PRAVILNIK
O INFORMATIČKOJ SIGURNOSTI
VODOVOD-OSIJEK d.o.o.

SADRŽAJ

Na temelju članka 422. Zakona o trgovačkim društvima (NN 152/11 - pročišćeni tekst, 111/12, 68/13, 110/15), članka 35. Društvenog ugovora VODOVOD-OSIJEK d.o.o., članka 5., 26., 27. i 28. Zakona o radu (NN 93/14, NN 127/17), , članak 3. Zakona o informacijskoj sigurnosti, članak 2. Opće uredbe o zaštiti podataka od 27. travnja 2016., članka 1. Uredbe o načinu pohranjivanja i posebnim mjerama tehničke zaštite posebnih kategorija osobnih podataka), i drugih podzakonskih akata kojima se uređuje i regulira zaštita osobnih podataka i provedba sustava tehničke zaštite, Pravilniku o zaštiti osobnih podataka VODOVOD-OSIJEK d.o.o. nakon prethodne suglasnosti radničkog vijeća, član Uprave-direktor VODOVOD-OSIJEK d.o.o. dana 24. svibnja 2018. godine donosi:

PRAVILNIK
O INFORMATIČKOJ SIGURNOSTI
VODOVOD-OSIJEK d.o.o.

I. OPĆE ODREDBE

Članak 1.

Ovim Pravilnikom se radi osiguravanja informatičke sigurnosti u VODOVOD – OSIJEK d.o.o. (u daljnjem tekstu Poslodavac), uređuju opće odredbe, mjere zaštite i sigurnosti informatičkog sustava, pravila korištenja informatičkog sustava i zaštita nadzorom prikupljenih osobnih podataka, evidencije Informatičke službe, zaštita privatnosti i povjerljivosti osobnih podataka i završne odredbe.

Članak 2.

Pojedini pojmovi u smislu ovoga Pravilnika imaju sljedeće značenje:

1. ***Informacijski sustav*** Poslodavca je skup svih podataka, informacija i dokumentacije koje isti na temelju zakona prikuplja, stvara, pohranjuje, čuva, obrađuje i daje na korištenje, bez obzira na to u kojem su obliku i na kojem mediju ubilježeni. Informacijski sustav Poslodavca obuhvaća i informatički sustav i ljudske resurse.
2. ***Informatički sustav*** Poslodavca obuhvaća svu informatičku opremu (središnje računalo, poslužitelje, osobna računala i drugo), računalno-komunikacijsku mrežnu infrastrukturu, sistemski i aplikativni software, baze podataka te računalne komponente (uključujući medije kao nositelje podataka) koje su u vlasništvu Poslodavca ili su u upotrebi kod Poslodavca. Informatički sustav je podrška informacijskom sustavu.
3. ***Informatička sigurnost*** je stanje povjerljivosti, cjelovitosti i raspoloživosti podataka, koje se postiže primjenom propisanih mjera i standarda informatičke sigurnosti.
4. ***Mjere informatičke sigurnosti*** su opća pravila zaštite informatičkog sustava na tehničkoj ili organizacijskoj razini.

5. ***Podaci*** su svi podaci koji se nalaze ubilježeni na bilo kojem mediju i u bilo kojem obliku, čineći cjelokupan informacijski sklop pojedinog radnika, korisnika usluga vodoopskrbe i odvodnje, poslovnih partnera, odnosno fizičkih ili pravnih osoba čiji se podaci, na temelju propisa, prikupljaju, bilježe i obrađuju kod Poslodavca. Kao podaci, podrazumijevaju se i ostali podaci ubilježeni kod Poslodavca, kao što su osobni podaci o radnicima, o imovini, podaci proizašli iz poslovnih procesa Poslodavca i slično.
6. ***Osobni podatak*** je, 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, posebno na osnovi identifikacijskog broja ili nekog drugog obilježja specifičnog za njezin fizički, psihološki, mentalni, gospodarski, kulturni ili socijalni identitet.
7. ***Zbirke osobnih podataka*** su evidencije koje Poslodavac vodi na temelju zakona i drugih propisa.
8. ***Povjerljivim podacima*** smatraju se osobni podaci radnika, korisnika usluga vodoopskrbe i odvodnje, te poslovnih partnera čije bi neovlašteno otkrivanje moglo štetiti interesu osobe na koju se podaci odnose ili članovima njene obitelji. Povjerljivim podacima Poslodavca smatraju se i svi drugi osobni podaci u zbirkama podataka koje Poslodavac tijekom poslovanja vodi na osnovi zakonskih propisa, sva dokumentacija koja sadrži osobne podatke te pisana i usmena priopćenja ili informacije koje sadrže osobne podatke.
9. ***Dokumentacija*** podrazumijeva svu dokumentaciju koja je dio informacijskog sustava Poslodavca, neovisno o tome je li zaprimljena ili je nastala kod Poslodavca.
10. ***Poslužitelj*** je namjensko računalo na mreži koje pruža različite podatke drugim računalima (klijentima).

