

Temeljem članka 38. stavka 3. Statuta Imunološkog zavoda, Rockefellerova 2, Zagreb, Upravno vijeće je na 88. sjednici održanoj 11. prosinca 2019. donijelo

PRAVILNIK O ZAŠTITI OSOBNIH PODATAKA U IMUNOLOŠKOM ZAVODU

I OPĆE ODREDBE

Članak 1.

Imunološki zavod je obveznik primjene Opće uredbe o zaštiti podataka.

Imunološki zavod je voditelj obrade osobnih podataka.

Imunološki zavod kao voditelj obrade osobnih podataka određuje svrhu i sredstva obrade osobnih podataka u skladu sa Općom uredbom o zaštiti podataka, važećim zakonodavstvom Republike Hrvatske (u daljnjem tekstu RH), pravom Europske Unije (u daljnjem tekstu EU) i drugim internim aktima Imunološkog zavoda kojima se uređuje zaštita osobnih podataka.

Predmet Pravilnika

Članak 2.

Ovaj Pravilnik o zaštiti osobnih podataka (u daljnjem tekstu Pravilnik) sadrži pravila za zaštitu osobnih podataka u postupku prikupljanja i obrade osobnih podataka koji se odnose na fizičke osobe, a do kojih Imunološki zavod dolazi tijekom svog redovitog poslovanja.

Svrha zaštite osobnih podataka je zaštita privatnog života i ostalih ljudskih prava i temeljnih sloboda u prikupljanju, obradi i korištenju osobnih podataka.

Zaštita osobnih podataka u Imunološkom zavodu osigurana je svakoj fizičkoj osobi bez obzira na državljanstvo i prebivalište te neovisno o rasi, boji kože, spolu, jeziku, vjeri, političkom ili drugom uvjerenju, nacionalnom ili socijalnom podrijetlu, imovinu, rođenju, naobrazbi, društvenom položaju ili drugim osobinama u skladu s odredbama Opće uredbe o zaštiti podataka.

Pravo na zaštitu osobnih podataka pripada svim ispitanicima na jednak način i pod jednakim uvjetima i ispitanici su ravnopravni u njegovu ostvarivanju.

Članak 3.

Ovaj Pravilnik sadrži odredbe koje su u skladu s Općom uredbom o zaštiti podataka i važećim zakonodavstvom RH na području zaštite osobnih podataka.

Pojmovi i definicije

Članak 4.

Pojedini izrazi u ovom Pravilniku imaju sljedeće značenje:

1. "*Opća uredba o zaštiti podataka*" je uredba koji je donijela EU komisija u travnju 2016. godine i koja ima zakonsku snagu za sve države članice EU. Uredba regulira prava i obveze u području zaštite osobnih podataka fizičkih osoba;
2. "*Osobni podaci*" znači svi podaci koji se odnose na pojedinca čiji je identitet utvrđen ili se može utvrditi;
3. "*Ispitanik*" je svaki pojedinac (fizička osoba) od koje Imunološki zavod prikuplja i obrađuje osobne podatke u smislu Opće uredbе o zaštiti podataka;
4. "*Voditelj obrade*" u smislu ovog Pravilnika je Imunološki zavod. Imunološki zavod određuje svrhe i sredstva obrade osobnih podataka;
5. "*Izvršitelj obrade*" je fizička ili pravna osoba, državno ili drugo tijelo, koje obrađuje osobne podatke u ime voditelja zbirke osobnih podataka;
6. "*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;
7. "*Sustav pohrane*" je zbirka osobnih podataka odnosno svaki strukturirani skup osobnih podataka koji je dostupan prema posebnim kriterijima;

8. "*Primatelj*" je fizička ili pravna osoba, državno ili drugo tijelo kojem se osobni podaci otkrivaju;
9. "*Privola ispitanika*" je svako dobrovoljno, posebno, informirano i nedvosmisleno očitovanje volje ispitanika kojom on izjavom ili jasnom potvrdnom radnjom izražava svoju suglasnost s obradom njegovih osobnih podataka u određene svrhe;
10. "*Službenik za zaštitu osobnih podataka*" ili „DPO“ je osoba imenovana od strane Imunološkog zavoda koja vodi brigu o zakonitosti obrade osobnih podataka i ostvarivanju prava na zaštitu osobnih podataka;
11. "*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;
12. „*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;
13. "*Nadzorno tijelo*" je Agencija za zaštitu osobnih podataka.

