DOM ZDRAVLJA ZAGREB-CENTAR

PRAVILNIK
O ZAŠTITI OSOBNIH PODATAKA

Zagreb, 20. prosinca 2018. godine

Sadržaj

1. UVODNE ODREDBE

Članak 1.

Na temelju Uredbe br. 2016/679 Europskog parlamenta i vijeća od 27.04.2016. god. i Zakona o provedbi opće uredbe o zaštiti podataka (NN 42/18) nakon prethodnog savjetovanja s Radničkim vijećem, Upravno vijeće Ustanove Dom zdravlja Zagreb-Centar na 24. redovitoj sjednici održanoj 20. prosinca 2018. godine, donijelo je ovaj Pravilnik o zaštiti osobnih podataka Ustanove.

2. SVRHA PRAVILNIKA O ZAŠTITI OSOBNIH PODATAKA

Članak 2.

Pravilnik o zaštiti osobnih podataka predstavlja sveobuhvatna pravila o glavnim obvezama svih Radnika/Suradnika Ustanove **Dom zdravlja Zagreb-Centar**, kao i posrednih i neposrednih dobavljača roba i usluga, a kojih se navedene osobe moraju pridržavati kako bi bili u skladu s Općom uredbom o zaštiti podataka.

Izrazi koji se koriste u ovom Pravilniku, a imaju rodno značenje koriste se neutralno i odnose se jednako na muški i ženski rod.

Članak 3.

Pojedinci, obveznici pridržavanja navedenih pravila – dalje u tekstu navedeni su kao: **Radnici/Suradnici;** dok se Ustanova **Dom zdravlja Zagreb-Centar** dalje u tekstu označuje kao: **Ustanova.** Ovaj Pravilnik o zaštiti osobnih podataka dostupan je na oglasnoj ploči Ustanove i na mrežnoj stranici Ustanove.

Članak 4.

Korištenje dokumenata, informacija, osobnih podataka, sustava te usluga Ustanove koje nije u skladu s pravilima uređenima ovim Pravilnikom može predstavljati razlog za pokretanje disciplinskog, kaznenog ili postupka za naknadu nastale štete Ustanovi.

3. DEFINICIJE

Članak 5.

Vlasnik procesa: označava osobu imenovanu od osobe ovlaštene za zastupanje u Ustanovi , a koja je unutar određenog okvira odgovorna pratiti i osiguravati usklađenost obrade osobnih podataka s Uredbom za zaštitu osobnih podataka Svaki vlasnik procesa može imenovati drugog vlasnika procesa, ovisno o potrebama i upravljačkoj ulozi koju ima unutar svoje specifične funkcije i odjela. Takvo imenovanje mora naznačiti zadaće za koje je zadužena delegirana osoba.

Savjetnik: označava osobu / funkciju čija je osnovna funkcija pružanje savjeta i podrške vezane za pitanja usklađenosti s Uredbom za zaštitu osobnih podataka.

Ispitanik: označava fizičku (i gdje je posebno predviđeno – pravnu) osobu, čiji se osobni podaci obrađuju od Ustanove, odnosno kojeg drugog njegovog tijela.

Informacija o zaštiti osobnih podataka označava dokument koji sadrži sve informacije za Ispitanika vezane za obradu njegovih osobnih podataka koje zahtijeva Opća uredba za zaštitu podataka.

Osobni podaci: označavaju sve podatke koji se odnose na pojedinca čiji je identitet utvrđen ili se može utvrditi („ispitanik"); pojedinac čiji se identitet može utvrditi jest osoba koja se može identificirati izravno ili neizravno, osobito uz pomoć identifikatora kao što su ime, identifikacijski broj, podaci o lokaciji, mrežni identifikator ili uz pomoć jednog ili više čimbenika svojstvenih za fizički, fiziološki, genetski, mentalni, ekonomski, kulturni ili socijalni identitet tog pojedinca.

Posebne kategorije osobnih podataka: označavaju osobne podatke o rasnom ili etničkom porijeklu, političkim stavovima, religijskim ili filozofskim uvjerenjima ili sindikalnom članstvu kao i obradu genetskih i bio metričkih podataka s ciljem jednoznačne identifikacije fizičke osobe, podatke povezane sa zdravljem ili seksualnim životom ili seksualnom orijentacijom pojedinca te podatke vezane za kaznene ili prekršajne postupke.

Obrada: označava 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, uključujući provedbu logičkih, matematičkih i drugih postupaka s osobnim podacima ili skupovima osobnih podataka.

Izrada profila: označava 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, kreditnom sposobnošću, zdravljem, osobnim sklonostima, interesima, pouzdanošću, ponašanjem, lokacijom ili kretanjem tog pojedinca.

Privola za obradu: 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. To bi moglo obuhvaćati označivanje polja kvačicom pri posjetu internetskim stranicama, izjavu ili ponašanje koje jasno pokazuje da ispitanik prihvaća predloženu obradu svojih osobnih podataka. Šutnja, unaprijed kvačicom označeno polje ili manjak aktivnosti stoga se ne bi smjeli smatrati privolom.

Izvršitelj obrade označava subjekt (Ustanovu ili pojedinca, upravno ili drugo tijelo) koje obrađuje osobne podatke u ime voditelja obrade. Izvršitelji obrade su subjekti izvan Ustanove koji obrađuju podatke u ime potonjeg. Subjekti Ustanove također mogu imati ulogu izvršitelja obrade u slučaju kada provode radnju obrade u ime klijenta ili drugog subjekta.

Platforma: označava automatizirani alat koji omogućava subjektima Ustanove da ispune zahtjeve Opće uredbe o zaštiti podataka te uključuje, ali se ne ograničava stvaranje i ažuriranje Registra podataka, prijave i revizije, procjenu učinka na zaštitu podataka, te obavijest o povredi osobnih podataka.

Podizvršitelj: označava subjekt (Ustanovu ili pojedinca) kojeg je izvršitelj obrade postavio da u ime voditelja obrade provodi obradu osobnih podataka, a kojeg nadzire izvršitelj obrade. Pod izvršitelji su subjekti izvan Ustanove koji obrađuju podatke u ime klijenata Ustanove.

Voditelj obrade: označava subjekt (Ustanovu ili pojedinca, upravno ili drugo tijelo) koji sam ili zajedno s drugima određuje ciljeve i obrade osobnih podataka.

Povreda osobnih podataka: označava 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.

Radnik/Suradnik: označava svakog radnika ili suradnika Ustanove kao obveznika pridržavanja pravila iz ovog Pravilnika.

Regulatorno tijelo: označava nacionalno nadzorno tijelo za zaštitu osobnih podataka koje je nadležno za određeni predmet, u Hrvatskoj to je AZOP. Moguće je da su različita Regulatorna tijela nadležna za predmete vezane za subjekte Ustanove, ovisno o specifičnostima svakog slučaja.

Dobavljač: označava treću stranu koja pristupa osobnim podacima koje obrađuje Ustanova / subjekt Ustanove kao voditelj ili izvršitelj obrade, ovisno o slučaju. Može uključivati, na primjer, trećeg pružatelja usluga ili poslovnu stranku.

Subjekti Ustanove: ovisno o kontekstu, Ustanova ili Ustanove koje djeluju u EU, koje mogu biti voditelji ili izvršitelji određene obrade osobnih podataka, ovisno o slučaju.

4. GLAVA 1 - PRAVILA ZA ADEKVATNU OBRADU OSOBNIH PODATAKA

4.1 OBRADA OSOBNIH PODATAKA

4.1.1 Opća načela obrade osobnih podataka

Članak 6.

Osobni podaci smiju se obrađivati, uz određene iznimke, u svrhe naznačene u Informaciji o zaštiti osobnih podataka danoj određenom ispitaniku. Osobni podaci:

- moraju se obrađivati na zakonit, pravilan i transparentan način;
- moraju se prikupljati i evidentirati u određenu, eksplicitnu i legitimnu svrhu te upotrebljavati u postupcima obrade koji su kompatibilni s tom svrhom;
- moraju biti precizni i, tamo gdje je to potrebno, ažurirani;
- moraju biti adekvatni, relevantni te ne ih ne smije biti više no što je potrebno za svrhu u koju su prikupljeni i obrađeni;
- moraju biti pohranjeni u obliku koji omogućava identifikaciju ispitanika na period ne duži nego što je to potrebno za svrhu u koju su prikupljeni i obrađeni; i
- moraju se obrađivati na način koji jamči odgovarajuću sigurnost, uključujući zaštitu odgovarajućim tehničkim i organizacijskim mjerama od neovlaštene ili nezakonite obrade, od gubitka, uništenja ili slučajnog oštećenja.