II. MJERE ZAŠTITE I SIGURNOSTI INFORMATIČKOG SUSTAVA

Članak 3.

Za informatičku sigurnost i za mjere zaštite informatičkog sustava Poslodavca, kao i za funkcioniranje sustava zaštite povjerljivosti podataka brine se unutar svog djelokruga Informatička služba.

2.1. Opće mjere zaštite

Članak 4.

Poslodavac provodi sljedeće opće mjere zaštite utvrđene zakonom, drugim propisima i općim aktima:

- mjere fizičke i tehničke zaštite imovine i osoba, mjere zaštite od požara
- organizacijske mjere za osiguranje ažurnosti, točnosti i pravilnosti obavljanja poslova, sprječavanje neovlaštene izmjene dokumentacije i podataka, neovlaštenog korištenja informatičke opreme i mreže, radne postupke utvrđene uputama i standardima Poslodavca, te mjere provođenja nadzora i kontrole
- mjere za održavanje informatičkog sustava u funkciji koje se poduzimaju radi sprječavanja opasnosti od zastoja u radu cjelokupne ili dijela informatičke opreme, odnosno sve aktivnosti i postupci kojima se osiguravaju tehnički i drugi uvjeti za rad, uključujući preventivne mjere i redovito održavanje informatičkog sustava.

2.2. Posebne mjere zaštite

2.2.1. Fizička sigurnost

Članak 5.

Prostorije pod posebnom zaštitom u Poslodavca su:

- prostorije u kojima je smješteno središnje računalo s pripadajućom informatičkom i komunikacijskom opremom (sistem sala) i prostorije, kao i ormari u kojima su smješteni poslužitelji te pripadajuća informatička i komunikacijska oprema

- prostorije i ormari u kojima su arhivirane sigurnosne kopije podataka te sistemske i aplikativne programske podrške (software-a).

Članak 6.

Mjere zaštite prostorija utvrđene člankom 5. ovoga Pravilnika su sljedeće:

- ulazak u prostorije dopušta se samo osobama koje su zaposlene u tim prostorijama i osobama koje imaju ovlaštenje za ulazak u te prostorije
- vanjski, ugovorni suradnici Poslodavca, ovlašteni za ulazak u prostorije pod posebnom zaštitom, mogu ući i boraviti u navedenim prostorijama samo u nazočnosti nadležnog radnika Poslodavca
- obvezna nazočnost radnika u tim prostorijama odnosno zaključavanje prostorije u slučaju nenazočnosti radnika u prostorijama i pri odlasku s posla te predaja ključa zaštitarskoj službi
- obvezno zaključavanje ormara s informatičkom i komunikacijskom opremom, bez obzira na to nalaze li se u prostorijama ili na hodnicima, ukoliko se ne nalaze u sistem sali
- zabrana iznošenja dokumentacije, informatičke opreme i nositelja podataka iz prostorije bez dopuštenja odgovorne osobe (uz obvezno vođenje evidencije), osim ako je to utvrđeno standardnim poslovnim procesom
- poimenično određivanje osoba odgovornih za održavanje odgovarajućih tehničkih uvjeta, čistoće i reda u prostoriji
- u prostorijama je zabranjeno audio i video snimanje
- instaliranje odgovarajuće opreme za protupožarnu zaštitu što obuhvaća i automatski sustav za gašenje i vatrodojavu u prostorijama iz članka 5., točka 1.
- druge mjere fizičke ili tehničke zaštite koje u posebnim slučajevima određuje rukovoditelj organizacijske cjeline.

