820

Na temelju Opće uredbe o zaštiti podataka (EU) 2016/679, Zakona o provedbi Opće uredbe o zaštiti podataka NN 42/18 i članka 63. Statuta Nastavnog zavoda za javno zdravstvo Primorsko–goranske županije, Krešimirova 52a, Rijeka (u nastavku Zavod), Upravno vijeće ustanove, na svojoj 185. sjednici održanoj 30.04.2019. godine, donosi:

PRAVILNIK O ZAŠTITI I OBRADI OSOBNIH PODATAKA

Nastavni ZAVOD ZA JAVNO ZDRAVSTVO PRIMORSKO-GORANSKE ŽUPANIJE
Primljeno: 15 -05- 2019
Ur.br.: 08-820-93/2-19

I. OPĆE ODREDBE

Članak 1.

U postupku obrade osobnih podataka i zaštite pojedinaca u pogledu obrade osobnih podataka i pravila povezana sa slobodnim kretanjem osobnih podataka Zavod je obveznik primjene Opće uredbe o zaštiti podataka (EU) 2016/679 te je dužan nadzirati prikupljanje, obradu, korištenje i zaštitu osobnih podataka svih fizičkih osoba čije podate prikuplja i obrađuje.

Članak 2.

Izrazi koji se koriste u ovom Pravilniku, a koji imaju rodno značenje, bez obzira na to jesu li korišteni u muškom ili ženskom rodu, obuhvaćaju na jednak način muški i ženski rod.

Članak 3.

(1) Zavod je sukladno članku 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 ili pravom EU.
(2) Zavod je sukladno članku 4. Opće uredbe izvršitelj obrade te obrađuje osobne podatke u ime voditelja obrade sukladno ugovoru.

Članak 4.

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 (ip adresa) ili uz pomoć jednog ili više čimbenika svojstvenih za fizički, fiziološki, genetski, mentalni, ekonomski, kulturni ili socijalni identitet tog 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” je 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, voditelja obrade ili posebnim kriterijima za njegovo imenovanje mogu se predvidjeti pravom Unije ili pravom države članice;

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

„primatelj" je 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" je 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 je 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;

Članak 5.

(1) Zavod osobne podatke obrađuje zakonito, pošteno i transparentno.
(2) Zavod obrađuje samo primjerene i relevantne osobne podatke i to isključivo u posebne, izričite i zakonite svrhe te se dalje ne obrađuju na način koji nije u skladu s tim svrhama.
(3) Osobne podatke koje Zavod obrađuje su točni te se po potrebi ažuriraju.
(4) Zavod osobne podatke čuva u obliku koji omogućuje identifikaciju ispitanika i to samo onoliko dugo koliko je potrebno u svrhe radi kojih se osobni podaci obrađuju. Iznimno, osobni podaci mogu se pohraniti i na dulja razdoblja, ali samo ako će se isti obrađivati isključivo u svrhe arhiviranja u javnom interesu, u svrhe znanstvenog ili povijesnog istraživanja ili u statističke svrhe.
(5) Zavod osobne podatke obrađuje isključivo na način kojim se osigurava odgovarajuća sigurnost osobnih podataka, uključujući zaštitu od neovlaštene ili nezakonite obrade te od slučajnog gubitka, uništenja ili oštećenja primjenom odgovarajućih tehničkih ili organizacijskih mjera.

II. SLUŽBENIK ZA ZAŠTITU PODATAKA

Članak 6.

(1) Ravnatelj Zavoda imenuje službenika za zaštitu podataka. Službenik za zaštitu podataka imenuje se iz redova zaposlenika Zavoda.
(2) Kontakt podatke službenika za zaštitu podataka Zavod objavljuje na svojim web stranicama te o osobi imenovanoj za službenika obavještava nadzorno tijelo.
(3) Službenik za zaštitu podataka dužan je čuvati povjerljivost svih informacija koje sazna u obavljanju svoje dužnosti.
(4) Službenik za zaštitu osobnih podataka ovlašten je pristupati svim sustavima kojima Voditelj obrade prikuplja, obrađuje i pohranjuje osobne podatke u svrhu procjene korištenja i sigurnosti osobnih podataka.

