

Hrvatski savez za rijetke bolesti, 10000 Zagreb, Ivanićgradska 38, OIB: 84873085315 donosi dana 21. svibnja 2020. godine ovaj

P R A V I L N I K

O ZAŠTITI OSOBNIH PODATAKA

Članak 1.

Ovim Pravilnikom uređuje se zaštita osobnih podataka fizičkih osoba (u daljnjem tekstu: ispitanik) u odnosu na prikupljanje, obradu i korištenje osobnih podataka, obveze udruge Hrvatski savez za rijetke bolesti, 10000 Zagreb, Ivanićgradska 38, OIB: 84873085315 (u daljnjem tekstu: Voditelj obrade), prava ispitanika te provedba organizacijskih, kadrovskih i tehničkih mjera zaštite.

Članak 2.

Značenje pojmova

„**Osobni podaci**“ su svi podaci koji se odnose na pojedinca čiji je identitet utvrđen ili se može utvrditi. Pojedinač 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. Osobni podatak je ime, adresa, e-mail adresa, IP i MAC adresa, GPS lokacija, RFID tagovi i kolačići na web stranicama telefonski broj, fotografija, video snimke pojedinaca, OIB, biometrijski podaci (otisak prsta, snimka šarenice oka), genetski podaci, podaci o obrazovanju i stručnoj spremi, podaci o plaći, podaci o kreditnom zaduženju, podaci o računima u banci, podaci o zdravlju, seksualnoj orijentaciji, glas i bilo koji drugi podaci povezani sa stvarnom osobom, tj. vlasnikom osobnog podatka koji se mogu upotrijebiti za direktno ili indirektno identificiranje točno te osobe.

„**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.

„**Voditelj obrade**“ znači fizička ili pravna osoba, tijelo javne vlasti, agencija ili drugo tijelo koje samo ili zajedno s drugima određuje svrhe i sredstva obrade osobnih podataka;

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

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

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

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

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

„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;

„Osoba koja se može identificirati” je osoba čiji se identitet može utvrditi (izravno ili neizravno) posebno na osnovi identifikacijskog broja ili jednog ili više obilježja specifičnih za njezin fizički, psihološki, mentalni, gospodarski, kulturni ili socijalni identitet;

„Posebna kategorija osobnih podataka” odnosi se na rasno ili etničko podrijetlo, politička stajališta, vjerska ili druga uvjerenja, sindikalno članstvo, zdravlje ili spolni život i osobnih podataka o kaznenom i prekršajnom postupku.

Članak 3.

Voditelj obrade obrađuje osobne podatke na način da su točni, potpuni i ažurni u svim evidencijama u kojima su podaci pohranjeni, neovisno o njihovu obliku vođenja.

Voditelj obrade prikuplja podatke samo u svrhu sa kojom je ispitanik upoznat, koja je navedena prilikom prikupljanja podataka te ih obrađuje samo u svrhu za koju su prikupljeni podaci, odnosno u svrhu koja je podudarna sa svrhom prikupljanja.

Voditelj obrade koristi osobne podatke samo u vremenu koje je nužno za ostvarenje određene svrhe, osim ako posebnim zakonom nije određeno duže razdoblje te se protekom vremena istog moraju brisati, ako posebnim zakonom nije što drugo određeno, odnosno sa sitima je potrebno postupati prema važećim propisima o arhiviranju.

Članak 4.

Voditelj obrade može na temelju ugovora, a koji mora biti u pisanom obliku, pojedine poslove u svezi s obradom osobnih podataka u okvirima svojeg djelokruga povjeriti drugoj fizičkoj ili pravnoj osobi (*izvršitelju obrade*).

Poslovi u svezi s obradom osobnih podataka mogu se povjeriti samo izvršitelju obrade koji je registriran za obavljanje takve djelatnosti i koji osigurava dovoljna jamstva u pogledu ostvarivanja

odgovarajućih mjera zaštite osobnih podataka, odnosno klasificiranih podataka ukoliko ispunjava uvjete utvrđene posebnim propisima koji uređuju područje informacijske sigurnosti.

Voditelj obrade obrađuje podatke koji su navedeni u katalogu podataka koji je sastavni dio ovog pravilnika.

Članak 5.

Voditelj obrade će odlukom utvrditi odgovornu osobu i njenu zamjenu u svakom pojedinom djelu obrade koji je naveden u prethodnom članku, a koja će odgovarati voditelju obrade za postupanje djelatnika unutar djela obrade sukladno odredbama ovog Pravilnika te koje će biti odgovorne za komunikaciju i pružanje informacija službeniku za zaštitu osobnih podataka.

Članak 6.

Osobni podaci navedeni u članku 4 obrađuju se radi izvršenja obveza iz Ugovora i poštivanja odredbi važećih zakonskih propisa.

