# PRAVILNIK O ZAŠTITI OSOBNIH PODATAKA




**WIN WIN GROUP d.o.o.**
**Rijeka**
**Datum: 21.05.2018.**

## 1 Pregled Pravilnika

**1.1** **Svrha donošenja:** Ovaj Pravilnik Društvo WIN WIN GROUP d.o.o., Rijeka, Riva 8, OIB 98396267134 (dalje u tekstu Društvo), usvaja na temelju Opće uredbe o zaštiti osobnih podataka (dalje u tekstu: GDPR) i Zakona o provedbi Opće uredbe o zaštiti podataka (NN 42/18) s ciljem postizanja i osiguravanja sukladnosti djelovanja Društva sa GDPR-om. Pravilnikom se utvrđuju obavezni opći standardi kojih se zaposlenici i djelatnici Društva moraju pridržavati pri obradi osobnih podataka ispitanika koji žive u Europskoj Uniji ("**EU osobni podaci**"). Izrazi koji se koriste u ovom Pravilnik, a imaju rodno značenje, koriste se neutralno i odnose se jednako na muški i ženski rod.

Pravilnik se temelji na načelima zakonitosti, transparentnosti, poštenja, cjelovitosti, povjerljivosti, pouzdanosti, ažurnosti i točnosti.

**1.2** **Područje primjene:** Pravilnik se primjenjuje na Društvo kada Društvo prikuplja, prima, pristupa ili na drugi način obrađuje EU osobne podatke. Društvo je dužno poduzeti potrebne mjere kako bi osigurao da treće strane kojima Društvo dostavlja EU osobne podatke provode svoje aktivnosti u ime Društva u skladu s ovim Pravilnikom. Konkretno, Pravilnik se primjenjuje na:

**1.2.1** Sve zaposlenike Društva, sve osobe koje na osnovi ugovora o djelu, autorskog ugovora ili na sličnoj osnovi (zbirno dalje u tekstu: "**djelatnici**") koji imaju pristup EU osobnim podacima koje obrađuje Društvo ili koji se obrađuju u ime Društva; ili koji upravljaju ili na drugi način imaju bilo kakvu odgovornost za obradu EU osobnih podataka;

**1.2.2** Sve aktivnosti koje vodi Društvo ili se vode u njegovo ime, a koje uključuju EU osobne podatke, kada Društvo nastupa u svojstvu Voditelja obrade, i

**1.2.3** Sve aktivnosti koje vodi Društvo ili se vode u njegovo ime, a koje uključuju EU osobne podatke, kada Društvo nastupa u svojstvu Izvršitelja obrade.

**Objava:** Pravilnik je dostupan svim djelatnicima na oglasnoj ploči Društva i na internet stranici WIN WIN GROUP d.o.o.

## 2 Primjena

**2.1** Djelatnici su odgovorni za poznavanje i postupanje sukladno ovom Pravilniku, kao i za informiranje svojih nadređenih, Društva ili imenovanog Službenika za zaštitu EU osobnih podataka o svakoj sumnji na kršenje odredbi ovog Pravilnika.

**2.2** Djelovanje u skladu s ovom Pravilnikom obavezno je za sve djelatnike Društva. Neusklađenost s Pravilnikom mogla bi izložiti Društvo i djelatnika/e značajnoj

građanskoj i/ili kaznenoj odgovornosti, imovinskoj šteti i gubitku ugleda. Društvo može, u mjeri u kojoj je to dopušteno važećim propisima, poduzeti odgovarajuće mjere sve do uključivo otkaza ugovora o radu ili raskida drugog ugovora zbog kršenja Pravilnika od strane bilo kojeg djelatnika Društva, kao i druge odgovarajuće mjere potrebne za otklanjanje štete nastale uslijed nepridržavanja odredaba ovog Pravilnika.

## 3 Pojmovi

**3.1** **Privola:** Svako dobrovoljno, izričito, informirano i nedvosmisleno iskazivanje želje ispitanika kojom on, bilo izričito ili nedvojbeno potvrdnom radnjom, daje pristanak za obradu osobnih podataka koji se na njega odnose. (web okvir i/ili potpis)

**3.2** **Voditelj obrade:** Fizička ili pravna osoba ili drugo tijelo koje, samo ili zajedno s drugima, određuje svrhe i sredstva obrade osobnih podataka.

**3.3** **Izvršitelj obrade:** Fizička ili pravna osoba ili drugo tijelo koje obrađuje osobne podatke u ime voditelja obrade.

**3.4** **Ispitanik:** Fizička ili pravna osoba, identificirana ili čiji se identitet može utvrditi, čiji se osobni podaci obrađuju.

