

Na temelju članka 28. i članka 53. Statuta Specijalne bolnice za medicinsku rehabilitaciju Stubičke Toplice od 28. svibnja 2009., 24. studenog 2011., 26. travnja 2013., 25. ožujka 2014. i 30. studenog 2016. godine, odredbi Uredbe (EU) 2016/679 Europskog parlamenta i vijeća od 27. travnja 2016. godine 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 42/18) Upravno vijeće Bolnice na svojoj 16. sjednici održanoj dana 21. prosinca 2018. godine, jednoglasno je donijelo sljedeći

PRAVILNIK O ZAŠTITI OSOBNIH PODATAKA

1. OPĆE ODREDBE

Članak 1.

Ovim Pravilnikom uređuje se zaštita pojedinaca, njihovih temeljnih sloboda i prava prilikom prikupljanja i obrade osobnih podataka u poslovanju Specijalne bolnice za medicinsku rehabilitaciju Stubičke Toplice (u dalnjem tekstu Bolnica) .

Članak 2.

Odredbe Pravilnika sukladne su 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 van snage Direktive 95/46/EZ (Opća uredba o zaštiti podataka), (u dalnjem tekstu: Opća uredba) i Zakona o provedbi opće uredbe o zaštiti podataka (NN 42/18) i primjenjuju se na zaštitu osobnih podataka pojedinaca, državljana država članica Europske unije bez obzira na nacionalnost, boravište pojedinaca ili teritorij države u kojoj se podaci obrađuju.

Članak 3.

Odredbe Pravilnika ne primjenjuju se na osobne podatke preminulih osoba, osobne podatke pojedinaca izvan država članica Europske unije te na anonimne podatke.

Članak 4.

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

2. DEFINICIJE

Članak 5.

Definicije pojmove za potrebe ovog Pravilnika, sukladno definicijama Opće uredbe:

1. OSOBNI PODACI su svi podaci 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 tog pojedinca;
2. OBRADA je svaki postupak ili skup postupaka koji se obavlja 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;
3. OGRANIČAVANJE OTRADE znači označivanje pohranjenih osobnih podataka s ciljem ograničavanja njihove obrade u budućnosti;
4. IZRADA PROFILA znači svaki oblik automatizirane obrade osobnih podataka koji se sastoji od uporabe osobnih podataka za ocjenu određenih osobnih aspekata povezanih s pojedincem, posebno za analizu ili predviđanje aspekata u vezi s radnim učinkom, ekonomskim stanjem, zdravlјjem, osobnim sklonostima, interesima, pouzdanošću, ponašanjem, lokacijom ili kretanjem tog pojedinca;
5. 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;
6. SUSTAV POHRANE znači svaki strukturirani skup osobnih podataka dostupnih prema posebnim kriterijima, bilo da su centralizirani, decentralizirani ili raspršeni na funkcionalnoj ili zemljopisnoj osnovi;
7. VODITELJ OTRADE 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;
8. IZVRŠITELJ OTRADE znači fizička ili pravna osoba, tijelo javne vlasti, agencija ili drugo tijelo koje obrađuje osobne podatke u ime voditelja obrade;
9. 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. Međutim, tijela javne vlasti koja mogu primiti osobne podatke u okviru određene istrage u skladu s pravom Unije ili države članice ne smatraju se primateljima; obrada tih podataka koju obavljaju ta tijela javne vlasti mora biti u skladu s primjenjivim pravilima o zaštiti podataka prema svrhama obrade;
10. 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;

11. PRIVOLA ISPITANIKA znači svako dobrovoljno, posebno, informirano i nedvosmisleno izražavanje želja ispitanika kojim on izjavom ili jasnom potvrđnom radnjom daje pristanak za obradu osobnih podataka koji se na njega odnose;
12. 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;
13. BIOMETRIJSKI PODACI znači osobni podaci dobiveni posebnom tehničkom obradom u vezi s fizičkim obilježjima, fiziološkim obilježjima ili obilježjima ponašanja pojedinca koja omogućuju ili potvrđuju jedinstvenu identifikaciju tog pojedinca, kao što su fotografije lica ili daktiloskopski podaci;
14. 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 njegovu zdravstvenom statusu;
15. NADZORNO TIJELO znači neovisno tijelo javne vlasti koje je osnovala država članica u skladu s člankom 51. Opće uredbe
16. PREKOGRANIČNA OBRADA znači ili obrada osobnih podataka koja se odvija u Uniji u kontekstu aktivnosti poslovnih nastana u više od jedne države članice voditelja obrade ili izvršitelja obrade, a voditelj obrade ili izvršitelj obrade ima poslovni nastan u više od jedne države članice; ili obrada osobnih podataka koja se odvija u Uniji u kontekstu aktivnosti jedinog poslovnog nastana voditelja obrade ili izvršitelja obrade, ali koja bitno utječe ili je izgledno da će bitno utjecati na ispitanike u više od jedne države članice.

