PRAVILNIK
o varovanju zaupnih in osebnih podatkov ter o varovanju dokumentarnega gradiva

I. SPLOŠNE DOLOČBE

1. člen
S tem pravilnikom se določajo postopki in ukrepi za zavarovanje zaupnih in osebnih podatkov vodenih v zbirkah podatkov, s katerimi upravlja družba.

2. člen
Za varovane osebne podatke štejejo tisti podatki o fizični osebi, ki kažejo na lastnosti, stanje ali razmerja posameznika, ne glede na obliko, v kateri so izraženi.
V smislu določbe 1.odstavka tega člena se šteje za osebne podatke o fizični osebi zlasti:
- identifikacijski podatki o posamezniku,
- podatki, ki se nanašajo na rasno poreklo in pripadnost narodu ali narodnosti,
- podatki, ki se nanašajo na družinska razmerja,
- podatki, ki se nanašajo na stanovanjske in bivalne pogoje posameznika,
- podatki o zaposlitvi,
- podatki o socialnem in ekonomskem stanju posameznika,
- podatki o izobrazbi in pridobljenih znanjih,
- podatki o uporabi komunikacijskih sredstev,
- podatki o zdravstvenem stanju posameznika,
- podatki o posamezniku na področju notranjih zadev

3. člen
Zavarovanje osebnih podatkov zajema pravne, organizacijske in ustrezne logistično tehnične postopke in ukrepe, s katerimi se:
- varujejo prostori, strojna in sistemska programska oprema,
- varuje aplikativna programska oprema, s katero se obdelujejo zaupni in osebni podatki,
- zagotavlja varnost posredovanja in prenosa osebnih podatkov,
- onemogoča nepooblaščenim osebam dostop do naprav, na katerih se obdelujejo osebni podatki in do njihovih zbirk,
- omogoča naknadno ugotavljanje kdaj so bili posamezni podatki uporabljeni in vnešeni v zbirko podatkov in kdo je to storil, in sicer za obdobje, za katero se posamezni podatki shranjujejo.

4. člen
V tem pravilniku uporabljeni izrazi imajo naslednji pomen:
1. zaupen podatek: podatek, ki je razglašen za tajnost, ker je tako pomemben, da bi z njegovim razkritjem lahko nastale škodljive posledice za delovanje družbe,
2. osebni podatek: podatek, ki kaže na lastnosti, stanja ali razmerja posameznika ne glede na obliko v kateri je izražen,
3. zbirka podatkov: zbirka, ki vsebuje zaupne in osebne podatke (npr. evidenca, register, baza podatkov), ki se vodi s sredstvi za avtomatsko obdelavo podatkov ali klasičnimi sredstvi in je namenjena izvajanju nalog družbe,

4. obdelava podatkov: postopki in procesi zbiranja, shranjevanja, spreminjanja, združevanja, uporabe, brisanja in posredovanja podatkov,
5. dokument: vsi pisni, tiskani, risani in posneti podatki,
6. nosilec podatkov: vse vrste sredstev, na katerih so zapisani ali posneti podatki,
7. varovani prostori: vsi prostori, v katerih se nahajajo nosilci zaupnih in osebnih podatkov ali prostori v katerih je oprema preko katere je mogoč dostop do teh podatkov.

II. VRSTE ZAUPNIH PODATKOV

5. člen

Zaupnost podatkov določi direktor ob nastanku posameznega dokumenta, vzpostavitvi zbirke podatkov oziroma ob začetku izvajanja ukrepov in postopkov družbe.
Vsak delavec družbe je dolžan v okviru svojih pristojnosti in ob določilih tega pravilnika presojati pomen dokumentov in ukrepov ter direktorju predlagati določitev njegove zaupnosti. Zaupnost podatka lahko spremeni ali prekliče direktor.