**3.5** **Procjena učinaka zaštite podataka:** definirano u članku 7.8

**3.6** **Službenik za zaštitu podataka:** definirano u članku 4.4

**3.7** **EU osobni podaci:** definirani u članku 1.1.

**3.8** **Izričita privola:** Privola dobivena po prijedlogu ispitaniku da se suglasi ili ne suglasi s određenom uporabom ili otkrivanjem osobnih podataka, a ispitanik aktivno odgovori na upit, usmeno ili u pisanom obliku (npr. vlastoručnim potpisom, elektronički označavajući okvir u kojem piše “Suglasan sam”).

**3.9** **Temeljni osobni podaci:** ime i prezime, adresa, osobni identifikacijski broj (OIB), datum rođenja, spol, državljanstvo i status radnih dozvola, broj mobitela i podaci (adresa e-pošte).

**3.10** **Ostali osobni podaci:** oni koje nam vi ili treće osobe stavljate na raspolaganje prilikom sklapanja ugovora ili tijekom trajanja ugovorenog odnosa, kao što su podaci iz osobne iskaznice, porezne kartice, bankovni račun, preslika svjedodžbe ili diplome, potvrda o radnom stažu, poznavanje jezika i ostalih vještina vezanih za posao raniji poslodavci kod kojih ste radili, liječničko uvjerenje (po potrebi), potvrda o nekažnjavanju (po potrebi), potvrda o školovanju, rodni list djeteta (po potrebi).

**3.11** **Povreda osobnih podataka:** Kršenje sigurnosti koje dovodi do slučajnog ili nezakonitog uništenja, gubitka, izmjene, neovlaštenog otkrivanja ili pristupa osobnim podacima koji su preneseni, pohranjeni ili obrađivani na drugi način.

**3.12** **Obrada:** 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.

**3.13** **Izrada profila:** Svaki oblik automatizirane obrade osobnih podataka koji se sastoji od uporabe osobnih podataka za ocjenu određenih osobnih značajki povezanih s ispitanikom, posebice za analizu ili predviđanje aspekata u vezi s radnim učinkom, ekonomskim stanjem, zdravljem, osobnim sklonostima, interesima, pouzdanošću, ponašanjem, lokacijom ili kretanjem tog ispitanika.

**3.14** **Rizik za prava i slobode ispitanika:** Obrada osobnih podataka predstavlja rizik za prava i slobode ispitanika onda kada takva obrada može rezultirati fizičkom, materijalnom ili nematerijalnom štetom, uključivo u sljedećim slučajevima: ako obrada osobnih podataka može dovesti do diskriminacije, krađe identiteta ili prijevare, financijskog gubitka, štete ugledu, gubitka povjerljivosti osobnih podataka zaštićenih poslovnom tajnom, neovlaštenog obrnutog postupka pseudonimizacije ili bilo koje druge znatne ekonomske ili socijalne štete; ako ispitanici mogu biti uskraćeni za svoja prava i slobode ili onemogućeni u vršenju kontrole nad svojim osobnim podacima; pri obradi osjetljivih osobnih podataka; pri izradi profila tijekom obrade osobnih podataka; pri obradi osobnih podataka ranjivih ispitanika, osobito djece; ili kad obrada uključuje veliku količinu osobnih podataka i utječe na velik broj ispitanika.

**3.15** **Osjetljivi osobni podaci:** Posebne kategorije osobnih podataka koji otkrivaju rasno ili etničko podrijetlo ispitanika, njegove političke stavove, njegova vjerska ili filozofska uvjerenja ili njegovo članstvo u sindikatu. Osjetljivi osobni podaci također uključuju genetske podatke, biometrijske podatke u svrhu jedinstvene identifikacije ispitanika, podatke koji se odnose na zdravlje i podatke koji se odnose na spolni život ili seksualnu orijentaciju ispitanika.

**3.16** **Nadzorno tijelo:** Agencija za zaštitu osobnih podataka, definirano 7.1.8

**3.17** "**Treća strana**" označava pojedinca ili pravnu osobu izvan Društva i djelatnika i ispitanika Društva, a kojima Društvo prenosi ili omogućava pristup osobnim podacima.

## 4 Odgovornosti

**4.1** **Svi djelatnici Društva.** Svi djelatnici Društva čije odgovornosti uključuju obradu

EU osobnih podataka moraju poznavati i djelovati u skladu s ovim Pravilnikom i odlukama, postupcima i smjernicama koje na polju zaštite osobnih podataka utvrdi Uprava Društva te donositi razumne odluke radi zaštite EU osobnih podataka u skladu s navedenim.