Članak 6.

Voditelj obrade u smislu članka 4. stavka 7. je Specijalna bolnica za medicinsku rehabilitaciju Stubičke Toplice.

Nadzorno tijelo u smislu članka 4. stavka 15. je Agencija za zaštitu osobnih podataka.

3. NAČELA I ZAKONITOST OBRADE OSOBNIH PODATAKA

Članak 7.

Bolnica obrađuje osobne podatke poštujući slijedeća načela:

- a) Načelo zakonitosti, poštenosti, transparentnosti – Osobni podaci se obrađuju zakonito, pošteno i transparentno s obzirom na ispitanika
- b) Načelo ograničavanja svrhe - Osobni podaci prikupljaju se u posebne, izričite i zakonite svrhe te se dalje ne smiju obrađivati na način koji nije u skladu s tim svrhama. Daljnja obrada u svrhe arhiviranja u javnom interesu, u svrhe znanstvenog ili povijesnog istraživanja ili u statističke svrhe ne smatra se neusklađenom s prvotnim svrhama
- c) Načelo smanjenje količine podataka - Osobni podaci koji e obrađuju su primjereni, relevantni i ograničeni na ono što je nužno u odnosu na svrhe u koje se obrađuju
- d) Načelo točnosti - Osobni podaci su točni i prema potrebi ažurni. Osobni podaci koji nisu točni, uzimajući u obzir svrhe u koje se obrađuju, bez odlaganja se brišu ili ispravljaju.

- e) Načelo ograničenja pohrane - Osobni podaci se čuvaju u obliku koji omogućuje identifikaciju ispitanikâ samo onoliko dugo koliko je potrebno u svrhe radi kojih se osobni podaci obrađuju. Osobni podaci mogu se pohraniti na dulja razdoblja ako će se osobni podaci obradivati isključivo u svrhe arhiviranja u javnom interesu, u svrhe znanstvenog ili povijesnog istraživanja ili u statističke svrhe u skladu s člankom 89. stavkom 1. Opće uredbe, što podliježe provedbi primjerenih tehničkih i organizacijskih mjera propisanih Općom uredbom radi zaštite prava i sloboda ispitanika.
- f) Načelo cjelovitosti i povjerljivosti - Osobni podaci obrađuju se 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

Članak 8.

Prema Općoj uredbi i ovom Pravilniku obrada osobnih podataka je zakonita samo i u onoj mjeri u kojoj je ispunjeno najmanje jedno od sljedećega:

1. ispitanik je dao privolu za obradu svojih osobnih podataka u jednu ili više posebnih svrha;
2. obrada je 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 radi poštovanja pravnih obveza Bolnice kao voditelja obrade;
4. obrada je nužna kako bi se zaštitili ključni interesi ispitanika ili druge fizičke osobe;
5. obrada je nužna za izvršavanje zadaće od javnog interesa ili pri izvršavanju službene ovlasti voditelja obrade;

4. OBRADA POSEBNIH KATEGORIJA OSOBNIH PODATAKA

Članak 9.

Posebne kategorije osobnih podataka u smislu Opće uredbe i ovog Pravilnika su slijedeće: podaci koji otkrivaju rasno ili etničko podrijetlo, politička mišljenja, vjerska ili filozofska uvjerenja ili članstvo u sindikatu te obrada genetskih podataka, biometrijskih podataka u svrhu jedinstvene identifikacije pojedinca, podataka koji se odnose na zdravlje ili podataka o spolnom životu ili seksualnoj orijentaciji pojedinca.

Članak 10.

