

## **Predlog:**

Predlagam Zakon o zasebnosti na delovnem mestu, ki naj vsebuje poleg vseh standardnih uvodnih členov, končnih členov in členov glede sankcij, naslednje:

### x. člen

S tem zakonom se določajo pravice, obveznosti delodajalca in delojemalca s katerimi se preprečujejo neustavni, nezakoniti in neupravičeni posegi v zasebnost in dostojanstvo posameznika oziroma posameznice na delovnem mestu zaradi zasebne rabe elektronskih komunikacijskih sredstev, ki so last delodajalca.

### x. člen (pomen izrazov)

- elektronsko komunikacijsko sredstvo last delodajalca je vsako osnovno sredstvo, ki omogoča izmenjavo govornih ali tekstovnih sporočil v elektronski obliki;
- zasebna raba je vsaka raba, katere namen in cilj ni povezan s poslovanjem delodajalca.

### x. člen

Vsak posameznik oziroma posameznica ima pravico do zasebnosti tudi na delovnem mestu.

### x. člen

Delodajalec lahko pod pogoji določenimi v tem zakonu nadzira zaposlene če pri tem upošteva naslednja osnovna načela:

- ◆ predstavniki delavcev (sindikati) morajo biti informirani o vsaki spremembi sistemov za nadzor delavcev; delodajalec naj upošteva mnenje predstavnika delavcev;
- ◆ sistemi za nadzor naj bodo odobreni s strani ustreznih državnih inštitucij (na primer urada Informacijskega pooblaščenca RS);
- ◆ stalen nadzor naj bo dovoljen le ko je potreben zaradi zdravja, varnosti ali zaščite;
- ◆ tajen nadzor naj bo dovoljen le v zakonsko določenih primerih;
- ◆ osebni podatki, ki se zbirajo z namenom zagotavljati varnost in zagotavljati nemoteno poslovanje, se naj ne bi uporabljali za kontrolo obnašanja posameznih delavcev razen ko je to del izvajanja poslovnega procesa;
- ◆ osebni podatki zbrani z elektronskim nadzorom naj ne bodo edini faktorji pri ocenjevanju delavčeve učinkovitosti in odločanja v zvezi s tem;
- ◆ razen za določene primere kot je avtomatičen nadzor zaradi varnostni in poslovanja (npr. kontrola prisotnosti virusov), rutinski nadzor vseh posameznih delavčevih elektronskih sporočil in uporabe interneta naj bo prepovedan; nadzor posameznika se lahko odredi le, ko je utemeljen sum kriminalne dejavnosti oziroma povzročanja velike škode in ne obstaja drugačen manj oseben način pridobivanja dokazov (npr. da zadostuje nadzor gostote prometa brez nadzora vsebine);
- ◆ v osnovi naj bo prepovedano odpirati delavčevo zasebno elektronsko pošto ali druge zasebne datoteke, še posebno, če so označene kot zasebne, ne glede na to ali so s strani delodajalca orodja dovoljena tudi za zasebne namene ali zgolj za poslovne namene; zasebna elektronska pošta in datoteke naj se obravnavajo kot zasebna korespondenca; zaupnost korespondence naj se ne neha s splošno privolitvijo delavca in še posebej tudi ne po prenehanju delovnega razmerja;
- ◆ komunikacija z zdravstvenimi ustanovami oziroma njihovim osebjem in s predstavniki delavcev naj bo še posebej zaščiten.

### x. člen

V skladu z načeli prejšnjega člena je pogoj, da delodajalec izvaja nadzor uporabe elektronskih komunikacijskih sredstev s strani zaposlenih naslednji:

- obstoj internih aktov, ki natančno urejajo pogoje zasebne rabe komunikacijskih sredstev,
- mehanizmi in drugi ukrepi, ki zagotavljajo, da so zaposleni seznanjeni z internimi akti, ki urejajo področje zasebnosti na delovnem mestu,
- mehanizmi in drugi ukrepi, ki zagotavljajo, da so zaposleni seznanjeni z implementiranimi sistemi za nadzor,
- implementirani sistemi za nadzor so potrjeni s strani ustreznih državnih inštitucij oziroma so ti sistemi na seznamu primernih za nadzor, ki ga objavlja ustrezna državna inštitucija,
- implementirani sistemi za nadzor vključujejo vse zaposlene brez izjem in
- implementirani sistemi za nadzor ne omogočajo nadzor vsebine komunikacij; glede prestrazanje vsebine komunikacij se strogo upoštevajo drugi zakoni, ki urejajo to področje (ZEKom-1, ...).