II PROCESI I PRAVILA U OBRADI OSOBNIH PODATAKA

Obrada osobnih podataka

Članak 5.

Imunološki zavod obrađuje osobne podatke samo uz uvjete određene Općom uredbom o zaštiti podataka i drugim internim aktima Imunološkog zavoda kojima se uređuje zaštita osobnih podataka.

Društvo obrađuje osobne podatke zakonito, pošteno i transparentno. Obraduju se samo primjereni i relevantni osobni podaci i to isključivo u posebne, izričite i zakonite svrhe te se dalje ne obrađuju na način koji nije u skladu s tim svrhama.

Osobni podaci moraju biti točni, potpuni i ažurni.

Osobni podaci koji nisu točni bez odlaganja se brišu ili ispravljaju.

Imunološki 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 i organizacijskih mjera.

Imunološki zavod osobne podatke čuva 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 ili druge svrhe propisane zakonodavstvom RH i predviđene posebnim propisom ili odlukom Imunološkog zavoda.

Svrha prikupljanja osobnih podataka

Članak 6.

Imunološki zavod prikuplja osobne podatke u svrhu s kojom je ispitanik upoznat, koja je izričito navedena i u skladu s Općom uredbom o zaštiti podataka i važećim zakonodavstvom RH.

Osobni podaci se dalje obrađuju samo u svrhu u koju su prikupljeni, odnosno u svrhu koja je podudarna sa svrhom prikupljanja.

Imunološki zavod neće prikupljati osobne podatke u većem opsegu nego što je to nužno da bi se postigla utvrđena svrha.

Imunološki zavod će osobne podatke koristiti samo u vremenu koje je nužno za ostvarenje određene svrhe, osim ako Općom uredbom o zaštiti podataka i/ili posebnim propisima RH ili EU nije određeno duže razdoblje, a protekom navedenog vremena Imunološki zavod će osobne podatke brisati.

Osnove za prikupljanje i daljnju obradu osobnih podataka

Članak 7.

Imunološki 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;
- da je obrada nužna radi poštovanja pravnih obveza Imunološkog 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 ili pri izvršavanju javnih ovlasti Imunološkog zavoda;
- da je obrada nužna za potrebe legitimnih interesa Imunološkog 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.

Informiranje ispitanika

Članak 8.

U postupku obrade osobnih podataka Imunološki zavod na odgovarajući način (pisano ili izravno usmeno) ispitaniku pruža sve informacije vezane za obradu njegovih osobnih podataka, a osobito o:

- identitetu Imunološki zavod kao voditelju obrade osobnih podataka;
- svrsi obrade podataka;
- pravnoj osnovu za obradu podataka;
- legitimnim interesima;
- namjeri predaji osobnih podataka trećim osobama;

- razdoblju u kojem će osobni podaci biti pohranjeni;
- o pravu na pristup osobnim podacima te na ispravak ili brisanje osobnih podataka i ograničavanje obrade;
- pravu na ulaganje prigovora.

Upravljanje zahtjevima ispitanika

Članak 9.

Imunološki zavod će odmah, a najkasnije u roku od mjesec dana od dana podnošenja zahtjeva ispitanika:

- informirati ispitanika o svrsi obrade njegovih osobnih podataka, kategorijama osobnih podataka koji se obrađuju, o primateljima ili kategorijama primatelja kojima su osobni podaci otkriveni ili će im biti otkriveni, predviđenom razdoblju u kojem će osobni podaci biti pohranjeni te u slučaju kada se osobni podaci ne prikupljaju od ispitanika o njihovu izvoru;
- dostaviti ispitaniku ispis osobnih podataka sadržanih u sustavu pohrane koji se na njega odnose;
- ispraviti netočne podatke ili podatke dopuniti;
- provesti brisanje osobnih podataka koji se na ispitanika odnose pod uvjetom da osobni podaci više nisu nužni u odnosu na svrhe za koje su prikupljeni ili ako ispitanik povuče privolu na kojoj se obrada temelji.

