SmartWay d.o.o., Glavna 23, Sveti Martin na Muri, 40313 Sveti Martin na Muri OIB: 94221886720 (dalje u tekstu: Društvo), dana 1.1.2024. donosi sljedeći

PRAVILNIK O ZAŠTITI OSOBNIH PODATAKA

I. OPĆE ODREDBE

Članak 1.

Ovim Pravilnikom uređuju se opći postupci obrade i mjere zaštite osobnih podataka koji se vode u evidencijama aktivnosti obrade Društva. Pravilnik obuhvaća opće mjere zaštite osobnih podataka tijekom njihovog prikupljanja, obrade, pohrane, prijenosa i korištenja.

Svrha Pravilnika je osigurati da Društvo prilikom obrade osobnih podataka postupa u skladu s propisima na području zaštite osobnih podataka, osobito u skladu s Uredbom (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 (Opća uredba o zaštiti podataka ili GDPR) kao i Zakonom o provedbi Opće uredbe o zaštiti podataka.

Članak 2.

Izrazi koji se koriste u ovom Pravilniku imaju značenje predviđeno GDPR-om i Zakonom o provedbi Opće uredbe o zaštiti podataka.

Članak 3.

Društvo će osobne podatke obrađivati zakonito, pošteno i transparentno u skladu s primjenjivim propisima.

Društvo prikuplja osobne podatke u sljedeće svrhe:

- pružanja usluga u okviru registriranih djelatnosti;
- ispunjenja ugovora (ugovora o zastupanju ili ugovora o nalogu odnosno na temelju punomoći);
- ako je obrada nužna za potrebe legitimnih interesa Društva ili treće strane;
- ispunjenja pravnih obveza;
- ostvarivanja prava i obveza iz ugovora o radu i radnog odnosa (isplate plaće ili drugih naknada, ostvarivanja prava na dnevni, tjedni i godišnji odmor, u svrhu zaštite prava radnika iz radnog odnosa, u svrhu ostvarivanja drugih prava i ispunjavanja obveza iz ugovora);
- edukacije radnika;

- kada je to nužno za poštivanje pravnih obveza Društva kao voditelja obrade, npr. u svrhu ostvarivanja prava iz mirovinskog i zdravstvenog osiguranja, vođenja evidencije o radnicima u skladu s mjerodavnim propisima, vođenje evidencija i procjena rizika u skladu sa Zakonom o sprječavanju pranja novca i financiranja terorizma;
- u eventualne dodatne svrhe na temelju suglasnosti/privole.

Društvo osobne podatke stranaka i drugih osoba u vezi sa pružanjem usluga, može obrađivati na temelju zakona, izdane punomoći, sklopljenog ugovora ili odluke nadležnog tijela.

Društvo obrađuje osobne podatke kako bi ispunio svoje pravne obveze kao voditelja obrade. Ovakva obrada može uslijediti iz prisilnih pravnih propisa npr. poreznih, trgovačkih, propisa o sprječavanju pranja novca, kaznenih odredbi i slično, dakle, uslijed državnog nadzora i kontrole te zakonske dužnosti dostavljanja podataka;

Društvo obrađuje osobne podatke ispitanika sa svrhom obavljanja poslovne aktivnosti (radnici, poslovni partneri). Ove osobne podatke Društvo obrađuje da bi ispunio svoje zakonske ili ugovorne obveze. Određene osobne podatke o ovim ispitanicima Društvo može obrađivati na osnovi svojeg legitimnog interesa (npr. fotografiranje/snimanje, videonadzor).

Društvo će obrađivati samo one osobne podatke koji su primjereni, relevantni i ograničeni na ono što je nužno u odnosu na svrhe u odnosu na koje se osobni podaci obrađuju.

Društvo poduzima odgovarajuće razumne mjere kako bi osobni podaci koje obrađuje bili točni i ažurni.

U svrhu zaštite osobnih podataka Društvo poduzima organizacijske, kadrovske i tehničke mjere zaštite osobnih podataka.