**4.2 Djelatnici zaduženi za odnose s Trećim stranama koje obrađuju EU osobne podatke u ime Društva ili na drugi način imaju pristup EU osobnim podacima.** Osim odgovornosti navedenih u članku 4.1 svaki djelatnik čija je primarna odgovornost upravljanje bilo kakvim sadašnjim ili budućim odnosom s izvršiteljem obrade ili bilo kojom drugom Trećom stranom koja ima pristup EU osobnim podacima djelatnika ili klijenata Društva, mora se konzultirati sa Službenikom za zaštitu osobnih podatka („Službenik za zaštitu“) Društva kako bi osigurao da ugovori s takvim trećim stranama sadrže odgovarajuće odredbe o zaštiti podataka. Povrh toga, takvi djelatnici odgovorni su za konzultacije s osobom zaduženom za informacijske tehnologije Društva radi procjene sigurnosnih mjera koje takve treće strane imaju uvedene za zaštitu EU osobnih podataka.

**4.3 Uprava Društva**. Uprava Društva je odgovorna za odluke koje se odnose na obradu EU osobnih podataka i usklađivanje tih odluka s primjenjivim europskim i nacionalnim propisima o zaštiti podataka.

**4.4 Službenik za zaštitu osobnih podataka.** Službenik za zaštitu je odgovoran za obavještavanje i savjetovanje Uprave i djelatnika Društva koji provode aktivnosti obrade EU osobnih podataka o njihovim obvezama prema GDPR; nadzire usklađenost s GDPR i drugim primjenjivim propisima o zaštiti podataka i ovim Pravilnikom; jača svijest o GDPR, drugim primjenjivim regulativama EU i država članica EU o zaštiti podataka i ovom Pravilniku te savjetuje i educira djelatnike Društva koji sudjeluju u obradi EU osobnih podataka; daje preporuke za izmjene i dopune Pravilnika i svih drugih povezanih akata ili postupaka kada je to prikladno; odgovara na upite djelatnika, klijenata i trećih strana o GDPR i Pravilniku te surađuje s nadzornim tijelima; pruža savjete u odnosu na procjene učinaka zaštite podataka (”Procjena učinka”) i obavlja prethodne konzultacije; vodi propisane evidencije koje se odnose na obradu EU osobnih podataka od strane Društva; savjetuje o odgovarajućim odredbama u vezi zaštite podataka koje treba uključiti u ugovore s trećim stranama koje obrađuju EU osobne podatke u ime Društva; te vrši svaku drugu ulogu službenika za zaštitu podataka zahtijevanu po GDPR ili drugim propisima o zaštiti podataka odnosno, kada je to prikladno, uz suglasnost Uprave imenuje drugog djelatnika Društva da vrši neke od zahtijevanih poslova.

**4.5 Osoba zadužena za informacijske tehnologije.** Vanjski pružatelj usluga za informacijske tehnologije u Društvu odgovoran je za praćenje stanja informacijske sigurnosti Društva, izvještavanje Uprave i Službenika za zaštitu o stanju informacijske sigurnosti, odrednicama informacijske sigurnosti, mogućim poboljšanjima informacijske sigurnosti, savjetuje te, po odobrenju Uprave i uz savjetovanje sa Službenikom za zaštitu provodi implementaciju novih sigurnosnih rješenja kojima se osigurava odgovarajuća razina sigurnosti s obzirom na rizik, uključujući prema potrebi pseudonimizaciju i enkripciju osobnih podataka,

sposobnost osiguravanja trajne povjerljivosti, cjelovitosti, dostupnosti i otpornosti sustava i usluga obrade, sposobnost pravodobne ponovne uspostave dostupnosti osobnih podataka i pristupa njima u slučaju fizičkog ili tehničkog incidenta i proces za redovno testiranje, ocjenjivanje i procjenjivanje učinkovitosti sigurnosnih mjera za osiguravanje sigurnosti obrade.

## 5 Zakoniti temelji za obradu, uključujući privolu

**5.1. Temelji za obradu osobnih podataka.** Prije svake obrade EU osobnih podataka Društvo će utvrditi postojanje zakonitog temelja za obradu EU osobnih podataka prema GDPR. Službenik za zaštitu je odgovoran za potvrđivanje da se takav zakonski temelj utvrdio prije nego Društvo pokrene predložene aktivnosti obrade EU osobnih podataka.

### 5.2. Privola

#### 5.2.1 Metode dobivanja privole:

**5.2.1.1 Općenito.** Kada se Društvo oslanja na privolu kao zakonitu osnovu za obradu podataka, ishodit će pristanak koji treba biti dobrovoljan (tj. ispitanik ima istinski slobodan izbor i ne postoji "očigledna neravnoteža" između Društva i ispitanika), koji je određen; informiran; nedvosmislen (tj. izražen izjavom ili jasnom potvrdnom radnjom, poput označavanja odgovarajućeg okvira na web stranici) i dobiven od ispitanika prije no što obrada započne te koji je moguće razlikovati od drugih informacija.

