Zavod za javno zdravstvo Zadar., kao Voditelj obrade, sukladno odredbama Uredbe (EU) 2016/679 Europskog parlamenta i vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (Opća uredba o zaštiti podataka) i Zakona o provedbi Opće uredbe o zaštiti podataka (NN 42/2018) i članka 24. Statuta, dana 25. svibnja 2018. godine donosi i objavljuje sljedeći

PRAVILNIK O SIGURNOSTI OSOBNIH PODATAKA

Članak 1.

Uvodne odredbe

Ovim Pravilnikom se utvrđuje djelotvoran, odgovoran i transparentan okvir za osiguravanje usklađenosti s Općom uredbom o zaštiti osobnih podataka.

Ovaj Pravilnik primjenjuje se na sve organizacijske dijelove Zavoda za javno zdravstvo Zadar (u daljnjem tekstu VODITELJ OBRADE) te na sve zaposlenike, uključujući honorarne djelatnike i privremene radnike jednako kao i na sve vanjske suradnike koji djeluju u ime voditelja obrade, te pacijente Zavoda.

Članak 2.

Opseg i ciljevi

(1) Ovim Pravilnikom o zaštiti osobnih podatka (u daljnjem tekstu: Pravilnik) uređuju se temeljne obveze i prava onih koji u ime Voditelja obrade provode obradu osobnih podataka ispitanika.

(2) Cilj ovog Pravilnika je:

* definiranim pravilima i procedurama zaštiti privatnost ispitanika i njihove osobne podatke, između ostalog, od slučajnog ili nezakonitog uništenja, gubitka, izmjene, neovlaštenog otkrivanja ili pristupa osobnim podacima te

* osigurati usklađenost poslovanja Voditelja obrade sa zahtjevima Opće uredbe o zaštiti podataka i Zakona o provedbi Opće uredbe o zaštiti podataka.

(3) Ovaj se Pravilnik primjenjuje na sve koji obradu osobnih podataka ispitanika, u ime Voditelja obrade, provode izvršavajući svoje obveze temeljem Ugovora o radu, koji se kod Voditelja obrade nalaze na stručnom osposobljavanju za rad bez zasnivanja radnog odnosa odnosno posao za Voditelja obrade obavljaju temeljem Ugovora o djelu (studenti i dr.), Autorskog ugovora ili drugog pravnog posla, trajno ili povremeno, kao i na članove Uprave i drugih tijela Voditelja obrade (u daljnjem tekstu: zaposlenici).

Članak 3.

Osobni podaci koje prikupljamo

1. Osobni podaci zaposlenika Voditelja obrade

Voditelj obrade, između ostalih, obrađuje sljedeće osobne podatke svojih zaposlenika:
ime i prezime,
* ime i prezime roditelja,
* mjesto rođenja,
* županija rođenja,
* država rođenja,
* jedinstveni matični broj građana,
* osobni identifikacijski broj,
* datum rođenja,
* spol,
* adresa prebivališta/boravišta,
* državljanstvo,
* broj telefona,
* broj mobilnog telefona,
* adresa elektronske pošte
* korisničko ime i lozinka (username i password),
* fotografija,
* obrazovanje (struka/završena škola ili fakultet, grad škole, fakulteta),
* trajanje ranijeg školovanja,
* naziv, broj i datum isprave kojom se dokazuje završeno obrazovanje,
* zanimanje,
* stupanj obrazovanja (stručna sprema),
* akademski stupanj,
* titula,
* godine radnog iskustva (staž)
* staž
* datum zapošljavanja.,
* radni status,
* naziv i opis radnog mjesta,
* odjel zaposlenja,
* vrsta ugovora o radu,
* tip zapošljavanja,
* satnica,
* način prestanka ugovora o radu,
* smjenski rad,
* popis projekata,
* institucija/tvrtka,
* plaća (bruto i neto)
* honorar,
* osobni odbitak,
* trošak prijevoza,
* način isplate,
* broj bankovnog računa/IBAN,
*rezultati natječaja za zapošljavanje,
*podaci iz rodnog lista, izjave o nekažnjavanju, osobne iskaznice, iskaznice tekućeg računa, domovnice, poreznog kartona, dokaza o završnom ispitu

Osobne podatke koje se stavljaju na raspolaganje prilikom obavljanja djelatnosti i to:

a) **SLUŽBE ZA EPIDEMOLOGIJU** – ime, prezime, ime oca, datum rođenja, mjesto rođenja, OIB, MBO, adresa prebivališta, za stranca – privremena adresa (smještaj – hotel ili privatni smještaj), radno mjesto, zanimanje, poslodavac (naziv, adresa, telefon/mobitel, fax, OIB), datum oboljenja, dijagnoza, opis rane, uzročnik, cjepni status (datum cijepljenja), datum prijave zarazne bolesti, datum ozljede, liječnik prijavitelj, broj telefona/mobitela ozlijeđenoga, ime i prezime, adresa te broj telefona/mobitela vlasnika životinje, titar protutijela, naziv i adresa objekta, uzorak (stolica, celofan, bris grla, nosa), brisevi/otisci na čistoću, datum otkrivanja kliconoštva/parazitonoštva, bilo koji drugi podatak koji može biti revelantan za obradu epidemije, datum, sat i mjesto uboda.