Obrada posebnih kategorija osobnih podataka je zabranjena izuzev u slučajevima kada je ispunjeno jedno od slijedećeg:

- ispitanik je dao izričitu privolu za obradu tih osobnih podataka za jednu ili više određenih svrha
- obrada je nužna za potrebe izvršavanja obveza i ostvarivanja posebnih prava Bolnice kao voditelja obrade ili ispitanika u području radnog prava i prava o socijalnoj sigurnosti te socijalnoj zaštiti
- obrada je nužna za zaštitu životno važnih interesa ispitanika ili drugog pojedinca ako ispitanik fizički ili pravno nije u mogućnosti dati privolu;

- 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
- i u ostalim slučajevima opisanim u članku 9. stavak 2 Opće uredbe

Članak 11.

Bolnica ne prikuplja i ne obrađuje podatke koji otkrivaju rasno ili etničko podrijetlo, politička mišljenja, vjerska ili filozofska uvjerenja, podatke o spolnom životu ili seksualnoj orientaciji pojedinaca niti ne obrađuje genetske podatke.

Članak 12.

Bolnica može prikupljati i obrađivati podatke koji se odnose na članstvo u sindikatu samo za radnike koji su zaposleni u Bolnici i isključivo uz njihovu izričitu privolu i na njihovo traženje.

Članak 13.

Osobni podaci koji se odnose na zdravlje obuhvaćaju sve podatke koji se odnose na zdravstveno stanje ispitanika, a koji otkrivaju informacije u vezi s prijašnjim, trenutačnim ili budućim fizičkim ili mentalnim zdravstvenim stanjem ispitanika.

Osobni podaci koji se odnose na zdravlje uključuju:

- a) informacije o pojedincu prikupljene tijekom registracije za ili tijekom pružanja tom pojedincu zdravstvenih usluga, a to su broj, simbol ili oznaka koja je pojedincu dodijeljena u svrhu njegove jedinstvene identifikacije za zdravstvene svrhe
- b) informacije izvedene iz testiranja ili ispitivanja dijela tijela ili tjelesne tvari, među ostalim iz genetskih podataka i bioloških uzoraka
- c) bilo kakvu informaciju o bolesti, invalidnosti, riziku od bolesti, medicinskoj povijesti, kliničkom tretmanu ili fiziološkom ili biomedicinskom stanju ispitanika neovisno o njegovu izvoru, kao na primjer od liječnika ili drugog zdravstvenog djelatnika, bolnice, medicinskog uređaja ili dijagnostičkog testa in vitro.

Članak 14.

Bolnica obrađuje osobne podatke putem video nadzora u svrhu zaštite osoba i imovine. Video nadzorom je obuhvaćen vanjski prostor (dvorište i parkirališta) i dijelovi prostora unutar Bolnice: kaffe bara, blagovaone, tri sobe za najteže bolesnike na neurološkom odjelu, prostor hidroterapija – bazena i prostor recepcije.

Prostori koji su pod video nadzorom su označeni.

Bolnica smije koristiti nadzorne uređaje kao sredstvo zaštite osoba i imovine pod uvjetima propisanima propisima s područja zaštite na radu.

Dopušteno je korištenje nadzornih uređaja radi kontrole ulazaka i izlazaka iz radnih prostorija i prostora te radi smanjenja izloženosti radnika, pacijenata i posjeta riziku od razbojstva, provala, nasilja, krađa i sličnih događaja na radu, u vezi s radom kao i boravkom u Bolnici.

Zabranjeno je postavljanje nadzornih uređaja u prostorijama za osobnu higijenu, presvlačenje i odmor radnika.

Bolnica ne smije koristiti snimljene materijale u svrhe koje nisu propisane ovim člankom, ne smije ih emitirati u javnosti niti pred osobama koje nemaju ovlasti na nadzor opće sigurnosti i

zaštite na radu te je obvezan osigurati da snimljeni materijali ne budu dostupni neovlaštenim osobama.

Odredbe ovoga članka o zabrani snimanja i zabrani korištenja snimljenih materijala obvezuju Bolnicu i u odnosu na djecu i maloljetnike, neovisno nalaze li se na mjestima rada u svojstvu maloljetnih radnika, osoba na radu ili pacijenata Bolnice.

Snimke dobivene putem video nadzora čuvaju se 45 dana te se automatski brišu iz sustava. U bolesničkim sobama odjela za neurološku rehabilitaciju snimke dobivene putem video nadzora ne sadržavaju tonski zapis i čuvaju se sedam dana nakon čega se automatski brišu iz sustava.

5. PRIVOLA ISPITANIKA

Članak 15.

