvezen je za organizacije z najmanj 50 zaposlenimi, notarje, odvetnike, zdravnike oz. vse upravljavce občutljivih osebnih podatkov);
- izjava o varnosti z oceno tveganja (delodajalec določi načine in ukrepe za zagotavljanje zdravja in jih dopolnjuje ob vsaki novi nevarnosti);
- pravilnik o računovodstvu.

Za določena podjetja, odvisno od dejavnosti, pa so obvezni na primer akt o davčnem potrjevanju računov, pravilnik o mobingu in trpinčenju na delovnem mestu ipd.

Poleg obveznih pa so priporočljivi še: pravilnik o plačah, delovnem času, pravilnik o delovnih razmerjih, pravilnik o uporabi računalnikov, pravilnik o odgovornosti zaposlenih, pravilnik o uporabi elektronske pošte in interneta ipd.

Standard ISO 9001:2015 predstavlja standardno organizacijsko strukturo v podjetjih, pri čemer pa glede na panogo in kontekst podjetja ta standard lahko nadgrajujemo z panožnimi standardi ali pa standardi, ki poudarjajo npr. okoljsko ozaveščenost, energetsko učinkovitost in drugimi, med katerimi je tudi standard ISO 27001:2013, ki ureja sisteme upravljanja informacijske varnosti. Ta standard še ni množično razširjen v Sloveniji, za njegovo uvajanje pa se odločajo predvsem organizacije, ki na osnovi ocene tveganj, zahtevane s standardom ISO 9001:2015, ocenijo, da so varnostna tveganja izgube ali zlorabe informacij tako velike, da bi želeli to področje sistemsko urediti.

Uvedba standarda ISO 27001:2013 predvsem predstavlja konkurenčno prednost za organizacije, kjer je pomembno, da na trgu predstavijo dokazila, da prepoznavajo in zmanjšujejo varnostna tveganja pri upravljanju z informacijami in obvladujejo procese obvladovanja informacij. Standard ISO 27001:2013 se osredotoča predvsem na tehnične ukrepe varovanja informacij in informacijskih sistemov ter preko organizacijskih ukrepov dviguje raven ozaveščenosti zaposlenih. Vedno večja odvisnost od informacijskih tehnologij ob njihovi neustrezni uporabi predstavlja grožnjo uporabnikom teh storitev, zato je dvigovanje nivoja informacijske varnosti ključnega pomena za zaupanje uporabnikov teh storitev.

# 5 »PRAVILNIK« O UPORABI ELEKTRONSKE POŠTE IN INTERNETA

Med najbolj uporabljeni storitvi interneta sodita svetovni splet in elektronska pošta; na teh dveh področjih se najpogosteje krši pravica do zasebnosti na delovnem mestu. V določenih primerih delodajalci uporabo interneta in e-pošte izrecno ali molče dopuščajo, saj na ta način delavca lahko dodatno motivirajo za delo, kajti le zaposleni, ki delodajalcu zaupa, je lahko resnično motiviran. Problem pa nastane, ko delavec začne to izkoriščati, zato je najbolje postaviti meje. Kot je bilo že povedano, je v času vse bolj razvite računalniške tehnologije in uporabe e-pošte izven delovnega časa in delovnega mesta prav, da vsako podjetje oziroma delodajalec sestavi in določi pravilnik o pravilni uporabi e-pošte na delovnem mestu in s tem seznani svoje zaposlene, kajti tukaj se vedno soočata dva pomembna interesa, na eni strani interes delodajalca, da delavec čim bolje in učinkoviteje dela, na drugi strani pa interes delavca, ki pričakuje del zasebnosti na delovnem mestu, lahko kmalu pride do konflikta tudi zaradi interesa tretjih oseb. V pravilniku moramo opredeliti, kako, na kakšen način, v kakšnem času morajo zaposleni odgovarjati na sporočila strank in partnerjev, katerih vsebin ne smejo razpošiljati, kako bodo pošiljali zaupne podatke, ali je dovoljena uporaba službenih elektronskih sredstev za zasebne namene ipd.