b) **SLUŽBE ZA MIKROBIOLOGIJU I PARAZITOLOGIJU** – ime, prezime, datum rođenja, JMBG, OIB, MBO, broj police dopunskog osiguranja, radno mjesto, poslodavac, dijagnoza, liječnik koji je uputio pacijenta, rezultat mikrobiološke analize, rezultat antibiograma.

c) **SLUŽBE ZA MENTALNO ZDRAVLJE I PREVENCIJU OVISNOSTI** – ime, prezime, spol, dob, datum rođenja, OIB, JMBG, MBO, kontakt telefon, adresa prebivališta, zanimanje, povijest liječenja, sociodemografski podaci, zlouporaba, rizično ponašanje, početni ishod liječenja, obiteljski podaci, sudski problemi, protekli tijek bolesti, zdravstveni problemi, dijagnoza.

d) **SLUŽBE ZA JAVNO ZDRAVSTVO** – ime i prezime, spol, dob, datum rođenja, mjesto rođenja, bračno stanje, radni status, OIB, MBO, JMBG, zamjenski identifikator, školska sprema, narodnost, broj zamjenskog identifikatora, platitelj, adresa prebivališta, šifra naselja prebivališta, šifra države, radni status, telefonski broj, šifra zanimanja, zanimanje – posao koji obavlja ili je obavljao prije umirovljenja, djelatnost, šifra djelatnosti, datum primitka i otpusta iz ustanove, glavna dijagnoza pri otpustu iz ustanove sa šifrom prema MKB-10, dodatne dijagnoze pri otpustu iz ustanove sa šifrom prema MKB-10, prijašnji pobačaji i porodi, antenatalni pregledi; vrijeme prvog antenatalnog pregleda u trudnoći, podaci o porodu, podaci o boravku u ustanovi, anamnestički podaci i status (prethodni podaci, trudnoće, prekidi…), vrsta sadašnjeg pobačaja, komplikacije i ishod, trudnoća nastala umjetnom oplodnjom, probir na malformacije, razlog namjernog pobačaja, podaci o novorođenčetu/novorođenčadi, podaci o uzroku smrti djeteta, vanjski uzrok ozljede za glavnu i za dodatne dijagnoze, osnovni uzrok smrti u slučaju smrtnog ishoda, obilježja nasilne smrti, vanjski uzrok ozljede u slučaju smrtnog ishoda, način otpusta, broj povijesti bolesti, šifre postupaka tijekom hospitalizacije, šifra liječnika otpusne djelatnosti, je li prije otkriven neki drugi primarni malignom, datum utvrđivanja sadašnjeg malignoma, dijagnostika i šifra anatomske lokalizacije maligne neoplazme, histološki tip i klinički stadij, terapija, je li maligna neoplazma registrirana u vezi sa skriningom Nacionalnog programa i podaci o smrti, naziv specijalizacije/stručne spreme, adresa ordinacije/djelatnosti.

e) **SLUŽBE ZA ŠKOLSKU I ADOLESCENTNU MEDICINU** – ime i prezime djeteta, datum i mjesto rođenja djeteta, OIB djeteta, MBO djeteta, ime i prezime roditelja/staratelja, godina rođenja roditelja/staratelja, stručna sprema, zanimanje, zdravstveni problemi, pušački status, zaposlenje, bračni status, uvjeti stanovanja, adresa prebivališta, ime i prezime izabranog pedijatra/liječnika obiteljske medicine, podaci o trudnoći i porodu, zdravstveno stanje djeteta (dosadašnje preboljene bolesti), nalaz pregleda djeteta, cjepni status djeteta, povijest bolesti djeteta, uputna dijagnoza djeteta.

f) **SLUŽBE ZA ZDRAVSTVENU EKOLOGIJU I ZAŠTITU OKOLIŠA** – ime i prezime, adresa prebivališta, e-mail adresa, broj telefona/mobitela, OIB, naziv objekta, adresa objekta, IBAN broj

g) **SLUŽBE ZA ZAJEDNIČKE POSLOVE** – ime i prezime, adresa prebivališta, IBAN broj, IP adresa, posjeti web stranici, podaci sa društvenih mreža i slični podaci u vezi korištenja Internet pretraživača.

Članak 4.