II. EVIDENCIJE AKTIVNOSTI OBRADE

Članak 4.

U evidencijama aktivnosti obrade koje vodi Društvo kao voditelj obrade navodi se:

1. naziv i kontaktni podaci voditelja obrade i, ako je primjenjivo, zajedničkog voditelja obrade;
2. svrhe obrade;
3. opis kategorija ispitanika i kategorija osobnih podataka;
4. kategorije primateljâ kojima su osobni podaci otkriveni ili će im biti otkriveni, uključujući primatelje u trećim zemljama ili međunarodne organizacije ako je primjenjivo;
5. ako je primjenjivo, prijenose osobnih podataka u treću zemlju ili međunarodnu organizaciju, uključujući identificiranje te treće zemlje ili međunarodne organizacije te u slučaju prijenosa iz članka 49. stavka 1. drugog podstavka GDPR-a, dokumentaciju o odgovarajućim zaštitnim mjerama;
6. ako je to moguće, predviđene rokove za brisanje različitih kategorija podataka;
7. ako je moguće, opći opis tehničkih i organizacijskih sigurnosnih mjera;
8. rokove čuvanja osobnih podataka.

Evidencije aktivnosti obrade vode se u pisanom obliku, uključujući elektronički oblik.

Evidencije aktivnosti obrade daju se na uvid nadzornom tijelu na njegov zahtjev.

III. OBRADA OSOBNIH PODATAKA

Članak 5.

Društvo osobne podatke obrađuje samo na nekom od propisanih temelja za obradu osobnih podataka i to na temelju ugovora, zakona ili suglasnosti.

Društvo prilikom svake obrade utvrđuje svrhe u koje se podaci obrađuju.

Rok čuvanja osobnih podataka utvrđuje se u odnosu na svaku pojedinu evidenciju aktivnosti obrade osobnih podataka te ovlaštena osoba za zaštitu podataka vodi računa o pravovremenom uništavanju/brisanju podataka na siguran način.

Društvo može prenijeti osobne podatke samo na izvršitelje obrade koji u dovoljnoj mjeri jamče provedbu odgovarajućih tehničkih i organizacijskih mjera tako da je obrada u skladu sa zahtjevima iz GDPR-a i da se njome osigurava zaštita prava ispitanika.

Društvo će s izvršiteljima obrade sklopiti odgovarajući ugovor o obradi podataka kojim će se regulirati sve okolnosti obrade.

Društvo osobne podatke može prenijeti izvan Republike Hrvatske i Europske unije samo na nekom od temelja koji je propisan GDPR-om.

Članak 6.

Prije obrade osobnih podataka Društvo izvješćuje ispitanike o svim bitnim okolnostima obrade njihovih osobnih podataka.

IV. OBRADA OSOBNIH PODATAKA RADNIKA

Članak 7.

Osobni podaci radnika smiju se prikupljati, obrađivati, koristiti i dostavljati trećim osobama samo ako je to određeno zakonom ili je potrebno radi ostvarivanja prava i obveza iz radnog odnosa, odnosno u svezi s radnim odnosom kao i u svrhu edukacije i dodatnog usavršavanja radnika i u svrhu liječničkih pregleda radnika na koje su radnici upućeni od strane Društva.

Radnici su obvezni dostaviti sve osobne podatke utvrđene propisima o evidencijama u području rada, a radi ostvarivanja prava i obveza iz radnog odnosa ili u svezi s radnim odnosima.

U slučaju prestanka radnog odnosa Društvo je ovlašteno nastaviti obrađivati osobne podatke samo u mjeri u kojoj je to potrebno radi ostvarivanja prava i obveza iz radnog odnosa (kao što su npr. isplata preostale plaće, bonusa, nagrada i sl.). Nakon prestanka radnog odnosa Društvo će osobne podatke radnika i članova njegove obitelji čuvati koliko je to propisano zakonom i drugim mjerodavnim propisima RH odnosno u evidenciji prikupljanja osobnih podataka radnika.