Članak 7.

(1) Radi provedbe mjera iz članka 6. ovog Pravilnika Informatička služba obvezno vodi popis svih radnika zaposlenih u njihovim prostorijama pod posebnom zaštitom, kao i osoba koje imaju ovlaštenje za ulazak u te prostorije, neovisno o tome jesu li radnici ili vanjski suradnici Poslodavca.

(2) Mjere iz članka 6. ovog Pravilnika neposredno provode radnici koji rade u tim prostorijama, osoba odgovorna za zaštitu osobnih podataka, a za nadzor nad provedbom tih mjera odgovoran je rukovoditelj Informatičke službe.

Članak 8.

Mjere zaštite za osiguranje točnosti ulaznih podataka u informatiziranim poslovnim procesima su sljedeće:

- podatke unosi isključivo ovlašteni radnik
- obveznu kontrolu unosa obavlja ovlašteni radnik (kontrola podataka i dokumentacije na osnovi koje se podaci unose)
- aplikativna i sustavna zaštita (formalne i logičke kontrole, kontrolne svote, verifikacija unosa, dvostruki unos i slično)
- obvezno testiranje programa
- obvezna provjera izlazne dokumentacije.

Članak 9.

(1) Mjere kontrole za pristup podacima u informatiziranim poslovnim procesima su sljedeće:

- pristup podacima dopušten je samo ovlaštenim radnicima u skladu s ovlaštenjima koja proizlaze iz pristupne lozinke
- programirano je praćenje i evidentiranje određenih aktivnosti na informatičkoj opremi odnosno računalno-komunikacijskoj mreži
- radnik smije koristiti samo svoju lozinku za pristup informatičkom sustavu Poslodavca
- radnik mora osigurati tajnost svoje lozinke
- pri dužem izbivanju s radnog mjesta kao i pri odlasku s posla radnik se mora obvezno odjaviti iz programa i sustava koje koristi
- pri odlasku s posla radnik mora obvezno isključiti informatičku opremu.

(2) Za provedbu mjera iz točke 1. do 2. stavka 1.ovoga članka odgovorna je Informatička služba, a za mjere iz točke 3. do 6. odgovorni su radnici Poslodavca.

2.2.2. Ovlaštenje za pristup podacima

Članak 10.

(1) Ovlaštenja za pristup, unos, kontrolu i opseg dostupnosti podataka rukovoditelji dodjeljuju radnicima, ovisno o njihovom radnom mjestu odnosno poslovima koje obavljaju, a dodjeljuje ih Informatička služba.

(2) Radnik koji svoju lozinku da na korištenje neovlaštenoj osobi, u slučaju zlouporabe odgovara zbog povrede radne obveze sukladno Pravilniku o radu Poslodavca i odgovoran je za nastalu štetu.

(3) Radnik koji je namjerno ili krajnjom nepažnjom unio ili dao pogrešne podatke ili je koristio tuđi pristup programu odgovara zbog teže povrede radne obveze sukladno Pravilniku o radu Poslodavca.

2.2.3. Sigurnost informatičkog sustava i opreme

Članak 11.

(1) Poslodavac obvezno primjenjuju mjere za zaštitu cjelovitosti programske podrške (software-a), podataka i informacija kojima se sprječava, otkriva i oporavlja od računalnih virusa i drugih štetnih programa i štiti informatička mreža od neovlaštenog pristupa.

(2) Za određivanje i provedbu mjera iz prethodnog stavka odgovorna je Informatička služba.

(3) Ozbiljniji sigurnosni incidenti i poduzete aktivnosti obvezno se dokumentiraju radi sprječavanja budućih i poduzimanja eventualnih dodatnih mjera zaštite.

Članak 12.