x. člen

Delodajalec v internih aktih ne sme prepovedati uporabe elektronskih komunikacijskih sredstev v zasebne namene, lahko le omeji uporabo v zasebne namene oziroma določi pravila.

x. člen

Delojemalec ne sme z uporabo elektronskega komunikacijskega sredstva v zasebne namene povzročiti delodajalcu škode.

x. člen

Tudi če delojemalec ne upošteva pravila uporabe elektronskih komunikacijskih sredstev v zasebne namene, ne pomeni, da je zato avtomatično dovoljen vpogled v osebne podatke kar vsebina komunikacij in podatki o prometu vsekakor so. Tudi v tem primeru se mora delodajalec ravnati v skladu z Zakonom o varstvu osebnih podatkov in internim pravilnikom glede varstva osebnih podatkov.

### **Obrazložitev predloga:**

Uporaba informacijske tehnologije na delovnem mestu hitro narašča. Vendar ne narašča le uporaba ampak tudi kompleksnost oziroma uporabnost tehnologije. Oboje prinaša nove izzive delodajalcem, delojemalcem in njihovim predstavnikom. Zelo občutljiva so od vedno področja nasprotnih interesov delodajalcev in delojemalcev. Eno takšnih je vsekakor potreba delojemalcev po zasebnosti tudi na delovnem mestu in potreba delodajalcev po nadzoru delojemalcev oziroma nadzoru nad uporabo tehnologije na delovnem mestu.

IT je danes pomemben element poslovanja vsake organizacije, ki omogoča učinkovitejše in boljše poslovanje, hkrati pa pomeni tudi nove nevarnosti predvsem pa:

- večja nevarnost dostopa do pomembnih podatkov (poslovne skrivnosti, osebni podatki) s strani nepooblaščenih oseb kar ustvarja potrebo po zaščiti in nadzoru dostopa do takšnih podatkov in
- nevarnost zlorabe IT s strani delodajalcev pri uporabi orodij za nadzor in zaščito, zlasti nadzor delojemalcev in njihovih aktivnosti; skrb delojemalcev in njihovih predstavnikov glede zasebnosti na delovnem mestu.

Evropska konvencija o varstvu človekovih pravic in temeljnih svoboščin (Svet Evrope, 1950), katere podpisnice so vse članice EU, v 8. členu določa:

**1. Vsakdo ima pravico do zasebnega in družinskega življenja, zasebnosti doma in zasebnosti korespondence.**

**Vmešavanja v zasebnost s strani institucij naj ne bi bilo razen v izjemnih primerih katere določa zakon zaradi interesa nacionalne varnosti, zaradi javnega dobrega, zaradi splošne koristi za vso državo, zaradi preprečevanja nemirov in kriminala, zaradi zaščite zdravja in moralnih načel ali zaradi zaščite pravic in svoboščin drugih.**

Evropsko sodišče za človekove pravice je določilo, da se zasebno življenje nanaša tudi na dejavnosti v službi in, da zasebnost korespondence velja tudi za telefonske razgovore v službi (poslovne in zasebne). Princip avtomatično vsiljuje enaka merila tudi za elektronsko pošto in uporabo interneta. Svet Evrope je takšno razširitev potrdil leta 2001.

Iz zakonodaj držav EU je mogoče potegniti kar nekaj načel v zvezi z zasebnostjo in nadzorom delavca na delovnem mestu. Ta načela so predvsem:

- načelo pomembnosti ali namena – namen nadzora delodajalca glede elektronske izmenjave informacij mora ustrezati statusu delavca;
- načelo proporcionalnosti – nadzor mora biti v vseh primerih potreben, ustrezen in proporcionalen glede na namen; to je stvar ravnotežja med interesi delodajalca in delavca;
- načelo transparentnosti ali previdnosti – kar konkretno pomeni, da ob uvedbi nadzora morajo biti delavčevi postopki usklajeni z delodajalcem in
- načelo nediskriminacije – implementirane mere ne smejo pomeniti diskriminacijo med delavci ali skupinami delavcev in morajo veljati za vse.