Opća uredba o zaštiti podataka zahtijeva da Ispitanik bude pravilno obaviješten o obradi svojih podataka kao što je propisano u članku 13 Opće uredbe o zaštiti podataka. Ispitanik mora dati svoju slobodnu, informiranu i jednoznačnu privolu za obradu svojih osobnih podataka ako će se ti osobni podaci obrađivati u druge svrhe osim u svrhu provedbe ugovora s ispitanikom ili ako ne postoji druga zakonita osnova za obradu podataka Ispitanika.

Svakom Ispitaniku mora se pružiti mogućnost kontaktirati voditelja obrade, odnosno odgovornu osobu voditelja obrade.

Ustanova je odredila odgovornu osobu unutar svoje organizacije kojoj je povjeren nadzor nad pridržavanjem propisa o zaštiti podataka - „Službenika za zaštitu podataka".

Svi zaposlenici Ustanove su obvezani pridržavati se pravila ovog Pravilnika o zaštiti osobnih podataka. Zaključenjem ugovora o radu/suradnji, svaki Radnik/Suradnik prihvaća obvezu pridržavati se svih pravila sadržanih u ovom Pravilniku kao svoju radnopravnu ugovornu obvezu te prima na znanje sadržaj Informacije o zaštiti osobnih podataka, koa je dostupna na mrežnoj stranici

Ustanove kao i Pravilnik.Ustanova će informirati Radnike/Suradnike s obzirom na obveze proizašle iz Uredbe i ovog Pravilnika o zaštiti osobnih podataka kako bi se osiguralo potpuno razumijevanje i znanje o obvezama vezanim za privatnost osobnih podataka.

Svaki Radnik/Suradnik Ustanove mora barem jednom godišnje proći edukaciju Ustanove o zaštiti osobnih podataka. Edukacija će se u pravilu izvršiti alternativno ili kao grupna edukacija za Radnik/Suradnike Ustanove uz evidentiranje prisustva edukaciji ili kao pojedinačna edukacija dostavom edukacijskih materijala u formi prezentacije Radnicima/Suradnicima/suradnicima putem e-maila i/ili mrežne stranice Ustanove za one Radnik/Suradnike koji nisu prisustvovali grupnoj edukaciji.

4.1.2 Uvjeti za obradu osobnih podataka u ime Voditelja obrade

Članak 7.

Ukoliko provodi obradu podataka u ime Voditelja obrade, Ustanova mora biti od strane Voditelja obrade imenovano Izvršiteljem obrade. U skladu s Općom uredbom o zaštiti podataka radnje obrade koje provodi Izvršitelj moraju biti uređene ugovorom između Voditelja obrade i Izvršitelja koji će se ugovoriti predmet i trajanje obrade, priroda i svrha obrade, vrsta osobnih podataka i kategorije ispitanika i obveze i prava voditelja obrade. Predmetnim ugovorom potrebno je utvrditi da Ustanova kao izvršitelj:

a) obrađuje osobne podatke samo prema jasnim i dokumentiranim uputama od voditelja;

b) osigura da su se osobe koje su ovlaštene da obrađuju osobne podatke obvezale na povjerljivost;

c) poduzme sve prikladne sigurnosne mjere;

d) ako ju je Voditelj obrade ovlastio za podizvršenje obrade, da u ugovoru s podizvršiteljem obrade nametne iste obveze zaštite podataka iznesene u ugovoru s voditeljem;

e) uzimajući u obzir prirodu obrade, pomaže Voditelju obrade koristeći prikladne tehničke i organizacijske mjere, koliko je to moguće, da ispuni Voditeljevu obvezu odgovora na zahtjeve za ispunjavanjem ispitanikovih prava;

f) pomaže Voditelju u osiguranju pridržavanja obveza iz čl. 32-36 Opće uredbe o zaštiti podataka (sigurnost obrade, obveza obavješćivanja u slučaju povrede osobnih podataka, procjena učinka na zaštitu podataka, prenosivosti), uzimajući u obzir prirodu obrade te informacije koje su dostupne izvršitelju obrade;

g) na zahtjev Voditelja obrade briše ili vrati sve osobne podatke voditelju obrade nakon završetka pružanja usluga;

h) učini dostupnim Voditelju obrade i nadležnom regulatornom tijelu za privatnost sve podatke potrebne da bi se pokazalo pridržavanje zakona o privatnosti podataka.

Svaki korisnik koji u kontekstu svojih zadaća obrađuje osobne podatke u ime voditelja obrade treba se pobrinuti da njegova radnja ne izlazi izvan okvira iznesenih u aktu kojim je imenovan izvršitelj obrade.

U slučaju da izvršitelj obrade prekrši Opću uredbu za zaštitu osobnih podataka, utvrđujući svrhe i sredstva obrade, smatrati će se voditeljem obrade u smislu obrade sa svim odgovornostima koje proizlaze iz toga.

4.2 INFORMACIJA O ZAŠTITI OSOBNIH PODATAKA

Članak 8.

Svaki ispitanik mora od Voditelja obrade dobiti informaciju o osobnim podacima vezanim za obradu njegovih osobnih podataka koja sadrži sve podatke koje zahtijeva Opća uredba za zaštitu podataka („Informacija o zaštiti osobnih podataka"). Takva Informacija o zaštiti osobnih podataka mora se predočiti najkasnije u trenutku prikupljanja osobnih podataka. Ako su osobni podaci nabavljeni od treće strane, Informacija o zaštiti osobnih podataka treba se predati:

a) unutar razumnog roka od trenutka nabave osobnih podataka, no u svakom slučaju najkasnije unutar mjesec dana od prikupljanja, uzimajući u obzir posebne okolnosti pod kojima se obrađuju osobni podaci

b) u slučaju da su osobni podaci namijenjeni komunikaciji s ispitanikom, najkasnije prilikom prvog mogućeg kontakta ili

c) ako je komunikacija zamišljena s drugim primateljem, najkasnije prilikom prve komunikacije, odnosno prikupljanja osobnih podataka.

Informacija o zaštiti osobnih podataka mora sadržavati određene podatke određene Općom uredbom o zaštiti podataka, uključujući, između ostalog, svrhe u koje se osobni podaci obrađuju, detalje o izvršitelju naloga, mogućnost ispitanika da iskoristi svoja prava iz Opće uredbe o zaštiti podataka, rok čuvanja podataka te mogućnost ulaganja prigovora nadležnom regulatornom tijelu za privatnost.

Isključivo Voditelj obrade mora dati ispitanicima Informaciju o zaštiti osobnih podataka dok Izvršitelj obrade mora obraditi osobne podatke u ime Voditelja obrade prema uputama Voditelja obrade i samo u svrhe koje je Voditelj obrade naznačio u pismenom imenovanju Izvršitelja obrade.

Kada nastupa kao voditelji obrade, Ustanova mora predati Informaciju o zaštiti osobnih podataka ispitanicima.

Informacija o zaštiti osobnih podataka je objavljena i uvijek dostupna na internetskim ili intranetskim stranicama i centralnoj oglasnoj ploči Ustanove.

4.3 PRIVOLA ISPITANIKA

Članak 9.

Privola ispitanika potrebna je za obradu osobnih podataka u svim slučajevima, osim u niže definiranim slučajevima prema člancima 6 i 9 Opće uredbe o zaštiti podataka.

Obrada osobnih podataka koji ne predstavljaju posebne kategorije osobnih podataka dopuštena je bez izražene privole ispitanika, ako postoji neki od sljedećih uvjeta:

- kada je obrada je nužna za izvršavanje ugovora u kojem je ispitanik stranka ili kako bi se poduzele radnje na zahtjev ispitanika prije sklapanja ugovora;
- obrada je nužna radi poštovanja pravnih obveza voditelja obrade;
- obrada je nužna kako bi se zaštitili ključni interesi ispitanika ili druge fizičke osobe;
- obrada je nužna za izvršavanje zadaće od javnog interesa ili pri izvršavanju službene ovlasti voditelja obrade;

- obrada je nužna za potrebe legitimnih interesa voditelja obrade 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.