Tomšič (2008, str. 63), pravi, da mora delodajalec pri pripravi pravilnika upoštevati naslednja načela:

- »popolnost,
- transparentnost,
- natančnost,
- nedvoumnost,
- zakonitost in ustavno dopustnost.«

Na podlagi rezultatov ankete o uporabi službene e-pošte in varstvu zasebnosti in na podlagi pogovora z zaposlenimi v različnih malih in večjih podjetjih smo ugotovili, da

večina podjetij nima pravilnika o uporabi elektronske pošte in interneta. Za vsako podjetje, še posebej v današnjem času, bi bilo to skoraj nujno. Načeloma do težav v podjetjih ne prihaja, če vsi spoštujejo nezapisana pravila, tako vodstvo kot zaposleni. Problem nastane, ko iz kakršnega koli vzroka pride do spora in takrat je pomembno, da so pravila zapisana. To področje ima po odgovorih sodeč samo 24,44 % podjetij v Sloveniji, mi pa menimo, da je pravilnik v vsakem podjetju potreben.

V prilogi je podan primer pravilnika za podjetje X, v katerem je zaposlenih 320 delavcev. Po Zakonu o gospodarskih družbah je organizirano kot družba z omejeno odgovornostjo, ukvarja se z gospodarsko dejavnostjo, natančneje s proizvodnjo in razvojem. Na slovenskem trgu je prisotno 25 let. Cilj družbe je partnerjem ponuditi prvovrstne izdelke, najboljšo možno podporo in pri tem presegati njihova pričakovanja. Delo temelji na avtomatizaciji, modernih strojih, na višjem nivoju zahtevnosti. Vizija družbe je s kakovostjo, tehnično dovršenostjo, lastnim razvojem, prilagodljivostjo zahtevam kupcev, produktivnostjo in s prijaznim odnosom do okolja ter zaposlenih dolgoročno postati najuspešnejše, najbolj zanesljivo in nepogrešljivo podjetje. Osnova za pripravo pravilnika je bil Pravilnik o uporabi računalniške opreme Računskega sodišča (Računsko sodišče, 2003).

# 6 ZAKLJUČEK

Brez sodobnih informacijskih tehnologij si poslovanja ne moremo več zamišljati, vendar se moramo zavedati, da vsako orodje, ki nam olajša delo, lahko tudi zlorabimo. Naloga zakonodajalca je, da zaščiti šibkejšega, v našem primeru zaposlenega pred različnimi delodajalskimi organizacijami. Cilj diplomske naloge je bil osvetliti določila zakonodajalca v povezavi z uporabo službene e-pošte ter osvetliti prakso, ki se pojavlja v različnih delovnih organizacijah.

Kot orodje za raziskavo je bila uporabljena anketa, pri čemer smo z odgovori poskušali priti do smiselnih zaključkov. Anketni vprašalnik je bil poslan zaposlenim v najrazličnejših delovnih organizacijah, ki niso bila izbrana glede na posamezno delovno panogo, ampak gre za zbir odgovorov zaposlenih iz najrazličnejših dejavnosti, od industrije, trgovine, šolstva, bančništva do javne uprave.

Interpretacija rezultatov je pokazala, da se določene organizacije že zavedajo pomena zasebnosti pri uporabi službene pošte, poznajo zakonske in zaposleni obvestijo o obveznostih in pravicah, ki iz tega izhajajo. Kljub temu rezultati ankete kažejo, da obstaja še vedno vse prevelik delež tistih, ki temu področju ne namenjajo potrebne pozornosti. To si lahko razlagamo tako s pomanjkanjem znanja s tega področja, kadrovskim primanjkljajem kot z načrtno ignoranco do zahtev zakonodaje. Vsekakor ostaja upanje, da organizacije zavestno ne kršijo zakonskih določil, za kar obstajajo v zakonodaji ustrezne kazni in posledice za odgovorne.

Iz rezultatov raziskave izhaja, da je zakonodaja na področju zasebnosti pri uporabi službene e-pošte ustrezna, vendar jo organizacije vse premalo upoštevajo. Če bi želeli ničelno toleranco do zasebnosti na tem področju, bi bilo smiselno, da bi zakonodajalec razmislil o zakonski obveznosti uvedbe pravilnika o informacijski zasebnosti na delovnem mestu, podobno kot je urejeno področje varstva pri delu.

