Na temelju članka 3. st1. Opće uredbe o zaštiti podataka (EU) 2016/679 (GDPR) i članka 39. Statuta Zavoda za javno zdravstvo Varaždinske županije, ravnatelj dana 24. svibnja 2018. godine donosi

PRAVILNIK O ZAŠTITI OSOBNIH PODATAKA
Zavoda za javno zdravstvo
Varaždinske županije

OPĆE ODREDBE

Članak 1.

Cilj ovog Pravilnika je zaštita temeljnih prava i sloboda pojedinaca u skladu sa propisima o zaštiti osobnih podataka (uključujući, ali ne ograničavajući se na europsku Opću uredbu o zaštiti osobnih podataka - GDPR, ako je primjenjivo).

Članak 2.

Pravilnik se primjenjuje na obradu osobnih te posebnih kategorija osobnih podataka koji se odnose na fizičke osobe koje se mogu identificirati na temelju tih podataka. Primjenjuje se na podatke koji se obrađuju elektronički ili u papirnatom formatu i koji se pohranjuju u odgovarajućem sustavu pohrane.

Članak 3.

U postupku obrade osobnih podataka i zaštite pojedinaca u pogledu obrade osobnih podataka i pravila povezana sa slobodnim kretanjem osobnih podataka Zavod za javno zdravstvo Varaždinske županije je obveznik primjene Opće uredbe o zaštiti podataka (EU) 2016/679.

Članak 4.

Zavod za javno zdravstvo Varaždinske županije je sukladno čl. 4. Opće uredbe voditelj obrade osobnih podataka koji sam ili zajedno s drugima određuje svrhu i sredstva obrade osobnih podataka u skladu s nacionalnim zakonodavstvom i/ili pravom EU.

DEFINICIJE

Članak 5.

Pravilnik se temelji na odredbama Opće uredbe o zaštiti osobnih podataka (GDPR) koji postavlja visoke standarde zaštite osobnih podataka koji se primjenjuju u državama članicama Europske unije, te u skladu sa Općom uredbom o zaštiti podataka pojedini izrazi u ovom Pravilniku imaju sljedeće značenje:

„osobni podatak" označava sve podatke koji se odnose na pojedinca čiji je identitet utvrđen ili se može utvrditi („ispitanik"); pojedinac čiji se identitet može utvrditi jest osoba koja se može identificirati izravno ili neizravno, osobito uz pomoć identifikatora kao što su ime, identifikacijski broj, podaci o lokaciji, mrežni identifikator ili uz pomoć jednog ili više čimbenika svojstvenih za fizički, fiziološki, genetski, mentalni, ekonomski, kulturni ili socijalni identitet pojedinca;

„obrada" znači svaki postupak ili skup postupaka koji se obavljaju na osobnim podacima ili na skupovima osobnih podataka, bilo automatiziranim bilo neautomatiziranim sredstvima kao što su prikupljanje, bilježenje, organizacija, strukturiranje, pohrana, prilagodba ili izmjena, pronalaženje, obavljanje uvida, uporaba, otkrivanje prijenosom, širenjem ili stavljanjem na raspolaganje na drugi način, usklađivanje ili kombiniranje, ograničavanje, brisanje ili uništavanje;

„sustav pohrane" znači svaki strukturirani skup osobnih podataka dostupnih prema posebnim kriterijima, bilo da su centralizirani, decentralizirani ili raspršeni na funkcionalnoj ili zemljopisnoj osnovi;

„voditelj obrade" znači fizička ili pravna osoba, tijelo javne vlasti, agencija ili drugo tijelo koje samo ili zajedno s drugima određuje svrhe i sredstva obrade osobnih podataka; kada su svrhe i sredstva takve obrade utvrđeni pravom Unije ili pravom države članice, voditelj obrade ili posebni kriteriji za njegovo imenovanje mogu se predvidjeti pravom Unije ili pravom države članice;

„primatelj" znači fizička ili pravna osoba, tijelo javne vlasti, agencija ili drugo tijelo kojem se otkrivaju osobni podaci, neovisno o tome je li on treća strana;

