

**SPECIJALNA BOLNICA ZA
MEDICINSKU REHABILITACIJU
VARAŽDINSKE TOPLICE**

**POLITIKA ZAŠTITE OSOBNIH PODATAKA
U SPECIJALNOJ BOLNICI VARAŽDINSKE TOPLICE**

svibanj 2018. godine

Temeljem članka 13. Statuta Specijalne bolnice za medicinsku rehabilitaciju Varaždinske Toplice a sukladno odredbama Opće uredbe o zaštiti podataka (Uredba EU 2016/679) i odredbama Zakona o provedbi Opće uredbe o zaštiti podataka (NN.br. 42/18), Upravno vijeće Specijalne bolnice Varaždinske Toplice je na 26. sjednici održanoj dana 30. svibnja 2018. godine donijelo slijedeći akt

POLITIKA ZAŠTITE OSOBNIH PODATAKA

I. POJMOVNIK

Osobni podatak - podatak koji se odnosi na pojedinca (ispitanika) čiji je identitet utvrđen ili se može utvrditi

Ispitanik - osoba koja se može identificirati izravno ili neizravno, osobito uz pomoć identifikatora kao što su ime i prezime, adresa stanovanja, identifikacijski broj, podatci o lokaciji, mrežni identifikator ili uz pomoć jednog ili više čimbenika svojstvenih za fizički, fiziološki, genetski, mentalni, ekonomski, kulturni ili socijalni identitet tog pojedinca

Obrada osobnih podataka - svaki postupak ili skup postupaka koji se obavljaju na osobnim podacima ili na skupovima osobnih podataka, bilo automatiziranim bilo neautomatiziranim sredstvima kao što je 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;

Podatci koji se odnose na zdravlje - osobni podatci povezani s fizičkim ili mentalnim zdravljem pojedinca, uključujući pružanje zdravstvenih usluga, kojima se daju informacije o njegovu zdravstvenom statusu;

Biometrijski podatci - osobni podatci 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 podatci ;

Voditelj obrade - fizička ili pravna osoba, koja sama ili zajedno s drugima određuje svrhe i sredstva obrade osobnih podataka;

Izvršitelj obrade - fizička ili pravna osoba, koja obrađuje osobne podatke u ime voditelja obrade;

Osobe ovlaštene za obradu – radnici i sve fizičke osobe koje obrađuju osobne podatke temeljem ovlasti izdane od ovlaštene osobe Bolnice i u okviru svoje dužnosti, temeljem opisa poslova svojeg radnog mjesta;

Primatelj - fizička ili pravna osoba, tijelo javne vlasti, agencija ili drugo tijelo kojem se otkrivaju osobni podatci , neovisno o tome je li on treća strana;

Informacijski sustav - sveobuhvatnost tehnološke infrastrukture, organizacije, ljudi i postupaka za prikupljanje, obradu, generiranje, pohranu, prijenos, prikaz te distribuciju informacija kao i raspolaganje njima. Informatički sustav moguće je definirati i kao međudjelovanje informacijske tehnologije, podataka i postupaka za procesiranje podataka te ljudi koji prikupljaju navedene podatke i njima se koriste;

Nadzorno tijelo - neovisno tijelo javne vlasti koje je osnovala Republika Hrvatska u svrhu kontrole i osiguranja provođenja Uredbe;

Povjerljivost - svojstvo informacija (podataka) da nisu dostupne ili otkrivene neovlaštenim subjektima;

Integritet - svojstvo informacija (podataka) i procesa da nisu neovlašteno ili nepredviđeno mijenjani;

Privola - 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;

Mjere sigurnosti – zaštitne i organizacijske mjere koje se poduzimaju radi osiguranja odgovarajuće razine sigurnosti osobnih podataka i privatnosti, primjereno rizicima i drugim obvezama određenim važećim propisima, uključujući aktivnosti koje se poduzimaju u slučaju povrede osobnih podataka, kako bi se spriječili i/ili smanjili nepovoljni učinci eventualne povrede;

Pseudonimizacija - obrada osobnih podataka na način da se osobni podatci 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 Politike zaštite osobnih podataka Bolnice, kako bi se osiguralo da se osobni podatci ne mogu pripisati pojedincu čiji je identitet utvrđen ili se može utvrditi;

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;

Izrada profila – 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, zdravljem, osobnim sklonostima, interesima, pouzdanošću, ponašanjem, lokacijom ili kretanjem tog pojedinca;

Sustav pohrane - svaki strukturirani skup osobnih podataka dostupnih prema posebnim kriterijima, bilo da su centralizirani, decentralizirani ili raspršeni na funkcionalnoj osnovi;

Treće strane –fizička ili pravna osoba, tijelo javne vlasti, agencija ili drugo tijelo koje nije ispitanik, voditelj obrade, izvršitelj obrade i osobe koje su ovlaštene za obradu osobnih podataka pod izravnom nadležnošću voditelja obrade ili izvršitelja obrade;

Distributivni kanali - predstavljaju sredstva i načine preko kojih je omogućen pristup, ugovaranje, narudžba proizvoda i usluga Bolnice te slanje informacija i ponuda vezanih uz proizvode i usluge Bolnice, a obuhvaćaju komunikaciju između Bolnice i ugovornih partnera (pravnih i fizičkih osoba) putem elektronske pošte i web stranice Bolnice: www.mikerva.hr, te ostalo. Informacije o dostupnim distributivnim kanalima Bolnice je korisniku u svakom trenutku dostupna pozivom na tel. centralu Bolnice ili druge kontakte objavljene na web stranici Bolnice.

Obvezujuća poslovna pravila – predstavljaju politike zaštite osobnih podataka kojih se voditelj obrade ili izvršitelj obrade s poslovnim nastanom na državnom području države članice EU pridržava za prijenose ili skupove prijenosa osobnih podataka voditelju obrade ili izvršitelju obrade u jednoj ili više zemalja unutar EU ili trećih zemalja, pravnih i fizičkih osoba, odnosno poduzeća koja se bave zajedničkom ili sličnom djelatnošću.

Ostali pojmovi koji se koriste u ovoj Politici imaju isto značenje kao u Općoj uredbi i važećim propisima o zaštiti osobnih podataka.