Svi radnici obvezni su sve osobne podatke drugih radnika i trećih osoba čije podatke Društvo obrađuje prikupljati, obrađivati, koristiti i dostavljati trećim osobama isključivo u skladu s ovim Pravilnikom i drugim aktima Društva kojima se regulira zaštita osobnih podataka te su radnici obvezni čuvati povjerljivost svih osobnih podataka za koje sazna. Obveza čuvanja povjerljivosti ostaje na snazi i nakon prestanka radnog odnosa.

VI. OSTALI ISPITANICI

Članak 8.

Pored osobnih podataka radnika, Društvo obrađuje i osobne podatke stranaka i poslovnih partnera.

U evidencijama aktivnosti obrade ovih ispitanika, Društvo utvrđuje svrhu obrade, kategorije ispitanika i kategorije podataka, kategorije primatelja osobnih podataka, rokove čuvanja uz naznaku da li se podaci prenose izvan Republike Hrvatske te naznaku poduzetih mjera zaštite osobnih podataka.

V. PRAVA ISPITANIKA

Članak 9.

Svaki ispitanik ima pravo zatražiti potvrdu od Društva da li se njegovi osobni podaci obrađuju, u koju svrhu i u kojoj mjeri.

Ako su osobni podaci ispitanika netočni ili nepotpuni, ispitanik ima pravo tražiti ispravak svojih osobnih podataka.

Ako je svrha prikupljanja osobnih podataka prestala, ako se radi o nezakonitoj obradi, ukoliko obrada nerazmjerno zadire u zaštićene legitimne interese ispitanika ili se obrada podataka temeljila na privoli ispitanika koja je povučena, ispitanik može podnijeti zahtjev za brisanje njegovih osobnih podataka.

Ispitanik ima pravo tražiti ograničenje obrade svojih podataka u sljedećim slučajevima:

- ako osporava točnost svojih osobnih podataka, i to tijekom razdoblja koje Društvu omogućuje provjeru točnosti podataka;

- ako je obrada nezakonita, ali je ispitanik odbio brisanje podataka te umjesto toga traži ograničavanje obrade podataka;

- ako Društvu za predviđenu svrhu osobni podaci više nisu potrebni, a ispitanik ih još uvijek treba za postavljanje ili obranu pravnih zahtjeva ;

- ako je ispitanik uložio prigovor na obradu osobnih podataka očekujući potvrdu nadilaze li legitimni razlozi voditelja obrade razloge ispitanika.

Zahtjeve zaprima službenik za zaštitu podataka, odnosno ovlaštena osoba Društva te će Društvo odgovoriti na zahtjev ispitanika odnosno pružiti informacije o poduzetim radnjama najkasnije u roku od mjesec dana od dana zaprimanja prigovora.

Ako je obrada zahtjeva složena ili se radi o velikom broju zahtjeva, rok iz prethodnog stavka se može produžiti za još dva mjeseca, u kojem slučaju će Društvo o produljenju roka izvijestiti podnositelja.

Ako Društvo nije u mogućnosti postupiti po zaprimljenom zahtjevu, Društvo će u pisanom obliku o takvoj odluci izvijestiti podnositelja uz navođenje razloga za takvu odluku, te mogućnosti podnošenja pritužbe Agenciji za zaštitu osobnih podataka.

Ako su zahtjevi očito neutemeljeni ili pretjerani, osobito zbog njihovog učestalog ponavljanja, Društvo ima pravo naplatiti razumnu naknadu na temelju administrativnih troškova ili odbiti postupati po zahtjevu odnosno prigovoru.

VI. MJERE ZAŠTITE OSOBNIH PODATAKA

Članak 10.