„treća strana" znači fizička ili pravna osoba, tijelo javne vlasti, agencija ili drugo tijelo koje nije ispitanik, voditelj obrade, izvršitelj obrade ni osobe koje su ovlaštene za obradu osobnih podataka pod izravnom nadležnošću voditelja obrade ili izvršitelja obrade;

„privola" ispitanika znači svako dobrovoljno, posebno, informirano i nedvosmisleno izražavanje želja ispitanika kojim on izjavom ili jasnom potvrdnom radnjom daje pristanak za obradu osobnih podataka koji se na njega odnose;

„povreda osobnih podataka" znači kršenje sigurnosti koje dovodi do slučajnog ili nezakonitog uništenja, gubitka, izmjene, neovlaštenog otkrivanja ili pristupa osobnim podacima koji su preneseni, pohranjeni ili na drugi način obrađivani;

„pseudonimizacija" znači obrada osobnih podataka na način da se osobni podaci više ne mogu pripisati određenom ispitaniku bez uporabe dodatnih informacija, pod uvjetom da se takve dodatne informacije drže odvojeno te da podliježu tehničkim i organizacijskim mjerama kako bi se osiguralo da se osobni podaci ne mogu pripisati pojedincu čiji je identitet utvrđen ili se može utvrditi;

„podaci koji se odnose na zdravlje" znači osobni podaci povezani s fizičkim ili mentalnim zdravljem pojedinca, uključujući pružanje zdravstvenih usluga, kojima se daju informacije o njegovom zdravstvenom statusu;

„zaposlenik" znači osoba zaposlena u Zavodu za javno zdravstvo Varaždinske županije;

„posebna kategorija osobnih podataka" znači posebnu kategoriju osobnih podataka koji otkrivaju rasno ili etničko podrijetlo, politička mišljenja, vjerska ili filozofska uvjerenja, članstvo u sindikatu te obradu genetskih podataka, biometrijskih podataka u svrhu jedinstvene identifikacije pojedinca, podataka koji se odnose na zdravlje ili podataka o spolnom životu ili seksualnoj orijentaciji pojedinca;

„izvršitelj obrade" znači fizička ili pravna osoba, tijelo javne vlasti, agencija ili drugo tijelo koje obrađuje osobne podatke u ime voditelja obrade;

„odgovorni službenik za zaštitu podataka" znači službenik za zaštitu podataka

„ograničavanje obrade" znači označivanje pohranjenih osobnih podataka sa ciljem ograničavanja njihove obrade u budućnost

NAČELA

Članak 6.

Obrada mora biti zakonita, poštena i transparentna. Obrada je zakonita ukoliko je:

a. ispitanik dao privolu za obradu svojih osobnih podataka;
b. obrada nužna za izvršavanje ugovora;
c. obrada nužna radi poštivanja pravnih obveza voditelja obrade;
d. obrada nužna kako bi se zaštitili ključni interesi ispitanika ili druge fizičke osobe;
e. obrada nužna za izvršavanje zadaće od javnog interesa i/ili
f. obrada nužna za potrebe legitimnih interesa voditelja obrade ili treće strane.

Članak 7.

Osobni podaci prikupljeni u posebne, izričite i zakonite svrhe ne smiju se obrađivati na način koji nije u skladu s tim svrhama.

Zavod za javno zdravstvo Varaždinske županije kao voditelj obrade neće obrađivati osobne podatke osim ako postoje uvjerljive legitimne osnove za obradu.

Članak 8.

Osobni podaci moraju biti primjereni, relevantni i ograničeni na ono što je neophodno u odnosu na svrhu za koju se obrađuju. Ukoliko nisu više potrebni, osobne podatke je potrebno izbrisati.

Svi zaposlenici dužni su redovito pregledavati svoje datoteke (najmanje jednom godišnje) te brisati sve osobne podatke koje ne koriste kako bi se osiguralo poštivanje svih odredbi (sukladno važećim računovodstvenim zakonima te Uredbi).

Za kontrolu provedbe pregledavanja i brisanja podataka odgovorni su rukovoditelji/voditelji Djelatnosti.

Svi zaposlenici moraju obavijestiti službenika za zaštitu podataka o eventualnim nepravilnostima koje se odnose na brisanje podataka.

Članak 9.