6. člen

Zaupni podatki družbe so podatki, ki so določeni kot zaupni in so tako pomembni, da bi z njihovo izdajo nastale ali bi očitno lahko nastale škodljive posledice za delovanje družbe in njegove koristi.
Zaupni podatki so:
- analize o poslovanju podjetja
- gradiva in zapisniki organov upravljanja
- poročila o inšpekcijskem nadzoru,
- kadrovska evidenca in evidenca o zdravstvenem stanju delavcev,
- evidenca avtorskih pogodb, podjemnih pogodb
- evidenca izplačanih plač in ostalih prejemkov
- evidenca uporabnikov storitev,
- načrti za zavarovanja in varnostni ukrepi za objekte,
- nabavni ceniki in pogoji
- drugi delovni materiali in dokumentacija, ki je tako označena, ali jo kot zaupno opredeljuje drug predpis.

III. VAROVANJE PROSTOROV IN RAČUNALNIŠKE OPREME

7. člen

Prostori, kjer se nahajajo nosilci varovanih osebnih podatkov - vsak dokument, na katerem je zapisan osebni podatek in vsak drug računalniški ali elektronski nosilec podatka - in strojna ter programska oprema (v nadaljevanju besedila: varovani prostori) morajo biti varovani z organizacijskimi ter fizičnimi in tehničnimi ukrepi, ki onemogočajo nepooblaščenim osebam dostop do podatkov.
Dostop v prostore iz prvega odstavka tega člena je mogoč in dopusten le v delovnem času, izven delovnega časa pa le na podlagi dovoljenja direktorja ali pooblaščene osebe.
Varovani prostori ne smejo ostati nenadzorovani, oziroma se morajo zaklepati ob odsotnosti delavcev, ki jih nadzorujejo.
Izven delovnega časa morajo biti omare in pisalne mize z nosilci podatkov zaklenjene.
Računalniki ali druga strojna oprema, na kateri se obdelujejo ali hranijo osebni podatki, mora biti izven delovnega časa fizično ali programsko zaklenjena.

Izven delovnega časa mora biti vključena alarmna naprava. Zaradi varnosti premoženja se na vhodu v družbo izvaja videonadzor. Na vhodu je ustrezno obvestilo o tem. Posnetke se sme hraniti največ eno leto.

8. člen
V varovane prostore (kadrovska služba, arhivi , sistemski prostor ipd.) nezaposlene osebe ne smejo vstopati brez spremstva ali prisotnosti zaposlenega delavca. Delavec, ki dela v varovanih prostorih, mora vestno in skrbno nadzorovati prostor in ob zapustitvi prostora zakleniti prostor.
Delavec, ki pri svojem delu uporablja osebne podatke ali jih kakorkoli obdeluje, ne sme med delovnim časom puščati nosilcev osebnih podatkov na pisalnih mizah ali jih kako drugače izpostavljati nevarnosti vpogleda vanje nepooblaščenim osebam oziroma delavcem.
V prostorih, kjer imajo vstop stranke oziroma osebe, ki niso zaposlene v podjetju, morajo biti nosilci podatkov in računalniški prikazovalniki nameščeni v času obdelave ali dela na njih tako, da strankam ne bo omogočen vpogled vanje.

9. člen
Nosilcev osebnih podatkov delavci podjetja ne smejo odnašati izven podjetja brez izrecnega dovoljenja direktorja.
Posredovanje varovanih podatkov pooblaščenim zunanjim institucijam in drugim, ki izkažejo zakonsko podlago za pridobitev osebnih podatkov, dovoli direktor.

Posredovanje osebnih podatkov iz predhodnega odstavka tega člena se vpiše v knjigo evidenc o manipulaciji z osebnimi podatki.

10. člen
Vzdrževalci prostorov in druge opreme v varovanih prostorih, poslovni partnerji in drugi obiskovalci se smejo gibati v varovanih prostorih le ob prisotnosti delavca družbe.

11. člen
Zaposleni tehnično vzdrževalni delavci in čistilke se lahko gibljejo v varovanih prostorih izven delovnega časa in brez prisotnosti odgovornega delavca le, če so nosilci podatkov shranjeni na način, ki ga določa ta pravilnik za čas izven delovnega časa.

