UDK 347.7 / 336.2

Interne politike zaštite osobnih podataka

Božo Prelević, dipl. iur.

Sastavljanje internih politika zaštite osobnih podataka obveza je voditelja obrade i izvršitelja obrade osobnih podataka prema Općoj uredbi o zaštiti osobnih podataka (GDPR). Prema Općoj uredbi interne politike moraju biti dokumentirane, što znači kako moraju biti sastavljene u pisanom obliku. Autor u stručnom članku analizira odredbe propisa o zaštiti osobnih podataka koji se odnose na interne politike te daje njihov ogledni primjer.

1. Uvod

U prošlim brojevima RiPup-a upoznali sa temeljnim odredbama propisa Europske unije o zaštiti osobnih podataka[1], pravima ispitanika[2], obvezama voditelja obrade osobnih podataka[3] te obvezama izvršitelja obrade osobnih podataka[4] koje proizlaze iz primjene Uredbe (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ[5] (u nastavku teksta: Opća uredba)[6], koja je stupila na snagu 24. svibnja 2016., a primjenjuje se od 25. svibnja 2018. te novog Zakona o provedbi Opće uredbe o zaštiti podataka[7] (u nastavku teksta: Zakon). U ovom broju RiPup-a dajemo primjer internih politika za obveznike Opće uredbe i Zakona. Ove interne politike zapravo moraju donijeti i voditelji i izvršitelji obrade osobnih podataka.

Opća uredba daje vrlo šture podatke o internim politikama zaštite osobnih podataka, ali iz njenih uvodnih izjava, kao i normativnog dijela teksta, zapravo proizlazi obveza donošenja pisanih internih politika zaštite osobnih podataka. Tako se u uvodnoj izjavi br. 78 Opće uredbe, između ostalog navodi kako bi voditelj obrade osobnih podataka radi dokazivanja sukladnosti s Općom uredbom, morao uvesti interne politike i provesti mjere koje osobito ispunjavaju načela tehničke zaštite podataka i integrirane zaštite podataka. U normativnom dijelu Opće uredbe, u dijelu koji se odnosi na obveze voditelja obrade osobnih podataka navodi se, između ostalog, kako uzimajući u obzir prirodu, opseg, kontekst i svrhe obrade, kao i rizike različitih razina vjerojatnosti i ozbiljnosti za prava i slobode pojedinaca, voditelj obrade provodi odgovarajuće tehničke i organizacijske mjere, koje se prema potrebi preispituju i ažuriraju, kako bi osigurao i mogao dokazati da se obrada osobnih podataka provodi sukladno Općoj uredbi.

2. Interne politike zaštite osobnih podataka

Obveza donošenja internih politika zaštite osobnih podataka proizlazi i iz odredbe čl. 39. st. 1. t. b) Opće uredbe.

ističemo...

Naime, ovom odredbom je određeno kako službenik za zaštitu osobnih podataka, između ostalog, mora pratiti poštovanje politika voditelja obrade, ili izvršitelja obrade u odnosu na zaštitu osobnih podataka.

Iz navedenog proizlazi kako se obveza donošenja internih politika odnosi kako na voditelje tako i na izvršitelje obrade osobnih podataka.

U praksi se postavlja pitanje moraju li interne politike biti sastavljene u pisanom obliku. Odgovor je potvrdan, jer dokazivanje obrade osobnih podatka suklano Općoj uredbi zapravo je moguće jedino pisanim aktom. U nastavku dajemo primjer internih politika zaštite osobnih podataka.

1 Prelević, Božo, stručni članak „Primjena novih pravila o zaštiti osobnih podataka od 25.5.2018. (I. dio)“, RiPup br. 3/18, str. 158.
2 Prelević, Božo, stručni članak „Primjena novih pravila o zaštiti osobnih podataka od 25.5.2018. (II. dio) – prava ispitanika“, RiPup br. 4/18, str. 150.
3 Prelević, Božo, stručni članak „Obveze voditelja obrade osobnih podataka“, RiPup br. 5/18, str. 148.
4 Prelević, Božo, stručni članak „Obveze izvršitelja obrade osobnih podataka“, RiPup, br. 6/2018, str. 167.
5 SL L 119, 4.5.2016.
6 http://eur-lex.europa.eu/legal-content/HR/TXT/PDF/?uri=CELEX:32016R0679&from=EN
7 Nar. nov., br. 42/18 od 9. svibnja 2018.