V diplomskem delu je kot osnutek predstavljen predlog pravilnika, ki ga je treba prilagoditi specifičnosti vsake posamezne organizacije. Nikakor ni zamišljeno, da bi predlagana obvezna uporaba pravilnika v podjetjih povzročala dodatno birokratizacijo poslovanja, ampak da bi uredila medsebojna razmerja med zaposlenimi in organizacijami, povečala zavedanje o pomenu zasebnosti na delovnem mestu ter usposobila zaposlene in delodajalce k odgovorni uporabi informacijskih tehnologij.

V diplomskem delu je tudi namig, da organizacija z nekaterimi rešitvami pri uporabi e-pošte lahko stopi naproti svojim zaposlenim, jim omogoči legalno uporabo službene e-pošte skladno s svojimi pravili tudi v zasebne namene. To je sicer korak naprej od namena naloge, ki pa vendarle omogoča večje zadovoljstvo zaposlenih in večjo učinkovitost na delovnem mestu.

# LITERATURA IN VIRI

Bien Karlovšek, S., Jerše, A., Mišič, K., Pirc Musar, N., Rupnik, J., & Tomšič, A. (2008). *Zasebnost delavcev in interesi delodajalcev – kje so meje?* Ljubljana: Uradni list Republike Slovenije.

Cerar, M. (30. avgust 2006). *IUS INFO, kolumne Zakaj zasebnost na delovnem mestu (2. del)*. Prevzeto 29. septembra 2016 iz IUS SOFTWARE pravne in poslovne informacije: http://www.iusinfo.si/DnevneVsebine/Kolumna.aspx?id=10141

Cerar, M. (23. avgust 2006). *IUS-INFO, kolumne Zakaj zasebnost na delovnem mestu (1. del)*. Prevzeto 29. septembra 2016 iz IUS sofrtware pravne in poslovne informacije: http://www.iusinfo.si/DnevneVsebine/Kolumna.aspx?id=10137

Finžgar, A. (1985). *Osebnostne pravice.* Ljubljana: SAZU.

Hvaliček, M. (1. junij 2012). *Eudace*. Prevzeto 1. septembra 2016 iz E-pošta in zasebnost na delovnem mestu: http://eudace.eu/knjiznica/clanki/2013021410315019/

Kovačič, M. (2003). *Mirovni inštitut 2003*. Prevzeto 9. oktobra 2016 iz Zasebnost na internetu: http://www2.mirovni-institut.si/slo_html/publikacije/pdf/MI_politike_zasebnost_na_internetu.pdf

Pirc Musar, N. (4. junij 2007). *Informacijski pooblaščenec*. Prevzeto 12. oktobra 2016 iz Iskalnik po odločbah VOP, Pravna podlaga za zbiranje osebnih podatkov: https://www.ip-rs.si/vop/pravna-podlaga-za-zbiranje-osebnih-podatkov-splosno-889/

Pirc Musar, N. (17. marec 2010). *Informacijski pooblaščenec*. Prevzeto 6. oktobra 2016 iz Iskalnik po odločbah VOP, Vpogled v elektronsko pošto zaposlenega: https://www.ip-rs.si/vop/vpogled-v-elektronsko-posto-zaposlenega-1865/

Prelesnik, M. (16. januar 2015). *Informacijski pooblaščenec*. Prevzeto 13. oktobra 2016 iz Iskalnik po odločbah VOP, Vpogled v e-pošto bivšega zaposlenega: https://www.ip-rs.si/vop/vpogled-v-e-posto-bivsega-zaposlenega-2473/

Računsko sodišče. (24. december 2003). *Računsko sodišče RS, Pravilnik o uporabi računalniške opreme.* Prevzeto 7. oktobra 2016 iz Računsko sodišče RS, Pravilnik o uporabi računalniške opreme 3101-2/2003-1: http://www.rs-rs.si/rsrs/rsrs.nsf/V/K5FB1F06043D0EA04C125719A002026DE/$file/Pravilnik_uporaba_rac.pdf

Resnik, S. (12. avgust 2010). *Prednosti in slabosti e-poslovanja*. Prevzeto 5. novembra 2016 iz http://mladipodjetnik.si/novice-in-dogodki/novice/prednosti-in-slabosti-e-poslovanja

Rovšek, J. (2005). *Mirovni inštitut.* Prevzeto 10. oktobra 2016 iz Zasebno in javno v medijih: http://mediawatch.mirovni-institut.si/edicija/seznam/16/mediawatch16.pdf

Solove, D. J. (2008). *Understanding Privacy.* Boston: Harward University Press.