Osobni podaci moraju biti točni i prema potrebi, ažurni. Mora se poduzeti svaka razumna mjera radi osiguravanja da se osobni podaci koji su identificirani kao netočni, uzimajući u obzir svrhe za koje se obrađuju, bez odlaganja izbrišu ili isprave.

Članak 10.

Osobni podaci se čuvaju u formatu koji dozvoljava identifikaciju ispitanika samo onoliko dugo koliko je neophodno u svrhe za koje se osobni podaci obrađuju.

Članak 11.

Osobni podaci obrađuju se na način koji osigurava odgovarajuću sigurnost osobnih podataka, uključujući zaštitu od neovlaštene ili nezakonite obrade te od slučajnog gubitka, uništenja ili oštećenja, koristeći odgovarajuće tehničke ili organizacijske mjere.

Članak 12.

Zavod za Javno zdravstvo Varaždinske županije kao voditelj obrade osigurava usklađenost s navedenim načelima Opće uredbe o zaštiti osobnih podataka. Svi zaposlenici su dužni završiti edukaciju o zaštiti osobnih podataka.

Voditelj obrade mora voditi cjeloviti zapis o obradi osobnih podataka. Svi zaposlenici (posebno rukovoditelji/voditelji Djelatnosti) dužni su prilikom planiranja nove ili promijeni postojeće obrade osobnih podataka obavijestiti službenika za zaštitu podataka sa ciljem prilagodbe zapisa o obradi osobnih podataka te da može provjeriti zahtjev za obradom.

Članak 13.

Kada se obrada osobnih podataka temelji na privoli, smatra se da je privola zakonita samo ako je dana jasnim, potvrdnim aktom te se njime utvrđuje da je ispitanik dao suglasnost za obradu osobnih podataka koji se odnose na njega. Suglasnost mora biti temeljena na slobodnoj, jedinstvenoj i nedvosmislenoj odluci ispitanika kojoj prethodi informiranje istog o obradi. Uz to, moraju se ispuniti i sljedeći uvjeti:

a) privola se vodi u formatu koji se može koristiti za dokazivanje da je ispitanik pristao na obradu njegovih osobnih podataka;
b) zahtjev za privolom u vidu pisane izjave koja se odnosi i na druga pitanja mora biti predočena na način da ga se jasno razlučuje od drugih pitanja, u razumljivom i lako dostupnom obliku, koristeći jasan i jednostavan jezik;
c) Ispitanik ima pravo u svakom trenutku povući svoju privolu. Prije davanja suglasnosti, ispitanik mora biti obaviješten o načinu na koji može povući privolu;

Članak 14.

Zabranjuje se obrada osobnih podataka osim:

a. ispitanik je dao izričitu privolu za obradu osobnih podataka;
b. obrada je nužna u području radnog prava i prava o socijalnoj sigurnosti;
c. obrada je nužna za zaštitu životno važnih interesa ispitanika;
d. obrada se provodi u sklopu legitimnih aktivnosti;
e. obrada se odnosi na osobne podatke za koje je očito da ih je objavio ispitanik;
f. obrada je nužna u svrhu medicinske dijagnostike, pružanja zdravstvene ili socijalne skrbi ili liječenja;
g. obrada je nužna u svrhu javnog interesa u području javnog zdravlja; u tim slučajevima podaci koji se obrađuju zaštićeni su obvezom čuvanja profesionalne tajne.

Obrada osobnih podataka koji se odnose na kaznene presude i kažnjiva djela ili s njima povezane mjere sigurnosti provodi se samo pod nadzorom službenih tijela ili kada je obrada odobrena nacionalnim zakonom.

PRAVA ISPITANIKA

Članak 15.

Svaki ispitanik ima sljedeća prava vezana uz osobne podatke:

- dobiti potvrdu obrađuju li se osobni podaci koji se odnose na njega te ako se takvi osobni podaci obrađuju, pristup osobnim podacima i sljedećim informacijama: svrsi obrade, kategorijama osobnih podataka, pravnoj osnovi za obradu podataka, razdoblju u kojem će osobni podaci biti pohranjeni, itd. Ispitaniku moraju biti dostupni podaci na njegov zahtjev (tzv. Zahtjev za pristup podacima).