Primjer – interne politike zaštite osobnih podatka

Temeljem čl. 24. Uredbe (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ te Zakona o provedbi Opće uredbe o zaštiti podataka, trgovačko društvo ABEBE d.o.o. Split, Marmontova 333 (u nastavku teksta: Društvo), zastupano po direktoru Stipi Stipić, dana 29. rujna 2018. donosi sljedeće

INTERNE POLITIKE ZAŠTITE OSOBNIH PODATAKA

I. OPĆE ODREDBE

Članak 1.

Društvo u svojem radu prikuplja, obrađuje, nadzire prikupljanje i obradu osobnih podataka te štiti prikupljene osobne podatke sukladno propisima o zaštiti osobnih podatka koji su na snazi i primjenjuju se u Republici Hrvatskoj.

Članak 2.

Ove Interne politike zaštite osobnih podataka sadrže pravila povezana sa zaštitom članova te drugih pojedinaca u pogledu obrade osobnih podataka i pravila povezana sa slobodnim kretanjem osobnih podataka.

Članak 3.

Sve osobe koje su zaposlene u Društvu i sva tijela Društva obvezno se pridržavaju i primjenjuju odredbe Internih politika.

Članak 4.

Pojedini pojmovi koji se koriste u Internim politikama imaju sljedeće značenje:

- „osobni podaci" su svi podaci pomoću kojih se izravno, ili neizravno može utvrditi identitet neke fizičke osobe, kao što su: ime, identifikacijski broj, podaci o lokaciji, mrežni identifikator i dr.;
- „obrada osbnih podataka" je svaki postupak, ili skup postupaka koji se obavljaju na osobnim podacima, ili na skupovima osobnih podataka, bilo automatiziranim, ili 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 podataka;
- „izrada profila" znači svaki oblik automatizirane obrade osobnih podataka koji se sastoji od uporabe osobnih podataka za ocjenu određenih osobnih aspekata povezanih s pojedincem, posebno za analizu, ili predviđanje aspekata u vezi s radnim učinkom, ekonomskim stanjem, zdravljem, osobnim sklonostima, interesima, pouzdanošću, ponašanjem, lokacijom ili kretanjem tog pojedinca;
- „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;
- „voditelj obrade" je Društvo kada samo, ili zajedno s drugim ovlaštenim fizičkim, ili pravnim osobama određuje svrhe i sredstva obrade osobnih podataka;
- „privola" ispitanika znači svako dobrovoljno, posebno, informirano i nedvosmisleno izražavanje želja ispitanika kojim on izjavom, ili jasnom potvrdnom radnjom daje pristanak za obradu osobnih podataka koji se na njega odnose.

II. OBRADA OSOBNIH PODATAKA

Članak 5.

Društvo obrađuje osobne podatke sukladno propisima o zaštiti osobnih podataka koji se primjenjuju u Republici Hrvatskoj i sukladno ovim Internim politikama.

Članak 6.

Društvo obrađuje osobne podatke na zakonit i transparentan način.

Članak 7.

Društvo obrađuje osobne podatke obrađuje ako je:

- obrada nužna radi ispunjenja zakonskih obveza Društva;
- ispitanik dao privolu za obradu svojih osobnih podataka u jednu, ili više posebnih svrha;
- obrada nužna za izvršavanje ugovora sklopljenog sa ispitanikom;
- obradu potrebno provesti radi zaštite ključnih interesa ispitanika.

Članak 8.

Osobni podaci koji se obrađuju moraju biti točni, potpuni i ažurni.

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

Članak 9.

U slučaju da su osobni podaci ispitanika nepotpuni, ili netočni, Društvo je obvezno samo ispraviti, ili ažurirati netočne i nepotpune osobne podatke ispitanika koji su mu poznati.

O postupku iz stavka 1. Društvo obavještava ispitanika u pisanom obliku u roku od 3 (slovima: tri) dana od ispravka i/ili ažuriranja njegovih osobnih podataka.

Članak 10.

U slučaju da Društvu nisu poznati točni podaci ispitanika koji su potrebni radi njihovog ažuriranja, ili ispravka, kao i u svim drugim slučajevima njihove netočnosti, ili nepotpunosti, Društvo je dužno omogućiti ispitaniku pravo na ispravak netočnih, ili nepotpunih osobnih podataka.