**5.2.1.2 Izričita privola.** Kada se Društvo oslanja na privolu kako bi legitimizirao obradu osjetljivih EU osobnih podataka, Društvo će od ispitanika ishoditi izričitu privolu.

**5.2.1.3 Povlačenje privole.** Društvo će dozvoliti ispitanicima da u svakom trenutku povuku privolu. Pri tome će ispitaniku povlačenje privole učiniti jednako jednostavnim kao i njezino davanje.

**5.2.1.4 Izražavanje privole.** Kada se oslanja na privolu kao zakoniti temelj za obradu Društvo će zadržati dokaz da je ispitanik dao privolu za obradu njegovih/njezinih EU osobnih podataka.

**5.3 Sigurnost obrade podataka.** Voditelj obrade i izvršitelj obrade provode odgovarajuće tehničke i organizacijske mjere kako bi osigurali odgovarajuću razinu sigurnosti s obzirom na rizik, a uzimajući u obzir sva raspoloživa IT dostignuća, troškove provedbe, prirodu i kontekst obrade te rizik različitih razina vjerojatnosti i ozbiljnosti za prava i slobode pojedinaca. Pojedinačnim ugovorima između Agencije i izvršitelja obrade definirat će se i uskladit će se obveze

koje proizlaze iz članka 32-36 Uredbe.

**5.3.1 Osobni podaci djece.** Društvo djeci mlađoj od 16 godina trenutačno ne nudi nikakve online usluge niti svjesno prikuplja bilo kakve EU osobne podatke od bilo kojeg djeteta mlađeg od 16 godina. Ukoliko Društvo ponudi bilo kakvu online uslugu djeci mlađoj od 16 godina ili svjesno prikupi bilo kakve EU osobne podatke od djece mlađe od 16 godina, Društvo će to učiniti uz pristanak roditelja u skladu s uvjetima navedenima u GDPR.

## 6 Privatnost podataka

U cilju osiguravanja sukladnosti s načelima obrade EU osobnih podataka, Društvo je usvojilo sljedeće standarde koji uređuju obradu EU osobnih podataka :

**6.1 Obavijest:** Tijekom ili uoči prikupljanja EU osobnih podatka Društvo će obavijestiti ispitanike o prikupljanju i obradi EU osobnih podatka od strane Društva.

**6.1.1. Oblik obavijesti**. Društvo će osigurati da obavijesti budu sažete, transparentne, razumljive (tj. jasnog i jednostavnog izričaja) i lako dostupne (web stranica)

**6.1.2. Sadržaj obavijesti.** Društvo će u obavijestima osigurati u najmanju ruku informacije koje se odnose na obradu EU osobnih podatka od strane Društva kako je to navedeno u Dodatku 1 ovog Pravilnika.

**6.1.3. Obavijest nužna za svaku novu svrhu obrade.** Prije svake obrade EU osobnih podatka u bilo koju svrhu, a koja se ne spominje u prethodnim obavijestima Društva, djelatnici Društva moraju se prije svake obrade EU osobnih podataka u nove svrhe savjetovati sa Službenikom za zaštitu koji će im pomoći pri izradi i davanju ažurirane obavijesti ispitanicima zahtijevane po GDPR.

## 7 Prava ispitanika:

**7.1 Djelovanje po zahtjevima ispitanika.** Društvo će omogućiti ostvarivanje sljedećih prava ispitanika:

**7.1.2** Pravo ispitanika na pristup njihovim EU osobnim podacima, dobivanje primjerka njihovih EU osobnih podataka koji se obrađuju (u mjeri u kojoj se davanjem takvih podataka ne krše prava neke treće strane) te pravo na sljedeće vrste informacija o njihovim EU osobnim podacima:

- svrhe obrade;
- kategorije njihovih EU osobnih podataka koji se obrađuju;

- primatelje ili kategorije primatelja kojima je Društvo otkrilo ili će otkriti njihove EU osobne podatke, uključivo s primateljima u trećim zemljama ili međunarodnim organizacijama;
- predviđeno razdoblje tijekom kojeg će Društvo čuvati njihove EU osobne podatke (ili kriterije korištene za utvrđivanje tog razdoblja);
- postojanje prava da zatraže brisanje ili ispravak; da zatraže ograničavanje obrade njihovih EU osobnih podataka; te da izjave prigovor na obradu.
- pravo ispitanika na podnošenje prigovora Agenciji za zaštitu osobnih podataka;
- izvor njihovih podataka (ukoliko Društvo nije prikupilo podatke izravno od ispitanika); i
- postojanje svakog automatskog odlučivanja, uključujući izradu profila, koje ima značajan utjecaj na ispitanika i objašnjavanje logike kao i značenja i mogućih posljedica takve izrade profila za ispitanika.