(1) Radi zaštite informatičkog sustava, pri radu se smije koristiti samo programska podrška (software) koji je Poslodavac sam razvio, odgovarajući licencirani i provjereni programi ili programi koje je razvio vanjski ugovorni partner uz nadzor ovlaštenih osoba u Informatičkoj službi.

(2) Nove programe ili nove inačice programa mogu instalirati samo ovlaštene osobe zaposlene u Informatičkoj službi ili uz njihov nadzor.

Članak 13.

Mjere aplikativne i sustavne zaštite podataka i programa unutar informatičkog sustava Poslodavca temelje se na sljedećim načelima:

- dodavanje, brisanje i izmjena programa i podataka u informatičkom sustavu može se izvoditi samo na temelju pisanog naloga ovlaštenog rukovoditelja
- sustavni i aplikativni programi koji bi, u slučaju oštećenja ili drugog načina prestanka rada, mogli narušiti cjelovitost sustava, moraju se pohraniti u posebnim, zaštićenim bibliotekama i zaštititi od neovlaštenog korištenja
- pristup podacima treba omogućiti samo ovlaštenim radnicima one organizacijske cjeline Poslodavca u čiji djelokrug spadaju ti podaci, odnosno drugim ovlaštenim radnicima
- obvezno evidentiranje rada ovlaštenih radnika u sustavu.

Članak 14.

(1) Za ispravno funkcioniranje informatičkog sustava i tehničko održavanje informatičke opreme u funkciji te sprječavanje opasnosti od nastupa dugotrajnijeg zastoja u radu odgovoran je rukovoditelj Informatičke službe.

(2) Rukovoditelji ostalih organizacijskih cjelina u kojima je smještena informatička oprema u slučaju zastoja ili problema u radu informatičke opreme, isti su dužne zastoj ili kvar prijaviti Informatičkoj službi.

Članak 15.

(1) Mjerama zaštite osigurava se redovito održavanje informatičke opreme u funkciji, odnosno njezina djelotvorna zamjena u slučaju zastoja u radu.

(2) Mjere zaštite su:

- donošenje plana za slučaj dugotrajnijeg zastoja u radu informatičkog sustava
- utvrđivanje i provedba standarda u radu i održavanju informatičke i pripadajuće opreme, a provodi ih Informatička služba.

Članak 16.

(1) Smatrat će se da je došlo do dugotrajnijeg zastoja u radu informatičkog sustava ako ključni dijelovi kao što su poslužitelji i računalno-komunikacijski sustav Poslodavca na

kojima se nalazi dokumentacija potrebna za rad, zbog kvara ili drugog uzroka, nisu raspoloživi u vremenu za koje se može ocijeniti da će prouzročiti značajnije poremećaje u radu.

(2) Ocjenu da se radi o dugotrajnijem zastoju sustava donosi Uprava, na prijedlog rukovoditelja Informatičke službe.

Članak 17.

(1) U slučaju izvanrednih okolnosti i dugotrajnijeg zastoja u radu informatičkog sustava postupa se prema planu koji donosi Uprava.

(2) Plan obvezno sadrži:

- unaprijed pripremljene pričuvne lokacije na kojima će Poslodavac obavljati pojedine poslove
- prioritete poslovnih aktivnosti koje će se odvijati na pričuvnim lokaciji
- prioritete obrade podataka koje se mogu obavljati na pričuvnom sustavu
- točan redoslijed ponovnog uspostavljanja poslovnih aktivnosti

2.2.4. Korištenje službenih mobilnih uređaja

Članak 18.

(1) Radnici koji zbog potreba posla ostvaruju pravo na korištenje službenih mobilnih uređaja, dužni su sukladno radnim uputama, voditi brigu o uređaju koji je vlasništvo Poslodavca, kao i snositi troškove prometa veće od dopuštenih.

(2) Radnici iz stavka 1. ovog članka dužni su potpisati izjavu o korištenju mobilnog uređaja u kojoj će biti utvrđena dodijeljena visina tarife i dopušteni iznos prekoračenja prometa izvan tarife.