12. člen
S štampiljkami, papirjem z glavo podjetja in drugimi pripomočki, s katerimi bi bilo mogoče ponarediti dokumente, je potrebno ravnati kot z zaupnimi podatki.

IV. ZAVAROVANJE SISTEMSKE IN APLIKATIVNE PROGRAMSKE RAČUNALNIŠKE OPREME TER PODATKOV, KI SE OBDELUJEJO Z RAČUNALNIŠKO OPREMO

13. člen
Dostop do računalniške programske opreme mora biti varovan, na način, ki omogoča dostop samo določenim pooblaščenim delavcem in delavcem, ki za podjetje na podlagi poslovnega odnosa opravljajo servisiranje računalniške in programske opreme.

14. člen
Vzdrževanje in popravila strojev in programske opreme je dovoljeno samo z vednostjo pooblaščene osebe, izvajajo pa ga lahko samo pooblaščeni servisi in vzdrževalci, ki so s podjetjem vstopili v poslovni odnos.

15. člen
Vzdrževalci prostorov, strojne in programske opreme, obiskovalci in poslovni partnerji se smejo gibati v teh prostorih samo z vednostjo pooblaščene osebe. Zaposleni, kot so npr. čistilke, varnostniki idr., se lahko izven delovnega časa gibljejo samo v tistih varovanih prostorih, kjer je onemogočen vpogled v podatke tako, da so nosilci podatkov shranjeni v zaklenjenih omarah in pisalnih mizah, računalniki in druga strojna oprema izklopljeni ali kako drugače fizično in programsko zaklenjeni.

16. člen
Dostop do programske opreme mora biti varovan tako, da dovoljuje dostop samo za to v naprej določenim zaposlenim ali pravnim in fizičnim osebam, ki opravljajo dogovorjene storitve.

17. člen
Popravljanje, spreminjanje in dopolnjevanje sistemske in aplikativne programske opreme je dovoljeno samo na podlagi odobritve pooblaščene osebe. Izvajalci morajo spremembe in dopolnitve sistemske in programske aplikativne opreme ustrezno dokumentirati.

18. člen
Za shranjevanje in varovanje aplikativne programske opreme veljajo enaka določila kot za ostale podatke iz tega pravilnika.

19. člen
Zaposleni ne smejo namestiti programske opreme brez vednosti pooblaščene osebe za posamezno delovno področje. Prav tako ne smejo odnašati programske opreme iz podjetja brez odobritve pooblaščene osebe.

20. člen
Pristop do podatkov preko aplikativne programske opreme se varuje s sistemom gesel za avtorizacijo in identifikacijo uporabnikov programov in podatkov.

21. člen
Vsa gesla in postopki, ki se uporabljajo za vstop in administriranje mreže osebnih računalnikov, administriranje elektronske pošte in administriranje programov se hranijo v zapečatenih ovojnicah in se jih varuje kot zaupni podatek. Uporabi se jih lahko samo v izrednih okoliščinah oziroma v nujnih primerih. Vsaka uporaba vsebine zapečatenih ovojnic se dokumentira. Pri vsaki takšni uporabi se določi nova vsebina gesel.

22. člen
Za potrebe restavriranja računalniškega sistema ob okvarah in drugih izjemnih situacijah se zagotavlja redna izdelava kopij mrežnega strežnika in lokalnih postaj (če se podatki nahajajo tam).

Te kopije se hranijo v zato določenih mestih, ki morajo biti ognjevarna, zavarovana proti poplavam in elektromagnetnim motnjam, v okviru predpisanih klimatskih pogojev ter zaklenjena.

23. člen
Dokumenti z zaupnimi podatki morajo na vidnem mestu imeti označbo, da so zaupni. Tako označbo morajo imeti tudi vse njihove priloge.
Pri izdelavi dokumentov, ki vsebujejo podatke, ki so zaupni se na originalu označi v koliko izvodih je bil izdelan (napisan, natiskan, narisan, razmnožen) in komu je bil posredovan. Vsak izvod takega dokumenta mora imeti svojo evidenčno številko.