Zaštita osobnih podataka obuhvaća organizacijske, tehničke i odgovarajuće tehničke postupke i mjere, kojima se sprječava slučajno ili namjerno neovlašteno uništavanje podataka, njihova izmjena, gubitak ili neovlaštena obrada kao i svaka druga povreda osobnih podatka, koja se sastoji od sljedećeg:

- zaštite prostorija u kojima se pohranjuju osobni podaci,
- zaštite aplikacijskih i sustavnih softvera pomoću kojih se obrađuju osobni podaci,
- osiguranje zaštite prosljeđivanja i prijenosa osobnih podataka,
- onemogućavanja neovlaštenim osobama pristup uređajima na kojima se obrađuju osobni podaci,
- omogućavanja efikasnog načina blokiranja, uništavanja, brisanja ili ako je moguće anonimiziranja osobnih podataka.

Uzimajući u obzir najnovija dostignuća, troškove provedbe te prirodu, opseg, kontekst i svrhe obrade, kao i rizik različitih razina vjerojatnosti i ozbiljnosti za prava i slobode pojedinaca, Društvo će poduzimati kontinuirane aktivnosti radi implementacije odgovarajućih tehničkih i organizacijskih mjera kako bi osigurao odgovarajuću razinu sigurnosti s obzirom na rizik.

S ciljem zaštite obrade, prikupljanja i procesiranja osobnih podataka, Društvo će poduzimati sljedeće mjere:

- na svim uređajima koje koristi instalirati isključivo licencirani softver;
- na svim uređajima instalirati adekvatni antivirus software;

- na svim uređajima ugraditi odgovarajuću šifru za ulazak od strane ovlaštenih osoba.
- ograničiti pristup/ulazak poslovnim prostorijama;
- provjeriti i osigurati mjesto za spremanje spisa;
- ne spremati ili arhivirati spise ili dokumente koji sadrže osobne podatke u poslovnim prostorijama ili na mjestima u kojima svi imaju slobodan pristup;
- ako je moguće postaviti alarme/videonadzor u poslovne prostorije i slično;
- osigurati da vanjski posjetitelji mogu pristupiti poslovnim prostorijama Društva samo uz prisutnost zaposlenika Društva.

Članak 11.

Društvo i/ili radnici zaposleni kod Društva, a koji u svom radu koriste osobne podatke ili ih na bilo koji način obrađuju, ne smiju tijekom radnog vremena ostavljati na radnim stolovima nosače osobnih podataka bez nadzora ili ih na neki drugi način izlagati opasnosti uvida od strane neovlaštenih osoba.

Prema trećim osobama nosači podataka i zasloni računala moraju u trenutku obrade ili rada na njima biti postavljeni tako da toj osobi nije omogućen uvid u njih.

Oprema za obradu osobnih podataka koristi se sukladno tehničkim uputama proizvođača opreme i odredbama ovog Pravilnika.

Oprema za obradu osobnih podataka nalazit će se i koristiti samo u prostorijama koje odgovaraju propisanim uvjetima za rad s tom opremom te će Društvo osigurati da istom upravljaju samo ovlašteni radnici Društva.

Izvan radnog vremena računala ili druga oprema na kojoj se obrađuju ili pohranjuju osobni podaci mora biti isključena i fizički ili programski zaključana, a pristup osobnim podacima, koji se čuvaju na disku računala, mora biti zaštićen zaporkom.

Članak 12.

Održavanje i popravak računalne i druge opreme kojom se obrađuju osobni podaci odnosno na kojoj se nalaze osobni podaci mogu vršiti samo osobe koje s Društvom imaju sklopljen odgovarajući ugovor kojim su se obvezali na zaštitu osobnih podataka.

Ako je za servisiranje, popravak, mijenjanje ili dopunjavanje sustavnog ili aplikacijskog softvera potrebno kopiranje osobnih podataka, osoba koja je ovlaštena za obradu i rukovanje osobnim podacima na računalu dužan je pobrinuti se da se po prestanku potrebe za kopijom ista uništi.

Članak 13.

Sadržaj diskova mrežnog servera i lokalnih radnih stanica na kojima se nalaze osobni podaci redovno se provjerava zbog moguće prisutnosti računalnih virusa.