Osim gore navedenog, obrada posebnih kategorija osobnih podataka dopuštena je bez eksplicitnog pristanka ispitanika, u sljedećim slučajevima:

- obrada je nužna za potrebe izvršavanja obveza i ostvarivanja posebnih prava voditelja obrade ili ispitanika u području radnog prava i prava socijalne sigurnosti i socijalne zaštite (uključujući kolektivne ugovore);

- obrada je potrebna za zaštitu života ili zdravlja ispitanika ili drugog pojedinca kada je ispitanik fizički ili pravno spriječen da da privolu;

- obrada je provedena u odnosu na njihove legitimne aktivnosti, s odgovarajućim jamstvima;

- obrada potrebna u svrhe preventivne medicine, medicinskih dijagnoza, upravljanja zdravstvom ili zdravstvenim uslugama, pod uvjetom da osobne podatke obrađuju zdravstveni djelatnici na osnovu posebnih regulative i pravila nadležnih tijela;

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

- obrada se odnosi na osobne podatke za koje je očito da ih je objavio ispitanik;

- obrada je potrebna iz razloga značajnog javnog interesa.

Za svaku obradu osobnih podataka u svrhe koje nisu povezane s provedbom ugovora ili zakona te u svim slučajevima kada se provodi obrada osobnih podataka u svrhe koje nisu povezane s posebnim ugovorom na koje se ovaj Pravilnik odnosi: mora se zahtijevati izričita i odvojena privola od ispitanika (npr. za marketing, u promidžbene svrhe, izradu profila, itd.).

U odnosu na usluge informacijskog društva (usluge pružene na mrežnim stranicama, aplikacijama, itd.), mora se pribaviti ili potvrda da ispitanik nije mlađi od 16 ili odobrenje roditelja/skrbnika u odnosu na usluge informacijskog društva pružene maloljetnicima.

Izričita privola ispitanika mora biti dana papirnato ili elektronički tako da postoji odgovarajući nedvojben dokaz da je privola dana.

4.4 PRAVA ISPITANIKA

Članak 10.

Ispitanici mogu zatražiti izvršenje svojih prava na način da u e-mail poruci pošalju zahtjev za izvršenje nekog od svojih prava osobi za kontakt koju je Ustanova za to odredila.

a) Svi zahtjevi ispitanika trebaju biti proslijeđeni Službeniku za zaštitu podataka Ustanove.

b) Isto tako, ako je zahtjev ispitanika naslovljen na treću stranu (npr., na dobavljača informacijske tehnologije ili na marketinšku agenciju) koja obrađuje osobne podatke

ispitanika u ime Ustanove, ta treća strana mora odmah proslijediti taj zahtjev osobi koja je unutar Ustanove odgovorna za taj ugovor koja će onda pak obavijestiti Službenika za zaštitu podataka. Gornje obveze (obavješćivanja Voditelja) moraju biti uključene u ugovore između Ustanove/voditelja i treće strane/izvršitelja. Službenik za zaštitu podataka mora provjeriti identitet ispitanika koji je podnio zahtjev, te usporediti podatke sadržane u zahtjevu s podacima koje Ustanova već ima.

c) Ako se pronađu nepodudarnosti, mora se kontaktirati ispitanik putem dostupnih podataka o kontaktu te zatražiti od ispitanika da pošalje identifikacijske podatke.

d) Nakon utvrđivanja identiteta ispitanika mora se;

   i) odmah zabilježiti takav zahtjev ispitanika kako bi se osigurala koordinacija i uključivanje drugih odjela Ustanove koji mogu biti mjerodavni - ovisno o zahtjevu, a kako bi se omogućilo identificiranje osobnih podataka koji su predmetom zahtjeva te zajamčilo da će se zahtjev provesti (npr. u slučaju zahtjeva za zaborav). Provedba zahtjeva je potrebna u odnosu na sve računalne sustave i dokumente Ustanove. i njihovih dobavljača. Službenik za zaštitu podataka mora osigurati da je pridržavanje zahtjeva ispitanika uredno zabilježeno.

   ii) Bez odgode pismeno (pismenim putem ili e-mailom) odgovoriti ispitaniku **unutar 30 kalendarskih dana od ispitanikovog zahtjeva.**

Ako je zahtjev posebno kompleksan, Službenik za zaštitu podataka Ustanove mora:

   iii) tamo gdje je to primjenjivo, **unutar 30 kalendarskih dana** od zahtjeva pismeno ispitaniku objasniti razloge zbog kojih je potrebno produljenje roka za odgovor;

   iv) U svakom slučaju, **unutar 60 kalendarskih dana** od obavijesti o produljenju pismeno odgovoriti ispitaniku.

Ne mogu se naplatiti troškovi ispunjenja zahtjeva ispitanika, osim u slučajevima kada (i) je ispitanikov zahtjev očito neosnovan ili pretjeran tj. repetitivan u slučaju kada ispitanik zatraži dodatne primjerke u odnosu na one predane na prvi zahtjev.

4.4.1 Pravo pristupa osobnim podacima

Članak 11.

Ispitanici imaju pravo ishoditi potvrdu o tome jesu li njihovi osobni podaci u postupku obrade te, ako je to slučaj, imaju pravu dobiti pristup svojim osobnim podacima kao i informacijama o sljedećim činjenicama:

a) podrijetlo osobnih podataka;

b) svrhe obrade;

c) kategorije predmetnih osobnih podataka;

d) gdje je moguće, predviđenom razdoblju pohrane osobnih podataka ili, ako to nije moguće, kriterijima koji se koriste u svrhu određivanja tog razdoblja;

e) postojanju prava na zahtjev za ispravljanjem ili brisanjem osobnih podataka ili ograničenjem obrade osobnih podatka koji se tiču ispitanika ili na prigovor takvoj obradi (prema postupcima opisanima u ovome članku);

f) o postojanju automatskog odlučivanja, uključujući izrade profila i, u tom slučaju, primijenjenoj logici i predviđenim posljedicama takve obrade za ispitanika;

g) o primateljima ili kategorijama primatelja kojima su osobni podaci otkriveni ili će biti otkriveni (u slučaju prijenosa osobnih podataka), posebice primateljima u trećim zemljama (ili međunarodnim organizacijama) i, ako je to slučaj, o postojanju odgovarajućih mjera zaštite tog prijenosa;

h) pravo na ulaganje prigovora nadležnom regulatornom tijelu.

Ispitanik može također zatražiti primjerak obrađenih podataka pod uvjetom da to ne krši prava i slobode ostalih ispitanika. Takve podatke vlasnik procesa mora elektronički predati ispitaniku koji postavlja zahtjev putem e-poruke, ili pismeno u drugim slučajevima, a detalje o trećim stranama mora prekriti ili izbrisati.

Kada nastupa kao izvršitelj obrade, Ustanova mora pomoći voditeljima obrade odgovarajućim tehničkim i organizacijskim mjerama za ispunjenje gornjih obveza. Pravo na ispravljanje i objedinjavanje

Ispitanici imaju pravo na ispravljanje netočnih osobnih podataka ili objedinjavanje nepotpunih osobnih podataka. Nakon što se podaci isprave, vlasnik će procesa e-mail porukom ili pismenim putem poslati potvrdu ispitaniku koji je podnio zahtjev, a detalji o trećim stranama moraju biti prekriveni ili izbrisani.

Kada nastupa kao izvršitelj obrade, Ustanova mora pomoći voditeljima obrade odgovarajućim tehničkim i organizacijskim mjerama za ispunjenje gornjih obveza. Ovo se mora urediti ugovorima u koje izvršitelj stupa sa svojim podizvršiteljima.. Službenik za zaštitu podataka je odgovoran za uključenje informacijsko-tehnološkog odjela i ostalih relevantnih odjela u procjenu tehničkih i organizacijskih mjera predviđenih u ugovoru s klijentima.

4.4.2 Pravo na brisanje („Pravo na zaborav")

Članak 12.

Ispitanici imaju pravo na brisanje osobnih podataka koji se odnose na njih kada:

a) osobni podaci više nisu potrebni za svrhe u koje su prikupljeni;

b) ispitanici povuku svoju privolu na osnovu koje se provodi obrada i ukoliko nema druge pravne osnove za daljnju obradu;

c) se ispitanici protive obradi (vidi odjeljak 8.6) - ispitanik uloži prigovor na obradu, te ne postoje jači legitimni razlozi za obradu;

d) su osobni podaci nezakonito obrađivani;

e) osobni podaci moraju biti obrisani kako bi se ispunila zakonska obveza; i

f) su osobni podaci prikupljeni u vezi ponude usluga informacijskog društva - nuđenja usluga informacijskog društva izravno djetetu.