Svrha prikupljanja osobnih podataka i pravna osnova obrade

Zavod određuje svrhu i sredstva obrade osobnih podataka te se u tom smislu smatra voditeljem obrade osobnih podataka. Osnovna svrha prikupljanja osobnih podataka je zakonska obveza i/ili sklapanje te izvršavanje ugovora, ili kako bi se poduzele radnje na zahtjev prije i tijekom ugovora. Pritom opseg osobnih podataka koji se prikupljaju ovisi o vrsti djelatnosti i/ili usluge. Radnje na zahtjev prije sklapanja ugovora podrazumijevaju provjeru zahtjeva i potreba, prema potrebi provjeru primjerenosti ili prikladnosti usluga posebnim okolnostima i potrebama. Ako ugovorna strana već osoba koja ostvaruje pravo iz ugovora, svrha prikupljanja Vaših osobnih podataka je ispunjenje obveze Zavoda koja proizlazi iz sklopljenog ugovora ili je prikupljanje osobnih podataka potrebno kako bi se ugovor sklopio ili identificirali korisnici usluge. U ovom slučaju opseg osobnih podataka koje prikupljamo ovisi o vrsti postavljenog zahtjeva, djelatnosti te informacijama koje će biti potrebne kako bi se zahtjev ispunio.

Osobni podaci navedeni pod **a)** prikupljaju se i obrađuju u svrhu: sanitarnih pregleda, prijave zaraznih bolesti, neobveznih cijepljenja, antirabične obrade, distribucije cjepiva, cijepljenja prema kalendaru obveznih cijepljenja, obrade kliconoša, kontakata oboljelih i sl., obrade epidemija i epidemijskih događaja, obrade ubodnih incidenata, provođenja tečaja zdravstvenog odgoja (hig. Minimuma), ispitivanja vode za potrebe tehničkog pregleda objekta, temeljem zakonske obveze Zakona o zdravstvenoj zaštiti, Zakona o obveznom zdravstvenom osiguranju, Zakona o zaštiti pučanstva od zaraznih bolesti, Pravilniku o načinu provođenja imunizacije, seroprofilakse, kemoprofilakse protiv zaraznih bolesti te o osobama koje se podvrgavaju toj obvezi, Provedbenog programa obveznog cijepljenja u RH, Zakonu o vodi za ljudsku potrošnju, Ugovora s HZZO-om, Plana i programa mjera iz obveznog zdravstvenog osiguranja.

Osobni podaci navedeni pod **b)** prikupljaju se i obrađuju u svrhu: provođenja dijagnostičkih postupaka za upućene pacijente, obrade uzoraka na kliconoštvo i parazitonoštvo, analitičkih izvješća traženih od drugih Službi Zavoda ili Odjela, slanja uzoraka u druge ustanove na pretrage koje se ovdje ne izvode – dodatne analize i testiranja (identifikacija, serotipizacija, određivanje mehanizma rezistencije, potvrda rezistencije, određivanje osjetljivosti na antimikotike itd.), sakupljanja značajnih izolata (izolati iz hemokultura i likvora) bolničkih pacijenata i slanja u suradne ustanove, temeljem zakonske obveze Zakona o zdravstvenoj zaštiti, Zakona o obveznom zdravstvenom osiguranju, Zakona o zaštiti pučanstva od zaraznih bolesti, Ugovora s HZZO-om, Plana i programa mjera iz obveznog zdravstvenog osiguranja.

Osobni podaci navedeni pod **c)** prikupljaju se i obrađuju u svrhu: praćenja registra ovisnika o psihoaktivnim drogama, praćenja osoba s poteškoćama mentalnog zdravlja u Odjelu za mentalno zdravlje, praćenja osoba upućenih u Odjel za mentalno zdravlje prema rješenjima Centra za socijalnu skrb, praćenja osoba upućenih u Odjel za mentalno zdravlje prema rješenjima Suda, Općinskog državnog odvjetništva, praćenja osoba upućenih u Odjel za mentalno zdravlje prema rješenjima Probacijskog ureda, temeljem zakonske obveze Zakona o zdravstvenoj zaštiti, Zakona o obveznom zdravstvenom osiguranju, Ugovora s HZZO-om, Plana i programa mjera iz obveznog zdravstvenog osiguranja, Zakona o suzbijanju zlouporabe droga, Obiteljskog zakona, Kaznenog zakona, Zakona o probaciji.

Osobni podaci navedeni pod **d)** prikupljaju se i obrađuju u svrhu: praćenja podataka o hospitalizacijama radi liječenja i rehabilitacije u stacionarnim zdravstvenim ustanovama u Zadarskoj županiji, praćenja podataka o porodima za žene koje su rodile u zdravstvenim ustanovama Zadarske županije, praćenja podataka o perinatalnoj smrti za djecu rođenu u stacionarnim zdravstvenim ustanovama u Zadarskoj županiji, praćenja podataka o prekidima trudnoće (pobačaj) u stacionarnim zdravstvenim ustanovama u Zadarskoj županiji, praćenje podataka o osobama liječenim zbog maligne bolesti, praćenja podataka o incidenciji maligne bolesti iz primarne zdravstvene zaštite u Zadarskoj županiji, praćenje podataka o patohistološkim i citološkim nalazima osoba koje su hospitalizirane u stacionarnoj zdravstvenoj ustanovi zbog