III. POVJERAVANJE OBRADE PODATAKA IZVRŠITELJU OBRADE

Članak 11.

Društvo može povjeriti obradu osobnih podataka izvršitelju obrade samo temeljem odluke Uprave Društva.

U slučaju iz stavka 1. sa izvršiteljem obrade sklapa se poseban ugovor.

Članak 12.

Ugovor sa izvršiteljem obrade mora imati najmanje sve elemente sadržaja određene propisima o zaštiti osobnih podataka koji se primjenjuju u Republici Hrvatskoj te Internim politikama.

Ugovor iz stavka 1. mora u potpunosti osiguravati zaštitu osobnih podataka ispitanika koji se privremeno ustupaju na obradu izvršitelju obrade.

IV. SIGURNOST OBRADE I ČUVANJE OSOBNIH PODATAKA

Članak 13.

Društvo obrađuje osobne podatke na način koji osigurava njihovu potpunu zaštitu i nepovredivost te zaštitu od slučajnog gubitka, uništenja, ili oštećenja osobnih podataka, primjenom odgovarajućih tehničkih i organizacijskih mjera, koje, između ostalog, uključuju:

- pseudonimizaciju osobnih podataka;
- enkripciju osobnih podataka;
- osiguravanja povjerljivosti, cjelovitosti, dostupnosti i otpornosti sustava i usluga obrade;
- osiguravanje pravodobne ponovne uspostave dostupnosti osobnih podataka i pristupa istima u slučaju fizičkog ili tehničkog incidenta na sustavu obrade, ili pohrane;
- redovito testiranje, ocjenjivanje i procjenjivanje učinkovitosti tehničkih i organizacijskih mjera za osiguravanje sigurnosti obrade.

Članak 14.

Osobni podaci ispitanika u elektroničkom obliku čuvaju se na računalu voditelja kadrovske službe Društva, koje je zaštićeno lozinkom.

Informaciju o lozinci zna samo voditelj kadrovske službe Društva i u pisanom obliku je pohranjuje u sigurnosni sef Društva u zapečaćenoj omotnici.

Pristup osobnim podacima iz stavka 1. ima samo voditelj kadrovske službe Društva.

Članak 15.

Osoba koja obavlja informatičke usluge u Društvu obvezna je prilikom ažuriranja računalnih programa koji sadrže osobne podatke na računalu iz članka 14. potpisati posebnu izjavu o povjerljivosti.

Članak 16.

Osobni podaci ispitanika u pisanom obliku čuvaju se u kancelariji voditelja kadrovske službe Društva u posebnom arhivskom ormaru sa sigurnosnim ključem.

Kancelarija voditelja kadrovske službe Društva iz stavka 1. u kojoj se nalazi arhivski ormar u njegovoj odsutnosti mora biti stalno zaključana.

Arhivski ormar iz stavka 1. mora biti stalno zaključan.

Ključ kancelarije voditelja kadrovske službe Društva nalazi se u sigurnosnom ormariću u kancelariji Direktora Društva.

V. BRISANJE OSOBNIH PODATAKA

Članak 17.

Osobni podaci ispitanika brišu se nakon proteka godine dana od njihovog prikupljanja, osim u slučaju da su potrebni radi izvršenja zakonskih obveza Društva, u kojem slučaju se brišu nakon isteka zakonskog roka čuvanja.

VI. POVREDA OSOBNIH PODATAKA

Članak 18.

O svakoj povredi osobnih podataka odmah mora biti obaviješten službenik za zaštitu osobnih podataka, ili osoba koja ga zamjenjuje.

Službenik za zaštitu osobnih podataka i/ili Društvo dužni su odmah obavijestiti ispitanika i nadzorno tijelo određeno propisima o zaštiti osobnih podataka o povredi osobnih podataka ispitanika.

U slučaju povrede osobnih podataka iz stavka 1. službenik za zaštitu osobnih podataka poduzima radnje predviđene posebnim aktom o postupku u slučaju povrede osobnih podataka.

VII. ZAŠTITA PRAVA ISPITANIKA

Članak 19.

Svaki ispitanik mora biti upoznat sa svrhom prikupljanja osobnih podataka.

Članak 20.

Za prikupljanje osobnih podataka ispitanika potrebna je njegova izričita privola u pisanom obliku, osim kada se osobni podaci prikupljaju radi izvršenja zakonskih obveza Društva, ili radi izvršenja ugovora sklopljenog sa ispitanikom.

