

Družba X Y d.o.o., _____, _____ (naslov), matična št. _____, na podlagi 25. člena Zakona o varstvu osebnih podatkov (Uradni list RS, 86/04 in 113/05),

sprejema naslednji

PRAVILNIK

O

VARSTVU OSEBNIH PODATKOV

I. SPLOŠNE DOLOČBE

1. člen

S tem pravilnikom se določajo postopki in ukrepi za zavarovanje osebnih podatkov, ki se zbirajo oziroma obdelujejo v družbi X Y d.o.o., z namenom, da se prepreči slučajno ali namerno nepooblaščen uničevanje podatkov, njihovo spremembo ali izgubo ter da se prepreči nepooblaščen obdelava, uporaba ali posredovanje osebnih podatkov.

Pravilnik ureja tudi postopek v zvezi z varstvom pravic, ki gredo posamezniku na podlagi obdelave osebnih podatkov.

Zaposleni in zunanji sodelavci, ki pri svojem delu obdelujejo in uporabljajo osebne podatke, morajo biti seznanjeni z Zakonom o varstvu osebnih podatkov, s področno zakonodajo, ki ureja posamezno področje njihovega dela ter z vsebino tega pravilnika.

2. člen

V tem pravilniku uporabljeni izrazi imajo enak pomen, kot izrazi določeni v Zakonu o varstvu osebnih podatkov (Uradni list RS, št. 86/04 in 113/05).

3. člen

Opis zbirk osebnih podatkov, katerih upravljavec je družba X Y d.o.o., se vodi v katalogu zbirk osebnih podatkov, ki vsebuje naslednje evidence:

- Evidenco o zaposlenih delavcih
- Evidenco o študentskem delu
- Evidenca o naročnikih geodetskih storitev in ostalih strankah postopka

Katalog zbirke osebnih podatkov se za vsako zbirko osebnih podatkov zagotovi najkasneje 15 dni pred vzpostavitvijo zbirke osebnih podatkov, v istem roku pa se podatki iz kataloga posredujejo tudi pristojnemu državnemu organu. Katalog zbirk osebnih podatkov se dopolnjuje ob vsaki spremembi vrste osebnih podatkov v posamezni zbirki, spremembe pa se v roku 8 dni posredujejo tudi pristojnemu državnemu organu.

Zaposleni, ki obdelujejo osebne podatke, morejo biti seznanjeni s katalogom zbirk osebnih podatkov, vpogled v katalog zbirk osebnih podatkov pa je potrebno omogočiti tudi vsakomur, ki to zahteva.

II. UKREPI ZA ZAVAROVANJE OSEBNIH PODATKOV

4. člen

Zavarovanje osebnih podatkov zajema vse postopke in ukrepe, s katerimi se varujejo prostori, sistemska in programska oprema, varuje aplikativna programska oprema, s katero se obdelujejo osebni podatki, preprečuje nepooblaščen dostop do osebnih podatkov pri njihovem posredovanju in prenosu v kakršnikoli obliki, omogoča naknadno ugotavljanje, kdaj so bili posamezni osebni podatki vneseni v zbirko, uporabljeni ali kako drugače obdelani ter kdo je to storil in sicer za celotno obdobje, v katerem se posamezni podatki shranjujejo.

II. 1 VAROVANJE PROSTOROV

5. člen

Prostori, v katerih se nahajajo nosilci osebnih podatkov (dokument na katerem je osebni podatek zapisan), strojna in programska oprema, morajo biti varovani z organizacijskimi ter fizičnimi in tehničnimi ukrepi, ki onemogočajo nepooblaščenim osebam dostop do podatkov.

Na tem mestu je potrebno zapisati konkretno varovanje osebnih podatkov, kot npr. prostor je varovan z alarmno napravo, kdo vse ima možnost deaktivacije alarma ter kdo razpolaga z ključem za vstop v prostore, kjer se osebni podatki nahajajo (opisno, kot npr. zaposleni, čistilke,...).

Posebej se omeni, da ima družbo tudi arhivsko sobo, ki je varovana s posebnim alarmom ali s posebno ključavnico, ipd.. Priporočljivo je zapisati, da je vsak dostop in razlog za dostop v arhiv evidentiran v knjigi vstopov, ki se nahaja npr. v tajništvu.

Nepooblaščene osebe ne smejo vstopati v prostore brez spremstva pooblaščene osebe.

Dostop je mogoč le v rednem delovnem času, izven tega časa pa samo na podlagi predhodnega dovoljenja direktorja družbe.

Varovani prostori ne smejo ostajati nenadzorovani, oziroma se morajo zaklepati ob odsotnosti delavcev, ki jih nadzorujejo.

Izven delovnega časa morajo biti omare in pisalne mize z nosilci osebnih podatkov zaklenjene, računalniki in druga strojna oprema izklopljeni in fizično ali programsko zaklenjeni.