novotvorina, nadopune podataka na kopijama prijava smrti DEM 2 na traženje HZJZ, praćenja Nacionalnog programa ranog otkrivanja raka dojke, praćenja Nacionalnog programa ranog otkrivanja raka vrata maternice, praćenja Nacionalnog programa ranog otkrivanja raka debelog crijeva, praćenje agregiranih podataka iz godišnjih izvješća o radu iz PZZ i SKZ o: zdravstvenim djelatnicima, praćenje rada, praćenje utvrđenih bolesti i stanja u PZZ i SKZ, temeljem zakonske obveze Zakona o zdravstvenoj zaštiti, Zakona o obveznom zdravstvenom osiguranju, Ugovora s HZZO-om, Plana i programa mjera iz obveznog zdravstvenog osiguranja, Zakona o službenoj statistici, Programa statističkih aktivnosti RH, Godišnjeg provedbenog plana statističkih aktivnosti RH, Nacionalnih programa ranog otkrivanja raka Ministarstva zdravstva RH.

Osobni podaci navedeni pod **e)** prikupljaju se i obrađuju u svrhu: sistematskih pregleda prilikom upisa u prvi razred osnovne škole, u petom i osmom razredu OŠ, prvom razredu srednje škole, za upis na fakultet i tijekom prve godine studija. Skrining za učenike 3., 6. i 7. razreda, cijepljenja po kalendaru cijepljenja, određivanja primjerenog oblika odgoja i obrazovanja, pregleda djeteta za smještaj u učenički ili studentski dom, upućivanja učenika na dodatnu poliklinički konzilijarnu obradu, zdravstvenog odgoja – predavanja, pregleda djeteta za upis u srednju školu ili fakultet, pregleda za natjecanje u školskim sportskim klubovima, pregleda za prilagodbu nastave tjelesnog odgoja, pregleda za sprječavanje i suzbijanje zaraznih bolesti, izdavanja ispričnice, temeljem zakonske obveze Zakona o zdravstvenoj zaštiti, Zakona o obveznom zdravstvenom osiguranju, Ugovora s HZZO-om, Plana i programa mjera iz obveznog zdravstvenog osiguranja, Zakona o zaštiti pučanstva od zaraznih bolesti, Pravilniku o načinu provođenja imunizacije, seroprofilakse, kemoprofilakse protiv zaraznih bolesti te o osobama koje se podvrgavaju toj obvezi, Provedbenog programa obveznog cijepljenja u RH, Pravilnika o osnovnoškolskom i srednjoškolskom odgoju i obrazovanju učenika s teškoćama u razvoju.

Osobni podaci navedeni pod **f)** prikupljaju se i obrađuju u svrhu: provođenja ugovornih obveza laboratorijskih ispitivanja vode za piće, bazenske vode, hrane, mikrobiološke čistoće, temeljem zakonske obveze Zakona o zdravstvenoj zaštiti, Plana i programa mjera iz obveznog zdravstvenog osiguranja, Zakona o hrani, Zakona o vodi za ljudsku potrošnju, Pravilnika o sanitarno-tehničkim i higijenskim uvjetima bazenskih kupališta te o zdravstvenoj ispravnosti bazenskih voda.

Osobni podaci navedeni pod **g)** prikupljaju se i obrađuju u svrhu: angažiranja osoba temeljem ugovora o djelu i autorskom djelu, sklapanja ugovora za obavljanje poslova iz djelatnosti Zavoda, izdavanje računa, praćenja posjećenosti web stranica Zavoda, temeljem zakonske obveze Zakona o zdravstvenoj zaštiti, Zakona o hrani, Zakona o vodi za ljudsku potrošnju, Pravilnika o sanitarno-tehničkim i higijenskim uvjetima bazenskih kupališta te o zdravstvenoj ispravnosti bazenskih voda, Zakona o obveznim odnosima.

Slijedom navedenog, prikupljanje osobnih podataka s obzirom na definiranu svrhu predstavlja zakonsku i ugovornu obvezu te nužan uvjet. Ako se odbiju dati pojedini podaci, neće se moći ispuniti zakonske ili ugovorne obaveze što će rezultirati nemogućnošću postupanja te ispunjenja obveze po ugovoru. S obzirom na brojnost informacija za sve detalje treba se obratiti službeniku za zaštitu osobnih podataka Zavoda.

Kontakt podaci u slučaju nužde obrađuju se temeljem legitimnih interesa odnosno potencijalne situacije kada je nužno i neodgodivo osobama prenijeti određene relevantne informacije (u slučaju izvanrednih okolnosti kao što su bolest, nezgoda itd.). Druge potrebne podatke odnosno e-mail adresu obrađuje se temeljem legitimnog interesa za kvalitetnom komunikacijom između ugovornih strana u svrhu ispunjenja svih aspekata ugovora, odnosno lakše komunikacije u smislu organizacije pružanja usluge.