Privola se treba dati jasnom potvrđnom radnjom kojom se izražava dobrovoljan, poseban, informiran i nedvosmislen pristanak ispitanika na obradu osobnih podataka koji se odnose na njega u obliku pisane izjave, uključujući elektroničku, ili usmene izjave koja jasno pokazuje da ispitanik prihvata predloženu obradu svojih osobnih podataka.

Šutnja ispitanika, nepotpunjavanje sadržaja pisane izjave djelomično ili u cijelosti ne smatraju se privolom.

Privola treba obuhvatiti sve aktivnosti obrade koje se obavljaju u istu svrhu.

Kada obrada ima višestruke svrhe, privolu bi trebalo dati za sve njih. Ako se privola ispitanika treba dati nakon zahtjeva upućenog elektroničkim putem, taj zahtjev mora biti jasan, jezgrovit i ne smije nepotrebno ometati upotrebu usluge za koju se upotrebljava.

Bolnica kao voditelj obrade mora moći dokazati da je ispitanik dao privolu za obradu svojih osobnih podataka.

Ako ispitanik da privolu u vidu pisane izjave koja se odnosi i na druga pitanja, zahtjev za privolu mora biti predočen na način da ga se može jasno razlučiti od drugih pitanja, u razumljivom i lako dostupnom obliku uz uporabu jasnog i jednostavnog jezika.

Ispitanik ima pravo u svakom trenutku povući svoju privolu. Povlačenje privole ne utječe na zakonitost obrade na temelju privole prije njezina povlačenja. Prije davanja privole, ispitanika se o tome obavješće. Povlačenje privole mora biti jednakoj jednostavno kao i njezino davanje. Kada se procjenjuje je li privola bila dobrovoljna, u najvećoj mogućoj mjeri uzima se u obzir je li, među ostalim, izvršenje ugovora, uključujući pružanje usluge, uvjetovano privolom za obradu osobnih podataka koja nije nužna za izvršenje tog ugovora.

6. PRAVA ISPITANIKA

Članak 16.

Bolnica poduzima odgovarajuće mjere kako bi se ispitaniku pružile sve informacije u vezi s obradom njegovih osobnih podataka u sažetom, transparentnom, razumljivom i lako dostupnom obliku, uz uporabu jasnog i jednostavnog jezika, osobito za svaku informaciju koja je posebno namijenjena djetetu.

Članak 17.

Bolnica pruža sljedeće informacije:

- d) identitet i kontaktne podatke voditelja obrade i, ako je primjenjivo, predstavnika voditelja obrade;
- e) kontaktne podatke službenika za zaštitu podataka
- f) svrhe obrade radi kojih se upotrebljavaju osobni podaci kao i pravnu osnovu za obradu;
- g) primatelje ili kategorije primatelja osobnih podataka
- h) ako je primjenjivo, činjenicu da namjerava osobne podatke prenijeti trećoj zemlji ili međunarodnoj organizaciji.

Članak 18.

Informacije se pružaju u pisanom obliku ili drugim sredstvima.

Ako to zatraži ispitanik, informacije se mogu pružiti usmenim putem, pod uvjetom da je neosporno utvrđen identitet ispitanika.

Bolnica će ispitaniku na zahtjev pružiti informacije u roku od mjesec dana od zaprimanja zahtjeva. Taj se rok može prema potrebi produljiti za dodatna dva mjeseca, ovisno o broju i složenosti zahtjeva Bolnica će obavijestiti ispitanika o svakom produljenju roka 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.

Članak 19.

Ako su zahtjevi ispitanika očito neutemeljeni ili pretjerani, osobito zbog njihova učestalog ponavljanja, Bolnica može:

- a) naplatiti razumno naknadu uzimajući u obzir administrativne troškove pružanja informacija ili obavijesti ili postupanje po zahtjevu
- b) odbiti postupiti po zahtjevu.

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

Članak 20.

Ispitanik ima pravo na pristup osobnim podacima koje Bolnica obraduje, tražiti ispravak netočnih podataka i dopuniti nepotpune osobne podatke davanjem dodatne izjave uzimajući u obzir svrhe obrade.

Članak 21.

Ispitanik ima pravo od Bolnice ishoditi ograničenje obrade ako je ispunjeno jedno od sljedećeg:

- a) ispitanik osporava točnost osobnih podataka, na razdoblje kojim se voditelju obrade omogućuje provjera točnosti osobnih podataka;
- b) obrada je nezakonita i ispitanik se protivi brisanju osobnih podataka te umjesto toga traži ograničenje njihove uporabe;
- c) voditelj obrade više ne treba osobne podatke za potrebe obrade, ali ih ispitanik traži radi postavljanja, ostvarivanja ili obrane pravnih zahtjeva;

Članak 22.