Kada nastupa kao izvršitelj obrade, Ustanova mora pomoći voditeljima obrade odgovarajućim tehničkim i organizacijskim mjerama za ispunjenje gornjih obveza, a mjere se moraju precizno opisati u ugovorima kojima se stupa u odnos s klijentima.

4.4.3 Pravo na ograničavanje obrade

Članak 13.

Ispitanici mogu ishoditi ograničenje obrade osobnih podataka koji se odnose na njih, što rezultira time da se podaci na ograničeno razdoblje ne mogu koristiti u sljedećim situacijama:

a) kada ispitanik osporava točnost osobnih podataka, i to na razdoblje potrebno Ustanovi da provjeri točnost takvih podataka;

b) kada je obrada nezakonita te se ispitanici protive brisanju osobnih podataka te zahtijevaju ograničenje njihove uporabe;

c) kada voditelj obrade više ne treba osobne podatke za potrebe obrade, ali ih ispitanik traži radi postavljanja, ostvarivanja ili obrane pravnih zahtjeva u nekom odvojenom postupku;

d) kada se ispitanici usprotive obradi, dok se od Ustanove čeka potvrda nadilaze li legitimni razlozi Ustanove razloge ispitanika.

U gornjim slučajevima, kada nastupaju kao voditelji obrade, subjekti Ustanove smiju osobne podatke ispitanika obrađivati samo u svrhe pohrane, u suradnji sa Službenikom za zaštitu podataka. i svim drugim relevantnim službama uključenima u tu svrhu.

U tim okolnostima, osim pohrane, Ustanova može obrađivati ispitanikove podatke – u očekivanju ograničenja obrade – samo u sljedećim okolnostima:

i) kada su ispitanici dali svoju privolu;

ii) radi ostvarivanja ili obrane pravnih zahtjeva ili zaštitu prava druge fizičke ili pravne osobe;

iii) kako bi se zajamčila zaštita prava Ustanove;

iv) relevantnih razloga javnog interesa.

Kada nastupa kao Izvršitelj obrade, Ustanova mora pomoći Voditeljima obrade odgovarajućim tehničkim i organizacijskim mjerama za ispunjenje gornjih obveza. Ovo se mora urediti ugovorima u koje se stupa s klijentima.

4.4.4 Pravo na prenosivost podataka

Članak 14.

Ispitanik ima pravo zaprimiti osobne podatke koji se odnose na njega, a koje je pružio Ustanovi , u strukturiranom, uobičajeno upotrebljavanom i strojno čitljivom formatu te ima pravo prenijeti te podatke drugom voditelju obrade bez ometanja od Ustanove ako je:

i) obrada provedena automatiziranim sredstvima

ii) obrada zasnovana na privoli ispitanika ili temeljem legitimnog interesa - ugovora čija je ispitanik strana; i

iii) one podatke koji su predmetom zahtjeva za prijenosom dao ili generirao sam ispitanik (isključujući informacije koje je Ustanova izvela ili zaključila na temelju informacija koje je dao isti ispitanik).

Kada nastupa kao Voditelj obrade, Ustanova mora implementirati odgovarajuće postupke kako bi se osiguralo ispunjenje gornjih uvjeta.

Kada nastupa kao Izvršitelj obrade, Ustanova mora pomoći voditeljima obrade odgovarajućim tehničkim i organizacijskim mjerama za ispunjenje gornjih obveza. Ovo se mora urediti ugovorima u koje se stupa s klijentima.

4.4.5 Pravo na prigovor

Članak 15.

Ispitanik ima pravo prigovoriti obradi osobnih podataka koji se odnose na njega kada te podatke Ustanova obrađuje, između ostaloga, u izravne marketinške svrhe, uključujući izradu profila.

4.4.6 Pravo da se na ispitanika ne odnosi odluka koja se temelji isključivo na automatiziranoj obradi

Članak 16.

Ispitanici imaju pravo da se na njih ne odnosi odluka koja se isključivo temelji na automatiziranoj obradi tj. bez ljudske intervencije, uključujući i izradu profila, osim u slučajevima kada:

a) je to potrebno za svrhe sklapanja ili ispunjenja ugovora između ispitanika i voditelja obrade;

b) se temelji na eksplicitnoj privoli ispitanika.

Gornji scenarij predviđen je, na primjer ako je tijekom postupka zaposlenja Ustanova zadala automatsku provjeru i odabir kandidata koji su stoga isključeni isključivo temeljeno na automatiziranoj odluci.

Kada nastupa kao Voditelj obrade, Ustanova mora implementirati odgovarajuće postupke kako bi se osiguralo ispunjenje gornjih uvjeta.

Kada nastupa kao Izvršitelj obrade, Ustanova mora pomoći voditeljima obrade odgovarajućim tehničkim i organizacijskim mjerama za ispunjenje gornjih obveza. Ovo se mora urediti ugovorima u koje se stupa s klijentima. Službenik za zaštitu podataka je odgovoran za uključenje informacijsko-tehnološkog odjela i ostalih relevantnih odjela u procjenu tehničkih i organizacijskih mjera predviđenih u ugovoru s klijentima.

4.5 UPRAVLJANJE OSOBNIM PODACIMA

Članak 17.

Osobni podaci ne mogu se otkriti trećoj strani ako ispitanik nije dao svoju privolu ili ako ne postoji druga pravna osnova za svrhe prijenosa podataka, na primjer - ako se ona odnosi na treću stranu koja obrađuje osobne podatke u ime Ustanove i čije su radnje potrebne za provedbu ugovora s trećom stranom (npr. informacijsko-tehnološke usluge) ili za pružanje usluga trećoj strani (npr. daljnje praćenje zahtjeva treće strane.

Kao općenito pravilo, osim u slučaju posebnih iznimki u skladu s mjerodavnim pravima, osobni podaci ne mogu se prenijeti izvan Europskog gospodarskog prostora (EU/EEU), osim ako se s

primateljem podataka ne provedu aranžmani iz Opće uredbe o zaštiti podataka koji odobravaju takve prijenose, kao na primjer tzv. Standardne ugovorne klauzule EU-a za prijenose podataka.

4.6 ROK ČUVANJA / POHRANE PODATAKA

Članak 18.

Osobni podaci moraju se obraditi unutar razdoblja koje je potrebno za određene svrhe obrade, kao što to primjerice može biti prikazano u Informaciji o zaštiti osobnih podataka koja je predana ispitaniku na koga se ti podaci odnose, odnosno sukladno odredbama Pravilnika o zaštiti i obradi arhivskog i registraturnog gradiva Ustanove, ili drugog pravnog izvora koji se primjenjuje na zaštitu i obradu arhivskog i registraturnog gradiva.U odnosu na svaku kategoriju osobnih podataka, Ustanova kao voditelj obrade primjenjuje pravila određena primjenjivim propisima, pravila određena u informacijama danim ispitanicima, kao i pravila određena ovim Pravilnikom. Nakon proteka roka za čuvanje podataka osobni se podaci moraju uništiti, izbrisati i/ili anonimizirati.

Voditelj obrade mora:

a) odrediti rok čuvanja podataka vezan za svaku zasebnu kategoriju osobnih podataka;

b) osigurati uredno bilježenje roka čuvanja podataka u registru podataka na kojemu su pohranjeni podaci, zajedno s povezanom dokumentacijom;

c) uključiti u postupak Službenika za zaštitu podataka kako bi se usvojile odgovarajuće mjere u svrhu sprječavanja da se podaci čiji je rok pohrane istekao koriste u druge svrhe osim ispunjenja zakonskih obveza;

d) osigurati brisanje tih podataka nakon isteka relevantnog razdoblja čuvanja podataka, odnosno sukladno odredbama Pravilnika o zaštiti i obradi arhivskog i registraturnog gradiva Ustanove ili drugog pravnog izvora koji se primjenjuje na zaštitu i obradu arhivskog i registraturnog gradiva.

O provođenju gornjih radnji mora postajati mogućnost dokazivanja njihova izvršenja u dokumentiranom obliku.

