

GRUPA MEDIKA

Zagreb, 23. travnja 2018.

Politika zaštite osobnih podataka i privatnosti

U postupku usklađivanja sa Općom uredbom o zaštiti osobnih podataka donose se zajednička načela zaštite osobnih podataka za sva Društva i ustanove koji čine Grupu Medika, dok će svako društvo i ustanova specifične zahtjeve rješavati zasebnim dokumentom, odnosno zasebnim tabličnim prikazom Zbirki podataka koje vodi.

Sadržaj:

1. UVOD
2. PRAVILA i POSTULATI
3. PRAVA I OBVEZE
4. ZBIRKE OSOBNIH PODATAKA MEDIKA d.d. i LJEKARNE PRIMA PHARME
5. VIDEO NADZOR
6. SLUŽBENIK ZA ZAŠTITU OSOBNIH PODATAKA
7. KODEKS PONAŠANJA

1. UVOD

Ovom politikom osigurava se odgovarajuća podrška u zaštiti osobnih podataka i privatnosti svih sudionika u poslovnim procesima društava i ustanova Grupe Medika: zaposlenika, članova nadzornih i upravnih tijela, poslovnih partnera, dobavljača, kupaca, korisnika usluga, pacijenata te članova Programa vjernosti Ljekarne.

Politika se odnosi na društva:

Medika d.d., Zagreb, Capraška 1,

Primus nekretnine d.o.o., Zagreb, Capraška 1, te ustanove

LJEKARNE PRIMA PHARME,

Ljekarne Ines Škoko

odnosno Društva i ustanove kojima je Medika d.d. ili LJEKARNE PRIMA PHARME osnivač.

Politika objašnjava sve relevantne informacije vezane za prikupljanje, obradu i korištenje osobnih podataka kao i postulate privatnosti.

Politika će omogućiti smjernice, stjecanje znanja te razumjevanje vaših obveza.

Politika stupa na snagu danom donošenja.

2. PRAVILA i POSTULATI

Politika i Kodeks ponašanja sadrže osnovna pravila o zaštiti privatnosti i zaštiti osobnih podataka. Pravila i postulati su u skladu s vrijednostima europske pravne stečevine te sa trenutno važećim propisima kojima se regulira zaštita privatnosti i zaštita osobnih podataka. Time se želi naglasiti obveza postupanja svih zaposlenika spram osobnih podataka.

Svi zaposlenici imaju specifičnu odgovornost za poštivanje obveza koje su navedene u ovoj politici.

Od zaposlenika se očekuje da budu u mogućnosti prepoznati da li zadiru u nečiju privatnost ili obrađuju li nečije osobne podatke. Zaposlenici moraju biti svjesni općih pravila i postulata da bi mogli za slučaj kršenja tih pravila i postulata izvršiti prijavu Službeniku za zaštitu osobnih podataka.

Ovdje se objašnjavaju osnovni pojmovi bitni za razumijevanje zaštite osobnih podataka.

PRIVOLA : 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.

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

OSJETLJIVI OSOBNI PODACI : „podaci koji se odnose na zdravlje” znači osobni podaci povezani s fizičkim ili mentalnim zdravljem pojedinca, uključujući pružanje zdravstvenih usluga, kojima se daju informacije o zdravstvenom statusu osobe.

Osobni podaci skupljaju se i obrađuju pošteno i transparentno u skladu sa zakonom. Ovom Politikom se propisuju slijedeće obveze za sve zaposlenike:

1. prikupljanje i obrada osobnih podataka moguća je ako za to postoji zakonom određena osnova (npr.: ugovor, privola ili zakon)
2. osoba čiji se osobni podaci prikupljaju mora biti obavještena o procesima prikupljanja i obrade
3. prikupljanje osobnih podataka može se odnositi na ispunjenje određene poslovne svrhe (podaci o kupcima, podaci o dobavljačima, podaci o korisnicima usluga, interventni uvoz lijekova, izravni marketing, program vjernosti Prima Pharme), a takvo prikupljanje je moguće jedino uz izričitu obavijest i pristanak (privolu) ispitanika
4. korištenje osobnih podataka je moguće samo na način koji neće imati utjecaja na osobe na koje se ti podaci odnose osim ako je takvo što predviđeno zakonom
5. ANONIMIZACIJA ili PSEUDONIMIZACIJA se koristi što je više moguće

ANONIMIZACIJA : proces prilagodbe osobnih podataka u kojoj se fizičke osobe u njima ne mogu identificirati.

PSEUDONIMIZACIJA : 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.