Članak 21.

Društvo je dužno odmah informirati ispitanika o svrsi obrade njegovih osobnih podataka.

Članak 22.

Svaki ispitanik ima pravo u pisanom obliku postaviti zahtjev prema Društvu u kojem se traži:

- ispravak i ažuriranje netočno obrađenog i zastarjelog osobnog podatka;
- podatak o načinu obrade njegovog osobnog podatka;
- podatak o tome je li njegov osobni podatak ustupljen trećoj fizičkoj, ili pravnoj osobi;
- brisanje njegovog osobnog podatka za koji više ne postoji svrha obrade.

Članak 23.

Društvo će najkasnije u roku od 3 (slovima: tri) dana od dana podnošenja pisanog zahtjeva ispitanika, na njegov osobni zahtjev, ili zahtjev njegovog zakonskog zastupnika, ili punomoćnika, dostaviti pisanu potvrdu:

- obrađuju li se njegovi osobni podaci;
- jesu li njegovi osobni podaci ispravljeni;
- na koji način se obrađuju njegovi osobni podaci;
- jesu li njegovi osobni podaci ustupljeni trećoj fizičkoj, ili pravnoj osobi;
- jesu li njegovi osobni podaci izbrisani povodom njegovog pisanog zahtjeva;

Članak 24.

Društvo će na pisani zahtjev ispitaniku omogućiti uvid u evidenciju aktivnosti obrade te uvid u osobne podatke sadržane u evidenciji aktivnosti obrade koji se odnose na njega te njihov ispis.

Članak 25.

Društvo pruža ispitaniku u svakom trenutku sve potrebne informacije u vezi obrade njegovih osobnih podataka.

Društvo osobito mora pružiti ispitanicima i informacije o:

- kontaktu službenika za zaštitu osobnih podataka;
- kontaktu osobe zadužene za davanje podataka o obradi i brisanju osobnih podataka;
- svrsi obrade osobnih podataka;
- pravnoj osnovi obrade osobnih podataka;
- legitimnim interesima;
- ustupanju osobnih podataka drugim fizičkim i pravnim osobama;
- razdoblju pohrane i čuvanja osobnih podataka;
- njihovom pravu na pristup osobnim podacima;
- njihovom pravu na ispravak i brisanje osobnih podataka;

- pravu na ulaganje prigovora;
- svim ostalim činjenicama bitnim za ostvarivanje njihovih prava sukladno propisima o zaštiti osobnih podataka koji su na snazi u Republici Hrvatskoj.

VIII. VOĐENJE EVIDENCIJA

Članak 26.

Društvo obrađuje sljedeće vrste osobnih podataka:

- osobni podaci o radnicima Društva;
- osobni podaci o članovima obitelji radnika Društva kada je to određeno zakonom, ili drugim propisom;
- osobni podaci o poslovnim partnerima;
- osobni podaci o drugim osobama na radu u Društvu;
- osobni podaci drugih osoba koji se prikupljaju temeljem zakonite svrhe.

Članak 27.

Osobni podaci iz članka 26. Internih politika obuhvaćaju:

- ime i prezime;
- adresu prebivališta ili boravišta;
- datum rođenja;
- osobni identifikacijski broj;
- broj telefona;
- adresu elektronske pošte;
- broj računa u instituciji za platni promet i/ili kreditnoj instituciji;
- druge potrebne podatke sukladno propisima kojima se uređuje zaštita osobnih podataka, Internim politikama i svrsi radi koje se osobni podaci prikupljaju.

Članak 28.

Za osobne podatke koje prikuplja Društvo vodi evidenciju aktivnosti obrade sukladno propisima o zaštiti osobnih podataka koji se primjenjuju u Republici Hrvatskoj.

IX. IMENOVANJE SLUŽBENIKA ZA ZAŠTITU OSOBNIH PODATAKA

Članak 29.

Društvo imenuje službenika za zaštitu osobnih podataka sukladno propisima o zaštiti osobnih podataka koji se primjenjuju u Republici Hrvatskoj te Internim politikama.

Članak 30.

Službenik za zaštitu osobnih podataka ne može biti osoba koja zastupa Društvo, član uprave, član nadzornog odbora, druga rukovodeća osoba, ili druga osoba u Društvu koja neposredno prikuplja osobne podatke ispitanika.

Članak 31.