Članak 5.

Izjava o politici

Voditelj obrade posvećen je osiguranju sigurnosti podataka, u skladu sa svim zakonima, regulativama te najvišim standardima etičnog poslovanja.

Ovaj pravilnik definira očekivano ophođenje zaposlenika voditelja obrade i njegovih vanjskih suradnika koji se bave prikupljanjem, upotrebom, čuvanjem, prijenosom, objavljivanjem ili uništavanjem bilo kakvih osobnih podataka koji pripadaju zaposlenicima, poslovnim partnerima i pacijentima voditelja obrade.
Svaki organizacijski dio voditelja obrade provesti će ovdje utvrđene fizičke, tehničke i organizacijske mjere kako bi osigurali sigurnost osobnih podataka. To uključuje prevenciju gubitka ili oštećenja podataka, nedopušten pristup, mijenjanje ili obradu podataka ili bilo koji drugi rizik kojemu su podaci izloženi od ljudskog ili prirodnog utjecaja.

Članak 6.

Posebne kategorije osobnih podataka

Ključna i zakonom propisana aktivnost Zavoda odnosi se na prikupljanje i obradu zdravstvenih podataka i podataka u vezi sa zdravljem ispitanika, spolnim životom i seksualnom orijentacijom pojedinca (u dijelu potrebne obrade podataka). **Odnosno, Zavod nije u mogućnosti postići svoju ključnu aktivnost i svrhu bez obrade zdravstvenih podataka iako isti predstavljaju posebnu kategoriju osobnih podataka prema kojima treba primijeniti posebne mjere zaštite. Prema Zakonu o zdravstvenoj zaštiti, Zavod jest zdravstvena ustanova za obavljanje javnozdravstvene djelatnosti na području jedinice područne (regionalne) samouprave. U svom radu Zavod obavlja djelatnost epidemologije, mirkobiologije s parazitologijom, javnog zdravstva, zdravstvene ekologije i zaštite okoliša, školske i adolescentne medicine, mentalnog zdravlja i prevencije ovisnosti na području jedinice područne samouprave.**

Gore navedene kategorije osobnih podataka Zavod obrađuje i u sljedećim situacijama: a) ispitanik je dao izričitu privolu za obradu tih osobnih podataka i to za jednu ili više određenih svrha, osim ako primjenjivi propisi navode da takva privola ne proizvodi učinak; b) obrada je nužna za potrebe izvršavanja obveza i ostvarivanja posebnih prava Zavoda ili ispitanika u području radnog prava i prava o socijalnoj sigurnosti te socijalnoj zaštiti u mjeri u kojoj je to odobreno u okviru primjenjivih propisa ili kolektivnog ugovora; c) obrada je nužna za zaštitu životno važnih interesa ispitanika ili drugog pojedinca ako ispitanik fizički ili pravno nije u mogućnosti dati privolu; d) obrada se odnosi na osobne podatke za koje je očito da ih je objavio ispitanik; e) obrada je nužna za uspostavu, ostvarivanje ili obranu pravnih zahtjeva ili kad god sudovi djeluju u sudbenom svojstvu; f) obrada je nužna za potrebe značajnog javnog interesa na temelju primjenjivih propisa koje je razmjerno željenom cilju te kojim se poštuje bit prava na zaštitu podataka i osiguravaju prikladne i posebne mjere za zaštitu temeljnih prava i interesa ispitanika; g) obrada je nužna u svrhu preventivne medicine ili medicine rada radi procjene radne sposobnosti radnika, medicinske dijagnoze, pružanja zdravstvene ili socijalne skrbi ili tretmana ili upravljanja zdravstvenim ili socijalnim sustavima i uslugama na temelju primjenjivi propisa u pogledu postupanja s posebnim kategorijama osobnih podataka, te je s tim u vezi potrebno savjetovati se sa službenikom za zaštitu podataka.
Svi Vaši osobni podaci koje ste nam Vi ili treća strana prenijeli obrađuju se sukladno svrsi njihove obrade (pri tome napominjemo da osobne podatke djece mlađe od 16 godina, neovisno o osnovi, obrađujemo samo na temelju izričitog pristanka roditelja ili skrbnika).

Članak 7.

Fizičke mjere zaštite
Voditelj obrade propisuje sljedeće mjere fizičke zaštite:
Tehničke mjere zaštite
Voditelj obrade propisuje sljedeće mjere tehničke zaštite:

Članak 8.

ANTIVIRUSNA ZAŠTITA

Ovdje opisana pravila odnose se na poslužitelje, radne stanice i infrastrukturu u Zavodu za javno zdravstvo Zadar uključujući prijenosna računala i tablete koji mogu biti korišteni izvan organizacije.