III. OBRADA OSOBNIH PODATAKA

Članak 7.

Zavod osobne podatke obrađuje samo i u onoj mjeri ako je ispunjen jedan od sljedećih uvjeta:

- da je ispitanik dao privolu za obradu svojih osobnih podataka u jednu ili više posebnih svrha;
- da je obrada nužna za izvršavanje ugovora u kojem je ispitanik stranka daje obrada nužna radi poštovanja pravnih obveza Zavoda;
- da je obrada nužna kako bi se zaštitili ključni interesi ispitanika ili druge fizičke osobe da je obrada nužna za izvršavanje zadaće od javnog interesa;
- da je obrada nužna za potrebe legitimnih interesa Zavoda ili treće strane, osim u slučaju kada su od tih interesa jači interesi ili temeljna prava i slobode ispitanika koji zahtijevaju zaštitu osobnih podataka, osobito ako je ispitanik dijete.

Članak 8.

(1) Privola kojom ispitanik Zavodu daje pristanak za obradu osobnih podataka koji se na njega odnose mora biti dobrovoljna, dana u pisanom obliku s lako razumljivim, jasnim i jednostavnim jezikom, jasno naznačenom svrhom za koju se daje i bez nepoštenih uvjeta.

(2) Ako se radi o obradi osobnih podataka djeteta ispod dobne granice od 16 godina, privolu na način opisanom u stavku 1. ovog članka daje nositelj roditeljske odgovornosti nad djetetom (roditelj ili zakonski skrbnik djeteta).

Članak 9.

U postupku obrade osobnih podataka Zavod na odgovarajući način (pisano ili izravno usmeno) ispitaniku pruža sve informacije vezano uz obradu njegovih osobnih podataka, a osobito o:

- identitetu i kontakt podacima voditelja obrade,
- kontakt podacima službenika za zaštitu osobnih podataka,
- svrsi obrade podataka,
- pravnoj osnovu za obradu podataka,
- legitimnim interesima Zavoda,
- namjeri predaji osobnih podataka trećim osobama,
- razdoblju u kojem će osobni podaci biti pohranjeni,
- o postojanju prava ispitanika na pristup osobnim podacima,
- te na ispravak ili brisanje osobnih podataka i ograničavanje obrade, prava na ulaganje prigovora,
- o namjeri dodatnog obrađivanja osobnih podataka u svrhu koja je različita od one za koju su osobni podaci prikupljeni.

Članak 10.

Zavod obrađuje posebne kategorije osobnih podataka u slučajevima:

(1) ispitanik je dao izričitu privolu za obradu tih osobnih podataka za jednu ili više određenih svrha;

(2) da je obrada nužna za izvršavanje ugovora u kojem je ispitanik stranka ili kako bi se poduzele radnje na zahtjev ispitanika prije sklapanja ugovora;

(3) obrada je nužna za potrebe izvršavanja obveza i ostvarivanja posebnih prava voditelja obrade ili ispitanika u području radnog prava i prava o socijalnoj sigurnosti te socijalnoj zaštiti u mjeri u kojoj je to odobreno u okviru prava Unije ili prava države članice ili kolektivnog ugovora u skladu s pravom države članice koje propisuje odgovarajuće zaštitne mjere za temeljna prava i interese ispitanika;

(4) obrada je nužna za zaštitu životno važnih interesa ispitanika ili drugog pojedinca ako

ispitanik fizički ili pravno nije u mogućnosti dati privolu;

(5) obrada se provodi u sklopu legitimnih aktivnosti s odgovarajućim zaštitnim mjerama zavoda, udruženja ili drugog neprofitnog tijela s političkim, filozofskim, vjerskim ili sindikalnim ciljem te pod uvjetom da se obrada odnosi samo na članove ili bivše članove tijela ili na osobe koje imaju redovan kontakt s njom u vezi s njezinim svrhama i da osobni podaci nisu priopćeni nikome izvan tog tijela bez privole ispitanika;

(6) obrada se odnosi na osobne podatke za koje je očito da ih je objavio ispitanik;