Zaposleni ne smejo puščati nosilcev osebnih podatkov na vidnem mestu v prisotnosti oseb, ki nimajo pravice vpogleda vanje.

6. člen

Iznos nosilcev osebnih podatkov je dopusten zgolj s pisnim soglasjem direktorja družbe X Y d.o.o., pod pogojem, da je iznos dopusten in v skladu z določili Zakona o varstvu osebnih podatkov.

Iznos nosilcev osebnih podatkov je potrebno na ustrezen način registrirati.

II. 2 VAROVANJE SISTEMSKE IN APLIKATIVNO PROGRAMSKE RAČUNALNIŠKE OPREME TER PODATKOV, KI SE OBDELUJEJO Z RAČUNALNIŠKO OPREMO

7. člen

Vzdrževanje in popravila strojne računalniške in druge opreme, kjer se nahajajo osebni podatki, je dovoljeno samo z vednostjo direktorja družbe, izvajajo pa ga lahko samo tisti vzdrževalci, ki imajo z družbo X Y d.o.o. sklenjeno ustrezno pogodbo oziroma opravljajo vzdrževalno delo na drugi ustrezni pravni podlagi.

Direktor družbe X Y d.o.o., za vsak konkreten primer vzdrževanja, imenuje odgovorno osebo, ki opravlja nadzira nad vzdrževalcem iz prvega odstavka tega člena.

8. člen

Dostop do programske opreme mora biti varovan tako, da dovoljuje dostop samo za to v naprej določenim zaposlenim osebam, ki v skladu s pogodbo iz prejšnjega člena tega pravilnika, izvajajo pogodbene storitve.

9. člen

Popravljanje, spreminjanje in dopolnjevanje systemske in aplikativne programske opreme je dovoljeno samo na podlagi odobritve direktorja družbe X Y d.o.o., izvajajo pa ga lahko samo pooblaščenih servisi, ki imajo z družbo X Y d.o.o. sklenjeno ustrezno pogodbo oziroma opravljajo vzdrževalno delo na drugi ustrezni pravni podlagi.

10. člen

Pristop do podatkov preko aplikativne programske opreme se varuje s sistemom gesel za identifikacijo uporabnikov programov in podatkov, sistem gesel pa mora omogočati tudi možnost naknadnega ugotavljanja, kdaj so bili posamezni osebni podatki vneseni v zbirko podatkov, uporabljeni ali drugače obdelovani ter kdo je to storil.

Sitem podeljevanja gesel določi in vodi direktor družbe X Y d.o.o..

Gesla se hranijo v zaklenjenem predalu direktorja družbe X Y d.o.o., vsaka njihova uporaba se na ustrezen način evidentira.

11. člen

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

Te kopije se hranijo na mestu, kjer je možno zagotoviti njihov ustrezno varstvo pred nepooblaščenim dostopom in pred naključnim uničenjem.

II. 3 UNIČENJE, IZBRIS, ANONIMIZIRANJE IN BLOKIRANJE OSEBNIH PODATKOV

12. člen

Anonimiziranje je takšna sprememba oblike osebnih podatkov, da jih ni več mogoče povezati s posameznikom ali pa bi bilo to povezano z nesorazmernimi napori in stroški.

Blokiranje je takšna označitev osebnih podatkov, da se omeji ali prepreči njihova nadaljnja obdelava.

Po preteku roka hranjenja se osebni podatki zbršejo, uničijo, blokirajo ali anonimizirajo, razen če zakon ali drug akt ne določa drugače.

Roki, po katerih se osebni podatki izbršejo iz zbirke podatkov, so razvidni iz 7. točke kataloga zbirke osebnih podatkov.

13. člen

Za brisanje podatkov iz računalniških medijev se uporabi takšen način, postopek oziroma metoda brisanja, da je onemogočena njihova ponovna vzpostavitev.

Podatki na klasičnih medijih se brišejo z fizičnim uničenjem nosilcev (razrez, zažiganje,...) v prostorih družbe ali drugje, pod nadzorom direktorja družbe in od njega pooblaščenih oseb. Na enak način se uničuje pomožno gradivo (npr. skice, poskusne oziroma neuspešne izpise, ipd.).

Pri prenosu nosilcev osebnih podatkov na mesto uničenja je potrebno zagotoviti ustrezno zavarovanje tudi v času prenosa.

O uničenju nosilcev in zavarovanju nosilcev v času prenosa, se sestavi zapisnik, ki ga podpišejo vse prisotne osebe.

II. 4 VAROVANJE OSEBNIH PODATKOV, KI SE VODIJO V INFORMACIJSKEMU SISTEMU PRED RAČUNALNIŠKIMI VIRUSI

14. člen

Vsebina diskov mrežnega strežnika in lokalnih delovnih postaj, kjer se nahajajo osebni podatki, se sprotno preverja glede na prisotnost računalniških virusov.