24. člen
Dokumenti z oznakami tajnosti morajo biti vedno zaklenjeni v železnih omarah.

V. SPREJEM IN POSREDOVANJE ZAUPNIH PODATKOV

25. člen
Zaupne in osebne podatke je dovoljeno prenašati z informacijskimi, telekomunikacijskimi in drugimi sredstvi le ob izvajanju postopkov in ukrepov, ki nepooblaščenim osebam preprečujejo prilaščanje ali uničenje podatkov ter neupravičeno seznanjanje z njihovo vsebino.

26. člen
Zbirajo in obdelujejo se lahko samo tisti podatki, ki imajo ustrezno zakonsko osnovo. Za vse ostale osebne podatke je potrebno pridobiti pisno privolitev posameznika, na katerega se podatki nanašajo.

27. člen
Osebni podatki se posredujejo samo tistim uporabnikom, ki se izkažejo z ustrezno zakonsko osnovo ali pisno privolitvijo posameznika, na katerega se podatki nanašajo.

28. člen
Za vsako posredovanje osebnih podatkov mora upravičenec vložiti pisno vlogo, na kateri mora biti navedena zakonska osnova za pridobitev osebnih podatkov ali predložiti pisno privolitev posameznika. Vsako posredovanje osebnih podatkov se mora beležiti tako, da je mogoče pozneje ugotoviti kateri podatki so bili posredovani, komu, kdaj.

VI. BRISANJE PODATKOV OZIROMA UNIČENJE NOSILCEV OSEBNIH PODATKOV

29. člen
Osebni podatki se lahko vodijo v zbirki osebnih podatkov le toliko časa, kolikor je potrebno, da se doseže namen, za katerega se zbirajo in vodijo.
Po prenehanju potrebe po vodenju osebnih podatkov, se podatki zbrišejo oziroma uničijo nosilci podatkov.

30. člen
Brisanje osebnih podatkov na računalniških medijih se opravi na način, po postopku in metodi, ki onemogoča restavriranje brisanih podatkov.
Osebni podatki, vsebovani na klasičnih nosilcih (listine, kartoteke, register, seznam) se brišejo z uničenjem nosilcev. Nosilci se fizično uničijo (zažgejo, razrežejo) v prostorih družbe

ali pod nadzorom pooblaščenega delavca družbe pri organizaciji, ki se ukvarja z uničevanjem zaupne dokumentacije.

VII UKREPANJE OB UGOTOVITVI O ZLORABI OSEBNIH PODATKOV ALI VDORU V ZBIRKE OSEBNIH PODATKOV

31. člen
Delavci družbe so dolžni izvajati ukrepe za preprečevanje zlorabe osebnih podatkov in morajo z osebnimi podatki s katerimi se seznanijo pri svojem delu, ravnati vestno in skrbno na način in po postopkih, ki jih določa ta pravilnik.
Delavec, ki izve ali opazi, da je prišlo do zlorabe osebnih podatkov (odkrivanje osebnih podatkov, nepooblaščeno uničenje, nepooblaščeno spreminjanje, poškodovanje zbirke, prilaščanje osebnih podatkov) ali do vdora v zbirko osebnih podatkov, mora takoj o tem obvestiti direktorja in pooblaščenega delavca, ki vodi in ureja zbirko osebnih podatkov, ki so bili zlorabljeni ali v katero se je vdrlo.

32. člen
Direktor mora zoper tistega, ki je zlorabil osebne podatke ali je nepooblaščeno vdrl v zbirko osebnih podatkov ustrezno ukrepati.
Če obstaja sum pri vdoru v zbirko osebnih podatkov, da je ta storjen z naklepom in namenom zlorabiti osebne podatke ali jih uporabiti v nasprotju z nameni, za katere so zbrani ali če je do zlorabe osebnih podatkov že prišlo, mora direktor poleg uvedbe disciplinskega postopka zoper storilca, če je ta delavec družbe, vdor ali zlorabo prijaviti organom pregona.
Za zlorabo osebnih podatkov šteje vsaka uporaba osebnih podatkov v namene, ki niso v skladu z nameni zbiranja, določenimi v zakonu na podlagi katerega se zbirajo ali nameni, določenimi v katalogu zbirk osebnih podatkov.