Službenik za zaštitu osobnih podataka je osoba koja je u radnom odnosu u Društvu, osim osobe iz članka 30. Internih politika.

U slučaju da nije moguće imenovati službenika za zaštitu podataka sukladno stavku 1., poslove službenika za zaštitu osobnih podataka obavlja druga osoba koja ispunjava uvjete iz Internih politika s kojom se sklapa ugovor o djelu temeljem odluke Uprave Društva.

Pri imenovanju službenika za zaštitu osobnih podataka, koliko je to moguće, vodit će se računa da ta osoba raspolaže određenim pravnim i informatičkim znanjima.

Članak 32.

Službenik za zaštitu osobnih podataka prati poštivanje odredbi propisa o zaštiti osobnih podataka koji se primjenjuju u Republici Hrvatskoj i Internih politika te se njihovim odredbama upoznaje osobe u Udruzi, posebno one koje se bave neposredno obradom osobnih podataka.

X. PRIJELAZNE I ZAVRŠNE ODREDBE

Članak 33.

Svaka obrada osobnih podataka suprotno Internim politikama nezakonita je i povlači za sobom sankcije sukladno ugovoru o radu, propisima o radu i zaštiti osobnih podataka.

Članak 34.

Ove Interne politike mijenjaju se i dopunjuju na način predviđen za njihovo donošenje.

Sve izmjene i dopune Internih politika valjane su ako su sačinjene sukladno stavku 1. i u pisanom obliku.

Članak 35.

Tumačenje odredbi Internih politika daje Uprava Društva.

Članak 36.

Interne politike objavljuju se na oglasnoj ploči Društva i stupaju na snagu u roku od 8 (slovima: osam) dana od dana objave.

Direktor
Stipe Stipić

Objavljeno na oglasnoj ploči dana 29.9.2018.
Interne politike stupile su na snagu dana 7.10.2018.

3. Zaključak

Obveznici primjene novih propisa o zaštiti osobnih podataka moraju voditi računa o donošenju niza pisanih akata. Jedan od tih pisanih akata koji se moraju donijeti radi pravilne primjene novih propisa jesu i interne politike. Odredbe propisa o zaštiti osobnih podataka su vrlo šture.

Ipak, jasno je da moraju biti dokumentirane, odnosno sastavljene u pisanom obliku. Također, mišljenja smo kako iz Opće uredbe proizlazi da interne politike moraju donijeti voditelji i izvršitelji obrade, pri čemu je potrebno voditi računa kako su izvršitelji obrade u pravilu u isto vrijeme i voditelji obrade za osobne podatke koje oni prikupljaju. Sa zanimanjem treba pratiti praksu nadzornog tijela koja će tijekom vremena pokazati smjer u kojem treba pristupati sastavljanju internih politika zaštite osobnih podataka.

Literatura:

1) Uredba (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (SL L 119, 4.5.2016);
2) Zakon o provedbi Opće uredbe o zaštiti podataka (Nar. nov., br. 42/18) - www.propisi.hr
3) Prelević, B., stručni članak „Primjena novih pravila o zaštiti osobnih podataka od 25.5.2018. (I. dio)", RiPup br. 3/18, str. 158.
4) Prelević, B., stručni članak „Primjena novih pravila o zaštiti osobnih podataka od 25.5.2018. (II. dio) – prava ispitanika", RiPup br. 4/18, str. 150.
5) Prelević, B., stručni članak „Obveze voditelja obrade osobnih podataka", RiPup br. 5/18, str. 148.
6) Prelević, Božo, stručni članak „Obveze izvršitelja obrade osobnih podataka", RiPup, br. 6/2018.

Ne zaboravite:

- **25. svibnja 2018. počela je primjena Opće uredbe, a istog datuma stupio je na snagu i primjenjuje se i novi Zakon.**
- **Iz Opće uredbe proizlazi obveza sastavljanja internih politika zaštite osobnih podataka.**
- **Obveznici moraju dokazati postojanje internih politika što pretpostavlja da moraju biti sastavljene u pisanom obliku.**
- **Interne politike moraju izraditi kako voditelji obrade tako i izvršitelji obrade osobnih podataka.**
- **Pri tome je potrebno voditi računa o tome kako su izvršitelji obrade osobnih podataka u pravilu u isto vrijeme i voditelji obrade kada prikupljaju osobne podatke.**

Bilješke