Ob pojavu računalniškega virusa se tega čimprej odpravi s pomočjo ustrezne strokovne službe družbe X Y d.o.o., obenem pa se ugotovi vzrok pojava virusa v računalniškem informacijskem sistemu družbe.

Vsi osebni podatki in programska oprema, ki so namenjeni uporabi v računalniškem informacijskem sistemu, in prispejo v družbo na medijih za prenos računalniških podatkov ali preko telekomunikacijskih kanalov, morajo biti pred uporabo preverjeni glede prisotnosti računalniških virusov.

15. člen

Zaposleni ne smejo inštalirati programske opreme, ki se nanaša na obdelavo osebnih podatkov brez vednosti osebe, zadolžene za delovanje računalniškega informacijskega sistema. Prav tako ne smejo odnašati programske opreme iz prostorov družbe X Y d.o.o. brez odobritve direktorja družbe. Vsak prenos programske opreme iz prostorov družbe X Y d.o.o. se ustrezno evidentira.

III. SPREJEM IN POSREDOVANJE OSEBNIH PODATKOV

16. člen

Delavec, ki je zadolžen za sprejem in evidenco pošte, mora izročiti poštno pošiljko z osebnimi podatki direktno posamezniku, ali službi, na katero je ta pošiljka naslovljena.

Delavec, ki je zadolžen za sprejem in evidenco pošte, odpira in pregleduje vse poštno pošiljke in pošiljke, ki na kakršenkoli drug način prispejo v družbo, razen naslednjih pošiljk:

- pošiljke naslovljene na drugega naslovnika
- pošiljke, ki so označene z besedno zvezo »osebno naslovniku«
- pošiljke iz katerih je mogoče sklepati, da so naslovljene osebno na zaposlenega, kljub temu, da so poslani in dostavljeni neposredno družbi ter
- drugih pošiljk, katerih nepooblaščen odpiranje bi bilo v nasprotju z zakoni ali podzakonskimi akti.

17. člen

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

Osebni podatki se pošiljajo naslovnikom v zaprtih ovojnica proti podpisu v dostavni knjigi ali priporočeno.

Občutljivi osebni podatki (19. točka prvega odstavka 6. člena Zakona o varstvu osebnih podatkov) se vselej pošiljajo priporočeno s povratnico.

Ovojnica, v kateri se posredujejo osebni podatki, mora biti izdelana na takšen način, da ovojnica ne omogoča, da bi bila ob normalni svetlobi ali pri osvetlitvi ovojnic z običajno lučjo vidna vsebina ovojnice. Prav tako mora ovojnica zagotoviti, da odprtja ovojnice in seznanitve z njeno vsebino ni mogoče opraviti brez vidne sledi odpiranja ovojnice.

18. člen

Občutljivi osebni podatki morajo biti pri obdelavi posebej označeni in zavarovani tako, da se nepooblaščenim osebam onemogoči dostop, razen če je posameznik, na katerega se nanašajo občutljivi osebni podatki, to javno objavil brez očitnega ali izrecnega namena, da omeji namen njihove uporabe.

Podatki iz prejšnjega odstavka se smejo posredovati preko telekomunikacijskih omrežij samo, če so posebej zavarovani s kriptografskimi metodami in elektronskim podpisom tako, da je zagotovljena nečitljivost podatkov med njihovim prenosom.

19. člen

Osební podatki se posredujejo samo tistim uporabnikom, ki se izkažejo z ustrežno zakonsko podlago ali s pisno zahtevo oziroma privolitvijo posameznika, na katerega se podatki nanašajo.

Za vsako posredovanje osebnih podatkov mora upravičenec vložiti pisno vlogo, v kateri mora biti navedena določba zakona, ki uporabniku omogoča njihovo posredovanje ali pa mora biti vlogi priložena izrecna pisna privolitev posameznika, na katerega se podatki nanašajo.

Vsako posredovanje osebnih podatkov se beleži v evidenco posredovanj, iz katere mora biti razvidno, kateri osebni podatki so bili posredovani, komu, kdaj in na kakšni podlagi in sicer za obdobje, ko je mogoče zakonsko varstvo pravice posameznika zaradi nedopustnega posredovanja osebnih podatkov.

IV. OSEBE ODGOVORNE ZA IZVAJANJE OZIROMA IZVRŠEVANJE TEGA PRAVILNIKA

IV. 1 NOTRANJE IZVRŠEVANJE PRAVILNIKA

20. člen

Vsak, ki obdeluje osebne podatke ali se na kakršenkoli drug način seznanja z osebnimi podatki, ki jih zbira družba, je dolžan izvajati predpisane postopke in ukrepe za zavarovanje podatkov in varovati podatke, za katere je zvedel oziroma bil z njimi seznanjen pri opravljanju svojega dela.