**7.1.3** Pravo ispitanika na **ispravljanje** netočnih EU osobnih podataka, uzimajući u obzir svrhu obrade, te upotpunjavanje nepotpunih EU osobnih podataka.

**7.1.4** Pravo ispitanika na **brisanje** EU osobnih podataka u slučaju da:

- njihovi EU osobni podaci više nisu potrebni u svrhe za koje su takvi podaci prikupljeni ili obrađeni na drugi način;
- zakoniti temelj za obradu je privola; ukoliko ispitanik povuče takvu privolu, a ne postoji drugi zakoniti temelj;
- ispitanik iskoristi svoje pravo na prigovor, a Društvo nema važnije legitimne temelje za nastavak obrade;
- su njihovi EU osobni podaci nezakoniti obrađeni;
- su njihovi EU osobni podaci prikupljeni u vezi s ponudom usluga informacijskog društva (tj. *online usluga*); ili
- brisanje je nužno radi postupanja u skladu s zakonskim propisima EU ili država članica.

uz uvjet da se pravo na brisanje ne primjenjuje ukoliko Društvo mora nastaviti s obradom EU osobnih podataka ispitanika radi postupanja sukladno zakonima EU ili država članica ili da bi utvrdio, koristio ili branio zakonska prava Društva.

**7.1.5** Pravo ispitanika na **ograničavanje obrade** EU osobnih podataka u slučaju da:

- ispitanik osporava točnost EU osobnih podataka (u tom će slučaju obrada biti ograničena na razdoblje potrebno da se Društvu omogući provjera točnosti EU osobnih podataka);
- obrada je nezakonita, pa ispitanik umjesto brisanja zahtijeva ograničavanje uporabe njegovih/njezinih podataka;

- Društvo više ne treba podatke u izvorne svrhe, no podaci su i dalje potrebni kako bi utvrdilo, koristilo ili branilo svoja zakonska prava;
- ispitanik je uložio prigovor na obradu i Društvo provjerava jesu li njegovi zakonski temelji za obradu podataka nadređeni interesima, pravima i slobodama na koje se ispitanik poziva.

**7.1.6** Pravo ispitanika na **prenosivost podataka** (odnosno pravo na dobivanje primjerka EU osobnih podataka u uobičajenom, elektronički čitljivom obliku te na prijenos njihovih EU osobnih podataka s jednog voditelja obrade na drugog ili vršenje prijenosa podataka izravno između voditelja obrade) ukoliko se obrada vrši na automatizirani način; te ukoliko pravni temelj za obradu čini ili privola ili ispunjenje ugovora u kojem je ispitanik ugovorna strana ili ukoliko se obrada vrši u svrhu poduzimanja mjera na zahtjev ispitanika prije sklapanja ugovora.

**7.1.7** Pravo ispitanika na **prigovor na obradu** EU osobnih podataka koji se odnose na njega, što uključuje i izradu profila, na temelju legitimnih interesa Društva ili treće strane ili za izvršenje zadaće koja se vrši u javnom interesu. Kad voditelj prvi puta kontaktira ispitanika za posao, mora ga upozoriti da ima pravo na prigovor vezano za obradu osobnih podataka. U slučaju podnošenja prigovora (u pisanom obliku) ako ispitanik ne želi daljnju obradu podataka, voditelj obrade mora brisati osobne podatke ispitanika i ne može s njima raspolagati bez njegove privole.

**7.1.8** Svaki ispitanik ima pravo pritužbe nadzornom tijelu – Agenciji za zaštitu osobnih podataka (AZOP) prema mjestu prebivališta ili prema mjestu gdje je njegovo radno mjesto ili prema mjestu gdje je počinjeno kršenje.
O povredi prava Agencija odlučuje Rješenjem. Rješenje je Upravni akt.

**7.1.9** Pravo ispitanika da ne bude podvrgnut odluci koja na njega značajno utječe utemeljenoj isključivo na automatiziranoj obradi (uključivo s izradom profila), osim ako je takva obrada neophodna za sklapanje ili izvršavanje ugovora s ispitanikom i postoje odgovarajuće zaštitne mjere; obrada je dopuštena prema zakonskim propisima EU ili države članice koji se primjenjuju na Društvo i koji propisuju odgovarajuće mjere za zaštitu prava i sloboda i legitimnih interesa ispitanika; ili je ispitanik dao izričitu privolu za takvu obradu i postoje odgovarajuće zaštitne mjere.