- Sva računala i uređaji koji pristupaju mreži Zavoda za javno zdravstvo Zadar moraju imati instaliranu antivirusnu zaštitu u skladu s najvišim standardima zaštite.
- Svi poslužitelji i radne stanice u vlasništvu Zavoda za javno zdravstvo Zadar ili trajno korišteni uređaji, moraju imati antivirusni program. Ovo pravilo se odnosi i na prijenosna računala koja se redovito povezuju s mrežom Zavoda.
- Računala koja rade u mreži drugih organizacija mogu biti izuzeta od prethodnog pravila ako to zahtijevaju sigurnosna pravila druge organizacije, pod uvjetom da su ta računala također zaštićena.
- Svi instalirani antivirusni programi trebaju imati uključeno automatsko ažuriranje.
- Svi uređaji gostiju, posjetitelja i ostala privatna infrastruktura nad kojom Zavod za javno zdravstvo Zadar ima nadzor mogu se spojiti samo na izdvojenu, za takve potrebe predviđenu internetsku mrežu. Nije dopušteno spajanje na glavnu mrežu Zavoda.

Članak 9.

KORIŠTENJE LOZINKI

- Sustavi koji obrađuju osobne podatke trebaju biti zaštićeni kontrolom pristupa koji se temelji na lozinki.
- Lozinke moraju biti sastavljene od kombinacije slova, brojeva i posebnih znakova (interpunkcijskih oznaka i simbola).
- Lozinke moraju imati kombinaciju velikih i malih slova.
- Lozinke ne bi trebale sadržavati očiti slijed znakova na tipkovnici (npr. qwertz ili 12345)
- Lozinke ne bi trebale sadržavati podatke kao što su osobni podaci o sebi, članovima obitelji, kućnim ljubimcima, vašoj djeci, rođendanima, adresama, telefonskim brojevima, lokacijama i sl.
- Ne preporuča se korištenje iste lozinke za pristup različitim sustavima.
- Voditelji nisu ovlašteni tražiti, prikupljati i pohranjivati lozinke zaposlenika.
- Dozvoljeno je korištenje zajedničke lozinke za više operatera, ako je to poslovno opravdano.
- Strogo je zabranjeno dijeljenje lozinki. Lozinke se ne smiju otkrivati ili javno prikazivati.
- Zabranjeno je slanje lozinki elektroničkom poštom.
- Uvijek kada se lozinka smatra kompromitiranom, odmah se mora promijeniti.

Organizacijske mjere zaštite

Voditelj obrade propisuje sljedeće organizacijske mjere zaštite:

Članak 10.

KORIŠTENJE INFORMATICKE OPREME

- Sva informatička infrastruktura može se koristiti isključivo u poslovnim aktivnostima za koje je namijenjena
- Svaki korisnik je odgovoran za očuvanje i ispravnu upotrebu informatičke infrastrukture koja mu je dana na korištenje
- Sva informatička infrastruktura mora biti na mjestima s kontroliranim pristupom.
- Aktivna radna površina i prijenosna računala moraju biti osigurana ukoliko nisu pod nadzorom. Kada je god moguće, spomenuto pravilo mora se provoditi automatski.
- Pristup infrastrukturi nije dozvoljen neovlaštenim osobama. Dodjeljivanje pristupa informatičkoj infrastrukturi i računalnim mrežama mora se obaviti putem odobrenih i prihvaćenih postupaka za upravljanje uslugama informatičke infrastrukture i nadziranim upravljanjem pristupom.

- Korisnici se moraju prema infrastrukturi, koja im je povjerena na korištenje, odnositi s punom pažnjom, te s njom pažljivo rukovati te izbjegavati nepravilno korištenje.
- Posebna se pažnja mora posvetiti zaštiti prijenosnih računala, tableta, pametnih telefona i drugih prijenosnih uređaja od krađe ili gubitka. Također, u obzir treba uzeti druge rizike oštećenja infrastrukture te oštećenja koji mogu rezultirati povredom ili gubitkom podataka kao što su ekstremne temperature, magnetska polja ili padovi.
- Prilikom putovanja (avionom) prijenosna oprema poput prijenosnih računala, tableta ili pametnih telefona, mora ostati u posjedu korisnika kao ručna prtljaga.
- Uvijek kada je moguće, neophodno je koristiti tehnologiju šifriranja i brisanja u slučaju gubitka ili krađe prijenosne infrastrukture.
- Gubitak, krađa, oštećenje, neovlašteno korištenje ili drugi incidenti moraju se, što prije od trenutka spoznaje, prijaviti voditelju informatičkog odjela.
- Zbrinjavanje imovine koja se više ne koristi mora se izvršiti u skladu s posebnim postupcima zbrinjavanja informatičkog otpada, uzimajući u obzir zaštitu svih informacija koji su predmet takvog oblika obrade. Imovina koja pohranjuje povjerljive podatke mora biti uništena u prisustvu člana tima za informacijsku sigurnost. Sredstva za čuvanje osjetljivih informacija moraju se prije odlaganja u potpunosti izbrisati u nazočnosti člana tima za informacijsku sigurnost

Članak 11.