Obveza varovanja podatkov ne preneha s prenehanjem delovnega razmerja.

Pred nastopom dela na delovno mesto, kjer se obdelujejo osebni podatki, mora zaposleni podpisati posebno izjavo, ki ga zavezuje k varovanju osebnih podatkov.

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

Izjava iz drugega odstavka tega člena je lahko sestavni del pogodbe o zaposlitvi.

Kršitev določil pravilnika o varstvu osebnih podatkov predstavlja razlog za izredno odpoved pogodbe o zaposlitvi delavca, ostale osebe pa so za kršitev tega pravilnika pogodbeno ali odškodninsko odgovorne.

21. člen

Za izvajanje postopkov in ukrepov za zavarovanje osebnih podatkov družbe X Y d.o.o. so odgovorne pooblašene osebe, ki jih imenuje direktor družbe.

Seznam pooblaščenih oseb mora biti na ustrezen način objavljen v prostorih družbe.

Nadzor nad izvajanjem postopkov in ukrepov, določenih s tem pravilnikom, opravlja direktor družbe.

22. člen

Zaposleni so dolžni o aktivnostih, ki so povezane z odkrivanjem ali nepooblaščenim uničenjem zaupnih podatkov, zlonamerni ali nepooblaščen uporabi, prilaščanju, spreminjanju ali poškodovanju takoj obvestiti pooblaščen osebno ali predstojnika, sami pa poskušajo takšno aktivnost preprečiti.

IV. 2 POGODBENO IZVRŠEVANJE PRAVILNIKA

23. člen

Družba X Y d.o.o. lahko posamezna opravila v zvezi z obdelavo osebnih podatkov zaupa pogodbenemu obdelovalcu, ki mora zagotavljati vse ustrezne ukrepe in postopke zavarovanja osebnih podatkov, kot to določa Zakon o varstvu osebnih podatkov in na njegovi podlagi sprejeti podzakonski akti.

Pogodbeni obdelovalec iz prejšnjega odstavka tega člena mora biti registriran za opravljanje dejavnosti, ki se mu v zvezi z obdelavo podatkov zaupa.

Pogodba o zunanji obdelavi podatkov mora biti sklenjena v pisni obliki in mora vsebovati dogovor o postopkih in ukrepih zavarovanja osebnih podatkov, način nadzora družbe Tedenski Žurnal d.o.o. ter namen obdelave osebnih podatkov.

V. PRAVICE POSAMEZNIKOV

24. člen

Družba X Y d.o.o. mora posamezniku na njegovo zahtevo in brez nepotrebnega odlašanja, po pooblaščenem predstavniku:

- omogočiti vpogled v katalog zbirke osebnih podatkov
- potrditi ali se podatki v zvezi z njim obdelujejo ali ne, in mu omogočiti vpogled v osebne podatke, ki so vsebovani v zbirki osebnih podatkov in se nanašajo nanj
- omogočiti kopiranje in prepisovanje osebnih podatkov, ki se nanašajo nanj
- posredovati izpis osebnih podatkov, ki se nahajajo v zbirki osebnih podatkov in ki se nanašajo nanj
- pojasniti vse okoliščine v zvezi z posredovanjem podatkov tretjim osebam
- posredovati podatke o virih in metodi obdelave osebnih podatkov, o vrsti osebnih podatkov, ki se obdelujejo in namen obdelave le-teh
- zagotoviti vse ostale zakonske pravice posameznika, ki se nanašajo na obdelavo oziroma vodenje evidenc osebnih podatkov

Zahteva posameznika iz prvega odstavka tega člena mora biti pooblaščenemu predstavniku družbe posredovana pod pogoji in na način določen z Zakonom o varstvu osebnih podatkov.

Pooblaščen predstavnik družbe lahko zavrne zahtevo posameznika iz tega člena zgolj če za to obstajajo zakonsko določeni razlogi. Zavrnitev zahteve mora biti izražena pisno.

25. člen

Glede obveščanja posameznika o obdelavi osebnih podatkov, glede pravice posameznika do dopolnitve, popravka, blokiranja, izbrisa in ugovora ter glede postopka uveljavljanja slednjih pravic, se neposredno uporabljajo določbe 19., 32. in 33. člena Zakona o varstvu osebnih podatkov

VI. PREHODNE IN KONČNE DOLOČBE

26. člen

Ta pravilnik stopi v veljavo z dnem __.__.2007, uporabljati pa se začne 15 dan po njegovi objavi na oglasni deski na sedežu družbe X Y d.o.o.

V Ljubljani, dne __.__._____

X Y d.o.o.
direktor _____