II. TEMELJNE ODREDBE

Zaštita podataka zauzima značajno mjesto u poslovanju Specijalne bolnice Varaždinske Toplice (u daljnjem tekstu: Bolnica) koja u svom svakodnevnom poslovanju prikuplja i obrađuje osobne podatke korisnika usluga (pacijenata, gostiju i dr.), radnika, poslovnih partnera ili drugih osoba s kojima ostvaruje poslovnu suradnju (u daljnjem tekstu: ispitanici). Ovom Politikom se definiraju osnovna načela i pravila zaštite osobnih podataka u skladu s

poslovnim i sigurnosnim zahtjevima Bolnice, kao i zakonskim propisima, najboljim praksama i međunarodno prihvaćenim standardima.

Politika zaštite osobnih podataka (u daljnjem tekstu: Politika) je temeljni akt koji opisuje svrhu i ciljeve prikupljanja, obrade i upravljanja osobnim podacima unutar Bolnice, a koji se temelji na vodećim svjetskim praksama iz područja zaštite osobnih podataka. Politika osigurava adekvatnu razinu zaštite podataka u skladu s Općom uredbom o zaštiti podataka* (u nastavku: Uredba) i drugim primjenjivim važećim zakonima vezanim uz zaštitu osobnih podataka što Bolnica dodatno osigurava detaljnim internim aktima.

** UREDBA (EU) 2016/679 EUROPSKOG PARLAMENTA I VIJEĆA (GDPR) 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)*

III. OPSEG I CILJ

Politika zaštite osobnih podataka je temeljni akt Bolnice koji za svrhu ima uspostavljanje okvira zaštite osobnih podataka sukladno Uredbi. Politika utvrđuje pravila povezana sa zaštitom pojedinaca u pogledu prikupljanja i obrade osobnih podataka i pravila povezana sa slobodnim kretanjem osobnih podataka.

Cilj Politike je uspostaviti primjerene procese zaštite i upravljanja osobnim podacima ispitanika, odnosno korisnika usluga, radnika, poslovnih partnera Bolnice i drugih osoba čiji se osobni podatci obrađuju u Bolnici i u komunikaciji Bolnice sa poslovnim partnerima.

Politika se primjenjuje na sve obrade osobnih podataka unutar Bolnice osim u slučajevima gdje se obrađuju anonimizirani podatci ili su obrade takve prirode da se radi o statističkim analizama iz kojih nije moguće identificirati pojedinca.

IV. NAČELA OBRADE PODATAKA

Načela obrade podataka su osnovna pravila kojih se Bolnica pridržava prilikom obrade osobnih podataka ispitanika, a obrade koje se provode sukladno niže navedenim načelima smatraju se zakonitima.

Svaka ustrojstvena jedinica Bolnice dužna je osigurati pridržavanje niže navedenih načela unutar vlastite domene i prilikom obrade osobnih podataka za koje je ustrojstvena jedinica utvrđena kao voditelj obrade.

Bolnica osobne podatke obrađuje u skladu sa sljedećim načelima obrade:

1. Zakonito i pošteno – s obzirom na ispitanike i njihova prava, Bolnica će obrađivati osobne podatke ispitanika sukladno važećim zakonima i poštujući sva prava ispitanika. Bolnica će ponekad ispitanike morati pitati i za neke osobne podatke koji nisu potrebni za ostvarenje konkretne usluge, no zakonom su obvezni za prikupljanje (npr. Zakon o mirovinskom osiguranju, Zakon o zaštiti prava pacijenata, Zakon o sprečavanju pranja novca i financiranja terorizma idr.). U skladu s tim, u Bolnici su definirana jasna pravila i procesi kako bi se osigurala zakonita i poštena obrada, a uspostavljeni su i kontrolni mehanizmi (npr. periodične revizije, tehničke mjere);

2. Transparentno – Bolnica će osigurati transparentnost obrade osobnih podataka te će, sukladno Uredbi, pružiti ispitanicima sve potrebne informacije i na zahtjev osigurati ispitanicima uvid u njihove podatke, obrazloženje obrade, temelje i zakonitosti obrade i sl. Kroz ovu Politiku, ali i kroz druge kanale koje će biti dostupni ispitanicima, Bolnica će osigurati informacije ispitanicima kako se osobni podatci koji se odnose na njih prikupljaju,

upotrebljavaju, daju na uvid ili na drugi način obrađuju, kao i do koje se mjere ti osobni podatci obrađuju ili će se obrađivati. Ispitanik će biti pravovremeno, odnosno prije samog prikupljanja podataka, upoznat sa svim relevantnim informacijama;

3. Uz ograničenje svrhe – osobni podatci moraju biti prikupljeni u posebne, izričite i zakonite svrhe te se dalje ne smiju obrađivati na način koji nije u skladu s tim svrhama. Primjerice, ako je ispitanik ustupio set osobnih podataka (npr. ime, prezime, OIB, status osiguranja, podatci o zdravstvenom stanju, visina primanja, broj računa i naziv banke i sl.) u svrhu realizacije nekog prava, Bolnica iste podatke neće obrađivati u neku drugu svrhu, osim ako postoje druge obrade koje su uvjetovane zakonom ili su neophodne za kvalitetno isporučivanje same usluge;

4. Uz ograničenje pohrane – Bolnica osigurava da su osobni podatci ispitanika čuvani u obliku koji omogućuje identifikaciju ispitanika samo onoliko dugo koliko je to potrebno u svrhu radi koje se osobni podatci obrađuju. Bolnica osobne podatke može pohraniti i dulje, ali za to mora imati jasnu svrhu u smislu zakonske obveze (npr. Zakona o arhivskom gradivu i arhivima) ili zakonski interes (npr. u slučaju sudskog spora);

5. Koristeći samo potrebne podatke (smanjenje količine podataka) – Bolnica osobne podatke prikuplja i obrađuje na način da su primjereni, relevantni i ograničeni na ono što je nužno u odnosu na svrhu za koju se obrađuju. Procesi u Bolnici su dizajnirani na način da se ne prikupljaju podatci za koje ne postoji opravdana potreba za prikupljanjem. Bolnica osigurava da se ovo načelo adekvatno primjenjuje;

6. Točnost – Bolnica osigurava da su podatci točni i prema potrebi ažurni; mora se poduzeti svaka razumna mjera radi osiguravanja da se osobni podatci koji nisu točni, uzimajući u obzir svrhu za koju se obrađuju, bez odlaganja izbrišu ili isprave. Bolnica osigurava primjenu ovog načela na način da je uspostavila redovite kontrole ali i transparentan proces komunikacije s ispitanicima kroz koji se može zatražiti ispravak podataka u slučaju da ispitanik primijeti da neki od njegovih osobnih podataka nije ispravno naveden;

7. Osigurava sigurnost, nadzor i kontrolu nad podacima i obradama podataka (Cjelovitost i povjerljivost) – Bolnica prikuplja i obrađuje podatke 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. Bolnica će u razumnom roku implementirati IT sustave koji će imati za cilj detekciju i sprječavanje curenja podataka, sustave za anonimizaciju/pseudonimizaciju podataka, metode nadzora nad pristupom podataka, ograničenja pristupa podacima sukladno potrebi radnog mjesta i sl.