Tomšič, A. (25. avgust 2016). Pravila in novosti varstva osebnih podatkov. Ljubljana: Forum Akademija.

Uradni list RS, PIS, Kazenski zakonik. (1. november 2008). *PIS – Pravno informacijski sistem*. Prevzeto 13. oktobra 2016 iz Kazenski zakonik (KZ-1) Kazenski zakonik (Uradni list RS, št. 50/12 – uradno prečiščeno besedilo, 6/16 – popr., 54/15 in 38/16): http://www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO5050

Uradni list RS, PIS, Ustava Republike Slovenije (URS). (23. december 1991). *PIS – pravno informacijski sistem*. Prevzeto 2. novembra 2016 iz Ustava Republike Slovenije (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 in 47/13 – UZ90,97,99): http://www.pisrs.si/Pis.web/pregledPredpisa?id=USTA1

Uradni list RS, PIS, Zakon o delovnih razmerjih. (12. april 2013). *PIS – pravno informacijski sistem*. Prevzeto 5. november 2016 iz Zakon o delovnih razmerjih (Uradni list RS, št. 21/13, 78/13 – popr., 47/15 – ZZSDT, 33/16 – PZ-F in 52/16): http://www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO5944#

Uradni list RS, PIS, Zakon o varstvu osebnih podatkov. (1. januar 2005). *PIS – pravno informacijski sistem*. Prevzeto 5. november 2016 iz Zakon o varstvu osebnih podatkov (ZVOP-1)(Uradni list RS, št. 94/07 – uradno prečiščeno besedilo): http://www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO3906

Waren, S., D., Brandeis, & Luis, D. (1890). The right to privacy. *Harwars Law Review*, str. 193–220.

# PRILOGA

Podjetje XX
Datum: 7. 10. 2016

PRAVILNIK O UPORABI ELEKTRONSKE POŠTE IN INTERNETA

I. SPLOŠNE DOLOČBE

1. člen

S tem pravilnikom se določajo organizacijski ter logično-tehnični postopki in ukrepi, povezani z uporabo elektronske pošte in interneta v podjetju XX z namenom, da se delavce seznani s pravilno uporabo elektronske pošte in interneta v podjetju XX.

Zaposleni, ki pri svojem delu uporabljajo elektronsko pošto in internet, morajo biti seznanjeni s področno zakonodajo, ki ureja posamezno področje njihovega dela, je povezana z uporabo elektronske pošte in interneta ter z vsebino tega pravilnika.

Uporaba elektronske pošte

1. Sistem za uporabo službene elektronske pošte se uporablja samo za službene namene.
2. Predal službene elektronske pošte mora biti ločen od zasebnega. Uporaba v delovnem času v zasebne namene je dopustna le izjemoma pod pogojem, da je primerno uporabljena oziroma nikakor ne vpliva na zmanjševanje produktivnosti, kar pomeni, da do njega lahko zaposleni dostopajo samo v času odmorov.
3. Pošiljanje e-pošte, ki je neprimerna in škoduje ugledu podjetja, ni dovoljeno.
4. Zaposlenim, ki za opravljanje svojega dela ne potrebujejo zunanjih komunikacij, se dodeli možnost uporabe e-pošte le znotraj družbe.
5. Zaposleni mora skrbno varovati svoje osebno geslo za dostop do e-pošte, nikoli ga ne sme razkriti ali deliti z drugimi.
6. Ko zaposleni ni prisoten na delovnem mestu, se mora odjaviti iz sistema in zakleniti delovno postajo.
7. Prepovedano je prenašanje nelicenčne programske opreme.
8. Zaposleni naj ne odpira e-pošte neznanega pošiljatelja ali sumljive e-pošte zaradi možnosti okužbe računalnika. Tako sporočilo je nujno takoj zbrisati in o njej obvestiti informatika.
9. Uprava družbe lahko zahteva pregled računalnika. Zahtevek mora vsebovati vzrok pregleda, utemeljen sum na dejanje, ki je v nasprotju z interesi podjetja. Pisna zahteva mora vsebovati vzrok, postopek pregleda, datum, osebo, ki bo pregled opravila. Odobrena pa mora biti s strani delavca in delodajalca. V e-pošto zaposlenega, vendar samo službeno, lahko pogleda tudi v izjemnih primerih, kot je smrt zaposlenega.
10. Po zaključku delovnega razmerja delodajalec e-naslov delavca nemudoma blokira, delavec pa podpiše izjavo, da je izbrisal sporočila.
11. Občutljive informacije oziroma zaupni podatki o podjetju ne smejo biti posredovani nikomur brez predhodne odobritve uprave.
12. Zaposleni mora poskrbeti za pravilno shranjevanje svoje službene e-pošte.

