



Gajeva 3, 52100 Pula
Telefon/faks: 052 506 065
e-mail: udruga-zelena-istra@pu.t-com.hr
url: www.zelena-istra.hr

Na temelju Zakona o zaštiti osobnih podataka – NN 103/03, 118/06, 41/08, 130/11, 106/12,
Skupština Zelene Istre na sjednici 9. rujna 2016. donosi

PRAVILNIK O ZAŠTITI INFORMACIJSKOG SUSTAVA I TAJNOSTI PODATAKA

I OPĆE ODREDBE

Članak 1.

Ovim Pravilnikom određuju se podaci u poslovanju koji se smatraju poslovnom tajnom, te njihova uporaba i zaštita, načini pribavljanja, obrade, pohrane i korištenje osobnih podataka koji se prikupe pri obavljanju djelatnosti, te mjere i načini zaštite informacijskog sustava, tj. točnost, dostupnost i povjerljivost podataka.

Članak 2.

Pojedini pojmovi u smislu ovog Pravilnika imaju sljedeće značenje:

Informacijski sustav je skup svih podataka, informacija i dokumentacije koja se na temelju zakona, propisa ili akata Udruge prikuplja, stvara, pohranjuje, čuva, obrađuje i daje na korištenje, bez obzira u kojem obliku i na kojem mediju su zabilježeni. Informacijski sustav obuhvaća informatički sustav i ljudske resurse.

Informatički sustav obuhvaća svu informatičku opremu, računalno-komunikacijsku mrežnu infrastrukturu, softvere, baze podataka te računalne komponente (uključujući medije kao nositelje podataka) koji su u vlasništvu ili u upotrebi u Udruzi.

Podaci su svi podaci koje se nalaze ubilježeni na bilo kojem mediju i u bilo kojem obliku.

Osobni podaci su, u smislu propisa o zaštiti osobnih podataka, svaka informacija koja se odnosi na identificiranu fizičku osobu ili fizičku osobu koja se može identificirati izravno ili neizravno na osnovu podataka ili bilo kojeg drugog specifičnog obilježja.

Zbirke osobnih podataka su evidencije koje Udruga vodi temeljem zakona ili drugih propisa, a koje sadrže osobne podatke.

Profesionalnom tajnom smatraju se svi osobni podaci čije bi eventualno otkrivanje moglo naštetiti osobi na koju se podaci odnose, ili članu njene obitelji.

Poslovnom tajnom smatraju se podaci koji su zakonom, drugim propisima ili aktima Udruge utvrđeni kao poslovna tajna, planovi i mjere fizičko-tehničke zaštite sigurnosti objekata i imovine te mjere informacijske sigurnosti, kao i podaci koje je Udruga primila kao poslovnu tajnu od drugih pravnih ili fizičkih osoba ili tijela javne vlasti.

Dokumentacija podrazumijeva svu dokumentaciju koja je dio informacijskog sustava.

II POSLOVNA TAJNA

Članak 2.

Ovim Pravilnikom kao poslovna tajna određuju se podaci koji se koriste u pripremi odluka, ugovori te drugi dokumenti ako bi njihovim priopćavanjem neovlaštenoj osobi mogle nastupiti štetne posljedice za interese Udruge, u skladu sa zakonskim propisima.

Članak 3.

Poslovnom tajnom smatraju se:

- podaci koji se proglase poslovnom tajnom od strane tijela upravljanja
- plan fizičko-tehničke zaštite radnika i imovine Udruge
- podaci koji se kao poslovna tajna saznaju od drugih pravnih osoba
- osobni podaci
- podaci o obustavama plaće i sl.
- podaci koji se zakonom, drugim propisima ili općim aktima Udruge utvrđeni kao tajni podaci

Članak 4.

Poslovna tajna može, a ne mora biti, naznačena na dokumentu.

Poslovna tajna može biti priopćena i usmenim putem i ima jednaku važnost kao i pisana oznaka tajnosti.

Članak 5.

Podaci koji se smatraju poslovnom tajnom ne smiju se priopćavati niti činiti dostupnim neovlaštenim osobama, ako posebnim zakonom nije drugačije određeno.

Članak 6.

Podatke koji se smatraju poslovnom tajnom drugim osobama mogu priopćavati samo osobe ovlaštene za zastupanje Udruge, ili posebno imenovane osobe.

Članak 7.

Poslovna tajna priopćuje se:

- osobama koje imaju pravo uvida temeljem zakona i drugih propisa, temeljem ovog Pravilnika ili drugih akata Udruge
- osobama koje trebaju biti upoznate s tajnom radi nesmetanog obavljanja poslova, radi realizacije poslovne suradnje sa drugim subjektima, odnosno radi ispunjavanja obveza Udruge propisanih zakonom.