(7) obrada je nužna za uspostavu, ostvarivanje ili obranu pravnih zahtjeva ili kad god sudovi djeluju u sudbenom svojstvu;

(8) obrada je nužna za potrebe značajnog javnog interesa na temelju prava Unije ili prava države članice 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;

(9) obrada je nužna u svrhu preventivne medicine ili medicine rada radi procjene radne sposobnosti zaposlenika, medicinske dijagnoze, pružanja zdravstvene ili socijalne skrbi ili tretmana ili upravljanja zdravstvenim ili socijalnim sustavima i uslugama na temelju prava Unije ili prava države članice ili u skladu s ugovorom sa zdravstvenim radnikom te u skladu s uvjetima i zaštitnim mjerama;

(10) obrada je nužna u svrhu javnog interesa u području javnog zdravlja kao što je zaštita od ozbiljnih prekograničnih prijetnji zdravlju ili osiguravanje visokih standarda kvalitete i sigurnosti zdravstvene skrbi te lijekova i medicinskih proizvoda, na temelju prava Unije ili prava države članice kojim se propisuju odgovarajuće i posebne mjere za zaštitu prava i sloboda ispitanika, posebno čuvanje profesionalne tajne;

(11) obrada je nužna u svrhe arhiviranja u javnom interesu, u svrhe znanstvenog ili povijesnog istraživanja ili u statističke svrhe na temelju prava Unije ili prava države članice koje je razmjerno cilju koji se nastoji postići te kojim se poštuje bit prava na zaštitu podataka i osiguravaju prikladne i posebne mjere za zaštitu temeljnih prava i interesa ispitanika.

IV. PRAVA ISPITANIKA I ZAŠTITA PRAVA

Članak 11.

(1) Zavod poduzima odgovarajuće mjere kako bi se ispitaniku pružile sve informacije u vezi s obradom u sažetom, transparentnom, razumljivom i lako dostupnom obliku, uz uporabu jasnog i jednostavnog jezika, osobito za svaku informaciju koja je posebno namijenjena djetetu. Informacije se pružaju u pisanom obliku ili drugim sredstvima, među ostalim, ako je prikladno, elektroničkim putem. Ako to zatraži ispitanik, informacije se mogu pružiti usmenim putem, pod uvjetom daje drugim sredstvima utvrđen identitet ispitanika.

(2) Voditelj obrade ispitaniku na zahtjev pruža informacije o poduzetim radnjama bez nepotrebnog odgađanja i u svakom slučaju u roku od mjesec dana od zaprimanja zahtjeva. Taj se rok može prema potrebi produljiti za dodatna dva mjeseca, uzimajući u obzir složenost i broj zahtjeva. Voditelj obrade obavješćuje ispitanika o svakom takvom produljenju u roku od mjesec dana od zaprimanja zahtjeva, zajedno s razlozima odgađanja. Ako ispitanik podnese zahtjev elektroničkim putem, informacije se pružaju elektroničkim putem ako je to moguće, osim ako ispitanik zatraži drugačije.

(3) Ako Zavod ne postupi po zahtjevu ispitanika, Zavod bez odgađanja i najkasnije jedan mjesec od primitka zahtjeva izvješćuje ispitanika o razlozima zbog kojih nije postupio i o mogućnosti podnošenja pritužbe nadzornom tijelu i traženja pravnog lijeka.

(4) Informacije pružene ispitaniku i sva komunikacija i djelovanja pružaju se bez naknade. Ako su zahtjevi ispitanika očito neutemeljeni ili pretjerani, osobito zbog njihova učestalog ponavljanja, Zavod može:

- naplatiti razumnu naknadu uzimajući u obzir administrativne troškove pružanja informacija ili obavijesti ili postupanje po zahtjevu; ili

- odbiti postupiti po zahtjevu.

Teret dokaza očigledne neutemeljenosti ili pretjeranosti zahtjeva jest na voditelju obrade.

(5) Ako Zavod ima opravdane sumnje u pogledu identiteta pojedinca koji podnosi zahtjev za brisanje, ispravak, pristup podacima, voditelj obrade može tražiti pružanje dodatnih informacija neophodnih za potvrđivanje identiteta ispitanika.