Pravo na brisanje („pravo na zaborav“) ograničeno je kada se obrada osobnih podataka ispitanika vrši radi zakonom i podzakonskim aktima utvrđenim obvezama Bolnice ili radi postavljanja, ostvarivanja ili obrane pravnih zahtjeva.

Članak 23.

Bolnica obavještava svakog primatelja o ispravku ili brisanju osobnih podataka ili ograničenju obrade. Bolnica obavještava ispitanika o tim primateljima ako to ispitanik zatraži.

7. OBVEZE VODITELJA OBRADE

Članak 24.

Bolnica provodi odgovarajuće tehničke i organizacijske mjere kako bi osigurala da se obrada provodi u skladu s Općom uredbom, pri tome uzimajući u obzir prirodu, opseg, kontekst i svrhe obrade, kao i rizike različitih razina vjerojatnosti i ozbiljnosti za prava i slobode pojedinaca. Te se mjere preispisuju i ažuriraju.

Članak 25.

Tehničkim i organizacijskim mjerama osigurava se da integriranim načinom budu obrađeni samo osobni podaci koji su nužni za svaku posebnu svrhu obrade. Ta se obveza primjenjuje na količinu prikupljenih osobnih podataka, opseg njihove obrade, razdoblje pohrane i njihovu dostupnost te se na taj način osigurava da osobni podaci nisu automatski, bez intervencije pojedinca, dostupni neograničenom broju pojedinca.

8. OBVEZE IZVRŠITELJA OBRADE

Članak 26.

Bolnica može za obradu podataka angažirati samo one izvršitelje obrade koji jamče provedbu odgovarajućih tehničkih i organizacijskih mjera sukladno zahtjevima Opće uredbe kojima se osigurava zaštita prava ispitanika.

Članak 27.

Izvršitelj obrade ne smije angažirati drugog izvršitelja obrade bez prethodnog posebnog ili opće pisanih odobrenja Bolnice.

Članak 28.

Obrada koju provodi izvršitelj obrade uređuje se ugovorom ili drugim pravnim aktom u skladu s važećim pravnim propisima Republike Hrvatske, Općom uredbom i Zakonom o provedbi Opće uredbe.

Članak 29.

Ugovorom ili drugim pravnim aktom uređuje se predmet i trajanje obrade, priroda i svrha obrade, vrsta osobnih podataka i kategorija ispitanika te obveze i prava Bolnice, a izvršitelj obrade obvezuje se da:

- a) obrađuje osobne podatke samo prema zabilježenim uputama Bolnice
- b) osigurava da su se osobe ovlaštene za obradu osobnih podataka obvezale na poštovanje povjerljivosti ili da podlige zakonskim obvezama o povjerljivosti;

- c) poduzima sve potrebne mjere vezane uz sigurnost obrade, sukladno s člankom 32. Opće uredbe;
- d) uzimajući u obzir prirodu obrade, pomaže Bolnici da ispunji obvezu voditelja obrade u pogledu odgovaranja na zahtjeve za ostvarivanje prava ispitanika iz poglavљa III Opće uredbe, primjenjujući odgovarajuće tehničke i organizacijske mjera
- e) pomaže Bolnici u osiguravanju usklađenosti s obvezama prema člancima od 32. do 36. Opće uredbe
- f) po izboru Bolnice, briše ili vraća Bolnici sve osobne podatke nakon dovršetka pružanja usluga vezanih za obradu te briše postojeće kopije osim ako postoji obveza pohrane osobnih podataka prema pravu Unije ili prema pravnim propisima Republike Hrvatske.
- g) Bolnici stavlja na raspolaganje sve informacije koje su neophodne za dokazivanje poštovanja obveza utvrđenih u ovom članku i koje omogućuju revizije.

Članak 30.