EU oziroma Evropska komisija je oktobra 2002 predlagala nova načela za zaščito podatkov na delovnem mestu. Vzrok za predlagane novosti so:

- ❖ uporaba sodobnih tehnologij in povečana uporaba informacijskih tehnologij, ki zmanjšuje meje med delom in privatnim življenjem,

- ❖ globalizacija in rast trenda dajanja izvajanja funkcij drugim (outsourcing) kar lahko povzroči težave, če so zakoni v zvezi z zaščito podatkov različni od države do države,
- ❖ nevarnosti po 11. septembru 2001; v ZDA so na primer družbe uvedle nadzor zaradi zahtev vlade po povečanju varnosti.

Evropska komisija je ugotovila, da je v državah članicah EU nadzor in kontrola delavcev s strani delodajalcev regulirano preko različnih določil in priporočil v različnih aktih – nacionalne ustave, zakoni s področja delovnih razmerij, zakoni s področja varstva podatkov in telekomunikacij in drugimi akti. Zaradi takšne razpršenosti so primeri, ko so definicije nejasne ali celo protislovne. Stanje postaja še bolj zaskrbljujoče, ko se tradicionalnim načinom nadzora telefonije in video nadzor, dodajo sodobne tehnologije kot so elektronska pošta in uporaba interneta, ki dajejo nove razsežnosti nadziranja delavcev. Evropska komisija zato predlaga naslednja osnovna načela:

- ◆ predstavniki delavcev (sindikati) morajo biti informirani o vsaki spremembi sistemov za nadzor delavcev; delodajalec naj upošteva mnenje predstavnika delavcev;
- ◆ sistemi za nadzor naj bodo odobreni s strani ustreznih državnih inštitucij;
- ◆ stalen nadzor naj bo dovoljen le ko je potreben zaradi zdravja, varnosti ali zaščite;
- ◆ tajen nadzor naj bo dovoljen le v zakonsko določenih primerih ali v primerih, ko je utemeljen sum kriminalne aktivnosti ali utemeljen sum povzročanje velike škode;
- ◆ osebni podatki, ki se zbirajo z namenom zagotavljanja varnosti in zagotavljanja nemoteno poslovanje, se naj ne bi uporabljali za kontrolo obnašanja posameznih delavcev razen ko je to del izvajanja poslovnega procesa;
- ◆ osebni podatki zbrani z elektronskim nadzorom naj ne bodo edini faktorji pri ocenjevanju delavčeve učinkovitosti in odločanja v zvezi s tem;
- ◆ razen za določene primere kot je avtomatičen nadzor zaradi varnostni in poslovanja (npr. kontrola prisotnosti virusov), rutinski nadzor vseh posameznih delavčevih elektronskih sporočil in uporabe interneta naj bo prepovedan; nadzor posameznika se lahko odredi le, ko je utemeljen sum kriminalne dejavnosti oziroma povzročanja velike škode in ne obstaja drugačen manj oseben način pridobivanja dokazov (npr. da zadostuje nadzor gostote prometa brez nadzora vsebine);
- ◆ v osnovi naj bo prepovedano odpirati delavčevo zasebno elektronsko pošto ali druge zasebne datoteke, še posebno, če so označene kot zasebne, ne glede na to ali so s strani delodajalca orodja dovoljena tudi za zasebne namene ali zgolj za poslovne namene; zasebna elektronska pošta in datoteke naj se obravnavajo kot zasebna korespondenca; zaupnost korespondence naj se ne neha s splošno privolitvijo delavca in še posebej tudi ne po prenehanju delovnega razmerja;
- ◆ komunikacija z zdravstvenimi ustanovami oziroma njihovim osebjem in s predstavniki delavcev naj bo še posebej zaščiten.

#### Primeri nacionalne zakonodaje v EU

**Belgija:** Nacionalni dogovor o varstvu zasebnosti delavca pri uporabi sodobnih komunikacijskih sredstev

*(Glede uporabe interneta se lahko zbira čas povezave delovne postaje z internetom, ne pa tudi podatkov o obiskanih straneh. Glede uporabe e-pošte se nadzira število in količino poslanih sporočil iz delovne postaje, ne pa tudi kdo je pošiljatelj. Delodajalec mora jasno in natančno definirati cilje nadzora. Vsebina podatkov se lahko nadzira le če delavec in druge vpletene strani (npr. prejemnik sporočila) so v to privolili. Pred implementacijo sistema za nadzor mora delodajalec o tem obvestiti delavce in njihove predstavnike.)*