KORIŠTENJE VLASTITIH UREĐAJA

Zavod za javno zdravstvo Zadar daje svojim zaposlenicima mogućnost kupnje i korištenja vlastitih pametnih telefona, tableta i laptopa po izboru, u poslovne svrhe društva. Istovremeno, Zavod zadržava pravo oduzimanja ove povlastice svima ili pojedincima ako se korisnici ne pridržavaju pravila i postupaka navedenih u nastavku.

Zavod za javno zdravstvo Zadar definira prihvatljivu poslovnu uporabu kao uporabu u svrhe koje izravno ili neizravno podupiru poslovanje voditelja obrade.

Zavod za javno zdravstvo Zadar definira prihvatljivu osobnu upotrebu u radnom vremenu zaposlenika ili vanjskog suradnika kao razumnu i ograničenu osobnu komunikaciju.

Zabranjuje se korištenje vlastite opreme:

• u svrhu kreiranja video ili zvučnih zapisa i fotografija u prostorijama voditelja obrade, ili na drugim mjestima u trenutku obavljanja poslovnih aktivnosti vezanih uz poslovanje voditelja obrade.

• radi pohrane ili prijenosa nedopuštenog materijala, povjerljivog materijala, osobnih podataka ili bilo kakvog materijala u vlasništvu voditelja obrade bez izričite suglasnosti voditelja odjela na koji se takvi materijali odnose

• radi pohrane ili prijenosa podataka koji pripadaju drugoj organizaciji

• za zlostavljanje drugih

• za vanjske poslovne aktivnosti.

Zavod za javno zdravstvo Zadar ima politiku nulte tolerancije za slanje SMS poruka i e-pošte tijekom vožnje. Dopušten je razgovor tijekom vožnje samo korištenjem Hands - free uređaja.

Sigurnost korištenja osobnih informacijskih i komunikacijskih uređaja:

Kako bi se spriječio neovlašteni pristup podacima u uređaju i ostalim podacima kojima uređaj ima pristup, uređaj mora biti zaštićen lozinkom.

Ukoliko postoji opcija kriptiranja uređaja, uređaj mora biti kriptiran. Pristup mreži s uređaja također mora biti zaštićen lozinkom s isključenom opcijom automatskog prepoznavanja mreže.

Nakon 5 neuspjelih pokušaja pristupa uređaju, isti mora ostati zaključan, a za ponovni pristup uređaju, mora se kontaktirati voditelj informatičkog odjela.

Uređaji koji su u vlasništvu zaposlenika i koriste se isključivo za privatne potrebe ne smiju se spajati na računalnu mrežu Zavoda za javno zdravstvo Zadar.

Gubitak ili krađa uređaja mora se prijaviti nadležnoj osobi voditelja obrade, najkasnije 24 sata od spoznaje o gubitku ili krađi. Zaposlenici su odgovori za obavješćivanje mobilnog operatera o krađi ili gubitku odmah nakon gubitka ili krađe uređaja.

Očekuje se da će svaki zaposlenik u svakom trenutku koristiti svoje uređaje na etičan način u skladu s pravilima tvrtke i etičkim kodeksom.
Zaposlenik preuzima punu odgovornost za rizike djelomičnog ili potpunog gubitka podataka pohranjenih na uređaju zbog nepravilnog korištenja ili grešaka koje uređaj cine neupotrebljivim.
Mrežna sigurnost
Voditelj obrade propisuje sljedeće mrežne mjere zaštite:
Pravila korištenja interneta i elektroničke pošte odnose se na sve korisnike interneta u Zavodu za javno zdravstvo Zadar uključujući i privremene korisnike (gosti, posjetitelji, vanjski suradnici) koji imaju privremeni pristup internetu te partnere s ograničenim ili neograničenim vremenom pristupa internetu.
Pravilnik zahtjeva i pretpostavlja usklađenost svih korisnika interneta s propisanom politikom.

Članak 12.

KORIŠTENJE INTERNETA
- Za sve korisnike interneta dopušten je ograničen pristup.
- Strogo je zabranjen pristup pornografskim web stranicama i svim drugim rizičnim stranicama.
- Pristup internetu uglavnom je predviđen za poslovnu namjenu.
- Pristup internetu u osobne svrhe je dopušten uz uvjet da se ne utječe na produktivnost rada.
- Obeshrabruje se korištenje interneta za osobne svrhe tijekom radnog vremena.
- Pristup internetu kontrolira se pomoću vatrozida.
- Pri pristupanju internetu, korisnici se moraju ponašati u skladu s pravilima koja osiguravaju ugled.
- Potrebno je poduzeti razumne mjere za otkrivanje i sprečavanje napada na servere i radne stanice.

Članak 13.