Rok iz stavka 1. ovog članka može se prema potrebi produljiti za dodatna dva mjeseca, uzimajući u obzir složenost i broj zahtjeva. Imunološki zavod obavješćuje ispitanika o svakom takvom produljenju u roku od mjesec dana od zaprimanja zahtjeva, zajedno s razlozima odgađanja.

Ako je zahtjev ispitanika podnesen elektroničkim putem, Imunološki zavod informaciju pruža elektroničkim putem ako je to moguće, osim ako ispitanik zatraži drugačije.

O razlozima odbijanja zahtjeva ispitanika iz stavka 1. ovog članka Imunološki zavod će bez odgađanja, a najkasnije u roku od mjesec dana od dana primitka zahtjeva, izvijestiti ispitanika o razlozima odbijanja zahtjeva.

Članak 10.

Imunološki zavod pruža informacije u skladu s člankom 8. ovog Pravilnika bez naknade.

Upravljanje incidentima u vezi povrede osobnih podataka

Članak 11.

Aktivnosti i postupci vezani za upravljanje incidentima u vezi povrede osobnih podataka odnose se na sve organizacijske cjeline i sve radnike Imunološkog zavoda i obuhvaćaju:

1. Evidentiranje dojave o povredi osobnih podataka odmah po saznanju
2. Slanje obavijesti o povredi osobnih podataka DPO-u
3. DPO obavještava nadzorno tijela o povredi osobnih podataka.

Provođenje kontrole i nadzor u procesima obrade osobnih podataka

Članak 12.

Provođenje kontrole i nadzor u procesima obrade osobnih podataka u nadležnosti je Službenika za zaštitu osobnih podataka i Agencije za zaštitu osobnih podataka.

Izvrješćivanje o zaštiti osobnih podataka

Članak 13.

Ispitanici se sa zahtjevima i prigovorima obraćaju Službeniku za zaštitu osobnih podataka te imaju pravo na izvrješćivanje o zaštiti osobnih podataka i pravo na obavijest o povredi osobnih podataka u slučaju povrede osobnih podataka.

Evidencija aktivnosti obrade

Članak 14.

Imunološki zavod prikuplja i obrađuje sljedeće vrste osobnih podataka:

- osobni podaci radnika Imunološkog zavoda;
- osobni podaci o kandidatima koji sudjeluju u natječajnom postupku za zasnivanje radnog odnosa;
- osobni podaci vanjskih suradnika;
- osobni podaci kupaca;
- osobni podaci dobavljača
- osobni podaci prikupljeni putem nadzornih kamera.

Imunološki zavod prikuplja i obrađuje sljedeće različite vrste osobnih podataka primjerice ime i prezime, adresa, datum rođenja, OIB, stručna sprema, e-mail adresa i druge osobne podatke u svrhe određene ovom Pravilnikom i drugim internim aktima Imunološkog zavoda kojima se uređuje zaštita osobnih podataka.

Imunološki zavod prikuplja i obrađuje osobne podatke u svrhu:

- evidencije radnika i obračuna plaće;
- ispunjavanja ugovornih obveza Imunološkog zavoda prema klijentima (knjigovodstveno evidentiranje kupaca i dobavljača);
- ispunjavanja zakonskih obveza Imunološkog zavoda;
- sigurnosti osoba i imovine (video nadzor).

Članak 15.

Za osobne podatke navedene u članku 14. ovog članka Imunološki zavod vodi evidenciju aktivnosti obrade za sve prikupljene osobne podatke.

Članak 16.

Evidencija aktivnosti obrade sadržava sve sljedeće informacije:

- ime i kontaktne podatke IMZ;
- svrhe obrade;
- opis kategorija ispitanika i kategorija osobnih podataka;
- kategorije primatelja kojima su osobni podaci otkriveni ili će im biti otkriveni;
- ako je primjenjivo, prijenose osobnih podataka u treću zemlju ili međunarodnu organizaciju;
- ako je to moguće, predviđene rokove za brisanje različitih kategorija podataka (rok čuvanja);
- mjere zaštite (opći opis tehničkih i organizacijskih sigurnosnih mjera).