VIII ODGOVORNOST ZA IZVAJANJE UKREPOV ZAVAROVANJA OSEBNIH PODATKOV

33. člen
Pred nastopom dela delavca na delovnem mestu, kjer se zbirajo, urejajo, obdelujejo, spreminjajo, shranjujejo, posredujejo ali uporabljajo osebni podatki ali nosilci osebnih podatkov, mora delavec podpisati izjavo, ki ga zavezuje k varovanju osebnih podatkov kot poklicne skrivnosti in ki ga opozarja na posledice kršitve zaveze.
Obveza varovanja osebnih podatkov, s katerimi se delavec seznani pri svojem delu v družbi traja tudi po prenehanju delovnega razmerja v družbi.

34. člen
Delavec stori kršitev delovne dolžnosti:
- če opusti vestno in skrbno nadzorovanje varovanih prostorov
- če opusti ravnanja za preprečitev vpogleda v ali na nosilce osebnih podatkov
- če ne uniči kopije osebnih podatkov
- če ni ves čas servisiranja računalnika in programske opreme prisoten
- če ne obvesti direktorja ali pooblaščenega delavca v primeru zlorabe osebnih podatkov ali vdora v zbirko osebnih podatkov
- če sporoča osebne podatke, s katerimi se je seznanil pri svojem delu sodelavcem ali drugim osebam,

• če opusti skrb in nadzor nad nosilci osebnih podatkov med delovnim časom in tako dopusti možnost vpogleda vanje nepooblaščenim osebam,
• če brez izrecnega dovoljenja odnaša iz družbe nosilce osebnih podatkov,
• če posreduje osebne podatke pooblaščenim zunanjim institucijam brez dovoljenja direktorja,
• če nepooblaščeno popravlja, spreminja ali dopolnjuje sistemsko ali aplikativno programsko opremo
• če namesti ali odnese programsko opremo iz družbe brez izrecnega dovoljenja direktorja
• če ne hrani računalniških kopij vsebin zbirk osebnih podatkov v zavarovanih zaklenjenih omarah.
Kršitve določil pravilnika so lahko razlog za odpoved pogodbe o zaposlitvi.

35. člen
Za izvajanje postopkov in ukrepov za varovanje zaupnih podatkov so odgovorni vodje služb in pooblaščene osebe, ki jih imenuje direktor.

Vodje služb so dolžni:
• poslovanje služb organizirati tako, da zagotovijo spoštovanje tega pravilnika,
• seznaniti delavce z dolžnostjo varovati zaupne in osebne podatke,
• v primeru dejavnosti neopravičene uporabe osebnih in zaupnih podatkov, takoj ukreniti vse, da se tako dejanje onemogoči ali prepreči.

IX PREHODNE IN KONČNE DOLOČBE

36. člen
Ta pravilnik sprejme direktor družbe. Spremembe in dopolnitve tega pravilnika sprejme direktor po postopku in na način kot velja za sprejem pravilnika.

37. člen
Z določbami tega pravilnika morajo biti seznanjeni vsi delavci družbe.
Ta pravilnik prejmejo službe oziroma delavci v čigar delovne obveznosti sodi zbiranje, urejanje, obdelava, spreminjanje, shranjevanje, posredovanje ali uporaba osebnih podatkov ali nosilcev osebnih podatkov ter ostalih zaupnih podatkov.

38. člen
Delavci, ki delajo na delovnih mestih, kjer se zbirajo, urejajo, obdelujejo, spreminjajo, shranjujejo, posredujejo ali uporabljajo osebni podatki ali nosilci osebnih podatkov, ter ostalimi zaupnimi podatki podatki morajo podpisati izjavo iz 34. člena tega pravilnika v roku 14 dni od dneva sprejema tega pravilnika.