- na ispravljanje osobnih podataka ako su netočni ili dopuniti nepotpune osobne podatke koji se odnose na njega (među ostalim i davanjem dodatne izjave), ako je primjenjivo. Zahtjevi se obrađuju bez nepotrebnog odgađanja.
- na brisanje svojih osobnih podataka koji se na ispitanika odnose pod uvjetom da osobni podaci više nisu nužni u odnosu na svrhe za koje su prikupljeni ili ako ispitanik povuče privolu na kojoj se obrada temelji. Ako je Zavod za javno zdravstvo Varaždinske županije, kao voditelj obrade, javno objavio osobne podatke, dužan je poduzeti razumne mjere kako bi se informirali svi oni koji obrađuju osobne podatke za koje je ispitanik zatražio brisanje („pravo na zaborav“).
- zahtijevati ograničenje obrade svojih osobnih podataka osim u slučajevima kada je to u suprotnosti s odredbama zakona i ostalih važećih propisa.
- zaprimiti kopije osobnih podataka koje je dostavio Zavodu za javno zdravstvo Varaždinske županije kao voditelju obrade, u strukturiranom, uobičajeno upotrebljavanom i strojno čitljivom formatu.
- tražiti prijenos podataka drugom voditelju obrade
- uložiti prigovor na obradu osobnih podataka koji se na njega odnose

Zavod za javno zdravstvo Varaždinske županije kao voditelj obrade dužan je poduzeti sve potrebne mjere kako bi provjerio identitet ispitanika prije pružanja odgovora na neko od navedenih prava.

Sve informacije i komunikacija koja se odnosi na obradu podataka moraju biti pružene ispitaniku na sažet, transparentan, razumljiv i dostupan način, pritom koristeći jasan i jednostavan jezik.

Podaci se dostavljaju u pisanoj formi, ili kad je moguće, elektronički.

Voditelj obrade dužan je dostaviti informacije bez nepotrebnog kašnjenja u roku od mjesec dana od zaprimanja zahtjeva od strane ispitanika, a koji rok se uzimajući u obzir složenost i broj zahtjeva može dodatno produljiti za najviše dva mjeseca. O produljenju roka ispitanik će biti obaviješten u roku od 30 dana od zaprimanja zahtjeva, zajedno s razlozima odgađanja.

Članak 16.

Bez obzira na to jesu li osobni podaci dobiveni izravno od ispitanika ili ne, Zavod za javno zdravstvo Varaždinske županije dužan je dostaviti sve potrebne informacije ispitaniku sukladno Uredbi. To se mora učiniti bilo u trenutku prikupljanja osobnih podataka ili u razumnom roku nakon dobivanja podataka ukoliko podaci nisu dobiveni od ispitanika.

MJERE ZA ZAŠTITU OSOBNIH PODATAKA

Članak 17.

Zavod za javno zdravstvo Varaždinske županije kao voditelj obrade provodi odgovarajuće tehničke i organizacijske mjere kako bi osigurao razinu sigurnosti koja odgovara riziku te kako bi se osigurala kontinuirana povjerljivost, cjelovitost, dostupnost i sigurnost sustava.

Članak 18.

Podaci u pisanom obliku obvezatno se čuvaju u registratorima i/ili za to posebno određenim uložnim košuljicama, u zaključanim ormarima i/ili ormarima u prostorijama koje se zaključavaju i u kojima je ulaz i/ili dostupnost podacima ograničen samo na zaposlenike zadužene za obradu podataka.

Podaci na računalu zaštićuju se dodjeljivanjem korisničkog imena i lozinke koja je poznata samo zaposlenicima zaduženim za obradu podataka.

Posebne kategorije osobnih podataka u papirnatom obliku obvezatno se čuvaju u zaključanim ormarima i zaključanim prostorijama sa strogo ograničenim pristupom, a posebne kategorije osobnih podataka na računalu zaštićuju se dodjeljivanjem korisničkog imena i lozinke koja je poznata samo zaposlenicima zaduženim za obradu podataka, te se svaki pristup automatski bilježi korisničkim imenom, danom i vremenom prijave i odjave.

Kako bi se smanjio rizik od gubitka/brisanja posebnih kategorija osobnih podataka Zavod za javno zdravstvo Varaždinske županije vrši pohranu/back up istih na posebnim serverima na način da su podaci prilikom pohrane zaštićeni posebnim enkripcijskim ključevima.