Evidencija iz stavka 1. ovog članka mora biti u pisanom obliku, uključujući elektronički oblik.

Imunološki zavod je dužan evidenciju iz stavka 1. ovog članka dati na uvid tijelu koje provodi nadzor nad zaštitom osobnih podataka u skladu sa propisima RH i EU.

Članak 17.

Imunološki zavod imenuje službenika za zaštitu osobnih podataka.

Povjeravanje poslova obrade osobnih podataka izvršitelju obrade

Članak 18.

Imunološki zavod može, uzimajući u obzir poslovne potrebe i opravdanost, te na temelju ugovora, pojedine poslove u vezi s obradom osobnih podataka u okvirima svog poslovanja povjeriti drugoj fizičkoj ili pravnoj osobi odnosno izvršitelju obrade. U takvim slučajevima ugovor između Imunološkog zavoda i izvršitelja obrade mora biti sklopljen u pisanom obliku.

Imunološki zavod će poslove u svezi s obradom osobnih podataka 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.

Ugovorom koji Imunološki zavod sklopi sa izvršiteljem obrade uredit će se međusobna prava i obveze, a osobito uz obvezu izvršitelja obrade da obavlja poslove na temelju naloga

Imunološkog zavoda, te da ne smije osobne podatke davati na korištenje drugim primateljima niti ih smije obrađivati za bilo koju drugu svrhu osim ugovorene. Izvršitelj obrade ujedno osigurava provođenje odgovarajućih tehničkih, organizacijskih i kadrovskih mjera zaštite osobnih podataka sukladno važećim zakonskim propisima kao i zahtjevima Imunološkog zavoda u području zaštite osobnih podataka.

Davanje podataka primateljima

Članak 19.

Imunološki zavod je ovlašteno osobne podatke dati na korištenje drugim primateljima na temelju pisanog zahtjeva primatelja ako je to potrebno radi obavljanja poslova u okviru zakonom utvrđene djelatnosti primatelja.

Pisani zahtjev mora sadržavati svrhu i pravni temelj za korištenje osobnih podataka te vrstu osobnih podataka koji se traže.

Iznošenje osobnih podataka

Članak 20.

Imunološki zavod će iznositi iz RH u svrhu daljnje obrade samo ako država ili međunarodna organizacija u koju se osobni podaci iznose ima na odgovarajući način uređenu zaštitu osobnih podataka odnosno osiguranu adekvatnu razinu zaštite.

Sigurnost obrade osobnih podataka

Članak 21.

Imunološki zavod će sukladno mogućnostima i procjeni učinka na zaštitu osobnih podataka provesti odgovarajuće tehničke i organizacijske mjere kako bi se osigurala odgovarajuća razina sigurnosti, a uključujući prema potrebi i:

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

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

III DUŽNOSTI I ODGOVORNOSTI

Službenik za zaštitu osobnih podataka

Članak 22.

Službenik za zaštitu osobnih podataka je osoba koja je u radnom odnosu u Imunološkom zavodu (radnika) i/ili vanjski suradnik odnosno osoba s kojom Imunološki zavod ima sklopljen ugovor.

Službenik za zaštitu osobnih podataka prati poštivanje pravila i načela Opće Uredbe o zaštiti podataka, te drugih propisa o zaštiti podataka, podiže svijest i osposobljava osobe unutar Imunološkog zavoda koje sudjeluju u postupcima obrade.

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

Službenik za zaštitu osobnih podataka ima najvišu odgovornost za usklađenost cjelokupnog sustava zaštite osobnih podataka u Imunološkom zavodu.

Službenik za zaštitu osobnih podataka imenuje se na temelju stručnih kvalifikacija, a osobito stručnog znanja o pravu i praksama u području zaštite podataka te sposobnosti izvršavanja zadaća utvrđenih Općom uredbom o zaštiti podataka.

Službenika za zaštitu osobnih podataka imenuje Ravnatelj Imunološkog zavoda.

Službenik za zaštitu osobnih podataka treba razumjeti postupak obrade podataka, informacijsku tehnologiju i sigurnost, poznavati sektor i organizaciju Imunološkog zavoda.

Službenik za zaštitu osobnih podataka treba imati sposobnost promicanja zaštite podataka unutar Imunološkog zavoda.