Sukladno navedenim načelima, podacima ispitanika pristupat će radnici Bolnice ovisno o njihovim ovlaštenjima i radnim mjestima, kako bi uspješno ispunili poslove definirane za njihovo radno mjesto. Također dio usluga za Bolnicu obavljaju i druge pravne osobe s kojima će podatci ispitanika biti podijeljeni samo ako su oni nužni za potrebe ispunjenja obveza iz zajedničkih Ugovora. Primjer toga je izdavanje popratne medicinske dokumentacije prilikom premještanja pacijenta, dostava podataka o radnicima Bolnice ZZJZ, pohrana dokumentacije u državni arhiv ili slanje medicinske dokumentacije i stvari pacijenta/gosta na kućnu adresu. Bolnica će podatke ispitanika proslijediti određenim fizičkim ili pravnim osobama ili državnim institucijama u slučaju kada za to postoji zakonska osnova (primjerice: za potrebe jedinstvenog registra REGZAP, COP, CEZIH, HZZO, ZZJZ i FINA-e i dr).

V. ZAKONITOST OBRADE

Bolnica osobne podatke ispitanika smatra njihovim vlasništvom te se prema njima tako i odnosi. Međutim, kako bi Bolnica bila u mogućnosti pružiti uslugu ispitaniku, a sukladno niže navedenim zakonitostima, potrebno je obrađivati minimalan set podataka neophodan za kvalitetno pružanje pojedine usluge. U suprotnom, odnosno ako ispitanik odbije ustupiti traženi set podataka, Bolnica neće biti u mogućnosti pružiti mu uslugu.

Sukladno tome, osobni podatci ispitanika obrađuju se kada je zadovoljen jedan od niže navedenih uvjeta:

a) obrada je nužna za izvršavanje ugovora u kojem je ispitanik stranka (pacijent, gost, djelatnik) ili kako bi se poduzele radnje na zahtjev ispitanika prije sklapanja ugovora;

b) obrada je nužna radi poštovanja pravnih obveza Bolnice (važeći zakonski propisi prema kojima je Bolnica dužna postupati) - u svakom trenutku kada zakon Bolnicu ovlašćuje ili obvezuje na određenu obradu, Bolnica će temeljem tog zakona obrađivati osobne podatke ispitanika. Na primjer, u slučaju postojanja zakonske obveze, kao što je Zakon o radu, Zakon o zaštiti na radu, Zakon o zdravstvenoj zaštiti, Zakon o obveznom zdravstvenom osiguranju, Zakon o sprječavanju pranja novca i financiranju terorizma, Bolnica će prikupljati i obrađivati zakonski definiran set podataka, te u slučaju da ispitanik odbije ustupiti traženi set podataka, Bolnica neće biti u mogućnosti pružiti mu uslugu;

c) obrada je nužna za potrebe legitimnih interesa Bolnice ili treće strane - osim kada su od tih interesa jači interesi ili temeljna prava i slobode ispitanika koji zahtijevaju zaštitu osobnih podataka, osobito ako je ispitanik dijete. Pod legitimnim interesom Bolnice podrazumijevaju se obrade koje služe kako bi se pružile kvalitetne usluge, unaprijedio proces rad, razvoj usluga i proizvoda i unapređenje poslovanja, modernizirale usluge, ponudili proizvodi i usluge za koje je razvidno da bi korisnicima olakšale poslovanje s Bolnicom, unaprijedilo njegovo zdravlje te u korist rješavanja sudskih sporova;

d) ispitanik je dao privolu za obradu svojih osobnih podataka u jednu ili više posebnih svrha - privola mora biti dokaziva i dobrovoljna, napisana lako razumljivim jezikom i ispitanik ima pravo u svakom trenutku povući svoju privolu (povlačenje privole mora biti jednako jednostavno kao i davanje privole). Bolnica će ispitanika zatražiti privole za obrade podataka i kontaktiranje zbog potreba direktnog marketinga putem kontakt podatka koje je ispitanik ustupio Bolnici. Prezentaciju novih proizvoda i usluga, određene usluge koje Bolnica komunicira putem dostupnih distributivnih kanala, Bolnica smatra dijelom usluge te za to neće zatražiti privolu ispitanika dok je sama obrada u skladu s načelima obrade navedenih u točki V. te se temelji na nekoj od navedenih zakonitosti obrade;

e) obrada je nužna kako bi se zaštitili ključni interesi ispitanika ili druge fizičke osobe;

f) obrada je nužna za izvršavanje zadaće od javnog interesa ili pri izvršavanju službene ovlasti voditelja obrade;

Svaka ustrojstvena jedinica unutar Bolnice dužna je identificirati zakonitost za svaku obradu koja je u njihovoj poslovnoj domeni. Pri identifikaciji zakonitosti obrade konzultirat će se Službenik za zaštitu podataka koji će prema jasnim i unaprijed definiranim kriterijima savjetovati radnike ustrojstvene jedinice prilikom identifikacije zakonitosti obrada.

VI. PRAVA ISPITANIKA

Bolnica je svjesna kako su osobni podatci ispitanika njegovo vlasništvo te iako su joj ti podatci neophodni za pružanje usluga, ispitanici u svakom trenutku zadržavaju određena prava u odnosu na obradu njihovih podataka te Bolnica podatke prikuplja i obrađuje samo uz postojanje gore navedenih zakonitosti obrade.

Bolnica će u trenutku prikupljanja informacija ispitaniku pružiti sljedeće informacije: identitet i kontaktne podatke voditelja obrade, kontaktne podatke službenika za zaštitu podataka, svrhe obrade radi kojih se upotrebljavaju osobni podatci kao i pravnu osnovu za obradu, legitimne interese, primatelje ili kategorije primatelja osobnih podataka, namjeru prijenosa osobnih podataka trećim zemljama (ako postoji), razdoblje pohrane podataka ili kriterije koji definiraju to razdoblje, prava vezana uz privole, potencijalno postojanje automatiziranog donošenja odluka što podrazumijeva i izradu profila (smislene informacije o kojoj je logici obrade riječ te potencijalnim posljedicama i važnosti same obrade za ispitanika) te postojanje niže navedenih prava. U slučaju da se podatci ne prikupljaju izravno od ispitanika, uz navedene podatke navodi se i izvor osobnih podataka.