Kada nastupa kao Izvršitelj obrade, Ustanova mora odmah uništiti, izbrisati, anonimizirati ili vratiti sve osobne podatke obrađene u ime Voditelja obrade nakon isteka sporazuma s tim voditeljem obrade, osim ako mjerodavno pravo ne nalaže pohranu tih podataka.

4.7 UGOVORNI AKTI – SMJERNICE ZA ODREĐIVANJE TREĆE STRANE IZVRŠITELJEM OBRADE

4.7.1 Određivanje Izvršiteljem obrade

Članak 19.

Kada dobavljač pristupa osobnim podacima koje obrađuje Ustanova, Ustanova će osigurati da je ta strana prikladna za obradu osobnih podataka u ime Ustanove u skladu s primjenjivim propisima tako da dobavljač ,

a) ispuni upitnik za za provjeru, dobavljača i njegovih podugovaratelja koji će imati pristup podacima – tzv. Podizvršiteljima obrade;

b) Ustanova ako je to potrebno, provede dodatne provjere prema odluci Ustanove u suradnji s odjelom nadležnim za nabavu i Službenikom za zaštitu podataka.

Ugovor se s dobavljačem ne može sklopiti ako gore navedene provjere pokažu da nije dovoljno zajamčeno pridržavanje propisa iz područja zaštite osobnih podataka, bilo iz tehničkih, organizacijskih ili drugih razloga.

U svakom slučaju, sporazum o obradi osobnih podataka mora prethodno odobriti Službenik za zaštitu podataka, koji također treba komunicirati s odjelom nadležnim za nabavu kako bi ishodio primjerak predloška sporazuma kojim se osigurava valjano postupanje s podacima koje je prikupio Voditelj obrade, odnosno Ustanova.

Ured odgovoran za ugovorni odnos s dobavljačem (obično odjel nabave) mora Službeniku za zaštitu podataka dati primjerak potpisanog sporazuma o obradi osobnih podataka u svrhe arhiviranja.

Određivanje izvršitelja obrade je neophodno primjerice prilikom sklapanja ugovora s informacijsko-tehnološkim savjetnicima, pružateljima informacijsko-tehnoloških usluga, trgovcima, dobavljačima kao što su to dobavljači financijskih usluga, pružatelji usluga, marketinške agencije, itd.

4.7.2 Određivanje podizvršiteljem obrade

Članak 20.

Kada Ustanova nastupa kao Izvršitelj obrade, kako bi odredila drugog izvršitelja obrade (tj. podizvršitelja), mora potvrditi da je taj podizvršitelj podoban za obradu osobnih podataka u ime Ustanove, ali i u ime relevantnog voditelja obrade. U tu svrhu, moraju se dodatno poduzeti i sljedeće radnje:

a) Vlasnik procesa mora prije odobravanja provedbe sporazuma s podizvršiteljem provjeriti je li postavljanje tog podizvršitelja odobrio voditelj obrade općenitim odobrenjem sadržanim u sporazumu između Ustanove i Voditelja obrade (npr. sporazum sadrži izričito odobrenje za postavljanje određene kategorije podizvršitelja obrade) te u slučaju da ne postoji općenito odobrenje, posebno se odobrenje mora ishoditi od Voditelja obrade;

b) U slučaju da je podizvršitelj obrade uredno odobren od Voditelja obrade u skladu s točkom a) gore, odjel nabave ili ured odgovoran za ugovorni odnos mora imenovati tog podizvršitelja, a koje imenovanje će biti evidentirano u sporazumu između Ustanove i podizvršitelja, a koji sadrži iste obveze prikazane u sporazumu između Ustanove i Voditelja obrade. Svaku izmjenu tog predloška mora odobriti Službenik za zaštitu podataka sukladno gore navedenoj točki a).

4.8 OSOBE ZADUŽENE ZA NADZOR NAD PRIDRŽAVANJEVM PROPISA O ZAŠTITI OSOBNIH PODATAKA – VLASNIK PROCESA I SLUŽBENIK ZA ZAŠTITU OSOBNIH PODATAKA

Članak 21.

Ustanova je imenovala Službenika za zaštitu podataka u cilju što kvalitetnijeg izvršenja svih obveza Ustanove u vezi sa zaštitom podataka.

Kako bi se pratilo pridržavanje Opće uredbe o zaštiti podataka, svaki vlasnik procesa unutar Ustanove na odgovarajući je način upućen o tome kako postupati u pitanjima zaštite osobnih podataka.. U situacijama gdje je to potrebno, vlasnik procesa treba se savjetovati sa Službenikom za zaštitu podataka, voditeljem pravnog odjela a po potrebi i uputi svojih internih funkcija unutar Ustanove i sa regulatornim tijelom.

Službenik za zaštitu podataka Ustanove mora se brzo i odgovarajuće uključiti u sva pitanja koja se tiču zaštite osobnih podataka. Službenik za zaštitu podataka je, između ostaloga, zadužen za sljedeće zadaće:

i) obavještavanje i savjetovanje u odnosu na obveze koje proizlaze iz Opće uredbe o zaštiti osobnih podataka kao i iz drugih odredbi koje se odnose na obradu osobnih podataka;

ii) podrška Ustanovi u zadaćama praćenja pridržavanja nadležnih zakona o privatnosti kako bi se izbjegle povrede te posljedični rizici za subjekte Ustanove;

iii) povećanje svjesnosti o obvezama vezanim za privatnost i provedba edukacija u vezi sa zaštitom osobnih podataka;

iv) davanje mišljenja, ako tako zatraži Ustanova, vezano za izradu procjene učinka na zaštitu podataka;

v) suradnja s klijentima i Ustanovom u svrhu osiguravanja pridržavanja načela tehničke i integrirane zaštite privatnosti;

vi) suradnja s nadležnim regulatornim tijelom za zaštitu osobnih podataka;

vii) djelovanje kao kontaktna točka za nadležno tijelo za privatnost/klijenta vezano za pitanja obrade osobnih podataka, uključujući prethodne konzultacije kako je propisano člankom 36 Opće uredbe o zaštiti podataka;

viii) podnošenje izvještaja upravi Ustanove o statusu pridržavanja Opće urede o zaštiti podataka te dostava relevantnih informacija, dokumenata te novosti vezanih za pridržavanje Uredbe (uključujući informacije o zahtjevima ili istragama nadležnog tijela za privatnost.

Službenik za zaštitu podataka kao i pojedini vlasnik procesa moraju biti uključeni u implementaciju svih postupaka vezanih za obradu osobnih podataka kako bi se (i) osiguralo da se Ustanova pridržava obveza određenih primjenjivim propisima i (ii) izbjegao rizik povrede osobnih podataka.

U slučaju da je vlasnik procesa upoznat s povredom nadležnih zakona o privatnosti, isti o povredi mora obavijestiti nadređenu osobu u Ustanovi .

Vlasnik procesa zajedno sa Službenikom za zaštitu podataka i pravnim odjelomprocijeniti će plan korektivnih radnji potrebnih radi usklađenja s pravilima o zaštiti osobnih podataka koji će se implementirati unutar Ustanove.

Svu komunikaciju s nadležnim regulatornim tijelom za privatnost čuva Službenik za zaštitu podataka.

4.9 PRIDRŽAVANJE NAČELA TEHIČKE I INTEGRIRANE ZAŠTITE PRIVATNOSTI (Data protection „by design“ and „by default“)

Članak 22.

Sve osobe unutar Ustanove koje provode novu radnju i/ili namjeravaju razviti novu uslugu koja uključuje obradu osobnih podataka moraju slijediti sljedeća načela:- Tehnička zaštita privatnosti: svaka usluga mora se razvijati tako da se zaštita osobnih podataka uzima u obzir od početne faze razvoja usluge;

- Integrirana zaštita osobnih podataka: svaka usluga mora imati implementirane mjere kako bi se osiguralo da se (kao kod tehničke zaštite), obrađuju samo osobni podaci koji su potrebni za te svrhe obrade, posebice u odnosu na količinu prikupljenih osobnih podataka, raspon njihove obrade, razdoblje pohrane i mogućnosti pristupa tim podacima.

U tu svrhu svaki Radnik/Suradnik Ustanove pri razvoju novih usluga mora slijediti pravila ovog Pravilnika.

Članak 23.