## 7.2 Potvrđivanje

**7.2.1** Društvo će uložiti sve razumne napore kako bi provjerio identitet ispitanika prije no što ispitanicima osigura pristup EU osobnim podacima ili udovolji drugim zahtjevima ispitanika.

**7.2.2** Ukoliko Društvo ima razumne dvojbe u pogledu identiteta osobe koja podnosi bilo kakav zahtjev kao ispitanik, Društvo može zatražiti dodatne informacije kako bi potvrdio identitet te osobe.

**7.2.3** Ukoliko Društvo ne može potvrditi identitet osobe koja podnosi zahtjev kao ispitanik, Društvo neće odgovoriti na takav zahtjev ispitanika.

**7.3 Odgovaranje na zahtjeve ispitanika.** Društvo može u svom poslovanju primiti pisani ili online zahtjev ispitanika odnosno telefonski zahtjev. Djelatnici moraju odmah obavijestiti Službenika za zaštitu ukoliko na bilo koji način zaprime neki zahtjev ispitanika te se savjetovati o odgovarajućem postupanju.

## 7.4 Treće strane

### 7.4.1 Upravljanje odnosima s izvršiteljima obrade

**7.4.1.1** Društvo će koristiti samo one izvršitelje obrade koji jamče primjenu odgovarajućih tehničkih i organizacijskih mjera potrebnih za usklađivanje s GDPR i za osiguravanje zaštite prava ispitanika.

**7.4.1.2** Društvo će sklopiti ugovore s izvršiteljima obrade u kojima će se utvrditi predmet i trajanje obrade, priroda i svrha obrade, vrsta EU osobnih podataka koji se obrađuju, kategorije ispitanika te obveze i prava Društva kao voditelja obrade.

## 7.5 Nastupanje u svojstvu Izvršitelja obrade

**7.5.1.** Kada nastupa u svojstvu Izvršitelja obrade, Društvo će postupati sukladno odredbama GDPR-a i nacionalnog zakonodavstva u mjeri u kojem su istim propisane obveze za Izvršitelja obrade i sukladno dokumentiranim uputama odnosnog voditelja obrade.

**7.5.2.** Prije početka ili prilikom pružanja usluga koje uključuju obradu EU osobnih podataka za odnosnog voditelja obrade, Društvo će provjeriti, potvrditi i prema potrebi pružiti odgovarajuće dokaze ispunjenja tehničkih i organizacijskih mjera zaštite potrebnih radi osiguranja odgovarajuće razine zaštite prava ispitanika.

**7.5.3.** Prije početka pružanja usluga obrade za odnosnog voditelja obrade, Društvo će zaposlenike uključene u odnosnu obradu upozoriti na činjenicu da se obrada vrši za odnosnog voditelja obrade i isključivo u skladu s njegovim dokumentiranim uputama, te osigurati odgovarajuće evidentiranje dokumentacije o uputama i poslovima obrade.

**7.5.4.** Sa svakim voditeljem obrade kojem Društvo pruža usluge koje uključuju obradu EU osobnih podataka, Društvo će sklopiti ugovor koji će sadržavati odredbe o predmetu i trajanju obrade, prirodi i svrsi obrade, vrsti EU osobnih podataka koji se obrađuju, kategoriji ispitanika, te obveze i prava Društva kao voditelja obrade sukladne GDPR-u i pobliže navedene u Dodatku 2 ovom

Pravilniku, koji se primjenjuje na odgovarajući način.

## 7.6 Prekogranični prijenosi

**7.6.1** Društvo će dozvoliti prekogranični prijenos EU osobnih podataka pojedincu ili tijelu u zemlji koja je izvan EU samo ako je:

- Europska Komisija ocijenila da treća zemlja, teritorij unutar treće zemlje, područje unutar treće zemlje ili međunarodna organizacija kamo Društvo prenosi EU osobne podatke osigurava odgovarajuću razinu zaštite (npr. Kanada, Švicarska, savezne države SAD koje sudjeluju u EU-SAD Štitu privatnosti);

- Društvo primijenilo zakonom dopušten mehanizam prijenosa podataka (npr. standardne ugovorne odredbe usvojene od strane Europske Komisije; obvezujuća korporativna pravila; odobreni kodeks ponašanja, zajedno s obvezujućim i izvršivim obvezama za osiguravanje odgovarajućih zaštitnih mjera); ili

- Na temelju iznimaka ili odricanja (npr. izričita privola ispitanika dana nakon što su obaviješteni o mogućim rizicima prijenosa).