**Danska:** Kazenski zakonik

*(Odpiranje oziroma dostop do tuje pošte je kriminalno dejanje. V to spada tudi elektronska pošta. Informacije o delavčevi elektronski pošti in katere spletne strani je obiskoval spadajo med osebne podatke in zato se z njimi ravna kot predpisuje Akt o obdelavi osebnih podatkov – nadzor je mogoč le, če v to privoli delavec. Leta 2001 je Agencija za zaščito podatkov določila, da je zaradi varnosti računalniških sistemov in nadzora ali delavci upoštevajo varnostno politiko, legitimno uvesti nadzorne mehanizme vendar morajo delavci biti z njimi seznanjeni. Državne inštitucije morajo o takšnih ukrepih obveščati Agencijo.)*

**Nemčija:** Akt o telekomunikacijah (TKG) in Akt o zaščiti podatkov komunikacijskih storitev (TDDSG) določa kdaj delodajalec omogoča delavcem zasebno rabo e-pošte in interneta.

*(Nadzor zasebne rabe je veliko bolj omejen kot nadzor poslovne rabe. Zbirajo se potrebni podatki za zaračunavanje storitev, za zagotavljanje storitev oziroma za normalen potek storitev. Kontrola vsebine ni dovoljena razen v primerih suma resnega kaznivega dejanja. Nadzor zasebne e-pošte in internet povezave mora biti minimalen oziroma da zagotavlja zaračunavanje stroškov. Če se storitev ne*

zaračunava, potem naj se ne zbirajo podatki potrebni zato z izjemo potrebnih za normalen potek storitve. Če ima delavec pravico do zasebne rabe interneta, potem delodajalec brez njegovega privoljenja ne sme zbirati podatke o obiskanih spletnih straneh. Če delodajalec dovoli uporabo sistema e-pošte v zasebne namene, potem Delavska ustavna listina (BertVG) določa, da so osnovna pravila glede uporabe odobrena s strani delavskega sveta in zapisani v delovni pogodbi.)

**Portugalska:** Nacionalna komisija za zaščito podatkov: Navodila v zvezi z uporabo e-pošte in interneta s strani delavcev

(Neproductivno je s strani delodajalcev določiti da je dovoljena uporaba samo za poslovne namene, vendar je želja delodajalca, da je uporaba v mejah normale in predvsem v poslovne namene. V ta namen je priporočljivo da:

- delodajalec naj definira jasna in natančna pravila v zvezi z zasebno rabo e-pošte in interneta,
- pravila naj slonijo na principu ustreznosti, proporcionalnosti, kooperativnosti in obojestranskem zaupanju,
- pravila morajo sprejeti delavci in njihovi predstavniki, morajo biti uradno objavljena in morajo natančno določati tudi stopnjo tolerance, način nadzora in kazenske določbe ne upoštevanja pravil.

Osnova za pravila so:

- delodajalec nima pravice brati pošte naslovljene na delavca,
- delodajalec ima možnost obdelave podatkov samo na podlagi privolitve osebe na katero se podatki nanašajo in na podlagi pravic in privilegijev dodeljenih s strani lastnika podatkov,
- delodajalec naj izbira ne vsiljive metode nadzora, ki so v skladu z veljavnimi normami in s katerimi so delavci seznanjeni,
- delodajalec ne nadzoruje e-pošte stalno in sistematično ampak le občasno in le na za družbo kritičnih področjih,
- smisel nadzora e-pošte je zagotavljanje varnosti sistema (zanesljivost in razpoložljivost),
- z vednostjo delavcev, delodajalec lahko implementira potrebne filtre glede pripetih datotek na elektronska sporočila v skladu z naravo dela, ki določa, da niso potrebna in zaželeni (npr. exe, mp3, ...),
- če delodajalec ugotovi neprimerno uporabo e-pošte in interneta, delavec dobi opomin in je potem lahko dodatno nadzorovan,
- dostop do vsebine e-pošte s strani delodajalca naj bo zadnji skrajni ukrep; pregled naj se izvede ob prisotnosti delavca in predstavnika sindikata; prva faza vsebinske kontrole naj bo omejena na naslov prejemnika/pošiljatelja, na zadevo in na datum in čas,
- določena je stopnja tolerance uporabe interneta v zasebne namene, še posebno izven delovnega časa,
- splošna statistika internetnega prometa naj bo osnovni nadzor; za ugotavljanje porabe delovnega časa za brskanje po internetu, ni potrebna kontrola katere spletne strani so bile obiskane.)