Članak 19.

Obrada koja se provodi u ime voditelja obrade (npr. pružatelj usluga u IT) dozvoljena je samo ako izvršitelj obrade pruža dovoljna jamstva u osiguranju zaštite prava ispitanika te je uređena međusobnim ugovorom.

Izvršitelj obrade mora biti pažljivo odabran te redovito provjeravan.

Zavod za javno zdravstvo Varaždinske županije poduzima sve mjere kako bi se osiguralo da izvršitelj obrade udovoljava standardima informacijske sigurnosti sukladno Uredbi i ostalim važećim propisima, te da obrađuje osobne podatke samo prema uputama voditelja obrade.

Članak 20.

Prilikom objave podataka koji bi se mogli pripisati određenom ispitaniku Zavod za javno zdravstvo Varaždinske županije provoditi će pseudonimizaciju kao jednu od mjera zaštite osobnih podataka.

Članak 21.

Zavod za javno zdravstvo Varaždinske županije i njezini zaposlenici dužni su surađivati s nadzornim tijelom za zaštitu osobnih podataka (Agencija za zaštitu osobnih podataka/AZOP). U slučaju da zaposlenika kontaktira AZOP, isti se odmah mora obratiti odgovornoj osobi unutar Zavoda.

Članak 22.

Svaka povreda osobnih podataka obvezatno i odmah se mora prijaviti odgovornoj osobi Zavoda za javno zdravstvo Varaždinske županije.

U slučaju povrede osobnih podataka Zavod za javno zdravstvo Varaždinske županije bez nepotrebnog odgađanja i, ako je izvedivo, najkasnije 72 sata nakon saznanja o toj povredi, izvješćuje sukladno Uredbi Agenciju za zaštitu osobnih podataka o povredi osobnih podataka, osim ako nije vjerojatno da će povreda osobnih podataka prouzročiti rizik za prava i slobode pojedinaca.

U slučaju povrede osobnih podataka koji predstavlja visok rizik za prava i slobode pojedinca, Zavod za javno zdravstvo Varaždinske županije će bez nepotrebnog odgađanja obavijestiti sve ispitanike za čije osobne podatke se ustanovila povreda, osim ako bi isto zahtijevalo nerazmjeran napor, u kojem slučaju će se ispitanici o povredi osobnih podataka obavijestiti putem nekog od javnih medija.

Članak 23.

Osobe zadužene za obradu osobnih podataka odgovorne su za zaštitu osobnih podataka od slučajnog gubitka ili uništenja, od nedopuštenog pristupa ili nedopuštene promjene, nedopuštenog objavljivanja i svake druge zlouporabe.

SLUŽBENIK ZA ZAŠTITU OSOBNIH PODATAKA

Članak 24.

Zavod za javno zdravstvo Varaždinske županije sukladno odluci ravnatelja imenuje službenika za zaštitu osobnih podataka koji mora imati odgovarajuću stručnu spremu (najmanje završeni VI. stupanj).

Službenik za zaštitu podataka odgovoran je za informiranje i savjetovanje Zavoda za javno zdravstvo Varaždinske županije kao voditelja obrade i izvršitelja obrade te njegovih zaposlenika.

Ravnatelj Zavoda za javno zdravstvo Varaždinske županije, kao voditelj obrade, mora osigurati, te je ujedno odgovoran da se poštuju svi zahtjevi koji se odnose na zaštitu podataka, a koji su propisani Uredbom, zakonom te ostalim podzakonskim aktima.

Službenik za zaštitu podataka dužan je pratiti i prijaviti ravnatelju svaku neusklađenost i moguće rizike vezane za obradu osobnih podataka.

ZAVRŠNE ODREDBE

Članak 25.

Ovaj Pravilnik o zaštiti osobnih podataka primjenjuje se od 25. svibnja 2018. godine.

Pravilnik će se objaviti na službenoj web stranici Zavoda za javno zdravstvo Varaždinske županije.

U Varaždinu, 24. svibnja 2018.

RAVNATELJ

Marin Bosilj, dipl. san. ing.

Broj:02/1-536/1-2018.