U slučajevima kada se osobni podaci ne prikupljaju temeljem ugovora ili važećih zakonskih propisa, voditelj obrade će prilikom prikupljanja osobnih podataka pribaviti privolu od ispitanika za prikupljanje i obradu osobnih podataka.

U slučaju ako voditelj obrade podatke obrađuje temeljem legitimnog interesa u smislu Opće uredbe o zaštiti osobnih podataka, tada je voditelj obrade dužan obaviti test ravnoteže kako bi opravdao legitimni interes.

Članak 7.

Prilikom prvog kontakta sa ispitanikom osobe koje prikupljaju osobne podatke od ispitanika u ime i za račun voditelja obrade, ili koje zaprimaju zahtjeve koji nisu preuzeti sa web stranice dužne su mu predati Izjavu o zaštiti osobnih podataka ili drugi dokument koji opisuje i upoznaje ispitanika sa njegovim pravima te u slučaju ako je za obradu pojedinog osobnog podatka potreba privola dužni su prije obrade osobnog podatka istu ishoditi a prema obrascu privole.

Nakon što je ispitaniku predana izjava o zaštiti osobnih podataka i predana privola, potvrde o primitku Izjave o zaštiti osobnih podataka i potvrde o privoli biti će uložene u predmet za u kojem se obrađuju osobni podaci.

Privole će se čuvati za vrijeme dok se čuvaju i osobni podaci na koje se ona odnosi te će se nakon prestanka potrebe za njihovo čuvanje uništiti fizički uz sastavljanje zapisnika o uništenju od strane odgovorne osobe.

U slučaju ako ispitanik izjavi da mu nije jasno pojedina pravo ili traži dodatna pojašnjenja ispitanik će se uputiti na službenika za zaštitu osobnih podataka koji mu je iste dužan pružiti.

Članak 8.

Ako voditelj obrade nije primio osobne podatke od ispitanika, prilikom prve komunikacije djelatnici odnosno osobe koje kontaktiraju ispitanika u ime voditelja obrade moraju pružiti ispitaniku sljedeće informacije:

- identitet i kontaktne podatke voditelja obrade i predstavnika voditelja obrade te kontakt podatke službenika za zaštitu osobnih podataka,
- svrhu obrade kojoj su namijenjeni osobni podaci kao i pravnu osnovu obrade
- kategoriju osobnih podataka koji se obrađuju,
- kategorije primatelja,
- ako postoji, namjeru o prijenosu podataka u treću zemlju ili međunarodnu organizaciju,
- razdoblje pohranjivanja, odnosno kriterije za utvrđivanje razdoblja,
- ako se obrada temelji na legitimnim interesima informirati ispitanika o legitimnom interesu voditelja obrade,
- postojanje prava na pristup osobnim podacima i ispravak ili brisanje osobnih podataka ili ograničavanje obrade koji se odnose na ispitanika i prava na ulaganje prigovora na obradu te prava na prenosivost podataka,
- pravo na povlačenje privole,
- pravo na podnošenje prigovora nadležnom tijelu,
- izvor osobnih podataka,
- informaciju da li postoji automatizirana obrada osobnih podataka.

Članak 9.

Voditelj obrade će imenovati službenika za zaštitu podataka.

Službenik za zaštitu podataka može biti i osoba koja nije zaposlenik Voditelja obrade osobnih podataka.

Službenik za zaštitu podataka direktno odgovara odgovornoj osobi voditelja obrade i ne smije primati upute od drugih zaposlenika Voditelja obrade podataka vezano za obradu osobnih podataka i zadužen je za izravan kontakt sa nadležnim nadzornim tijelom.

Voditelj obrade je dužan javno objaviti kontakt podatke Službenika za zaštitu podataka na svojim web stranicama i na svaki drugi prikladan način.

Članak 10.

Prilikom obrade osobnih podataka, Voditelj obrade dužan je voditi računa osobito o sljedećim rokovima i obavezama:

- Kada se obrada temelji na privoli ispitanika, Voditelj obrade dužan je pribaviti privolu za obradu osobnih podataka te mora u svakom trenutku moći dokazati da je ispitanik dao privolu za obradu svojih podataka.