Odgovorno upravljanje prikupljenim osobnim podacima bitan je element zaštite tih osobnih podataka te zaštita privatnosti. Jednom kad osobni podaci budu zavedeni u nekom od sustava osobnih podataka po nekoj od dopuštenih osnova za prikupljanje i obradu, osobni podaci se ne smiju mijenjati. Eventualna promjena može ovisiti o volji osobe na koju se ti osobni podaci odnose, odnosno na promjene zakonom predviđene ili dopuštene.

PREDEFINIRANA PRIVATNOST (Privacy by default): osigurati da se kao početna vrijednost obrađuju samo osobni podaci koji su nužni za svaku određenu svrhu obrade i osobito da se ne obrađuju više i dulje od nužnog minimuma za te svrhe (količina, razdoblje pohrane).

PRIVATNOST PO DIZAJNU (Privacy by design): predstavlja pristup projektima (projekti koje vodi Ustanova) koji promoviraju usklađenost privatnosti i zaštite osobnih podataka od samih početaka projekta.

PROCJENA UTJECAJA na zaštitu osobnih podataka - Data Privacy Impact Assessments (DPIAs) predstavlja analizu (alat) kojim se nastoje identificirati mogući rizici koji bi utjecali na privatnost i zaštitu osobnih podataka.

Svaki zaposlenik društava i ustanova Grupe Medika koji je zadužen za prikupljanje i obradu osobnih podataka mora voditi brigu o:

1. točnosti prikupljenih podataka (od prikupljanja i obrade do njihova uništenja)
2. zabrani dijeljenja osobnih podataka s drugim osobama unutar Društva/Ustanove koje nisu ovlaštene te zabrani dijeljenja podataka izvan Društva/Ustanove prema trećim osobama
3. informatičkoj sigurnosti prilikom obrade i spremanja osobnih podataka
4. preveniranju zloupotrebe osobnih podataka
5. osiguranju praćenja osobnih podataka dok su oni još potrebni
6. prikupljanju i obradi osobnih podataka dok traje svrha zbog koje su oni prvotno prikupljeni i obrađivani, trajanje obrade može biti definirano zakonom
7. probijanju privatnosti i „curenju“ osobnih podataka izvan svakog od Društava ili Ustanove

3. PRAVA I OBVEZE

Ovom Politikom definiraju se prava i obveze za sve fizičke osobe (zaposlenike, članove nadzornih i upravnih tijela, poslovne partnere, dobavljače, kupce, korisnike usluga, pacijente te korisnike Programa vjernosti Ljekarne) o kojima postoje osobni podaci zavedeni u sustavima osobnih podataka po zakonom dopuštenoj osnovi.

Postoje određene kategorije osobnih podataka koje Društvo/Ustanova mora prikupljati da bi ispunila zakonom i podzakonskim aktima propisane obveze, npr. Zakon o radu, Zakon o mirovinskom osiguranju, Zakon o zaštiti na radu, Zakon o zdravstvenoj zaštiti, porezni propisi itd.. Podaci koji se prikupljaju na temelju zakona i podzakonskih akata moraju biti točni i ažurni.

Fizičke osobe na koje se ti podaci odnose (prvenstveno zaposlenici) imaju obvezu da za slučaj bilo kakve promjene podataka koje su dali Društvu/Ustanovi, istu promjenu jave nadležnoj Službi da bi moglo biti provedeno točno ažuriranje (npr.: promjena prezimena, adrese, bilo kakva promjena osobnog statusa). Prijava promjene se mora izvršiti što prije, osobno ili putem punomoćnika, a najkasnije u roku od 8 dana od promjene.

Zaposleniku kao i svakoj fizičkoj osobi pripada pravo informirati se kod Društva/Ustanove koje osobne podatke Društvo/Ustanova ima o njoj. Svoje pravo ostvaruje postavljanjem pisanog zahtjeva prema Društvu/Ustanovi koja ima obvezu u roku od 30 dana odgovoriti na zahtjev. (čl. 19. Zakona o zaštiti osobnih podataka). Društvo/ Ustanova u postupku je osiguravanja tehničkih preduvjeta i informatičkog sustava kako bi svaki zaposlenik imao neposredan uvid u osobne podatke koje Društvo/Ustanova ima o njoj.