Bolnica osobne podatke obrađuje sukladno pravima ispitanika definiranim unutar Uredbe, a koja su navedene u nastavku:

1. Pravo na brisanje („pravo na zaborav“) - ispitanik ima pravo od Bolnice ishoditi brisanje osobnih podataka koji se na njega odnose, a Bolnica ima obvezu obrisati osobne podatke bez nepotrebnog odgađanja ako je ispunjen jedan od sljedećih uvjeta:

- a. osobni podatci više nisu nužni u odnosu na svrhu za koje su prikupljeni ili na drugi način obrađeni,
- b. ispitanik povuče privolu na kojoj se obrada temelji, a ne postoji druga pravna osnova za obradu,
- c. ispitanik uložiti prigovor na obradu, a legitimni razlozi za realizaciju prava na brisanje imaju veću težinu od legitimnog interesa Bolnice za obradu i/ili čuvanje osobnih podataka,
- d. osobni podatci su nezakonito obrađeni,
- e. osobni podatci se moraju brisati radi poštivanja određene pravne obveze;

2. Pravo na pristup podacima - ispitanik ima pravo dobiti od Bolnice potvrdu obrađuju li se njegovi osobni podatci te ako se takvi osobni podatci obrađuju, pristup osobnim podacima i pojašnjenje o svrsi obrade, kategorijama podataka, potencijalnim primateljima kojima će osobni podatci biti otkriveni, i sl.;

3. Pravo na ispravak - ispitanik ima pravo bez nepotrebnog odgađanja ishoditi od Bolnice ispravak netočnih osobnih podataka koji se na njega odnose. Uzimajući u obzir svrhu obrade, ispitanik ima pravo dopuniti nepotpune osobne podatke, među ostalim i davanjem dodatne izjave. Dodatno, ispitanici imaju obvezu ažuriranja osobnih podataka u poslovnom odnosu s Bolnicom;

4. Pravo na prijenos podataka - ispitanik ima pravo tražiti prijenos (ispis) osobnih podataka koji se odnose na njega, a koje je pružio Bolnici u strukturiranom, uobičajeno korištenom i strojno čitljivom formatu te ima pravo prenijeti te podatke drugom voditelju obrade. Potrebno je uzeti u obzir da se pravo prijenosa odnosi isključivo na osobne podatke ispitanika;

6. Pravo na prigovor - ispitanik ima pravo na temelju svoje posebne situacije u svakom trenutku uložiti prigovor na obradu osobnih podataka koji se odnose na njega. Bolnica u

takvoj situaciji više ne smije obrađivati osobne podatke osim ako dokaže da postoje uvjerljivi legitimni razlozi za obradu koji nadilaze interese, prava i slobode ispitanika ili radi postavljanja, ostvarivanja ili obrane pravnih zahtjeva. Nadalje, ako se osobni podatci obrađuju za potrebe izravnog marketinga, ispitanik u svakom trenutku ima pravo uložiti prigovor na obradu osobnih podataka koji se na njega odnose za potrebe takvog marketinga, što uključuje izradu profila u mjeri koja je povezana s takvim izravnim marketingom;

7. Pravo na ograničenje obrade – ispitanik ima pravo od Bolnice tražiti ograničenje obrade podataka kada smatra da je obrada nezakonita te se protiviti brisanju osobnih podataka i umjesto toga traži ograničenje njihove uporabe. U slučaju kada je ispitanik uložio prigovor na obradu i očekuje potvrdu nadilaze li legitimni razlozi voditelja obrade razloge ispitanika, Bolnica je dužna u razumnom roku izdati takvu potvrdu.

Ispitanik ima pravo u svakom trenutku zahtijevati realizaciju bilo kojeg od gore navedenih prava. Bolnica ispitaniku na zahtjev pruža informacije o poduzetim radnjama vezanim uz navedena prava, najkasnije u roku od 3 mjeseca od zaprimanja zahtjeva (ovisno o količini i kompleksnosti zahtjeva) - svi zahtjevi će se pokušati riješiti unutar 1 mjeseca. Rok će se produljiti najviše za dodatna 2 mjeseca kada je to nužno. Ako Bolnica ne postupi po zahtjevu ispitanika bez odgađanja odnosno najkasnije jedan mjesec od primitka zahtjeva, izvijestit će ispitanika o razlozima zbog kojih nije postupila po zahtjevu. Razlozi za ne postupanje po zahtjevu podrazumijevaju postojanje zakonskih razloga i obveze obrade koja Bolnicu onemogućava u postupanju.

Dodatno, ispitanik ima pravo tražiti da se na njega ne odnosi odluka koja se temelji isključivo na automatiziranoj obradi, uključujući izradu profila, koja proizvodi pravne učinke koji se na njega odnose ili na njega značajno utječu, osim ako je ta odluka:

- potrebna za sklapanje ili izvršenje ugovora između ispitanika i Bolnice
- dopuštena zakonom
- temeljena na izričitoj privoli ispitanika.

VII. OBVEZE BOLNICE SUKLADNO UREDBI (Mjere sigurnosti)

Bolnica sukladno Uredbi na sebe preuzima određene obveze. Obveze ovise o ulozi u kojoj se Bolnica nalazi u odnosu na određenu obradu podataka. Bolnica se u nekim poslovnim procesima pojavljuje kao voditelj obrade, u drugima kao zajednički voditelj obrade, a može biti i izvršitelj obrade. Bolnica je voditelj obrade u poslovnim procesima gdje je samostalno odredila svrhu i način obrade podataka, dok je zajednički voditelj obrade u poslovnim procesima gdje s drugim voditeljima obrade, npr. poslovnim partnerima (HZZO; MZ; Agencije; Osiguravajuća Društva, JLU i dr) određuje svrhu i načine obrade osobnih podataka korisnika usluga. Pojedina ustrojstvena cjelina (odjeli Bolnice) mogu biti izvršitelji obrade u situacijama u kojima obrađuju podatke u ime voditelja obrade (npr. vođenje evidencije rada, rješavanje pojedinačnih prava radnika, vođenje medicinske dokumentacije i postupovnika, predlaganje elementa ugovora o uslugama sa drugom pravnom osobom, prosljeđivanje popisa korisnika usluga temeljem zaključenog ugovora i dr.).

Bolnica kontinuirano provodi odgovarajuće tehničke i organizacijske mjere zaštite uzimajući u obzir prirodu, opseg, kontekst i svrhu obrade, kao i rizike različitih razina utjecaja, vjerojatnosti i ozbiljnosti ugroze prava i slobode ispitanika.