Članak 8.

Povredom obveze čuvanja tajne ne smatra se priopćavanje tajne u slučajevima iz članka 7. ovog Pravilnika, kao ni u drugim zakonom propisanim slučajevima.

Članak 9.

Povreda dužnosti čuvanja poslovne tajne smatra se osobito teškom povredom obveza iz radnih odnosa.

Članak 10.

Poslovnu tajnu dužni su čuvati svi radnici Udruge i članovi tijela Udruge koji na bilo koji način saznaju podatke koji se smatraju poslovnom tajnom.

Članak 11.

Dužnost čuvanja poslovne tajne ne prestaje nakon prestanka radnog odnosa, niti nakon prestajanja obavljanja dužnosti člana tijela Udruge, sve dok se podatak smatra poslovnom tajnom.

Članak 12.

Ne smatra se povredom čuvanja poslovne tajne priopćavanje podataka ako se priopćavanje obavlja osobama kojima se takvi podaci mogu ili moraju priopćiti:

- na temelju zakona ili drugih propisa
- na temelju ovlasti koja proizlazi iz dužnosti koju obavljaju ili
- radnog mjesta na kojemu su zaposleni.

Članak 13.

Odgovorni zaposlenik ili član tijela Udruge za povredu poslovne tajne odgovara stegovno, materijalno i kazнено, ovisno o posljedicama nestanka ili otkrivanje tajne.

Članak 14.

Kaznenim zakonom predviđena su kaznena djela u svezi neovlaštenog odavanja poslovne tajne koju je zaposlenik ili član tijela Udruge saznao u obavljanju svog posla.

Članak 15.

Zaposlenik ili član tijela Udruge kazнено odgovara neovisno o stegovnoj odgovornosti.

III OSOBNİ PODACI

Članak 16.

Osobni podaci prikupljaju se, obrađuju, pohranjuju i s njima se raspolaže na način i u skladu sa Zakonom o zaštiti osobnih podataka.

Članak 17.

Osobni podaci smiju se prikupljati i dalje obrađivati isključivo:

- uz privolu ispitanika samo u svrhu za koju je ispitanik dao privolu, ili
- u slučajevima određenim zakonom, ili
- u svrhu izvršavanja zakonskih obveza voditelja zbirke osobnih podataka, ili

- u svrhu sklapanja i izvršenja ugovora u kojem je ispitanik stranka, ili
- u svrhu zaštite života ili tjelesnog integriteta ispitanika ili druge osobe u slučaju kada ispitanik fizički ili pravno nije u mogućnosti dati svoj pristanak, ili
- ako je obrada podataka nužna radi ispunjenja zadataka koji se izvršavaju u javnom interesu ili u izvršavanju javnih ovlasti koje ima voditelj zbirke osobnih podataka ili treća strana kojoj se podaci dostavljaju ili
- ako je obrada podataka nužna u svrhu zakonitog interesa voditelja zbirke osobnih podataka ili treće strane kojoj se podaci otkrivaju, ili
- ako je ispitanik sam objavio te podatke.

Članak 18.

Zabranjeno je prikupljanje i daljnja obrada osobnih podataka koji se odnose na rasno ili etničko podrijetlo, politička stajališta, vjerska ili druga uvjerenja, sindikalno članstvo, zdravlje ili spolni život i osobnih podataka o kaznenom i prekršajnom postupku.

Iznimno, podaci iz stavka 1. ovoga članka mogu se i prikupljati i dalje obrađivati:

- uz privolu ispitanika, ili
- ako je obrada podataka potrebna u svrhu izvršavanja prava i obveza koje ima voditelj zbirke osobnih podataka na temelju posebnih propisa, ili
- ako se obrada provodi u okviru djelatnosti Udruge, pod uvjetom da se obrada isključivo odnosi na članove te da podaci ne budu otkriveni trećoj strani bez pristanka ispitanika, ili
- ako je obrada podataka potrebna radi uspostave, ostvarenja ili zaštite potraživanja propisanih zakonom, ili
- ako je ispitanik sam objavio te podatke.

Članak 19.

Za potrebe formiranja, vođenja i drugih postupanja sa evidencijama zbirke osobnih podataka imenovat će se Službenik za zaštitu osobnih podataka.

Članak 20.

Postupanja službenika za zaštitu osobnih podataka moraju biti u skladu sa Zakonom o zaštiti osobnih podataka te sa svim propisima i uredbama proizašlim iz Zakona.