KORIŠTENJE ELEKTRONIČKE POŠTE
- Sve dodijeljene adrese elektroničke pošte i mjesta za pohranu pošte moraju se koristiti isključivo u poslovne svrhe.
- Povremeno korištenje osobne e-mail adrese na internetu za osobnu namjenu može biti dopušteno ako korištenje ne uzrokuje vidljivu potrošnju resursa i ne utječe na produktivnost rada.
- Strogo je zabranjeno korištenje resursa organizacije za neovlašteno oglašavanje, neželjenu elektroničku poštu, političke kampanje i drugo korištenje koje nije povezano s poslovanjem Zavoda za javno zdravstvo Zadar.
- Ni na koji način se resursi i adrese elektroničke pošte ne smiju koristiti za otkrivanje povjerljivih ili osjetljivih informacija koje posjeduje Zavod za javno zdravstvo Zadar osim u slučaju otkrivanja podataka ovlaštenim osobama i na autorizirane adrese elektroničke pošte.
- Korištenje resursa i adresa elektroničke pošte Zavoda za javno zdravstvo Zadar za širenje poruka koje se smatraju uvredljivima, rasističkim ili na bilo koji način protivnih zakonu i etici, apsolutno se zabranjuju.
- Elektronička pošta koristi se samo u mjeri koja je potrebna za obavljanje poslovnih zadaća. Kada korisnik i Voditelj obrade prekinu poslovni odnos, elektronička pošta mora biti deaktivirana.
- Korisnici moraju imati privatni identitet da bi pristupili vlastitoj elektroničkoj pošti i resursima za pohranu elektroničke pošte osim u posebnim slučajevima kada pristupaju elektroničkoj pošti dodijeljenoj grupi djelatnika.
- Privatnost nije zajamčena. Ukoliko se pojave posebni zahtjevi povjerljivosti, vjerodostojnosti i integriteta, omogućiti će se korištenje elektronički potpisanih poruka.

Članak 14.

POLITIKA UDALJENIH PRISTUPA

Politika udaljenih pristupa definira uvjete za siguran daljinski pristup unutarnjim resursima organizacije.

- Da bi pristupili internim resursima Zavoda za javno zdravstvo Zadar s udaljenih lokacija, korisnici moraju imati potrebna autorizacijska prava. Pristup zaposlenika s udaljenih lokacija može zatražiti samo njemu nadređena osoba, odobrava ga direktor, a omogućava voditelj informatičkog odjela ili djelatnik informatičkog odjela po nalogu voditelja informatičkog odjela.
- Pristup s udaljenih lokacija mora biti omogućen samo sigurnim kanalima uz međusobnu provjeru autentičnosti između poslužitelja i klijenta. I poslužitelj i klijent moraju prepoznati međusobno pouzdane certifikate.
- Nije dozvoljen pristup povjerljivim informacijama s udaljenih lokacija. Iznimka od ovog pravila može se odobriti samo u slučajevima u kojima je to strogo potrebno.
- Korisnici se ne smiju povezivati s javnih računala osim ako se radi o pristupu javnom sadržaju (npr. web stranicama).

Članak 15.

Ostale mjere sigurnosti

Voditelj obrade propisuje ostale sigurnosne mjere kako slijedi:

POSTUPAK POVJERAVANJA POSLOVA IZVRŠITELJU OBRADE (OUTSOURCING)

Postupak izdvajanja poslova definira zahtjeve koji su potrebni kako bi se smanjili rizici povezani s povjeravanjem poslova obrade podataka drugim izvršiteljima obrade.

- Prije izdvajanja poslova pružanja bilo kojih usluga, funkcija ili procesa, mora se obaviti procjena rizika izdvajanja poslova, ocijeniti utjecaj na obradu podataka te financijske učinke.
- Kada je god moguće, treba objaviti natječaj za odabir između više pružatelja usluga.
- Pružatelj usluge trebao bi biti odabran nakon procjene njegovog ugleda, iskustva u vrsti tražene usluge, ponudama i jamstvima.
- Ugovori o pružanju usluga i definirane razine usluga moraju sadržavati i odredbe o zaštiti osobnih podataka.
- Izvršitelj obrade mora dobiti odobrenje Zavoda za javno zdravstvo Zadar ako namjerava angažirati treću stranu (podugovaratelja) na poslovima pružanja ugovorene usluge, funkcije ili procesa.

Završne odredbe

Svi djelatnici koji obrađuju osobne podatke moraju biti upoznati sa ovim pravilnikom i izvršavati njegove odredbe.

Ovaj pravilnik sadrži povjerljive informacije i njegov sadržaj ne smije se otkrivati neovlaštenim osobama.

Pravilnik stupa na snagu s danom donošenja.

Broj: 01-1320/18
Zadar, 25. 05. 2018.

ZAVOD ZA JAVNO ZDRAVSTVO 1 ZADAR Kolovare 2 ZADAR

Ravnatelj:
Zoran Škrgatić, dr. mrd. spec. psih