(3) Troškove koji prelaze granicu dopuštenih troškova iz stavka 2. ovog članka, operater će naplatiti radniku sukladno tehničkoj specifikaciji mjesečnog računa prometa.

(4) Poslodavac može priznati dio troškova koji prelaze dodijeljenu visinu tarife, a odnosili su se na službene troškove, na temelju ispisa razgovora u minutama, porukama i potrošnji interneta koji će se uz suglasnost radnika zatražiti od operatera.

2.2.5. Sigurnost razmjene podataka u poslovnoj suradnji

Članak 19.

(1) U suradnji s fizičkim i pravnim osobama, državnim i drugim tijelima i ustanovama u Republici Hrvatskoj, Poslodavac će utvrditi moguće rizike za informatičku sigurnost te poduzimati mjere zaštite za uklanjanje ili smanjivanje rizika.

(2) U suradnji koja se očituje u davanju na korištenje ili razmjeni osobnih podataka, primjenjuju se propisi o zaštiti osobnih podataka, osim ako posebnim zakonom nije drukčije određeno.

Članak 20.

(1) Mjere zaštite informatičkog sustava i povjerljivosti prenesenih podataka Poslodavac će utvrditi sporazumom o povjerljivosti podataka, uz specificiranje sigurnosnih zahtjeva za pristup i postupanje s povjerljivim i drugim podacima.

(2) U slučaju da se poslovnim sporazumima za razvoj, izradu ili instaliranje programa, ugovornim partnerima osigura dostupnost osobnih podataka, Informatička služba i rukovoditelj organizacijske cjeline koji je odgovoran za prijenos podataka, izradit će procjenu rizika za podatke koji se prenose, a dostupnost podataka osigurat će se tek nakon potpisivanja Sporazuma o povjerljivosti podataka, o čemu će se pravovremeno obavijestiti Službenik za zaštitu osobnih podataka.

Članak 21.

Prije sklapanja sporazuma o povjerljivosti podataka iz članka 19. ovog Pravilnika, na temelju kojeg bi pravna ili fizička osoba imala pristup povjerljivim podacima Poslodavca, potrebno je provesti i provjeru druge ugovorne strane koja obuhvaća utvrđivanje je li ta pravna ili fizička osoba registrirana za obavljanje potrebne djelatnosti, osigurava li dovoljno jamstava da će poduzeti odgovarajuće mjere zaštite osobnih i drugih povjerljivih podataka Poslodavca sukladno Pravilniku o zaštiti osobnih podataka i ovom Pravilniku.

Članak 22.

(1) Osoba odgovorna za praćenje izvršenja sporazuma i rukovoditelj organizacijske cjeline iz čijeg su djelokruga rada podaci, poduzimaju sve mjere za zaštitu podataka tijekom izvršavanja ugovora o poslovnoj suradnji uključujući i nadzor nad izvršenjem i kontrolu mjera zaštite podataka odnosno informacijskog sustava koje provodi druga ugovorna strana.

(2) U slučaju kada je za sklapanje ugovora o poslovnoj suradnji prethodno nužno omogućiti pristup podacima, obvezno se sklapa sporazum o povjerljivosti kojim se druga strana obvezuje na poštivanje ili osiguravanje mjera zaštite informatičkog sustava, a pristup informatičkom sustavu Poslodavca ne može se omogućiti prije početka važenja sporazuma o povjerljivosti.

III. PRAVILA KORIŠTENJA RAČUNALNO – KOMUNIKACIJSKOG SUSTAVA I ZAŠTITA NADZOROM PRIKUPLJENIH OSOBNIH PODATAKA

3.1. Uvjeti korištenja službenog informatičkog sustava, interneta i elektroničke pošte

Članak 23.

(1) Informatički sustav i usluge dostupne putem tog sustava, a osobito internet i elektronička pošta, moraju se koristiti za obavljanje poslova Poslodavca.

(2) Radnik koji zlorabi informatički sustav ili usluge Poslodavca iz stavka 1. ovoga članka odgovara zbog povrede radne obveze sukladno Pravilniku o radu.

Članak 24.