Ako izvršitelj obrade angažira drugog izvršitelja obrade za provođenje posebnih aktivnosti obrade u ime Bolnice, iste obveze za zaštitu podataka kao one koje su navedene u ugovoru ili drugom pravnom aktu između Bolnice i izvršitelja obrade vrijede i za drugog izvršitelja obrade sukladno ugovoru ili drugom pravnom aktu, a osobito obveza davanja dostatnih jamstava za provedbu odgovarajućih tehničkih i organizacijskih mjera na način da se obradom udovoljava zahtjevima iz ovog Pravilnika. Ako taj drugi izvršitelj obrade ne ispunjava obveze zaštite podataka, početni izvršitelj obrade ostaje u cijelosti odgovoran Bolnici za izvršavanje obveza tog drugog izvršitelja obrade.

Članak 31.

Ugovor ili drugi pravni akt kojim se uređuje pravni odnos između Bolnice i izvršitelja obrade te između izvršitelja obrade i drugog angažiranog izvršitelja obrade mora biti u pisnom obliku, uključujući elektronički oblik.

9. SLUŽBENIK ZA ZAŠTITU PODATAKA

Članak 32.

Bolnica imenuje službenika za zaštitu podataka, objavljuje njegove kontaktne podatke i o imenovanju obavještava Agenciju za zaštitu podataka.

Službenik za zaštitu podataka imenuje se na temelju stručnih kvalifikacija, a osobito stručnog znanja o pravu i praksama u području zaštite podataka.

Članak 33.

Službenik za zaštitu podataka obavlja sljedeće zadaće:

- a) informiranje i savjetovanje voditelja obrade ili izvršitelja obrade te zaposlenika koji obavljaju obradu o njihovim obvezama iz Opće uredbe i iz drugih pravnih propisa kojima je regulirano prikupljanje i obrada osobnih podataka

- b) praćenje poštovanja odredbi Opće uredbe te drugih odredaba o zaštiti podataka, raspodjela odgovornosti, podizanje svijesti i osposobljavanje zaposlenih koji sudjeluju u postupcima obrade.
- c) pružanje savjeta, kada je to zatraženo, u pogledu procjene učinka na zaštitu podataka i praćenje njezina izvršavanja u skladu s člankom 35. Opće uredbe
- d) suradnja s Agencijom za zaštitu osobnih podataka

Službenik za zaštitu podataka pri obavljanju svojih zadaća vodi računa o riziku povezanom s postupcima obrade i uzima u obzir prirodu, opseg, kontekst i svrhe obrade

10. EVIDENCIJA AKTIVNOSTI OBRADE

Članak 34

Bolnica vodi evidenciju aktivnosti obrade za koje je odgovorna. Ta evidencija sadržava sljedeće informacije:

- a) ime i kontaktne podatke voditelja obrade i, ako je primjenjivo, zajedničkog voditelja obrade, predstavnika voditelja obrade i službenika za zaštitu podataka;
- b) svrhe obrade
- c) opis kategorija ispitanika i kategorija osobnih podataka
- d) kategorije primateljâ kojima su osobni podaci otkriveni ili će im biti otkriveni, uključujući primatelje u trećim zemljama ili međunarodne organizacije
- e) ako je primjenjivo, prijenose osobnih podataka u treću zemlju ili međunarodnu organizaciju, uključujući identificiranje te treće zemlje ili međunarodne organizacije
- f) predviđene rokove za brisanje različitih kategorija podataka
- g) opći opis tehničkih i organizacijskih sigurnosnih mjera u obradi osobnih podataka

Evidencija obrade vodi se u pisnom obliku, uključujući i elektronički oblik.

Bolnica ili izvršitelj obrade te predstavnik Bolnice ili izvršitelja obrade, evidenciju daje na uvid Agenciji za zaštitu osobnih podataka kao nadzornom tijelu na njihov zahtjev.

11. SIGURNOST OSOBNIH PODATAKA

Članak 35.

Bolnica i angažirani izvršitelji obrade provode odgovarajuće tehničke i organizacijske mjere kako bi osigurali odgovarajuću razinu sigurnosti obrade osobnih podataka s obzirom na rizik, pri tome uzimaju u obzir najnovija dostignuća, troškove provedbe te prirodu, opseg, kontekst i svrhe obrade, kao i rizik različitih razina vjerojatnosti i ozbiljnosti za prava i slobode pojedinaca, uključujući prema potrebi:

- a) pseudonimizaciju i enkripciju osobnih podataka;
- b) sposobnost osiguravanja trajne povjerljivosti, cjelovitosti, dostupnosti i otpornosti sustava i usluga obrade;

- c) sposobnost pravodobne ponovne uspostave dostupnosti osobnih podataka i pristupa njima u slučaju fizičkog ili tehničkog incidenta;
- d) proces za redovno testiranje, ocjenjivanje i procjenjivanje učinkovitosti tehničkih i organizacijskih mjera za osiguravanje sigurnosti obrade.