Kontakt podatke Službenika za zaštitu osobnih podataka Imunološki zavod objavljuje na svojoj web stranici.

Odgovornost radnika Imunološkog zavoda

Članak 23.

Svi radnici zaposleni u Imunološkom zavodu odgovorni su za obradu osobnih podataka u skladu sa Općom uredbom o zaštiti podataka i drugim internim aktima Imunološkog zavoda kojima se uređuje zaštita osobnih podataka i važećim propisima RH na području zaštite osobnih podataka.

Svaka organizacijska jedinica unutar Imunološkog zavoda sa voditeljem organizacijske jedinice poduzima i provodi odgovarajuće tehničke i organizacijske mjere.

Radnici Imunološkog zavoda su dužni prijaviti sve nepravilnosti vezane za obradu osobnih podataka na e-mail adresu zpelin@imz.hr ili drugu adresu koju objavi Imunološki zavod za ovu namjenu.

Imunološki zavod će kontinuirano i u skladu s potrebama poslovanja osigurati edukaciju svojih radnika u području zaštite osobnih podataka.

Odgovornost drugih osoba

Članak 24.

Sve pravne i/ili fizičke osobe u tijeku poslovanja s Imunološkim zavodom dužne su pridržavati odredbi ovog Pravilnika i drugih internih akata Imunološkog zavoda kojima se uređuje zaštita osobnih podataka, a Imunološki zavod će ih upoznati sa pravilima i procesima zaštite osobnih podataka u Imunološkom zavodu.

IV ZAŠTITA PRAVA ISPITANIKA

Članak 25.

Imunološki zavod će najkasnije u roku od 15 dana od podnošenja zahtjeva svakom ispitaniku na osobni zahtjev, odnosno na zahtjev njegovog zakonskog zastupnika ili punomoćnika:

- dostaviti potvrdu o tome da li se osobni podaci koji se odnose na njega obrađuju ili ne;
- dati obavijest u razumljivom obliku o podacima koji se odnose na njega, te čija je obrada u tijeku kao i o izvoru tih podataka;
- omogućiti uvidu u evidenciju aktivnosti obrade te uvid u osobne podatke sadržane u evidenciji aktivnosti obrade koji se odnose na njega te njihovo prepisivanje;
- dostaviti izvatke, potvrde ili ispile osobnih podataka sadržanih u evidenciji aktivnosti obrade koji se odnose na njega, a koji moraju sadržavati i naznaku svrhe i pravnog temelja prikupljanja, obrade i korištenja tih podataka;
- dostaviti ispis podataka o tome tko je i za koje svrhe i po kojem pravnom temelju dobio na korištenje osobne podatke koji se odnose na njega;
- dati obavijest o automatskoj obradi podataka koja se odnosi na njega.

Imunološki zavod će na zahtjev ispitanika, odnosno njegovih zakonskih zastupnika ili punomoćnika dopuniti, izmijeniti ili brisati osobne podatke ako su podaci nepotpuni, netočni ili neažurni, te ako njihova obrada nije u skladu s Općom uredbom o zaštiti podataka i važećim propisima RH na području zaštite osobnih podataka.

Neovisno o zahtjevu ispitanika, IMZ će u slučaju da utvrdi da su osobni podaci nepotpuni, netočni ili neažurni brisati, dopuniti i/ili izmijeniti osobne podatke ispitanika.

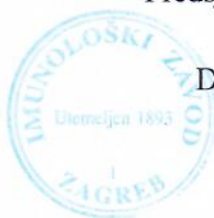
V PRIJELAZNE I ZAVRŠNE ODREDBE

Članak 26.

Ovaj Pravilnik stupa na snagu osmog dana od dana objave na oglasnim pločama Imunološkog zavoda.

Predsjednica Upravnog vijeća

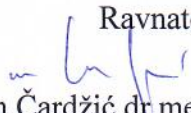
Danica Kramarić dr. med.



[Handwritten signature of Danica Kramarić]

Ovaj Pravilnik objavljen ja na oglasnoj ploči Imunološkog zavoda dana 13.12.2013 i stupa
na snagu dana 24.12.2013.



Ravnatelj

Vedran Čardžić dr.med.