- Voditelj obrade dužan je bez odgode, a najkasnije u roku od mjesec dana dostaviti ispitaniku sve informacije u vezi obrade njegovih osobnih podataka, a na koje ima pravo sukladno Općoj uredbi. U slučaju složenosti i većeg broja zahtjeva taj se rok može produžiti za dodatna dva mjeseca, a u kojem slučaju je potrebno izvijestiti ispitanika o toj činjenici u roku od mjesec dana od primitka zahtjeva sa obrazloženjem za produženje roka.
- U slučajevima da informacije nisu dobivene od ispitanika, Voditelj obrade dužan je odmah kod prve komunikacije sa ispitanikom, a najkasnije u roku od mjesec dana od dobivanja osobnih podataka, pružiti ispitaniku informaciju o obradi njegovih osobnih podataka sukladno odredbama Opće uredbe.
- Voditelj obrade dužan je obavijestiti ispitanika o pravu na prigovor prilikom prve komunikacije sa ispitanikom.
- U slučaju povrede osobnih podataka, Voditelj obrade dužan je izvijestiti nadzorno tijelo bez odgode, a najkasnije u roku od 72 sata od saznanja za nastalu povredu. U slučaju kašnjenja izvješćivanja, potrebno je dostaviti nadzornom tijelu i razloge kašnjenja.
- U slučaju povrede osobnih podataka koje će prema procijeni Voditelja obrade vjerojatno prouzročiti visok rizik za prava i slobode pojedinca, Voditelj obrade dužan je o istome bez odgode obavijestiti ispitanika.
- Kada je vjerojatno da će neka vrsta obrade prouzročiti visok rizik za prava i slobode ispitanika, Voditelj obrade je dužan provesti procjenu učinka na zaštitu podataka prije početka obrade podataka.
- U slučajevima kada se temeljem provedene procjene učinka na zaštitu podataka utvrdilo da bi obrada bez donošenja dodatnih mjera zaštite za ublažavanje rizika dovela do visokog rizika za prava i slobode pojedinca, Voditelj obrade dužan je prije obrade savjetovati se sa nadzornim tijelom.
- Voditelj obrade dužan je sve osobne podatke brisati (ili anonimizirati) prestankom svrhe u koju su prikupljeni, povlačenjem privole najkasnije po isteku svih zakonskih obveza povezanih s čuvanjem osobnih podataka, osim u slučaju da je pokrenut postupak prisilne naplate neplaćenih potraživanja ili ako je uložena prigovor na proizvod ili uslugu u roku, sve do konačnog dovršetka postupka po prigovoru u skladu s važećim propisima.
- U slučajevima kada je na zahtjev ispitanika izvršena dopuna, izmjena ili brisanje osobnih podataka, o izvršenom ispravku potrebno je izvijestiti osobu na koju se osobni podaci odnose i primatelje osobnih podataka i to u roku od 30 dana od ispravka.

Članak 11.

Voditelj obrade dužan postupati sukladno Protokolu o pristupu i korištenju informacijskih sustava.

Članak 12.

Voditelj obrade je dužan osigurati zaštitu informatičkog sustava sukladno Protokolu o pristupu i korištenju informacijskih sustava.

Članak 13.

Zahtjevi ispitanika kojima ispitanik traži od voditelja obrade neko od svojih prava iz uredbe moraju biti u pisanom obliku.

Na zahtjeve ispitanika voditelj obrade je dužan odgovoriti u što kraćem roku, ali najdulje u roku od mjesec dana od dana primitka zahtjeva.

Prilikom podnošenja zahtjeva potrebno je utvrditi identitet osobe koja podnosi zahtjev uvidom u osobnu iskaznicu, ili uvidom u putovnicu.

Nije moguće postupanje po zahtjevu prije nesumnjivog utvrđivanja identiteta ispitanika. Voditelj obrade ne smije prenijeti osobi niti jedan osobni podatak prije nego što se utvrdi identitet.

Članak 14.

Voditelj obrade vodi evidenciju obrade osobnih podataka.

Evidencija obrade osobnih podataka sadrži:

- Ime i kontakt podatke voditelja obrade;
- Ime i kontakt podatke službenika za zaštitu osobnih podataka;
- Svrhu obrade;
- Opis kategorija ispitanika;
- Opis kategorija osobnih podataka;
- Kategorija primatelja kojima će podaci biti otkriveni;
- Rokove za brisanje;
- Tehničke i organizacijske mjere zaštite osobnih podataka.

Za vođenje evidencije obrade osobnih podataka osoba ovlaštena na zastupanje voditelja obrade će imenovati odgovornu osobu.

Članak 15.

Voditelj obrade ima izrađene procjene učinka na privatnost za obrade za koje je utvrdio da mogu prouzročiti visok rizik za prava i slobode pojedinaca.

U slučaju novih vrsta obrade koje bi putem novih tehnologija i uzimajući u obzir prirodu, opseg, kontekst i svrhe obrade, mogle prouzročiti visok rizik za prava i slobode pojedinaca, voditelj obrade prije obrade je obavezan izraditi procjenu učinka predviđenih postupaka obrade na zaštitu osobnih podataka.

Prilikom procjene učinka na privatnost voditelj obrade je dužan zatražiti savjet od službenika za zaštitu podataka.

Članak 16.

Za pitanja koja nisu navedena ovim Pravilnikom primjenjuju se odredbe Opće uredbe o zaštiti osobnih podataka.

Članak 17.

Ovaj Pravilnik stupa na snagu danom objave na oglasnoj ploči.

Vlasta Zmazek, predsjednica