13. Informatik tedensko arhivira elektronsko pošto iz službenih predalov.
14. Pri pisanju sporočil več prejemnikom morajo zaposleni uporabljati polje Kp (da se vidi, komu v vednost je sporočilo poslano) in polje Skp (se ne vidi, komu vse je sporočilo poslano), tako se ne razpošiljajo razni e-poštni naslovi, kar je prepovedano (osebni podatek).
15. Pri pisanju e-sporočila se vedno izpolni polje zadeva (za kaj gre). Vsebina sporočila se napiše kratko in jedrnato, pri pisanju sporočila se ne uporablja velikih tiskanih črk, izogiba se klicajem, uporablja se knjižni jezik in slovnična pravila, ne uporablja se smeškov. Na koncu sporočila se doda vizitka zaposlenega. Na sporočila se odgovarja v roku 24 ur.
16. Ob odsotnosti z dela mora zaposleni svoj računalnik nastaviti na avtomatsko obveščanje o svoji odsotnosti.

Uporaba interneta

1. Zaposlenemu je dostop do interneta omogočen zaradi dostopa do podatkov in storitev, ki jih potrebuje pri svojem delu.
2. Omrežje lahko uporablja le na službenem računalniku.
3. Pri vključitvi ne sme uporabljati lažnih osebnih podatkov.
4. Zaposleni ne smejo pošiljati nestrokovnih ali osebnih zadev, verižnih pisem oziroma karkoli bi zmotilo delo drugih uporabnikov.
5. Zaposleni ne smejo objavljati tajnih, zaščitenih podatkov.
6. Zaposleni ne smejo uničevati ali spreminjati podatkov, ki so last drugih.
7. Uporaba družabnih omrežij (facebook, twiter, instagram) so dovoljeni samo za uporabo v službene namene.

## UKREPANJE OB SUMU NEUPOŠTEVANJA PRAVILNIKA

Zaposleni so dolžni o aktivnostih, ki so povezane z neupoštevanjem tega pravilnika, takoj obvestiti pooblaščeno osebo ali predstojnika, sami pa poskušajo takšno aktivnost preprečiti.

## ODGOVORNOST ZA IZVAJANJE PRAVILNIKA

Za izvajanje postopkov in ukrepov pravilnika so odgovorni vodje enot in pooblaščene osebe, ki jih imenuje uprava podjetja XX .

Nadzor nad izvajanjem postopkov in ukrepov, določenih s tem pravilnikom, opravlja oseba XX.

Vsak zaposleni, je dolžan upoštevati predpisane določbe v pravilniku, za katere je izvedel oziroma je bil z njimi seznanjen pri opravljanju svojega dela. Obveza varovanja podatkov ne preneha s prenehanjem delovnega razmerja.

Pred nastopom dela na delovno mesto mora zaposleni podpisati posebno izjavo, ki ga zavezuje k upoštevanju tega pravilnika.

Iz podpisane izjave mora biti razvidno, da je podpisnik seznanjen z določbami tega pravilnika, izjava pa mora vsebovati tudi pouk o posledicah kršitve.

Za kršitev določil so zaposleni disciplinsko odgovorni, ostali pa na temelju pogodbenih obveznosti.

Ta pravilnik začne veljati .. ... .....

V Kranju, 7. 10. 2016

Podpis odgovorne osebe:
xxxxx

Podpis zaposlenega:
xxxxx