IV MJERE SIGURNOSTI INFORMACIJSKOG SUSTAVA

Članak 21.

Zaposlenici i članovi tijela Udruge se obavezno, pri zaposlenju ili imenovanju, moraju upoznati sa važećim propisima i aktima Udruge.

Članak 22.

Stupanjem na snagu ovog Pravilnika svi budući zaposlenici ili članovi tijela Udruge, pri zaposlenju ili imenovanju, dužni su potpisati Izjavu o povjerljivosti.

Za ostale zaposlenike i članove tijela Udruge, koji u momentu stupanja na snagu ovog Pravilnika, obnašaju dužnost ili se nalaze u radnom odnosu, odluku o obvezi potpisivanja Izjave donose osobe ovlaštene za zastupanje na temelju slobodne procjene.

Članak 23.

U Udruzi se provode opće mjere zaštite, utvrđene zakonom, drugim propisima ili općim aktima Udruge:

- mjere zaštite od požara
- mjere za sprječavanje neovlaštenog korištenja informatičke opreme i mreže
- mjere za održavanje informatičke opreme i mreže

Članak 24.

Mjere zaštite prostorija u kojima se nalazi dokumentacija u sklopu informacijskog sustava su:

- ulazak u prostoriju i boravak u istoj nije dozvoljen bez prisustva nadležnog zaposlenika
- obveza zaključavanja prostorije u tijeku trajanja odsustva tijekom radnog vremena i po završetku radnog vremena
- zabrana iznošenja dokumentacije i informatičke opreme iz prostorija bez dopuštenja odgovorne osobe
- osiguravanje opreme mjerama protupožarne zaštite

Članak 25.

Mjere zaštite dokumentacije su:

- pristup dokumentaciji, posebice onoj koja sadrži zakonom zaštićene podatke, dopušta se samo ovlaštenim osobama
- papirnata dokumentacija čuva se i pohranjuje u zaštićenim prostorijama, s mogućnošću zaključavanja
- dokumentacija za koju istekne obveza čuvanja uništava se na odgovarajući način

Članak 26.

Mjere zaštite i kontrole za pristup podacima u poslovnim procesima su sljedeće:

- pristup podacima dopušten je samo ovlaštenim osobama
- za pristup i postupanje sa osobnim podacima ovlaštena osoba je Službenik za zaštitu osobnih podataka
- zaposlenici su dužni lozinkom zaštititi pristup informatičkoj opremi
- internet mreža mora biti ograničena za korištenje isključivo za zaposlenike
- osobni podaci, odnosno računalne mape (folderi) u kojima se čuvaju ovakve baze podataka, moraju biti dodatno zaštićeni dodatnom lozinkom ili odgovarajućim programom
- pri duljem izbivanju sa radnog mjesta, kao i pri odlasku sa posla, zaposlenik se mora obavezno odjaviti sa aplikacija i sustava koje koristi

Članak 27.

Zaposlenik koji svoju lozinku da na korištenje neovlaštenoj osobi, u slučaju zlouporabe odgovara zbog povreda radne obveze i (su)odgovoran je za eventualnu štetu.

Članak 28.

Računalno-komunikacijski sustav i usluge dostupne putem sustava, osobito Internet i mail , moraju se koristiti prvenstveno za obavljanje poslova Udruge.

Članak 29.

Zaposlenik koji zlouporabi informatički sustav odgovara zbog povrede radne obveze.

Pod zluporabom se podrazumijeva:

- pristup, prijenos ili učitavanje podataka i instaliranje programa koji sigurnosno mogu ugroziti informatičku opremu i mrežu
- pristup, prijenos ili učitavanje sadržaja koje sadrže diskriminirajuće i slične podatke neprimjerene prirode
- korištenje mreže i komunikacijskih alata u privatne komercijalne svrhe

Članak 30.

Za osiguravanje i provedbu mjera odgovorne su osobe za zastupanje Udruge.

V ZAVRŠNE ODREDBE

Članak 31.

U slučaju nesuglasja neke od odredbi Pravilnika s odredbama zakona donesenog nakon stupanja Pravilnika na snagu, do usklađenja odredbi Pravilnika izravno se primjenjuju zakonske odredbe.

Članak 32.

Ovaj prijedlog Pravilnika stupa na snagu danom donošenja od strane Upravnog odbora, dok će njegova konačna potvrda uslijediti na prvoj sljedećoj sjednici Skupštine Udruge.

U Puli, 9. rujna 2016.

Za Udrugu Zelena Istra,
Predsjednica
Dušica Radojčić