Vlasnik procesa uz savjetovanje sa Službenikom za zaštitu podataka mora procijeniti je li potrebno:

- provesti procjenu učinka na zaštitu podataka; i

- uključiti osoblje iz drugih odjela u procjenu učinka na zaštitu podataka, pritom osiguravajući da se redovni sastanci održavaju tijekom razvoja usluge, u svrhu zajedničke analize:

rizika vezanih za obradu osobnih podataka koji proizlaze iz nove usluge;

akcijskog plana prema kojemu je potrebno implementirati potencijalne korektivne mjere kako bi se otklonili rizici ili, ako to nije moguće, barem minimizirali;

toga je li nova usluga razvijena u skladu s akcijskim planom.

Članak 24.

Po završetku radnji opisanih u čl. 23, Vlasnik procesa mora poslati Službeniku za zaštitu podataka izvještaj u kojem će opisati kako su se riješila pitanja vezana za privatnost, a koja su se pojavila tijekom provođenja opisanih radnji.

Gore prikazani postupak mora se poštivati u odnosu na sve promjene ili ažuriranja postojećih proizvoda, usluga ili radnji koje dovode do promjene u količini ili vrsti obrađenih osobnih podataka ili do postupka za obradu osobnih podataka.

Zabranjeno je razvijati ili provoditi radnje povezane s bilo kojim novim proizvodom, uslugom alatom ili tehničkom aplikacijom koji su usmjereni prema ispitanicima ili s drugim funkcionalnostima koje dovode do obrade osobnih podataka, a da se pritom ne prati postupak prikazan u ovom odjeljku.

Vlasnik procesa mora uredno dokumentirati i pokrenuti gornji postupak te osigurati da se Radnici/Suradnici i odjeli koji će biti uključeni mogu lako pristupiti platformi na kojoj su dokumentirani postupci i procjene od strane Radnika/Suradnika kako bi dali svoj doprinos i dovršili svoje zadaće.

4.10 VRŠENJE PROCJENE UČINKA NA ZAŠTITU PODATAKA

Članak 25.

Ako tijekom ili nakon analize opisane u članku 23., ili u nekim drugim okolnostima vlasnik procesa u suradnji sa Službenikom za zaštitu podataka procijeni da je potrebno izvršiti Procjenu učinka na zaštitu podataka (PUZP) u skladu s člankom 35 Uredbe, Procjena učinka na zaštitu podataka će se izvršiti procjenom prema sljedećim kriterijima:

Primjeri obrade	**Mogući relevantni kriteriji**
Ustanova koja sustavno prati radnje svojih Radnika/Suradnika, uključujući i praćenje radnih mjesta Radnika/Suradnika, aktivnost na internet itd.	- sustavno praćenje - podaci vezani za ranjive ispitanike

Pohrana u svrhe arhiviranja pseudonimiziranih osobnih posebno osjetljivih podataka vezano za ranjive ispitanike u istraživačkim projektima ili kliničkim studijama	- posebno osjetljivi podaci - podaci vezani za ranjive ispitanike - sprječava ispitanika da iskoristi pravo, koristi uslugu ili ugovor
Obrada biometrijskih ili genetskih podataka	- posebno osjetljivi podaci - podaci vezani za ranjive ispitanike - sprječava ispitanika da iskoristi pravo, koristi uslugu ili ugovor

Kada nastupa kao Izvršitelj obrade, Ustanova, gdje je to zatraženo, mora pomoći Voditelju obrade pri vršenju PUZP-a i pritom uzeti u obzir prirodu obrade i informacije dostupne izvršitelju.

4.11 UPRAVLJANJE I PRAĆENJE E-ADRESE NAMIJENJENE ZA KOMUNIKACIJU VEZANU ZA PITANJA PRIVATNOSTI

Članak 26.

Radnici/suradnici Ustanove sva pitanja i zahtjeve koji se odnose na obradu njihovih podataka ili bilo što drugo povezano s privatnosti podataka trebaju dostavljati na sljedeću e-mail adresu:

zastitaosobnihpodataka@dzz-centar.hr

Službenik za zaštitu podataka prati tu e-mail adresu kako bi osigurao da se dolazna pošta stalno analizira te da se brzo obradi ili proslijedi nadležnim odjelima.

4.12 PRAĆENJE I IZVJEŠTAVANJE

Članak 27.

Svaka odgovorna osoba mora periodično provjeriti radnje vezane za obradu podataka koju provodi Ustanova.

Nakon tih provjera vlasnik procesa, a posebice u hitnim slučajevima (npr. u slučaju povrede osobnih podataka) mora poslati Službeniku za zaštitu podataka i voditelju pravnog odjela izvještaj u kojem će navesti između ostalog: (i) sve potencijalne povrede pri obradi osobnih podataka i povezane korektivne mjere, (ii) predmetne značajne rizike ili probleme pri obradi osobnih podataka, (iii) sve provedene procjene učinka na zaštitu podataka te one preporučene, i (iv) nove projekte i njihovu usklađenost s načelima tehničke i integrirane zaštite podataka.

4.13 BILJEŽENJE RADNJI OBRADE – EVIDENCIJE AKTIVNOSTI OBRADE

Članak 28.

Ustanova mora stvoriti i ažurirati bilješke o radnjama obrade, što izvršava upotrebom pripremljenih obrazaca Evidencije aktivnosti obrade, koje su dostupne svim Vlasnicima procesa i ostalim Radnicima/Suradnicima ustanove i koje se redovito ažuriraju. Radnje obrade koje provodi Ustanova

kao Voditelj obrade moraju biti odvojene od onih radnji koje Ustanova provodi kao Izvršitelj obrade u ime klijenta. U tu svrhu svaki Vlasnik procesa kojeg je odredila Ustanova mora biti zadužen za stvaranje, ispunjavanje i održavanje dviju različitih bilješki o obradi podataka koji spadaju pod njegovo područje odgovornosti (za tim, projekte, područja, usluge, klijente i isporuku za koje je odgovoran):

i) Evidencija o radnjama obrade kao voditelja obrade:

Evidencija o radnjama obrade Ustanove koja nastupa kao Voditelji obrade mora sadržavati najmanje sljedeće informacije:

a) ime i podatke o kontaktu Voditelja obrade (tj. Ustanove) i, gdje je to primjenjivo, zajedničkog voditelja obrade, predstavnika voditelja obrade i službenika za zaštitu podataka, ako je imenovan;

b) svrhu obrade;

c) opis kategorija ispitanika i kategorija osobnih podataka;

d) kategorije primatelja kojima se daju ili moraju biti dani osobni podaci, uključujući primatelje iz treće zemlje;

e) gdje je to primjenjivo, prijenose osobnih podataka u treću zemlju s naznakom treće zemlje te dokumentacijom vezanom za odgovarajuća jamstva;

f) rokove za brisanje raznih kategorija osobnih podataka; i

g) općeniti opis usvojenih sigurnosnih tehničkih i organizacijskih mjera.

ii) Evidencija o radnjama obrade kao izvršitelja obrade:

Evidencija o radnjama obrade subjekata Ustanove koji nastupaju kao izvršitelji obrade mora sadržavati najmanje sljedeće informacije:

a) ime i podaci o kontaktu izvršitelja obrade (tj. Ustanove) te svakog voditelja obrade u čije ime izvršitelj obrade djeluje i, gdje je to primjenjivo, predstavnika voditelja ili izvršitelja obrade i službenika za zaštitu podataka, ako je imenovan;

b) kategorije obrade provedene u ime svakog voditelja obrade;

c) gdje je to primjenjivo, prijenose osobnih podataka u treću zemlju s naznakom treće zemlje i dokumentacijom vezanom za prikladna jamstva;

d) općeniti opis usvojenih sigurnosnih tehničkih i organizacijskih mjera.

Predmetni vlasnik procesa odgovoran je za ažuriranje gornjih evidencija.

5. GLAVA 2 - PRAVILA ZA ODGOVARAJUĆU POHRANU DOKUMENATA USTANOVE

5.1 POHRANA

Članak 29.

Ustanova mora osigurati da svi Radnici/Suradnici slijede sljedeća pravila vezana za sigurnost i zaštitu podataka u Ustanovi. Svi prostori i spremnici za dokumente u kojima se nalaze dokumenti koji

sadrže povjerljive podatke ili osobne podatke korištene za radnje Ustanove moraju biti zaključani pri napuštanju radnog mjesta.;

Dokumenti koji sadrže osobne podatke ne smiju biti dostupni neovlaštenim osobama, posebice u slučaju odsustva odgovorne osobe s posla, već se moraju držati u ladicama u stolu i arhivima koji moraju biti zaključani;

Pristup arhivima gdje se drže osobni podaci mora biti ograničen samo na Radnike/Suradnike čiji je pristup opravdan njihovim radnim zadatkom.