**7.6.2** Djelatnici Društva moraju se konzultirati sa Službenikom za zaštitu prije pokretanja nove vrste prijenosa EU osobnih podataka izvan EU kako bi bili sigurni da postoji zakonit temelj za takav prijenos. „**Prijenos**“ uključuje i EU osobne podatke koji ostaju unutar EU, ali su dostupni jednom ili više Djelatnika Društva izvan EU.

**7.7 Postupanje u slučaju povrede EU osobnih podataka.** Uprava društva će u slučaju povrede EU osobnih podataka imenovati Tim za reakciju i postupanje u slučaju incidenata (*Incident Response Team*) koji je dužan poduzeti mjere vezane uz utvrđivanje povrede osobnih podataka i oporavka osobnih podataka u skladu s GDPR-om i drugim mjerodavnim propisima, uz odgovarajuće pravovremeno obavještavanje Nadležnih tijela.

## 7.8 Procjena učinka na zaštitu podataka i prethodne konzultacije

### 7.8.1 Procjena je obavezna:

**7.8.1.1** U slučaju kad Društvo želi provesti novu aktivnost obrade, posebice aktivnost koja uključuje nove tehnologije i za koju je izgledno da može rezultirati visokim rizikom za prava i slobode pojedinaca, Društvo će prije takve aktivnosti obrade provesti procjenu učinka na zaštitu podataka (“**Procjena učinka**”). Društvo će razmotriti narav, opseg, kontekst i svrhe obrade kako bi procijenilo utjecaj

mogućih novih aktivnosti obrade na zaštitu EU osobnih podataka.

**7.8.1.2** Društvo će provesti postupak Procjene učinka ako njegove aktivnosti obrade uključuju bilo što od sljedećeg:

- sustavnu, opsežnu procjenu osobnih značajki ispitanika koja se temelji na automatiziranoj obradi, uključivo s izradom profila, na temelju koje Društvo donosi odluke koje proizvode pravne učinke u odnosu na takve ispitanike ili na drugi način značajno utječu na takve ispitanike;
- opsežnu obradu osjetljivih EU osobnih podataka ili obradu EU osobnih podatka u vezi s kaznenim osudama ili kaznenim djelima;
- sustavno praćenje velikih razmjera javno dostupnog područja; ili
- svaku drugu aktivnost obrade za koju Agencija za zaštitu osobnih podataka zahtjeva provedbu Procjene učinka.

**7.9 Postupak Procjene učinka.** Društvo će provesti i primijeniti svoj postupak Procjene učinka i preglede postupaka Procjene učinka savjetujući se sa Službenikom za zaštitu i koristeći smjernice za postupanje prilikom provedbe postupka Procjene učinka koje je izradila Europska komisija, odnosno Nadzorno tijelo.

**7.10 Prethodno savjetovanje s Nadzornim tijelom.** Gdje provedeni postupak pokaže da bi obrada rezultirala visokim rizikom za prava i slobode ispitanika ukoliko voditelj obrade podataka ne poduzme mjere smanjenja rizika ili kada zakon propisuje prethodno savjetovanje s Nadzornim tijelom i njegovo odobrenje u odnosu na obradu, prije pokretanja takvih aktivnosti obrade Službenik za zaštitu će se prethodno savjetovati s Nadzornim tijelom.

**7.11 Vođenje evidencije.** Društvo će sačiniti, ažurirati i čuvati evidenciju svojih aktivnosti obrade u skladu s zahtjevima GDPR koji se odnose na vođenje evidencija.

## 8 Upiti i kontakt podaci

**8.1.** Djelatnici koji imaju pitanja u vezi ovog Pravilnika trebaju se obratiti Upravi ili Službeniku za zaštitu osobnih podataka.

**8.2.** Ime i kontakt podaci Službenika za zaštitu jesu:

WIN WIN GROUP d.o.o.
Riva 8, 51000 Rijeka
Ime i prezime Službenika za zaštitu osobnih podataka: Sara Grujić
e-mail: osobnipodaci@winwin-group.com

## 9 Stupanje na snagu

**9.1.** Ovaj Pravilnik o osobnim podacima donesen je na dan 21.05.2018.

**9.2.** Društvo će odredbe ovog Pravilnika učiniti dostupnim svim zaposlenicima na oglasnoj ploči i web stranici Društva. Pravilnik stupa na snagu dana 25.05.2018.

**Društvo:**

WIN WIN GROUP d.o.o.