Spomenute mjere uključuju provedbu odgovarajućih politika zaštite podataka:

- Bolnica osigurava dovoljne mjere fizičke sigurnosti za poslovne prostore u kojima se nalaze uređaji i sustavi koji se koriste za obradu osobnih podataka smještajem opreme u zaštićene prostorije s ograničenim pristupom (mrežna jedinica i računala u nadziranim prostorima, ormari sa mogućnošću zaključavanja za priručno odlaganje spisa s podacima, arhiva pod nadzorom i dr), kako bi isti bili dostupni samo ovlaštenim osobama (radnicima). Na svim razinama u objektima Bolnice, odnosno u neposrednoj blizini prostorija u kojima se nalaze računala, ormari i drugi spremnici osobnih podataka, te neposrednoj blizini arhive instalirati su aparati za gašenje požara, uz upute za uporabu. Za računala i ostale radne jedinice će se osigurati izvor neprekidnog napajanja. U prostorijama u kojima se nalaze računala ne smiju se nalaziti izvori čestica agresivne prašine, lakozapaljivih sredstava ili tekućina, električnih ili magnetskih polja, te vode, što će nadzirati voditelji pojedinih ustrojstvenih jedinica;

- Osobni podatci ispitanika čuvaju se u skladu s internim standardima sigurnosti Bolnice. Bolnica kontinuirano poduzima značajne organizacijske i tehničke mjere kako bi zaštitila osobne podatke ispitanika. Gdje je to primjenjivo, Bolnica primjenjuje kriptografske metode zaštite podataka te kontinuirano radi na unaprjeđenju sigurnosnih mjera na razini Bolnice. Uz navedeno, koriste se napredni alati za zaštitu i sprječavanje curenja podataka, nadziru se kritični sustavi unutar Bolnice i sl., tako da će sva računala, uključujući i prijenosne i mobilne uređaje redovito ažurirati pomoću sigurnosnih programskih alata tj. ispravaka koje izdaje proizvođač operativnog i aplikacijskog sustava;

- Bolnica ne dopušta neovlašteno prikupljanje, obradu ili korištenje osobnih podataka. Primjenjuje se pravilo ograničavanja pristupa podacima samo na one podatke koji su potrebni za obavljanje pojedinih poslovnih zadataka. U skladu s tim, jasno su definirane uloge i odgovornosti unutar Bolnice. Radnicima Bolnice je strogo zabranjeno korištenje osobnih podataka ispitanika u bilo koju svrhu koja nije u skladu s uvjetima definiranim u poglavlju V. ove Politike (*V. Zakonitost obrade*). Dodatno se naglašava da pojedine ustrojstvene jedinice unutar Bolnice, a sukladno važećim zakonima (npr. Zakon o zdravstvenoj zaštiti, Zakon o dopunskom osiguranju, Zakon o sprječavanju pranja novca i financiranja terorizma i dr.) imaju pravo uvida i obrade dijela osobnih podataka u opsegu koji je potreban da bi se ispunili regulirani zahtjevi ili kako bi se izvršio ugovor s ispitanikom ili njegovom agencijom (zavodom), odnosno realizirala usluga temeljem traženja i/ili odobrenja (narudžbenice). Ti procesi su pod strogom kontrolom i obuhvaćeni su sustavima nadzora i mehanizmima zaštite poslovnih procesa od neovlaštenog pristupa (neodobrenim modifikacijama, kopiranjima, brisanjem, pregledavanjem i prosljeđivanjem);

-Bolnica će u primjerenom roku implementirati sustav identifikacije i autorizacije korisnika na svim uređajima i sustavima koji se koriste za obradu osobnih podataka na način da bude moguće jednoznačno odrediti aktivnosti svakog pojedinog korisnika (korisničko ime, zaporka ili PIN, registriranje vremena korištenja podataka i sl.). Bolnica koristi samo ovlašteni i uredno licencirani softver na svim uređajima tj. radnim stanicama, prijenosnim i mobilnim uređajima, definirala je i koristiti snažne zaporce, izbjegava uporabu jedinstvenih korisničkih imena i zaporki za više ovlaštenih osoba. Bolnica je aktivirala antivirusni sustav na svim uređajima, fiksnim i prijenosnim računalima i mobilnim uređajima, te je osigurala da antivirusni sustav permanentno radi, radi čega ga redovito ažurira s najnovijim nadogradnjama prema preporuci proizvođača;

- Osobni podatci se štite od neovlaštenog pristupa, korištenja, izmjene i gubitka. Mehanizmi zaštite se primjenjuju na osobne podatke unutar Bolnice bez obzira u kojem se obliku oni

čuvaju, papirnatom ili elektroničkom. Kod spremanja elektroničkih podataka na vanjske medije (CD, Disk, USB, i sl.) podatci će se dodatno zaštititi zaporkom ili kriptirati kako ne bi bili čitljivi u slučaju neovlaštenog pristupa (uslijed gubitka ili krađe). Bolnica će prilikom otpisa i ekološkog zbrinjavanja računala i računalne opreme osigurati da su svi podatci trajno i nepovratno izbrisani korištenjem nekog od alata za sigurno brisanje i fizičko uništenje;

■ Za obradu podataka dobivenih temeljem video nadzora donijet će se poseban interni akt o video nadzornom sustavu koji će uključiti svrhu i pravni temelj postavljanja sustava video nadzora. Navedenim aktom će se utvrditi lista osoba s pravom pristupa u datoteku video nadzora, procedura za pohranu i brisanje snimaka, obveza isticanja oznake da je prostor pod video nadzorom - s podacima Bolnice, utvrdit će se metode fizičke zaštita uređaja za pohranu snimaka koje odgovaraju opremi za obradu osobnih podataka. U navedenom internom aktu će se utvrditi da video nadzor mora biti postavljen tako da snimka bude odgovarajućeg opsega i sadržaja, te ujedno paziti na privatnost, naročito kod video nadzora pacijenata u zajedničkim prostorima i radnika na radnom mjestu;

- Bolnica će osigurati poslovna pravila (kodeks) temeljem kojih će radnici Bolnice biti obvezni pridržavati se odredbi ove Politike te ostalih politika i procedura vezanih uz zaštitu podataka što će se također redovito provjeravati unutar Bolnice od strane nadležnih osoba. Bolnica će onemogućiti pristup prostorijama, sustavima i opremi ranije ovlaštenim osobama tj. radnicima koji su raskinuli radni odnos s Bolnicom i to danom prestanka ovlaštenja odnosno raskida radnog odnosa. Provjeru pridržavanja odredbi ove Politike i ostalih politika ili drugih akata i pravnih propisa iz domene zaštite osobnih podataka provodi Službenik za zaštitu podataka.