Pri pojavi računalnog virusa potrebno je učiniti sve da kako bi se uz pomoć stručnjaka virus otklonio i utvrdio uzrok pojava virusa.

Svi podaci i softver, koji su namijenjeni korištenju u računalnom informacijskom sustavu Društva i stižu Društvu na medijima za prijenos računalnih podataka ili putem telekomunikacijskih kanala, moraju prije uporabe biti provjereni zbog moguće prisutnosti računalnih virusa.

Članak 14.

Serveri na kojima se nalaze podaci moraju biti fizički, organizacijski i tehnički zaštićeni. Izravan pristup podacima u zbirkama podataka na serverima mora biti zaštićen na isti način kao što je zaštićen aplikacijski pristup tim podacima.

Članak 15.

Osobni podaci tijekom prijenosa putem telekomunikacijskih sredstava i mreža moraju biti zaštićeni (npr. enkripcija prijenosa podataka).

VII. ORGANIZACIJA RADNIH POSTUPAKA VEZANO NA OBRADU OSOBNIH PODATAKA

Članak 16.

Društvo će redovno educirati svoje radnike o obvezama u pogledu zaštite osobnih podataka te ih obvezati na čuvanje povjerljivosti osobnih podataka.

Radnici koji obrađuju osobne podatke, radnici koji rade na poslovima informatičke potpore kadrovskoj evidenciji, radnici koji rade na obračunu plaća i ostali radnici koji se u svom radu moraju koristiti osobnim podacima te dobiju pravo na pristup osobnim podacima radnika, podatke koje saznaju u obavljanju svojih poslova moraju brižljivo čuvati.

Članak 17.

Sve osobe zaposlene kod Društva, koje dolaze u doticaj s osobnim podacima dužne su poduzimati mjere za sprječavanje zlouporabe osobnih podataka i moraju osobne podatke, koje obrađuju u svojem radu, obrađivati savjesno, na način i po postupcima koje određuje ovaj Pravilnik i drugi propisi i interni akti.

Osoba koji dozna ili sumnja da je došlo do zlouporabe osobnih podataka (otkrivanje osobnih podataka, neovlašteno uništenje, neovlaštena preinaka, oštećenje zbirke, prisvajanje osobnih podataka) ili do upada u zbirku osobnih podataka mora o tome odmah obavijestiti Društvo, odnosno ovlaštenu osobu za zaštitu osobnih podataka.

U slučaju povrede osobnih podataka, Društvo će bez nepotrebnog odgađanja, napraviti procjenu rizika.

Ako Društvo utvrdi da je nastupio nizak rizik za prava i slobode pojedinaca, upisat će povredu u registar povreda osobnih podataka te neće obavijestiti Agenciju za zaštitu osobnih podataka i ispitanike.

Ako Društvo utvrdi da je nastupio srednji rizik, Društvo će obavijestiti Agenciju za zaštitu osobnih podataka putem za to predviđenog obrasca te evidentirati povredu osobnih podataka u registar povreda osobnih podataka, a najkasnije u roku od 72 sata od dana saznanja za povredu.

Ako Društvo utvrdi da je nastupio visok rizik za prava i slobode pojedinaca, obavijest će Agenciju za zaštitu osobnih podataka i ispitanike, a najkasnije u roku od 72 sata od dana saznanja za povredu.

Ako izvješćivanje nije učinjeno unutar 72 sata, Društvo će dokumentirati razloge uslijed kojih nije u ovom roku podnio obavijest.

VIII. PRIJELAZNE I ZAVRŠNE ODREDBE

Članak 18.

Ovaj Pravilnik predstavlja okvir za postupanje Društva vezano na zaštitu osobnih podataka ispitanika.

Društvo će Pravilnik mijenjati/dopunjavati ovisno o okolnostima i potrebama organizacije rada kao i u slučaju promjene relevantnih propisa.

SmartWay d.o.o.

dr. sc. Petra Mesarić