## Sindikat

Bruselj 2000 konferenca združenja UNI – Akt o uporabi interneta na delovnem mestu. Akt je razdeljen na štiri področja:

- ◆ komunikacija predstavnikov delavcev – sindikatov, ki zahteva pravice do uporabe IT delodajalca za komuniciranje delavcev s sindikati in sindikalnih predstavnikov s sindikalnimi organizacijami,
- ◆ zasebno komuniciranje, ki zahteva pravice delavcev do uporabe IT delodajalca za zasebne namene, če to ne vpliva na poslovne procese,
- ◆ nadzor komunikacij, ki omejuje pravice delodajalca glede nadzora uporabe IT s strani delavcev (npr. dostop do podatkov vezanih na posameznika le ob prisotnosti predstavnika sindikata oziroma druge osebe določene s strani posameznika – priča dogodka!) in
- ◆ pogoji uporabe IT, ki določa pogoje pod katerimi lahko delavec uporablja IT delodajalca v zasebne namene (zakonitost, skrb za moralne in etične vrednote, varnost, diskretnost, državna varnost, skrb za človekove pravice, ...)

## Slovenija

Ustava RS, 35. člen

- Pravica do varstva zasebnosti in osebne integritete posameznika je temeljna osebnostna pravica.

Zakon o delovnih razmerjih RS

- vsak akt delodajalca, ki vpliva na obveznosti delavcev mora pred sprejetjem v presojo sindikatu,
- pogodba o zaposlitvi mora vsebovati seznam aktov, ki jih mora delavec poznati,
- delavec mora upoštevati delodajalčeva navodila,
- delavec se mora vzdržati ravnanj, ki moralno ali materialno škodijo delodajalcu,
- delavec je dolžan varovati poslovno skrivnost,

- delodajalec mora varovati in spoštovati delavčevo osebnost ter upoštevati in ščititi delavčevo zasebnost,
  - delodajalec mora ravnati z osebnimi podatki v skladu z zakoni.
- Kazenski zakonik RS – kazniva dejanja:
- neupravičeno prisluškovanje in zvočno snemanje,
  - neupravičeno slikovno snemanje,
  - kršitev tajnosti občil.

Dario Medoš

Viri:

EIRO: <http://www.eiro.eurofound.eu.int/2003/07/study/TN0307101S.html>

Zakoni in akti EU: <http://europa.eu.int/eur-lex/lex/en/index.htm>

U.S. Code Collection, Title 18, Part I, Chapter 119: <http://www4.law.cornell.edu/uscode/>

Državni zbor RS – Sprejeti zakoni in akti: <http://www.dz-rs.si/>

Prepoved avtomatičnega nadzora IS, ki jih uporabljajo zaposleni.

- Nadzor zaposlenega le ob utemeljenem sumu njegove protipravne dejavnosti.
- Popolna prepoved uporabe službene opreme v zasebne namene ne bo dovoljena.
- Nadzor s strani delodajalca dopusten zgolj ob izrecni zakonski podlagi ali ob izrecni vednosti in vnaprejšnjem določnem soglasju zaposlenega

Omejen nadzor zaposlenih;

- Ukrepi sorazmerni legitimnemu cilju, ki ga zasleduje;
- Zaposleni VNAPREJ seznanjeni z razlogi in obsegom nadzora;
- Oblikovanje in objava internega akta o uporabi e-pošte in/ali mobilnih telefonov;
- Določiti tiste izjemne okoliščine in NAČIN, v katerih je dopustno pregledati e-predal ali izpiske tel. klicev.

Podobno kot pri drugih segmentih nadzora nad uporabo elektronskih sredstev– vnaprej opredeliti pravila igre v internih aktih:

kdaj in pod katerimi pogoji je dopustna uporabe zasebnih naprav katerih naprav: prenosni računalniki, tablice, pametni telefoni, prenosni mediji...

kako je z nameščanjem programske opreme na te naprave omejitev delovanja zasebnih naprav (npr. dostop do določenih IT sredstev)

upravljanje incidentov v primeru uporabe zasebnih naprav odgovornost za varnost zasebnih naprav opredelitev morebitnega nadzora (upoštevanje priporočil za pripravo internih aktov) – natančnost, popolnost...