Zaposleniku kao i svakoj fizičkoj osobi čiji se osobni podaci nalaze u sustavima osobnih podataka Društva/Ustanove ima „Pravo na brisanje“. Pravo na brisanje inicira proceduru u kojoj se svi podaci o fizičkoj osobi/zaposleniku brišu iz svih evidencija u koje su njihovi osobni podaci dospjeli na temelju PRIVOLE (iznimka su osobni podaci prikupljeni na temelju zakona i drugih propisa koji se čuvaju u rokovima predviđenim istim zakonima i podzakonskim akima).

Zaposlenik kao i svaka fizička osoba čiji se osobni podaci nalaze u sustavima osobnih podataka Društva/Ustanova, ima pravo na temelju svoje posebne situacije u svakom trenutku uložiti PRIGOVOR na obradu osobnih podataka ili OGRANIČENJE OBRADE podataka koji se odnose na njega, u skladu s člankom 6. stavkom 1. točkom (e) ili (f) (Zakonitost obrade) Opće uredbe o zaštiti osobnih podataka, uključujući izradu profila koja se temelji na tim odredbama. Voditelj obrade više ne smije obrađivati osobne podatke osim ako voditelj obrade dokaže da postoje uvjerljivi legitimni razlozi za obradu koji nadilaze interese, prava i slobode ispitanika ili radi postavljanja, ostvarivanja ili obrane pravnih zahtjeva.

Za slučaj da je koji osobni podatak pogrešno unesen (pogreška u pisanju), zaposleniku/fizičkoj osobi pripada pravo zahtijevati od Društva/Ustanove korekciju tog osobnog podatka. Korekcija se realizira postavljanjem pisanog zahtjeva prema Društvu/Ustanovi. Uz zahtjev potrebno je priložiti dokument koji sadrži ispravan osobni podatak s ciljem korigiranja. Korekcija će biti izvršena u najkraćem mogućem roku.

Korisnicima usluga interventnog uvoza, izravnog marketinga i Programa vjernosti LJEKARNE PRIMA PHARME pripada pravo prijenosa ustupljenih podataka temeljem privole na neku drugu pravnu/fizičku osobu koja obrađuje osobne podatke. Pravo prijenosa se ostvaruje postavljanjem pisanog zahtjeva prema Društvu/Ustanovi.

Društvu/Ustanovi pripada pravo za slučaj sumnje da osobni podaci nisu ažurni, tražiti od zaposlenika/fizičke osobe ispravak osobnog podatka.

PROBOJ PRIVATNOSTI PODATAKA (Data Privacy Breach) obuhvaća svaki neovlašteni pristup, obradu, korištenje, otkrivanje, prikupljanje bez dozvole, uništenje odnosno svaku radnju koju nije poduzela ovlaštena osoba u pogledu osobnih podataka i privatnosti. Ukoliko dođe do proboja ili curenja svaki zaposlenik je dužan obavijestiti Društvo/Ustanovu i Službenika za zaštitu osobnih podataka radi poduzimanja mjera kojima se nastoji detektirati problem, spriječiti daljnji proboj te sanirati nastalu štetu. Društvo/Ustanova ima obvezu o svakom proboju koji ima ozbiljne posljedice u roku od 72h od proboja obavijestiti Regulatorno tijelo (Agencija za zaštitu osobnih podataka).

4. ZBIRKE OSOBNIH PODATAKA

Društvo/Ustanova zbog ispunjavanja zakonom propisanih obveza mora imati u svom posjedu osobne podatke svojih zaposlenika. Osobni podaci se prikupljaju i obrađuju u onoj mjeri kako je to određeno zakonskim i podzakonskim aktima na transparentan način. Obrada osobnih podataka zaposlenika Društva/Ustanove u nadležnosti je ovlaštenih osoba nadležnih Službi koje obavljaju pravne, kadrovske poslove, obračun plaće te računovodstvene i financijske poslove.

Radi ostvarenja prava i obveza iz radnih odnosa, a dijelom zbog poslovno uvjetovanih razloga osobni podaci zaposlenika dostavljaju se nadležnim državnim tijelima poput Hrvatskog zavoda za mirovinsko osiguranje, Hrvatskog zavoda za zdravstveno osiguranje, Hrvatskog zavoda za javno zdravstvo, Porezne uprave, te zbog specifičnosti djelatnosti strukovnim organizacijama poput Hrvatske ljekarničke komore, Hrvatske gospodarske komore, Hrvatske udruge poslodavaca. Sve navedene institucije sa svoje strane provode sve potrebne mjere s ciljem zaštite osobnih podataka.