Prilikom procjene odgovarajuće razine sigurnosti u obzir se posebno uzimaju rizici koje predstavlja obrada, posebno rizici od slučajnog ili nezakonitog uništenja, gubitka, izmjene, neovlaštenog otkrivanja osobnih podataka ili neovlaštenog pristupa osobnim podacima koji su preneseni, pohranjeni ili na drugi način obradivani.

Poštovanje odredbi ovog Pravilnika ponašanja dokazuje sukladnost sa zahtjevima iz stavka 1. ovog članka.

Svaki pojedinac koji djeluje pod odgovornošću voditelja obrade ili izvršitelja obrade obvezan je obrađivati osobne podatke prema uputama Bolnice kao voditelja obrade.

Članak 36.

U slučaju povrede osobnih podataka Bolnica bez nepotrebnog odgađanja, ako je izvedivo, najkasnije 72 sata nakon saznanja o toj povredi, izvješće nadzorno tijelo nadležno u skladu s člankom 55. Opće uredbe 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.

Izvršitelj obrade bez nepotrebnog odgađanja izvješće voditelja obrade nakon što sazna za povredu osobnih podataka.

U izvješćivanju nadzornog tijela mora se:

- 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.

Bolnica dokumentira sve povrede osobnih podataka, uključujući činjenice vezane za povredu osobnih podataka, njezine posljedice i mjere poduzete za popravljanje štete.

Članak 37.

U slučaju povrede osobnih podataka koje će vjerojatno prouzročiti visok rizik za prava i slobode pojedinaca, voditelj obrade bez nepotrebnog odgađanja obavješće ispitanika o povredi osobnih podataka.

Obavješćivanjem ispitanika iz stavka 1. ovog članka opisuje se priroda povrede osobnih podataka uporabom jasnog i jednostavnog jezika te ono sadržava informacije o službeniku za zaštitu podataka, opis vjerojatnih posljedica povrede osobnih podataka i mjere koje je Bolnica poduzela ili namjerava poduzeti za rješavanje problema povrede osobnih podataka.

Obavješćivanje ispitanika iz stavka 1. nije obvezno ako je ispunjen bilo koji od sljedećih uvjeta:

- a) Bolnica je poduzela odgovarajuće tehničke i organizacijske mjere zaštite i te su mjere primijenjene na osobne podatke pogodjene 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.

12. PRIJENOSI OSOBNIH PODATAKA TREĆIM ZEMLJAMA ILI MEĐUNARODNIM ORGANIZACIJAMA

Članak 38.

Prijenos osobnih podataka koji se obrađuju ili su namijenjeni za obradu nakon prijenosa u treću zemlju ili međunarodnu organizaciju moguće je isključivo u skladu s uvjetima propisanim u Poglavlju V Opće uredbe.

13. PRIJELAZNE I ZAVRŠNE ODREDBE

Članak 39.

U slučaju da odredbe ovog Pravilnika ne rješavaju pojedinačni slučaj obrade osobnih podataka, primjenjuju se odredbe Opće uredbe i Zakona o provedbi Opće uredbe te odredbe odgovarajućih pravnih propisa Republike Hrvatske.

Članak 40.

Ovaj Pravilnik objavljuje se na oglasnoj ploči Bolnice i na internetskoj stranici Bolnice s ciljem informiranja ispitanika čiji se osobni podaci obrađuju.

Pravilnik stupa na snagu osmog dana od dana objave na oglasnoj ploči Bolnice.

Ur. broj: 01-7-12/3-5-2018.

Predsjednica
Upravnog vijeća:

SPECIJALNA BOLNICA ZA
MEDICINSKU REHABILITACIJU
6 STUBIČKE TOPLICE

Ana Klanjčić, dr. dent. med.

Pravilnik je objavljen na oglasnoj ploči Bolnice te na vidljivom mjestu u zajedničkim prostorijama ustrojstvenih jedinica dana 24.12. 2018. godine, a stupio je na snagu dana 02.01. 2019. godine.

Ravnatelj:

Davor Gredičak, dr. med.

spec. fizijatar

SPECIJALNA BOLNICA ZA
MEDICINSKU REHABILITACIJU
2 STUBIČKE TOPLICE