Članak 12.

(1) Ispitanik ima pravo pristupa osobnim podatcima sadržanim u sustavu pohrane Zavoda koji se na njega odnose.
(2) Ispitanik ima pravo ispisa osobnih podataka sadržanih u sustavu pohrane koji se na njega odnose.
(3) Zavod će bez odgađanja, na zahtjev ispitanika ispraviti netočne podatke koji se na njega odnose odnosno temeljem traženja ispitanika iste dopuniti.
(4) Zavod će bez odgađanja, temeljem zahtjeva ispitanika, provesti brisanje osobnih podataka koji se na njega 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.
(5) U slučaju da Zavod utvrdi da su osobni podaci nepotpuni, netočni ili neažurni, dužan ih je sam dopuniti ili izmijeniti neovisno o zahtjevu ispitanika.
(6) Ispitanik koji smatra da mu je povrijeđeno neko pravo zajamčeno Općom uredbom o zaštiti podataka ima pravo podnijeti zahtjev za utvrđivanje povrede prava nadležnom tijelu.

Članak 13.

U svrhu zaštite osobnih podataka Zavod, u svim slučajevima kada je to moguće, a posebice prilikom javnog objavljivanja informacija sukladno Zakonu o pravu na pristup informacijama, provodi pseudonimizaciju podataka.

V. SUSTAV POHRANE

Članak 14.

(1) Zavod o osobnim podacima koje prikuplja i obrađuje vodi evidenciju aktivnosti obrade.
(2) Evidencija aktivnosti obrade sadrži najmanje sljedeće podatke:
   - ime i kontaktne podatke Zavoda, predstavnika Zavoda i službenika za zaštitu podataka;
   - svrha obrade;
   - opis kategorija ispitanika i kategorija osobnih podataka;
   - kategorije primatelja kojima su osobni podaci otkriveni ili će im biti otkriveni;
   - predviđene rokove za brisanje različitih kategorija podataka;
   - opći opis tehničkih i organizacijskih sigurnosnih mjera za zaštitu podataka;

VI. MJERE ZA ZAŠTITU OSOBNIH PODATAKA

Članak 15.

Da bi se izbjegao neovlašteni pristup osobnim podacima, podaci u pisanom obliku čuvaju se u registratorima, u zaključanim ormarima kojima imaju pristup osobe zadužene za obradu podataka, a podaci u računalu zaštićuju se dodjeljivanjem korisničkog imena i lozinke koja je poznata zaposlenicima zaduženim za obradu podataka.

Članak 16.

Osobe zadužene za obradu osobnih podataka dužne su poduzeti tehničke, kadrovske i organizacijske mjere zaštite osobnih podataka koje su potrebne da bi se osobni podaci zaštitili od slučajnog gubitka ili uništenja, od nedopuštenog pristupa ili nedopuštene promjene, nedopuštenog objavljivanja i svake druge zlouporabe.

VII. RUKOVANJE POVREDAMA OSOBNIH PODATAKA

Članak 17.

(1) U slučaju povrede osobnih podataka Zavod bez nepotrebnog odgađanja i, ako je izvedivo, najkasnije 72 sata nakon saznanja o toj povredi, izvješćuje nadležno nadzorno o povredi osobnih podataka, osim ako nije vjerojatno da će povreda osobnih podataka prouzročiti rizik za prava i slobode pojedinaca. Ako izvješćivanje nije učinjeno unutar 72 sata, mora biti popraćeno razlozima za kašnjenje.

(2) U izvješćivanju iz stavka 1. mora se barem:
   (a) opisati priroda povrede osobnih podataka, uključujući, ako je moguće, kategorije i približan broj dotičnih ispitanika te kategorije i približan broj dotičnih evidencija osobnih podataka;
   (b) navesti ime i kontaktne podatke službenika za zaštitu podataka ili druge kontaktne točke od koje se može dobiti još informacija;
   (c) opisati vjerojatne posljedice povrede osobnih podataka;
   (d) opisati mjere koje je voditelj obrade poduzeo ili predložio poduzeti za rješavanje problema povrede osobnih podataka, uključujući prema potrebi mjere umanjivanja njezinih mogućih štetnih posljedica.