VIII. OBRADA POSEBNIH KATEGORIJA OSOBNIH PODATAKA

Bolnica ne obrađuje podatke koji otkrivaju rasno ili etničko podrijetlo, politička mišljenja, vjerska ili filozofska uvjerenja, članstvo u sindikatu i drugoj asocijaciji ili seksualnoj orijentaciji pojedinca.

Obrada gore navedenih posebnih kategorija osobnih podataka provodit će se od strane Bolnice iznimno u sljedećim uvjetima:

- 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 ili ispitanika (radnika) u području radnog prava i prava o socijalnoj sigurnosti te socijalnoj zaštiti u mjeri u kojoj je to odobreno u okviru prava Europske Unije, prava Republike Hrvatske ili kolektivnog ugovora u skladu s pravom Republike Hrvatske koje propisuje odgovarajuće zaštitne mjere za temeljna prava i interese ispitanika;
- obrada je nužna za zaštitu životno važnih interesa ispitanika ili drugog pojedinca;
- obrada se odnosi na osobne podatke za koje je očito da ih je objavio sam ispitanik;
- obrada je nužna za uspostavu, ostvarivanje ili obranu pravnih zahtjeva.

Bolnica posebno štiti osobne podatke djece, budući su djeca manje svjesna rizika, posljedica, raspoloživih zaštitnih mjera te svojih prava u vezi s obradom osobnih podataka. Djecom se smatraju osobe mlađe od šesnaest godina.

IX. AUTOMATSKA OBRADA PODATAKA

Obrada podataka i donošenje odluka temeljem automatske obrade sastavni je dio poslovanja Bolnice i kao takva je neophodna, a provodi se:

- sukladno važećim zakonima kojima podliježe Bolnica, među ostalim u svrhu: praćenja „liste čekanja“, radom u aplikaciji CEZIH, vođenjem podataka o radnicima radom u aplikaciji REGZAP, vođenja evidencije rada i obračuna plaća putem aplikacije COP, vođenje evidencije i prijava gostiju u aplikaciju eVisitor, izrade u računalnim programima odgovarajućih pojedinačnih akata o pravima i obvezama ispitanika, provođenja ostalih poslovnih procesa;
- u osiguravanju i provođenju mjera pouzdanosti i sigurnosti usluge koju pruža Bolnica;
- ako je nužno za sklapanje ili izvršavanje ugovora između ispitanika i voditelja obrade što uključuje unaprjeđenje poslovanja i određenih obrada koje su sastavni dio IT sustava i sl.;
- kada je ispitanik izričito dao svoju privolu.

U skladu s Uredbom, Bolnica omogućava ispitanicima pravo prigovora na automatsku ali i ručnu obradu podataka u svrhu zdravog marketinga, uključujući izradu profila u mjeri u kojoj je povezana s takvim izravnim marketingom, bilo u odnosu na početnu ili daljnju obradu, u bilo koje vrijeme i besplatno.

X. PRIJENOS OSOBNIH PODATAKA

Bolnica čini jedinstvenu cjelinu u nastupanju prema vanjskim subjektima, a surađuje sa ostalim zdravstvenim ustanovama i ostalim subjektima u zdravstvu i drugim pravnim osobama na više razina i u cilju pružanja što kvalitetnije usluge. Kako bi se ova suradnja mogla odvijati nesmetano postoji potreba za razmjenom osobnih podataka između Bolnice i tih pravnih osoba.

Bolnica s vanjskim subjektima međusobno razmjenjuje osobne podatke ako je to potrebno kako bi se ispitaniku pružila usluga koju je zatražio, odnosno samo ako postoji potreba temeljem uvjeta navedenih u poglavlju V. ove Politike (*V. Zakonitost obrade*) ili za potrebe poslova koje su korisnici povjerali Bolnici, a što je regulirano posebnim ugovorima (ili narudžbenicama, uputnicama).

Dodatno, na zahtjev ispitanika prijenos osobnih podataka je moguć i pojedinim partnerima Bolnice kojima je povjereno obavljanje određenih usluga (druge zdravstvene ustanove, ZZJZ, HZMO, HZZO, klasteri i dr). Prilikom prijena podataka ispitanika Bolnice vanjskim partnerima strogo se poštuje načelo ograničenja obrade uz prijenos minimalne količine podataka koja je potrebna kako bi se realizirala tražena usluga. Dodatno, Bolnica će uspostaviti zahtjeve i kontrolne mehanizme koji od partnera zahtijevaju minimalno jednaku razinu zaštite osobnih podataka.

Radi umanjenja rizika poslovanja Bolnica će prilikom sklapanja ali i za vrijeme trajanja odnosa s ispitanikom (korisnikom usluga) imati potrebu utvrđivati određeni status (zdravstveni, radni, status osiguranja isl.) i financijsku sposobnost te pratiti ispunjenje prava i obveza temeljem određenog pravnog posla. Status osiguranika će se utvrđivati na temelju podataka dobivenih od samog korisnika usluge, od strane osiguravajućih tvrtki, iz dostupnih registara podataka te iz povijesti poslovanja Bolnice, ako je riječ o korisniku za kojeg postoji povijest poslovnog odnosa.

Prema potrebi, a isključivo temeljem uvjeta navedenih u poglavlju V. Politike (*V. Zakonitost obrade*), Bolnica podatke prenosi trećim zemljama ili međunarodnim organizacijama. U takvim situacijama se primjenjuju dodatne kontrole i zaštitne mjere za iznošenje osobnih podataka sukladno Uredbi. Te mjere mogu podrazumijevati pravno obvezujući i provedivi

instrument, obvezujuća pravila Bolnice i pravnih subjekata, certificiranje i sl., sukladno važećim propisima.

XI. KORIŠTENJE OSOBNIH PODATAKA U POSLOVANJU S KORISNICIMA

Korisnici usluga Bolnice mogu biti fizičke i pravne osobe, tijela državne vlasti, jedinica lokalne ili područne samouprave te njihova tijela, udruge i društva (sportsko, kulturno, dobrotvorno i sl.), kao i svaka fizička osoba koja djeluje unutar područja svoje registrirane gospodarske djelatnosti ili slobodnog zanimanja.