(1) Pod zlouporabom se podrazumijeva:

- pristup, prijenos ili učitavanje podataka i instaliranje programa koji sigurnosno mogu ugroziti integritet mreže Poslodavca
- instaliranje nelicenciranih programa
- pristup, prijenos ili učitavanje sadržaja diskriminirajuće, uznemiravajuće, ponižavajuće ili druge neprimjerene prirode koji su kao takvi utvrđeni posebnim propisima
- korištenje mreže i komunikacijskih alata u privatne komercijalne svrhe

(2) Usluge iz stavka 1. ovog članka kontrolira i nadzire Informatička služba.

(3) Poslodavac ima pravo uvida i nadzora u sadržaj svih službenih računala o čemu Odluku donosi Uprava na prijedlog Informatičke službe, a za provedbu istih odgovorna je Informatička služba.

Članak 25.

(1) Podatke u informatičkom sustavu Poslodavca mogu dodavati, brisati ili mijenjati samo osobe ovlaštene od strane Poslodavca.

(2) Ovlašteni radnici, odnosno ovlašteni korisnici računa su osobe koje sustav može identificirati na osnovi korisničkog imena i lozinke.

3.2. Svrha nadzora službene elektroničke pošte

Članak 26.

(1) Svrha nadzora službene elektroničke pošte je zaštita opravdanih interesa Poslodavca koji se tiču zaštite ugleda, opreme, programskog sustava, zaštite i osiguranja baze poslovnih podataka od uništenja, zaštita od prijenosa poslovnih informacija trećim osobama, te zaštite od zlouporabe radnog vremena u privatne svrhe.

(2) Korisnicima je zabranjeno putem službene elektronične pošte slanje poruka nedoličnog, lažnog ili uvredljivog sadržaja.

(3) Poslodavac može isključivo u slučaju nužne i opravdane potrebe odnosno u slučaj sumnje na povredu, izvršiti uvid u elektroničku poštu o čemu Odluku donosi Uprava, a o čemu će treća strana biti pravovremeno obaviještena.

3.3. Transparentnost nadzora

Članak 27.

(1) Poslodavac će sve zaposlene radnike kao i nove radnike kao korisnike prilikom zapošljavanja na jasan i transparentan način ovim Pravilnikom upoznati s mogućnošću i svrhom nadzora, specifičnim razlozima, okolnostima i načinu na koji će se nadzor provoditi, podacima koji se prikupljaju nadzorom kao i mogućnošću uvida u nadzirane podatke na zahtjev radnika.

(2) Neposredno prije samog nadzora korisnik će biti upoznat o tome tko i kada će provoditi nadzor, o opsegu nadzora kao i o konkretnoj svrsi nadzora, prikupljeni podaci neće se prenositi trećim osobama izvan legitimne svrhe prikupljanja, a brisat će se ispunjenjem svrhe prikupljanja.

Članak 28.

Radi potpune informacije o nadzoru i prikupljanju podataka kroz nadzor, Poslodavac će ovaj Pravilnik učiniti dostupnim na oglasnoj ploči Društva, središnjoj bazi uputa i akata kao i na web stranici Društva.

3.4. Nužnost nadzora

Članak 29.

Opseg nadzora elektroničke pošte ograničen je na elektronsku poštu za koju se sumnja da je njome povrijeđena svrha nadzora, a uvid će se izvršiti u promet podataka korisnika i vrijeme komunikacije, dok će u slučaju iznimne potrebe uvida u sadržaj komunikacije (povreda radnih obveza, sigurnosni incidenti, odavanje poslovnih informacija, sumnja na diskriminaciju radnika) Poslodavac zaštititi privatnost i dostojanstvo korisnika i trećih osoba.

3.5. Pohranjivanje, povjerljivost i zaštita podataka

Članak 30.

(1) Zapis elektronske pošte nakon preuzimanja s poslužitelja pohranjuje se isključivo na službeno računalo ili službeni telefon radnika, a zadržavanje zapisa, brisanje ili čuvanje ovisi o potrebama radnika.