Dokumenti uklonjeni iz arhiva ili radnih prostora moraju se pohraniti čim je njihova potrebna uporaba gotova, a arhivi i/ili radni prostori moraju biti zaključani.

Zabranjeno je koristiti USB-memorijske stick-ove, memorijske kartice, vanjske tvrde diskove, uređaje, laptope, računala i uređaje za pohranu podataka osim ako ih je informacijsko-tehnološki ili drugi odgovarajući odjel predmetnih subjekata Ustanove posebno odobrio ili nabavio. Nije dopušteno prenositi podatke sadržane unutar ili na bilo koji način povezane s radnim zadatkom na privatne USB-memorijske stick-ove, memorijske kartice, vanjske tvrde diskove, uređaje ili računala, privatne račune e-pošte ili bilo koje račune osim onog zadanog od predmetnog subjekta Ustanove, na internetske platforme za spremanje podataka i općenito na bilo koji uređaj, platforma ili račun koji ne dolaze ili nisu odobreni od subjekata Ustanove.

Zabranjeno je spremiti bilo koji dokument, datoteku ili sadržaj na bilo koje računalo osim na računalo Ustanove ili uređaj dan od Ustanove za provedbu radnog zadatka, ili u mrežne datoteke Ustanove.

Dokumenti koji sadrže povjerljive informacije ili osobne podatke moraju se što prije ukloniti iz printera i telefaksa.

Dokumenti, elektronički uređaji i uređaji za pohranu podataka ne smiju se ostaviti u sobama za sastanke te mjestima koja se nalaze izvan neposredne kontrole predmetnog Radnika/Suradnika.

Dokumenti, informacije ili osobni podaci povezani s radnim zadatkom koji provode subjekti Ustanove ne smiju se fotografirati niti snimati video uređajem ili općenito snimati ni na koji način, osim u slučaju medicinske obrade.

Mora se spriječiti da gore spomenuti dokumenti, elektronički uređaji i uređaji za pohranu podataka postanu dostupni osobama koje u tu svrhu nisu dobile izričito odobrenje ili da se isti ostavljaju na nedozvoljenim mjestima u uredima ili na putu, na javnim mjestima ili drugim lokacijama dostupnima javnosti.

Službenik za zaštitu podataka mora pratiti pridržavanje gore opisanih obveza te pismeno obavijestiti Upravu Ustanove u slučaju bilo kakve povrede. Uprava Ustanove i Službenik za zaštitu podataka moraju zajedno s odjelom ljudskih resursa koordinirati svaku disciplinsku mjeru te s voditeljem pravnog odjela procijeniti svaki daljnji postupak.

Ustanova mora osigurati da arhivima ne mogu pristupiti neovlaštene osobe izvan relevantnog odjela. U slučaju odsustva s posla, imenovana osoba mora odrediti zamjenu koja ima pravo pristupa arhiviranim podacima.

6. GLAVA 3 – PRAVILA ZA ODGOVARAJUĆU UPORABU INFORMACIJA, SUSTAVA I USLUGA USTANOVE

6.1 DOPUŠTENA UPORABA

6.1.1 Svrha

Članak 30.

Svi Radnici/Suradnici obvezni su slijediti sljedeća pravila vezana za informacijsku sigurnosti unutar Ustanove;

6.1.2 Tehnološki uređaji

Članak 31.

Svi su Radnici/Suradnici odgovorni za upravljanje i čuvanje tehničkih uređaja koji im je dala Ustanova za provedbu radnog zadatka. Takvi uređaji uključuju računala i/ili prijenosne uređaje poput laptopa, pametnih mobitela, tableta, token-a ili vanjskih memorija. Radnici/Suradnici moraju:

a) osigurati da se prijenosni uređaji uvijek čuvaju na zaštićenom mjestu (npr. tijekom putovanja, u uredu izvan radnog vremena ili izvan ureda) te se pobrinuti da nisu izloženi daljnjim rizicima kao što je to ostavljanje uređaja u automobilu na vidljivom mjestu bez nadzora;

b) uvijek zaključati ili ugasiti računalo prije nego što ga se ostavi bez nadzora;

c) ugasiti svoje računalo na kraju svakog radnog dana, ili ostaviti uključeno ali zaključano radi potrebe održavanja ili druge slične potrebe;

d) suzdržati se od pokušaja uklanjanja, deinstalacije, onesposobljavanja, kršenja ili zaobilaženja mjera implementirane za zaštitu uređaja;

e) suzdržati se od spajanja svojih uređaja na mreže ili sustave koji nisu sigurni i/ili pouzdani;

f) izbjegavati spajanje bilo kojeg osobnog uređaja i uređaja treće strane, uključujući mobilne uređaje i vanjske memorije na uređaje i mreže Ustanove;

g) Suzdržati se od pokušaja instalacije aplikacija ili software-a na uređaje Ustanove. Samo služba za podršku Ustanove ima odobrenje da instalira software na uređaje Ustanove.

6.1.3 Korisnički računi

Članak 32.

Većina Radnika/Suradnika Ustanove mora imati pristup – unutar granica koje su potrebne za provedbu njihovog radnog zadatka – sustavima i uslugama i stoga i osobnim podacima jednog ili više ispitanika Ustanove. Pristup računalnim sustavima dopušten je samo s jedinstvenim identitetom i lozinkom. Korisnički su računi postavljeni tako da svaki radnik/suradnik može imati pristup samo informacijama za provedbu svog radnog zadatka te se slijedom toga gore navedene vjerodajnice moraju adekvatno zaštititi. Konkretno, Radnici/Suradnici moraju:

a) suzdržati se od dijeljenja, komuniciranja ili provođenja bilo koje radnje koja može dovesti do toga da treća strana nabavi njihove vjerodajnice, uključujući i članove obitelji ili njima bliske osobe;

b) u slučaju sumnje da su im vjerodajnice kompromitirane, smjesta promijeniti PIN i lozinku;

c) suzdržavati se od pristupa ili pokušaja pristupa informacijama, sustavima i uslugama Ustanove za pristup kojima nemaju odobrenje;

d) suzdržati se od korištenja računa drugih Radnika/Suradnika ili provođenja drugih radnji povezanih s računom koji im ne pripada;

e) suzdržati se od ponovnog korištenja ili kopiranja njihovih vjerodajnica za račun (npr. korisničkog identiteta i lozinki) kako bi stvorili druge, posebice osobne račune, kao i od spremanja ili kopiranja njihovih vjerodajnica na uređaje, dokumente i druga pomagala;

f) suzdržati se od korištenja iste lozinke sa svog osobnog računa za njihov račun pri Ustanovi;

g) suzdržati se od korištenja javnih računala za pristup informacijama, sustavima i uslugama subjekata Ustanove;

h) osigurati da su sve lozinke i PIN-ovi u skladu sa zahtjevima lozinki Ustanove, kao što je to definirano u donjim člancima.

Ustanova je usvojila sustave obavještavanja koji (i) sprečavaju nedopušten pristup podacima za koji radnik/suradnik nema odobrenje i (ii) prijavljuju sve sumnjive uporabe uređaja nadležnom odjelu.

6.1.4 Korisničke lozinke

Članak 33.

Korisničke lozinke za sustave Ustanove moraju slijediti format lozinke koji se sastoji od minimalno osam znakova, od kojih je najmanje jedan znak veliko slovo, najmanje jedan znak broj i najmanje jedan znak poseban dijakritički simbol (primjerice #, &, /, ?, *, ' ili slično).

6.1.5 Lozinka/PIN za mobilne uređaje

Članak 34.

Lozinke i PIN-ovi za mobilne uređaje (npr. pametni telefon, i tablet) moraju slijediti format lozinke koja se sastoji od minimalno četiri do najviše dvanaest brojeva.

Elektronička komunikacija

Članak 35.