Osim zakonom obvezujućih zbirki Društva/Ustanove posjeduju zbirke osobnih podataka koje same formiraju zbog poslovnih razloga, s ciljem bolje organizacije rada te u marketinške svrhe. Te zbirke su formirane na temelju pristanka fizičkih osoba putem izričite pisane privole, ili su podaci dobiveni od bolnica, ustanova u kojima se pacijent liječi odnosno izabranog liječnika a u svrhu ostvarivanja zdravstvene zaštite osobe odnosno ostarivanja prava na lijek.

Obrada osobnih podataka u okviru Društva/Ustanove (osobnim podacima svih sudionika u poslovnim procesima društava i ustanova Grupe Medika: zaposlenika, članova nadzornih i upravnih tijela, poslovnih partnera, dobavljača, kupaca, korisnika usluga, pacijenata te članova Programa vjernosti Ljekarne) vrši se elektroničkim putem uz odgovarajuću ručnu datoteku. Svi osobni podaci zaštićeni su adekvatno. Pravo pristupa ručnim datotekama te elektronički pristup imaju samo ovlaštene osobe.

Obrada osobnih podataka može se vršiti samo ako je to nužno radi poslovnih aktivnosti same Ustanove. Ne dozvoljava se ovlaštenim osobama da samoinicijativno vrše

obradu osobnih podataka koja nije u skladu sa ciljevima što ih je Ustanova odredila. Zaposlenicima se ne dozvoljava bilo kakava obrada osobnih podataka osim ako na tu obradu budu izričito ovlašteni od strane Voditelja zbirke osobnih podataka Društva/Ustanove.

Zbirke osobnih podataka kojima raspolažu društva/ustanove navedene su u tabličnim prikazima, zasebno za Društva a zasebno za Ustanove.

Tablični prikaz sadrži osnovu prikupljanja te rok čuvanja osobnih podataka. Rokovi koji su navedeni definiraju se zakonom.

Ova Politika navodi sadržaj Zbirke osobnih podataka. Za svaku zbirku navedena je svrha/osnova prikupljanja, lokacija, poduzete mjere za čuvanje osobnih podataka te zakonom određen rok čuvanja osobnih podataka.

Za sve kategorije osobnih podataka je zajedničko da protekom roka odnosno prestankom svrhe njihova obrađivanja osobni podaci se uništavaju na način da nije moguća njihova obnova.

Zbirke podataka sadržane su u pisanom dokumentu, dostupnom na uvid na zahtjev.

Uvažavajući sve poslovne zahtjeve i zadatke vezane za obavljanje djelatnosti apelira se na sve zaposlenike koji dolaze u doticaj s gore navedenim zbirkama osobnih podataka da se služe tim zbirkama s povećanom pažnjom.

Ako prilikom rada nastanu kopije materijala sadržanih u zbirkama, protekom rada navedene materijale potrebno je arhivirati kako je određeno pozitivnim propisima ili internim aktima ili ih uništiti (cijepanjem papira do nemogućnosti obnove ili usitnjavanjem- uništavač dokumentacije).

Ako zaposlenik naiđe na materijale koji su po svom sadržaju element zbirke osobnih podataka, dužan je obratiti se Službeniku za zaštitu osobnih podataka koji će na propisan način arhivirati ili uništiti ili uputiti na način uništenja pronađenih materijala.

Zaposlenici koji printaju, odnosno fotokopiraju materijale koji sadrže osobne podatke ili predstavljaju internim aktima definiran TAJNI PODATAK dužni su što prije preuzeti navedene materijale. Time se sprječava da neovlaštene osobe imaju pravo uvida ili manipulacije tim materijalima. Ako se dogodi da zaposlenik naiđe na materijal koji sadržajem upućuje na tajni podatak dužan ga je odmah uništiti i o tome kontaktirati Službenika za zaštitu osobnih podataka.

Smisao navedenih postupanja jest smanjenje rizika od odavanja i prijenosa osobnih podataka i tajnih podataka.

5. VIDEO NADZOR

Temeljem Zakona o provedbi opće uredbe o zaštiti podataka i odredbom članka 43. stavkom 1. Zakona o zaštiti na radu, kao posebnog zakona, regulirano je da poslodavac smije koristiti nadzorne uređaje kao sredstvo zaštite na radu pod uvjetima propisanim istim Zakonom.

Videonadzor ne obuhvaća, odnosno zabranjeno je uspostavljati nadzor nad prostorijama za osobnu higijenu i prostorijama namjenjene za presvlačenje radnika (svlačionice). Prostorije koje su pod videonadzorom označene su adekvatnim oznakama koje nedvosmisleno daju svim radnicima i trećim osobama do znanja da je prostorija pod videonadzorom.