(2) Nadzor nad prikupljanjem, obradom i distribucijom podataka obavljat će Nadzornik kao ovlaštena osoba Poslodavca, na temelju unaprijed postavljenog zahtjeva na propisanom obrascu uz naznaku svrhe i uz prethodno odobrenje Službenika za zaštitu osobnih podataka, a podatke koje sazna u obavljanju dužnosti obvezni su čuvati sukladno izjavi o povjerljivosti podataka.

IV. EVIDENCIJE KOJE SE VODE U INFORMATIČKOJ SLUŽBI

Članak 31.

U Informatičkoj službi Poslodavca vode se sljedeće evidencije:

1. Evidencija o dodijeljenim ovlaštenjima
2. Evidencija informatičke opreme i pripadajućih programskih podrški (software-a) instaliranih kod Poslodavca
3. Evidencija o obradi osobnih podataka prikupljenih nadzorom sadržaja službenog računala i elektroničke pošte

Članak 32.

(1) Obvezno se vodi Evidencija o dodijeljenim ovlaštenjima i svim izmjenama u ovlaštenjima koja sadrži najmanje sljedeće podatke:

- korisničko ime (userid)
- datum promjene ovlaštenja
- projekt ID
- naziv forme
- skup podataka
- ime i prezime radnika koji je dao ovlaštenje

(2) Informatička služba vodi i Evidenciju informatičke opreme i pripadajućih programskih podrški (software-a) instaliranih kod Poslodavca, koja sadrži sljedeće podatke:

- ime i prezime radnika
- inventurni broj
- naziv opreme
- vrsta opreme
- datum zaduženja
- instalirani programi (ukoliko su vezani za opremu)

(3) Evidencija o obradi osobnih podataka prikupljenih nadzorom službenog računala i elektroničke pošte sadrži slijedeće podatke:

- ime i prezime radnika
- ime i prezime treće osobe
- elektronska adresa treće osobe
- točno vrijeme i datum slanja i primitka e-pošte
- poslodavac
- razmjenjivani sadržaji (prikuplja se samo ukoliko je to u određenom slučaju nužno)

V. ZAŠTITA PRIVATNOSTI I POVJERLJIVOSTI PODATAKA I ROKOVI ČUVANJA

Članak 33.

(1) Zaštita privatnosti i povjerljivosti podataka uređena je Pravilnikom o zaštiti osobnih podataka VODOVOD-OSIJEK d.o.o.

(2) Podaci na poslužiteljima od posebne važnosti kao i podaci o aktivnostima korištenja programa, čuvaju se najmanje jedanaest godina nakon prestanka produkcije pojedinog projekta, odnosno dulje, ako je tako utvrđeno općim aktom o zaštiti arhivskog i registraturnog gradiva.

(3) Podaci iz stavka 2. ovog članka obvezno se pohranjuju i na odgovarajućim sistemskim i aplikativnim programima, kao i eventualno potrebna oprema za učitavanje odnosno pristup podacima ili se podaci pravodobno snimaju na novije nositelje podataka.

VI. ZAVRŠNE ODREDBE

Članak 34.

(1) Radnici čiji se podaci prikupljaju upoznat će se sa sadržajem Pravilnika o zaštiti osobnih podataka VODOVOD-OSIJEK d.o.o. i ovog Pravilnika putem oglasne ploče Društva i na web stranici Poslodavca.

(2) Prava ispitanika koja nisu regulirana ovim Pravilnikom, biti će regulirana Pravilnikom o zaštiti osobnih podataka VODOVOD-OSIJEK d.o.o.

Članak 35.

Ovaj Pravilnik donesen je uz suodlučivanje Radničkog vijeća i smatra se dijelom Pravilnika o radu.

Članak 36.

Ovaj Pravilnik o zaštiti osobnih podataka stupa na snagu u roku od osam dana od njegove objave na oglasnoj ploči Društva i web stranici www.vodovod.com.

U Osijeku, 24. 05. 2018. godine

VODOVOD-OSIJEK d.o.o.
član Uprave - direktor
mr. sc. Ivan Jukić, dipl. oec.

VODOVOD - OSIJEK
d.o.o. OSIJEK 7E