Bolnica prikuplja i obrađuje podatke o korisnicima usluga i osobne podatke fizičkih osoba koje djeluju unutar područja svoje registrirane gospodarske djelatnosti ili slobodnog zanimanja te osobne podatke fizičkih osoba (radnika, pacijenata, gostiju) koje su povezane s Bolnicom i poslovnim korisnicima.

Povezane osobe s poslovnim korisnikom (suradnom tvrtkom ili sl.) u kontekstu ove Politike mogu biti fizičke osobe članovi poslovnog korisnika, osobe ovlaštene za zastupanje poslovnog korisnika, prokuristi, opunomoćenici poslovnog korisnika, predstavnici poslovnog korisnika, opunomoćenici po transakcijskom računu, drugi korisnici usluga Bolnica, dužnici i založni dužnici i druge fizičke osobe čije je osobne podatke poslovni korisnik dao Bolnici na korištenje za svrhe uspostave i održavanja poslovnog odnosa.

Bolnica prikuplja, obrađuje i dijeli podatke o poslovnim korisnicima koji uključuju osobne podatke poslovnih korisnika i povezanih osoba u skladu sa odredbama točke V. ove Politike (*V. Zakonitost obrade*).

Bolnica može obrađivati prikupljene podatke poslovnih korisnika koji uključuju osobne podatke fizičkih osoba koje djeluju unutar područja svoje registrirane gospodarske djelatnosti ili slobodnog zanimanja i povezanih osoba koje joj je na korištenje dao poslovni korisnik za sljedeće slučajeve:

- Utvrđivanje identiteta;
- Usklađivanje sa zakonskim i regulatornim propisima unutar i izvan područja RH;
- Ugovaranje i korištenje proizvoda i usluga koje Bolnica pruža;
- Izvršenje svih vrsta obveza unutar i izvan područja Republike Hrvatske;
- Utvrđivanje statusa osiguranja;
- Naplata potraživanja;
- Izvješćivanje;
- Statističke obrade na traženje državnih tijela;
- Razvijanje i poboljšanje proizvoda i usluga kako bi poslovnim korisnicima omogućili bolje iskustvo korištenja;
- Definiranje proizvoda i usluga koji bi korisnicima usluga Bolnice bili od koristi;
- Kontaktiranje u svrhe ispunjenja ugovornih obveza unutar Bolnice i
- Kontaktiranje u marketinške svrhe.

Bolnica može podijeliti podatke o poslovnim korisnicima koji uključuju osobne podatke fizičkih osoba koje djeluju unutar područja svoje registrirane gospodarske djelatnosti ili slobodnog zanimanja i povezanih osoba koje joj je na korištenje dao poslovni korisnik uz zadovoljenje zakonitosti obrada definiranih u točki V. *Zakonitost obrade* te sukladno načelima obrade definiranim u točki IV. *Načela obrade podataka*, i to prema:

- Zakonodavnim, nadzornim i regulatornim tijelima unutar i izvan područja Republike Hrvatske;
- Pravnim osobama s kojima Bolnica surađuje;

- Ministarstvima, jedinicama lokale i područne samouprave s kojima Bolnica surađuje
- Revizorskim tijelima unutar i izvan Bolnice te ostalim tijelima koji su ovlašteni za reviziju;
- Poslovnim bankama s kojima Bolnica surađuje;
- Agencijama, institucijama, udrugama, osiguravajućim tvrtkama i drugim tvrtkama s kojima Bolnica ima sklopljen ugovor o poslovnoj suradnji temeljem kojeg korisnici usluga mogu ugovarati i koristiti proizvode i usluge koje Bolnica pruža i dr.

XII. SLUŽBENIK ZA ZAŠTITU PODATAKA (DPO)

Bolnica je imenovala Službenika za zaštitu podataka koji je neovisan i kao takav djeluje u interesu zaštite prava ispitanika i njihovih osobnih podataka. Njegova je odgovornost da se unutar Bolnice primjenjuje Uredba i Politika zaštite osobnih podataka te ostale politike i procedure koje definiraju pravila postupanja prilikom prikupljanja i obrade osobnih podataka ispitanika. Službenik za zaštitu podataka je na primjeren način i pravodobno uključen u sva pitanja u pogledu zaštite osobnih podataka. Sudjeluje u procesima Bolnice koji se odnose na upravljanje promjenama i projektima što mu omogućuje pravovremeni pristup informacijama. Službenik za zaštitu podataka izravno odgovara ravnatelju Bolnice i obvezan je tajnošću i povjerljivošću u vezi s obavljanjem svojih zadaća. Službenik za zaštitu podataka obavlja najmanje sljedeće zadaće u Bolnici:

- informiranje i savjetovanje rukovodstva Bolnice i radnika koji obavljaju obradu podataka o njihovim obvezama iz Uredbe, drugih propisa Europske unije ili Republike Hrvatske o zaštiti podataka i ove Politike;
- praćenje poštivanja i primjene Uredbe i ove Politike te drugih propisa Europske Unije ili Republike Hrvatske o zaštiti podataka i drugih propisa Bolnice, bilo da se pojavljuje u ulozi voditelja obrade ili izvršitelja obrade, u odnosu na zaštitu osobnih podataka, uključujući raspodjelu odgovornosti, podizanje svijesti i osposobljavanje osoblja koje sudjeluje u postupcima obrade te povezane revizije;
- pružanje savjeta, kada je to zatraženo, u pogledu procjene učinka na zaštitu podataka i praćenje njezina izvršavanja
- suradnja s nadzornim tijelom;
- djelovanje kao kontaktna točka za nadzorno tijelo (AZOP) o pitanjima u pogledu obrade, te savjetovanje, prema potrebi, o svim drugim pitanjima.

Službenik za zaštitu podataka ne prima nikakve upute u pogledu izvršenja navedenih zadaća, što mu dodatno osigurava neovisnost.

Službenik za zaštitu podataka je ujedno i glavna točka za kontakt ispitanicima koji žele ostvariti svoja prava (*pitanja povezana s obradom osobnih podataka i ostvarivanja prava ispitanika iz Uredbe*) ili poslati upit vezan uz zaštitu osobnih podataka, zatražiti dodatne informacije, izraziti brigu oko obrade njegovih osobnih podataka, podnijeti prigovor vezano uz zaštitu osobnih podataka te ostvarivanja svojih prava iz Uredbe. Ispitanici mogu Službenika za zaštitu podataka kontaktirati putem email adrese: zastita.op@sbvzt.hr

Bolnica ima pravo naplatiti razumnu naknadu na temelju administrativnih troškova ili odbiti postupiti po zahtjevu ako su zahtjevi ispitanika očito neutemeljeni ili pretjerani, a osobito zbog njihovog učestalog ponavljanja.