Poslovne aktivnosti Ustanove zahtijevaju sposobnost efikasne komunikacije s , Radnicima/Suradnicima, klijentima i poslovnim partnerima. Elektronički kanali komunikacije poput e-mailova i instant poruka olakšavaju dnevni tijek komunikacija unutar i izvan organizacije. Pri elektroničkom komuniciranju informacija Radnici/Suradnici moraju:

a) suzdržati se od slanja dokumenata, informacija ili osobnih podataka e-porukom ili drugim komunikacijskim sredstvima osim ako:

   i) nisu adekvatno zaštićene koristeći kriptografski sustav;

   ii) ne postoji ugovor o povjerljivosti s predmetnom trećom stranom;

   iii) ne postoji privola primatelja e-poruke.

b) suzdržavati se od slanja informacija, dokumenata i osobnih podataka vezano za radni zadatak iz bilo kojeg razloga, uključujući i rad na daljinu, na račune e-pošte ili račune koji im nije zadala Ustanova. Pristup na daljinu može se zatražiti i odobriti pismenim putem slijedom određenog zahtjeva.

c) suzdržavati se od automatiziranih sustava prosljeđivanja/slanja informacija koje se tiču radnih zadataka izvan Ustanove;

d) suzdržavati se od slanja, pokušaja nabave ili pristupa neprikladnom materijalu ili materijalu koji bi mogao biti prijeteći ili zastrašujući prema druge osobama ili ih zlostavljati.

e) Obratiti pažnju pri primitku priloga, e-poruka i poveznica koje nisu zatražene, i od poznatih i od nepoznatih izvora. U slučaju sumnjivih e-poruka, nije dopušteno , otvarati ili skidati priloge te nipošto nije dopušteno slijediti poveznice.

Internet, Društvene mreže i mediji

Članak 36.

Ustanova mora osigurati da se svi Radnici/Suradnici pridržavaju uputa Ustanove i primjenjivih pravila vezanih za korištenje interneta, Društvenih mreža i medija koji bi trebali regulirati uvjete za pristup i korištenje Društvenih medija (poput Facebooka, Twittera, YouTubea, itd.) putem radnih uređaja i mreža.

Radnicima/Suradnicima pri navedenom korištenju nije dozvoljeno:

a) pokušati pristupiti stranicama i sadržajima koji sadrže neprikladan materijal poput kockanja ili pornografskih stranica kao i stranica koje promiču nasilna ili diskriminatorna ponašanja;

b) izdati ili objaviti diskriminatorne izjave, objaviti informacije ili sudjelovati u radnjama koje bi mogle oklevetati ili naštetiti ugledu Ustanove, osobama i trećim stranama koje surađuju s Ustanovom. To uključuje ponašanja na internetu i/ili na Društvenim mrežama i medijima i izvan radnog vremena;

c) koristiti unutarnje ili vanjske Društvene mreže i forume na neodgovoran način te kršeći primjenjive propise i/ili obveze Ustanove ;

d) dijeliti informacije, dokumente i osobne podatke vezane za korisnike zdravstvenih usluga, Radnike/Suradnike ili dobavljače subjekata, uključujući i povjerljive informacije subjekata na internetu, na Društvenim mrežama ili medijima osim ako to nije dopušteno posebnom odlukom Ustanove ili nekim primjenjivim pravilnikom Ustanove;

e) koristiti korisnički račun Ustanove da bi se registrirali na društvene mreže i/ili vanjske forume ako to nije dopušteno posebnom odlukom ili primjenjivim pravilnikom Ustanove;

f) namjerno objavljivati, slati ili primati, stavljati na internet/skidati s interneta, nabavljati, spremiti ili dijeliti bilo koji sadržaj ili materijal koji krši, neprimjereno koristi ili na drugi način povrjeđuje prava na intelektualno vlasništvo, privatnost i povjerljivost bilo kojeg pojedinca, skupine ili subjekta, uključujući i Ustanovu.

Ako postoje sumnje u buduće ponašanje ili u način na koji se druge osobe trebaju ponašati na internetu i Društvenim medijima, potrebno je obavijestiti Službenika za zaštitu podataka.

6.1.6 Osobna uporaba informacijsko-tehnoloških sustava Ustanove

Članak 37.

Ustanova mora osigurati da se svi Radnici/Suradnici pridržavaju posebnih odluka i pravilnika Ustanove koja trebaju regulirati uvjete za osobnu uporabu sustava i usluga Ustanove.

6.1.7 Upravljanje povjerljivim i/ili osjetljivim informacijama

Članak 38.

Ustanova često upravlja i obrađuje informacije osjetljive ili povjerljive prirode. To između ostalog uključuje i:

a) informacije o pojedincu koje su predmetom zakona i propisa o privatnosti

b) osjetljive komercijalne i financijske informacije koje bi mogle dovesti do kazni ako se njima ne upravlja na prikladan način

c) materijal zaštićen intelektualnim vlasništvom koji predstavlja značajno ulaganje Ustanove.

Upravljanje i obrada povjerljivih i/ili osjetljivih informacija mora se provoditi uz pridržavanje sljedećih pravila:

i) ne koristiti informacije koje su povjerljive ili na bilo koji način povezane s radnim zadatkom, iz bilo kojeg razloga koji nije povezan s tim radnim zadatkom:

ii) upravljati svim informacijama, u elektroničkom i papirnatom obliku, u skladu s odredbama ovog Pravilnika;

iii) odnositi se prema informacijama, dokumentima i datotekama povezanima s radnim zadacima koji još nisu određeni kao povjerljivi s maksimalnom revnošću i pažnjom;

iv) pohranjivati dokumente u skladu s odredbama ovog Pravilnika;

v) ne otkrivati povjerljive informacije ili razgovarati o njima na javnim mjestima;

vi) pobrinuti se da su informacije ispravno spremljene. U tu je svrhu potrebno spremiti dokumente na mrežu Ustanove radije nego putem sredstava dodijeljenih za osobnu upotrebu kao što je mail Ustanove ili tvrdi disk dodijeljenog računala.

Ako postoje sumnje oko primjenjivih rokova pohrane, potrebno je kontaktirati Službenika za zaštitu podataka. Moguće je kontaktirati vlasnika procesa ili ured za privatnost kako je to odredio subjekt Ustanove.

6.1.8 Prijava povrede osobnih podataka

Članak 39.

U slučaju povrede osobnih podataka ili zbog sigurnosnog incidenta ili zbog kršenja primjenjivih propisa i/ili ovog Pravilnika ili iz bilo kojeg drugog razloga, Radnici/Suradnici moraju odmah obavijestiti direktno Službenika za zaštitu podataka ili tako da pošalju e-poruku na adresu e-pošte koju je Ustanova dodijelila u tu svrhu. Radnik/Suradnik mora opisati okolnosti pod kojima je došlo do povrede osobnih podataka uključujući, gdje je to moguće, kategorije i približan broj ispitanika u pitanju i kategorije i približan broj bilježaka o osobnim podacima u pitanju. Primjerice, povreda osobnih podataka uključuje sljedeće slučajeve:

6.3 SIGURNOSNI SUSTAVI NA INTERNETU

Članak 41.

Svi radnici/suradnici pridržavati će se sljedećih pravila i uputa:

- Pristup internetu dopušten je Radnicima/Suradnicima kako bi izvršili svoj radni zadatak te uvijek u skladu s unutarnjim postupcima i mjerodavnim zakonima.
- U svrhu očuvanja integriteta sustava pristup internet je opremljen sigurnosnim sustavom vatrozida.
- Moguće je implementirati filtere kako bi se blokirao pristup Radnicima/Suradnicima na potencijalno opasne stranice.

7. ZAVRŠNE ODREDBE

Članak 42.

Ovaj Pravilnik objavljuje se na oglasnoj ploči i na mrežnim stranicama Ustanove, stupa na snagu osmog dana od dana objave na oglasnoj ploči Ustanove, a primjenjuje se od 25.05.2018. godine.

KLASA: 006-25/18-01/018
URBROJ: 251-510-03-20-18-03

Zagreb, 20. prosinca 2018. godine

Predsjednik Upravnog vijeća
prof. dr. sc. Zdravko Žvorc

Dom zdravlja Zagreb - Centar je dana 29. studenog 2018. godine, sukladno odredbi članka 126. Zakona o radu, proveo savjetovanje s Radničkim vijećem u svezi donošenja ovoga Pravilnika o zaštiti osobnih podataka, te je Radničko vijeće nakon provedenog savjetovanja dalo pozitivno mišljenje na tekst istoga.

Pravilnik o zaštiti osobnih podataka objavljen je na oglasnoj ploči dana 20.12.2018. 2018. godine, te stupa na snagu dana 28.12.2018. 2018. godine.

Ravnateljica
doc. dr. sc. Antonija Balenović, dr. med.