Podaci dobiveni uporabom videonadzora sukladno odredbama Zakona o provedbi opće uredbe o zaštiti podataka su adekvatno zaštićeni jer pravo pristupa ima samo ovlaštena osoba. Treće osobe nemaju pristup.

Podaci se mogu dati nadležnim i mjerodavnim tijelima na njihov zahtjev.

6. SLUŽBENIK ZA ZAŠTITU OSOBNIH PODATAKA

Poštujući pozitivne propise Republike Hrvatske i zakonodavstvo Europske unije Medika d.d. i Ljekarne Prima Pharme su imenovale Službenika za zaštitu osobnih podataka. Isto se odnosi i na ustanove čiji su osnivač LJEKARNE PRIMA PHARME.

Zadaće službenika za zaštitu podataka

1. Službenik za zaštitu podataka obavlja najmanje sljedeće zadaće:

(a) informiranje i savjetovanje voditelja obrade ili izvršitelja obrade te zaposlenika koji obavljaju obradu o njihovim obvezama iz ove Uredbe te drugim odredbama Unije ili države članice o zaštiti podataka;

(b) praćenje poštovanja ove Uredbe te drugih odredaba Unije ili države članice o zaštiti podataka i politika voditelja obrade ili izvršitelja obrade u odnosu na zaštitu osobnih podataka, uključujući raspodjelu odgovornosti, podizanje svijesti i osposobljavanje osoblja koje sudjeluje u postupcima obrade te povezane revizije;

(c) pružanje savjeta, kada je to zatraženo, u pogledu procjene učinka na zaštitu podataka i praćenje njezina izvršavanja u skladu s člankom 35.;

(d) suradnja s nadzornim tijelom;

(e) djelovanje kao kontaktna točka za nadzorno tijelo o pitanjima u pogledu obrade, što uključuje i prethodno savjetovanje iz članka 36. Uredbe te savjetovanje, prema potrebi, o svim drugim pitanjima.

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

Za sve upite povodom ove Politike i upite koji proizlaze iz praktične primjene ove Politike te upite općenito o zaštiti osobnih podataka i privatnosti zaposlenika/pacijenata/kupaca/članova programa vjernosti na raspolaganju stoji Službenik za zaštitu osobnih podataka.

KONTAKT

LJEKARNE PRIMA PHARME : szop@primapharme.hr

Ljekarna INES ŠKOKO : szop@primapharme.hr

Medika d.d.: szop@medika.hr

7. KODEKS PONAŠANJA

Opća uredba o zaštiti osobnih podataka potiče sastavljanje Pravila/kodeksa ponašanja sa ciljem pravilne primjene regulacija sadržanih u samoj Uredbi i Zakonu o provedbi opće uredbe o zaštiti osobnih podataka. Uzimajući u obzir procese rada u okviru Grupa Medika d.d. donosimo Kodeks ponašanja koji sadrži bitne smjernice kojima se zaposlenici Grupe Medika trebaju voditi.

- a) obrada osobnih podataka mora biti zakonita, poštena i transparentna
- b) Voditelj obrade mora imati legalnu osnovu i legitiman interes za obradu osobnih podataka
- c) prikupljanje osobnih podataka mora biti u skladu sa pozitivnim propisima i ovom Politikom
- d) pri obradi osobnih podataka Voditelj treba koristiti što više pseudonimizaciju osobnih podataka
- e) Voditelj obrade mora transparentno informirati ispitanika (radnika/ pacijenta) o osobnim podacima koje prikuplja za svoje potrebe
- f) Voditelj obrade mora zakonito, transparentno i nedvosmisleno informirati ispitanika o ostvarivanju njegovih prava zajamčenih ovom Politikom i pozitivnim propisima
- g) Voditelj obrade mora posebno voditi računa o obradi osobnih podataka djece i zaštiti djece te načina pribavljanja privole nositelja roditeljske odgovornosti nad djetetom
- h) Voditelj obrade mora poduzeti sve mjere i postupke s ciljem ispunjenja sigurnosnih obveza propisanih članakom 24. i 25. te mjera za osiguravanje sigurnosti obrade iz članka 32. Opće uredbe o zaštiti osobnih podataka
- i) izvješćivanje nadzornih tijela o povredama osobnih podataka i obavješćivanja ispitanika o takvim povredama u roku koji određuje Politika
- j) omogućiti prijenos osobnih podataka trećim zemljama ili međunarodnim organizacijama;
- k) omogućiti ulaganje prigovora na obradu osobnih podataka samo u onom djelu koji se odnose na ispitanika