Kontakt podatci Službenika za zaštitu osobnih podataka dostupni su javnosti na web stranici Bolnice: www.minerva.hr.

XIII. PROCJENA UČINKA

Ako je vjerojatno da će neka vrsta obrade, osobito putem IT sustava i uzimajući u obzir prirodu, opseg, kontekst i svrhu obrade, prouzročiti visok rizik za prava i slobode ispitanika, Bolnice će prije obrade provesti procjenu učinka predviđenih postupaka obrade na zaštitu osobnih podataka. Jedna procjena može se odnositi na niz sličnih postupaka obrade koji predstavljaju sličan visoki rizik. Dodatno, Bolnica će provesti redovnu procjenu učinka na sve obrade koje su trenutno aktivne, a odgovaraju navedenim kategorijama.

Svaka pojedina ustrojstvena jedinica unutar Bolnice dužna je provoditi procjenu učinka sukladno gore navedenim kriterijima i primjenjivim interno definiranim pravilima i procedurama. Ustrojstvene jedinice će kontaktirati službenika za zaštitu podataka u slučaju da nisu sigurni treba li provesti procjenu učinka na određenu obradu podataka ili ne.

Službenik za zaštitu podataka odgovoran je za organiziranje provedbe procjene učinka na zaštitu podataka, odnosno da bude podrška prilikom izrade procjene.

Bolnica obvezno provodi procjenu učinka na zaštitu podataka u slučaju:

- sustavne i opsežne procjene osobnih podataka u vezi s pojedincima koja se temelji na automatiziranoj obradi, uključujući izradu profila i na temelju koje se donose odluke koje proizvode pravne učinke koji se odnose na pojedinca ili na sličan način značajno utječu na pojedinca;
- opsežne obrade posebnih kategorija osobnih podataka (npr. posebni zdravstveni podatci, podatci o djeci);
- sustavnog praćenja javno dostupnog područja u velikoj mjeri (CEZIH, REGZAP, COP)
- u slučajevima obrada koje propiše nadzorno tijelo tj. Agencija za zaštitu osobnih podataka (AZOP)

Procjena učinka sadrži minimalno:

- sustavan opis predviđenih postupaka obrade i svrhe obrade, uključujući legitimni interes Bolnice;
- procjenu nužnosti i proporcionalnosti postupaka obrade povezanih s njihovom svrhom;
- procjenu rizika za prava i slobode ispitanika;
- mjere predviđene za rješavanje problema rizika, što uključuje zaštitne mjere, sigurnosne mjere i mehanizme za osiguravanje zaštite osobnih podataka i dokazivanje sukladnosti s Uredbom, uzimajući u obzir prava i legitimne interese ispitanika i drugih uključenih osoba.

XIV. REGISTAR OBRADA OSOBNIH PODATAKA

Bolnica vodi evidenciju zbirki podataka i aktivnosti obrada za koje je odgovorna. Evidencija se vodi u elektroničkom i papirnatom obliku i sadržava najmanje sljedeće informacije:

- ime i kontaktne podatke voditelja obrade i službenika za zaštitu podataka;
- svrhu obrade podataka;
- opis kategorija ispitanika i kategorija osobnih podataka;
- popis računala na kojima se obrađuju osobni podatci i popis zaduženih osoba za računala;
- kategorije primatelja kojima su osobni podatci otkriveni ili će im biti otkriveni, uključujući primatelje u trećim zemljama ili međunarodne organizacije;
- prijenose osobnih podataka u treću zemlju ili međunarodnu organizaciju, uključujući ime treće zemlje ili naziv međunarodne organizacije;
- predviđene rokove za brisanje različitih kategorija podataka, ako je to moguće;
- opći opis tehničkih i organizacijskih sigurnosnih mjera.

Službenik za zaštitu podataka odgovoran je za održavanje registra obrada podataka, a svi voditelji organizacijskih jedinica unutar Bolnice su odgovorni za dostavu točnih i pravovremenih informacija kako bi se registar obrada adekvatno popunio i ažurirao.

XV. INCIDENTI/CURENJE PODATAKA I PRAVO NA PRITUŽBU

Bolnica poduzima značajne procesne i tehnološke mjere kako bi zaštitila osobne podatke ispitanika. Dodatno, svi radnici Bolnice imaju dužnost obavijestiti odgovorne osobe (prvenstveno Službenika za zaštitu podataka i voditelje odjela) u slučaju incidenta vezanog uz zaštitu osobnih podataka. U slučaju povrede osobnih podataka Bolnica je incident dužna prijaviti Agenciji za zaštitu podataka (AZOP) unutar 72 sata nakon saznanja o povredi, ako je to izvedivo. Voditelji organizacijskih jedinica i službenik za informiranje dužni su u najkraćem mogućem roku o incidentu obavijestiti odgovornu osobu Bolnice tj. ravnatelja ili njegovog zamjenika.

Također, u slučaju povrede osobnih podataka koje će vjerojatno prouzročiti visok rizik za prava i slobode pojedinaca, Bolnica bez nepotrebnog odgađanja obavještava ispitanika o povredi osobnih podataka.

Iznimno, Bolnica neće obavijestiti ispitanika u slučaju povreda osobnih podataka ako je ispunjen barem jedan od sljedećih uvjeta:

- Bolnica je poduzela 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;
- Bolnica je poduzela naknadne mjere kojima se osigurava da više nije vjerojatno da će doći do visokog rizika za prava i slobode ispitanika;
- Obavještavanjem ispitanika bi se zahtijevao povećan tj. nerazmjeran napor za Bolnicu.

U takvom slučaju Bolnica će javno obavijestiti sve korisnike usluga ili će poduzeti slične mjere kojima će se ispitanici obavijestiti o povredi osobnih podataka na jednako djelotvoran način.

Ispitanik ima pravo podnijeti pritužbu nadzornom tijelu (AZOP) u slučaju incidenta koji se tiče njegovih osobnih podataka ili ako smatra da Bolnica krši njegova prava definirana Uredbom.

XVI. ZAVRŠNE ODREDBE

Ova Politika stupa na snagu i primjenjuje se danom donošenja.

Politika će se objaviti na oglasnim pločama Bolnice.

U Varaždinskim Toplicama 30. 05. 2018.g.

Broj: 01-634/1-2018



Predsjednica Upravnog vijeća:
Ivana Golubić Horvat, mag. iur.