(3) Ako i u onoj mjeri u kojoj nije moguće istodobno pružiti informacije, informacije je moguće postupno pružati bez nepotrebnog daljnjeg odgađanja.

(4) Zavod dokumentira sve povrede osobnih podataka, uključujući činjenice vezane za povredu osobnih podataka, njezine posljedice i mjere poduzete za popravljanje štete. Ta dokumentacija nadzornom tijelu omogućuje provjeru poštovanja ovog članka.

Članak 18.

(1) U slučaju povrede osobnih podataka koje će vjerojatno prouzročiti visok rizik za prava i slobode pojedinaca, Zavod bez nepotrebnog odgađanja obavješćuje ispitanika o povredi osobnih podataka.

(2) Obavješćivanjem ispitanika iz stavka 1. ovog članka opisuje se priroda povrede osobnih podataka uporabom jasnog i jednostavnog jezika te ono sadržava barem informacije i mjere iz članka 16. stavka 2. točaka (b), (c) i (d).

(3) Obavješćivanje ispitanika iz stavka 1. nije obvezno ako je ispunjen bilo koji od sljedećih uvjeta:
   (a) voditelj obrade poduzeo je odgovarajuće tehničke i organizacijske mjere zaštite i te su mjere primijenjene na osobne podatke pogođene povredom osobnih podataka, posebno one koje osobne podatke čine nerazumljivima bilo kojoj osobi koja im nije ovlaštena pristupiti, kao što je enkripcija;
   (b) voditelj obrade poduzeo je naknadne mjere kojima se osigurava da više nije vjerojatno da će doći do visokog rizika za prava i slobode ispitanika iz stavka 1;
   (c) time bi se zahtijevao nerazmjeran napor. U takvom slučaju mora postojati javno obavješćivanje ili slična mjera kojom se ispitanici obavješćuju na jednako djelotvoran način.

(4) Ako voditelj obrade nije do tog trenutka obavijestio ispitanika o povredi osobnih podataka, nakon razmatranja razine vjerojatnosti da će povreda osobnih podataka prouzročiti visok rizik, nadzorno tijelo može od njega zahtijevati da to učini ili može zaključiti da je ispunjen neki od uvjeta navedenih u stavku 3.

VIII. PRIJELAZNE I ZAVRŠNE ODREDBE

Članak 19.

U dijelu o zaštiti, nadzoru nad prikupljanjem, obradi i korištenju osobnih podataka koji nije uređen ovim Pravilnikom, neposredno se primjenjuje Opća uredba o zaštiti osobnih podataka (GDPR).

Članak 20.

Ovaj Pravilnik stupa na snagu osmog dana od dana objave na oglasnoj ploči Zavoda, na službenim web stranicama Zavoda www.zzjzpgz.hr.

Rijeka, 30.04.2019. godine.

Broj: 08-820-93/2-19

PREDSJEDNIK UPRAVNOG VIJEĆA

dr. sc. Davor Širola, dipl. oec.

Utvrđuje se da je ovaj Pravilnik objavljen na oglasnoj ploči Zavoda dana 15. 05. 2019. godine i da je stupio na snagu dana 23. 05. 2019. godine.

RAVNATELJ

prof. dr. sc. Vladimir Mićović, dr. med.

Nastavni ZAVOD ZA JAVNO ZDRAVSTVO PRIMORSKO-GORANSKE ŽUPANIJE RIJEKA, Krešimirova 52/A

SADRŽAJ

I. OPĆE ODREDBE 1

II. SLUŽBENIK ZA ZAŠTITU PODATAKA 2

III. OBRADA OSOBNIH PODATAKA 3

IV. PRAVA ISPITANIKA I ZAŠTITA PRAVA 4

V. SUSTAV POHRANE 5

VI. MJERE ZA ZAŠTITU OSOBNIH PODATAKA 5

VII. RUKOVANJE POVREDAMA OSOBNIH PODATAKA 6

VIII. PRIJELAZNE I ZAVRŠNE ODREDBE 7