## Dodatak 1 : Sadržaj obavijesti

Društvo će u obavijestima ispitanicima koje se odnose na prikupljanje i obradu EU osobnih podataka od strane Društva osigurati sljedeće informacije :

- identitet i kontakt podatke izvršitelja obrade podataka;
- kontakt podatke Službenika za zaštitu osobnih podataka
- svrhu i pravni temelj za obradu;
- legitimne interese za obradu, kada one čine zakoniti temelj za obradu;
- primatelje ili kategorije primatelja EU osobnih podatka, ukoliko postoje;
- kategorije odnosnih EU osobnih podataka (ukoliko se EU osobni podaci ne prikupljaju od ispitanika);
- informacije o svakom prekograničnom prijenosu podataka i moguće rizike povezane s takvim prijenosima;
- razdoblje tijekom kojeg će Društvo pohranjivati EU osobne podatke (ili ako nije moguće odrediti točno razdoblje kriterije za određivanje tog razdoblja);
- postojanje specifičnih prava ispitanika, uključujući pravo zahtijevati pristup, ispravak ili brisanje EU osobnih podataka; ograničavanje obrade koja se odnosi na ispitanika; pravo na prigovor u odnosu na obradu; te prenosivost podataka;
- kada privola ispitanika čini zakoniti temelj za obradu, postojanje prava na povlačenje privole u svakom trenutku (bez utjecaja na zakonitost obrade temeljene na privoli prije povlačenja);
- pravo podnošenja prigovora Agenciji za zaštitu osobnih podataka;
- je li davanje EU osobnih podatka zakonski ili ugovorni uvjet ili preduvjet potreban za sklapanje ugovora; je li ispitanik dužan dati svoje EU osobne podatke; te moguće posljedice u slučaju uskrate davanja EU osobnih podatka;
- postojanje automatiziranog odlučivanja, uključivo s izradom profila (kad takve odluke imaju pravne učinke ili značajno utječu na ispitanika) i davanje smislene informacije u vezi logike i mogućih posljedica takve obrade za ispitanika; i
- informacije o izvorima EU osobnih podataka (ukoliko Društvo ne prikuplja takve podatke izravno od ispitanika) i, gdje je primjenjivo, dolaze li iz javno dostupnih izvora.

## Dodatak 2 : Odredbe u ugovorima u kojima je Društvo izvršitelj obrade

Ugovori koje Društvo sklapa i temeljem kojih je Društvo izvršitelj obrade podataka moraju sadržavati sljedeće odredbe kojima se utvrđuje da će Društvo kao izvršitelj obrade:

- obrađivati EU osobne podatke samo prema dokumentiranim uputama izdanim od Društva (uključivo s uputama za prekogranični prijenos EU osobnih podataka), osim u ograničenim okolnostima u kojima je obrada propisana zakonom EU ili države članice mjerodavnim za izvršitelja obrade, u kojem slučaju izvršitelj obrade mora prije započinjanja obrade obavijestiti Društvo o takvom zakonskom zahtjevu, osim ako je davanje takvih informacija zabranjeno zakonom na temelju značajnog javnog interesa;

- nametnuti obveze čuvanja povjerljivosti za svo osoblje izvršitelja obrade koje sudjeluje u obradi EU osobnih podataka;

- primijeniti odgovarajuće tehničke i organizacijske mjere u svrhu osiguravanja odgovarajuće razine sigurnosti u svjetlu izvjesnosti i razine rizika negativnog učinka na prava i slobode ispitanika u skladu s GDPR;

- poštivati sve zahtjeve sadržane u GDPR u vezi angažiranja podizvršitelja obrade;

- pružati Društvu pomoć u ispunjavanju obveze Društva da odgovori na zahtjeve ispitanika u vezi EU osobnih podataka koje izvršitelj obrade obrađuje;

- osigurati usklađenost sa sigurnosnim obvezama izvršitelja obrade, njegovim obvezama provođenja procjene utjecaja na zaštitu podataka i, gdje je to primjenjivo, obvezama da se prije obrade savjetuje s Nadzornim tijelom i obveze da izvijesti Društvo bez odgode nakon saznanja da je došlo do povrede EU osobnih podatka.

- izbrisati ili Društvu vratiti, po izboru Društva, sve EU osobne podatke kada je cijela obrada gotova ili je poslovni odnos okončan na drugi način, te izbrisati bilo koju i sve kopije EU osobnih podataka, osim ako primjenjivi propisi EU ili države članice ne zahtijevaju njihovo daljnje čuvanje; i

- dostaviti Društvu sve informacije potrebne za uvjeravanje da izvršitelj obrade djeluje sukladno GDPR te dopustiti i surađivati u svim revizijama i/ili inspekcijama koje provodi Društvo ili revizor angažiran od strane Društva.

Sve navedeno u ovom Dodatku primjenjuje se i na ugovore koje bi Društvo sklapalo s trećim osobama koje bi u odnosu na Društvo bile Izvršitelji obrade.