

Temeljem 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 - General Data Protection Regulation - Opća uredba o zaštiti podataka (Službeni list Europske unije L 119/1 od 04.05.2016.g., u nastavku GDPR-OUZP Uredba, te važećih zakona Republike Hrvatske koji reguliraju zaštitu podataka, **Turistička zajednica Općine Motovun**, 52424 Motovun, Trg Andrea Antico 1, OIB: 07435219275u ulozi Voditelja osobnih podataka, dana 15. svibnja 2018. godine donosi

INTERNI PRAVILNIK O ZAŠTITI OSOBNIH PODATAKA

Članak 1.

SVRHA

Svrha ovog Pravilnika je normiranje i propisivanje pravila povezana sa zaštitom pojedinaca u pogledu obrade osobnih podataka i pravila povezana sa slobodnim kretanjem osobnih podataka unutar tvrtke, s ciljem zaštite temeljnih prava i slobode pojedinaca, a posebno njihovo pravo na zaštitu osobnih podataka.

Normiranje i propisivanje postupaka odnose se na postupke prikupljanja, obrade, pohrane, prilagodbe ili izmjene, prosljeđivanja i/ili uništavanja osobnih podataka ispitanika, prava te obaveze voditelja i izvršitelja obrade i prava ispitanika.

Članak 2.

ZNAČENJE POJMOVA I NAČELA

(1) Značenje pojmova

Pojedini pojmovi korišteni u izradi ovog Pravilnika i popratnih akata imaju sljedeće značenje:

„**Osobni podaci**” - 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.

„**Obrada**” - znači 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;

„**Evidencija aktivnosti obrade**” (dalje: Evidencija) - svaki voditelj i izvršitelj obrade vodi Evidenciju za osobne podatke s kojim raspolaže i s kojom je u doticaju. Svaki Voditelj i Izvršitelj obrade treba voditi Evidenciju pod svojom odgovornošću radi dokazivanja sukladnosti s GDPR-OUZP Uredbom, surađivati s nadzornim tijelom i omogućiti mu, na zahtjev, uvid u Evidenciju.

„**Ograničavanje obrade**” - znači označavanje pohranjenih osobnih podataka s ciljem ograničavanja njihove obrade u budućnosti.

„**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.

„Sustav pohrane” znači svaki strukturirani skup osobnih podataka dostupnih prema posebnim kriterijima, bilo da su centralizirani, decentralizirani ili raspršeni na funkcionalnoj ili zemljopisnoj osnovi.

„Voditelj obrade” - znači fizička ili pravna osoba, tijelo javne vlasti, agencija ili drugo tijelo koje samo ili zajedno s drugima određuje svrhe i sredstva obrade osobnih podataka; kada su svrhe i sredstva takve obrade utvrđeni pravom Unije ili pravom države članice, voditelj obrade ili posebni kriteriji za njegovu imenovanje mogu se predvidjeti pravom Unije ili pravom države članice.

„Izvršitelj obrade” - znači fizička ili pravna osoba, tijelo javne vlasti, agencija ili drugo tijelo koje obrađuje osobne podatke u ime voditelja obrade.

„Primatelj” - znači fizička ili pravna osoba, tijelo javne vlasti, agencija ili drugo tijelo kojem se otkrivaju osobni podaci, neovisno o tome je li on treća strana. Međutim, tijela javne vlasti koja mogu primiti osobne podatke u okviru određene istrage u skladu s pravom Unije ili države članice ne smatraju se primateljima; obrada tih podataka koju obavljaju ta tijela javne vlasti mora biti u skladu s primjenjivim pravilima o zaštiti podataka prema svrhama obrade.

„Treća strana” - znači fizička ili pravna osoba, tijelo javne vlasti, agencija ili drugo tijelo koje nije ispitanik, voditelj obrade, izvršitelj obrade ni osobe koje su ovlaštene za obradu osobnih podataka pod izravnom nadležnošću voditelja obrade ili izvršitelja obrade.

„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. Ispitanik ima pravo u svakom trenutku povući svoju privolu. Uvjeti privole propisani su člankom 7. GDPR-OUZP Uredbe.

„Legitimni interes” - znači legitimni interes voditelja obrade mogu predstavljati pravnu osnovu za obradu i predstavljaju aktivnosti u vezi s prodajom robe ili pružanjem usluga na tržištu te nužnosti prikupljanja podataka radi identifikacije potencijalnih kupaca ili korisnika usluga, aktivnosti radi izravnog marketinga prilikom kojih prikuplja osobne podatke, pod uvjetom da interesi ili temeljna prava i slobode ispitanika nemaju prednost, uzimajući u obzir razumna očekivanja ispitanika koja se temelje na njihovom odnosu s voditeljem obrade.

„Povreda osobnih podataka” - znači 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.

„Genetski podaci” - znači osobni podaci koji se odnose na naslijeđena ili stečena genetska obilježja pojedinca koja daju jedinstvenu informaciju o fiziologiji ili zdravlju tog pojedinca, i koji su dobiveni osobito analizom biološkog uzorka dotičnog pojedinca.

„Biometrijski podaci” - znači osobni podaci dobiveni posebnom tehničkom obradom u vezi s fizičkim obilježjima, fiziološkim obilježjima ili obilježjima ponašanja pojedinca koja omogućuju ili potvrđuju jedinstvenu identifikaciju tog pojedinca, kao što su fotografije lica ili daktiloskopski 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 njegovu zdravstvenom statusu.

„Glavni poslovni nastan” - znači:

(a) što se tiče voditelja obrade s poslovnim nastanima u više od jedne države članice, mjesto njegove središnje uprave u Uniji, osim ako se odluke o svrhama i sredstvima obrade osobnih podataka donose u drugom poslovnom nastanu voditelja obrade u Uniji te je potonji poslovni nastan ovlašten provoditi takve odluke, u kojem se slučaju poslovni nastan u okviru kojeg se donose takve odluke treba smatrati glavnim poslovnim nastanom;

(b) što se tiče izvršitelja obrade s poslovnim nastanima u više od jedne države članice, mjesto njegove središnje uprave u Uniji, ili, ako izvršitelj obrade nema središnju upravu u Uniji, poslovni nastan izvršitelja obrade u Uniji u kojem se odvijaju glavne aktivnosti obrade u kontekstu aktivnosti poslovnog nastana izvršitelja obrade u mjeri u kojoj izvršitelj obrade podliježe posebnim obvezama u skladu s ovom Uredbom.

„**Predstavnik**” - znači fizička ili pravna osoba s poslovnim nastanom u Uniji koju je voditelj obrade ili izvršitelj obrade imenovao pisanim putem u skladu s člankom 27., a koja predstavlja voditelja obrade ili izvršitelja obrade u pogledu njihovih obveza na temelju GDPR-OUZP Uredbe.

„**Poduzeće**” - znači fizička ili pravna osoba koja se bavi gospodarskom djelatnošću, bez obzira na pravni oblik te djelatnosti, uključujući partnerstva ili udruženja koja se redovno bave gospodarskom djelatnošću.

„**Grupa poduzetnika**” - znači poduzetnik u vladajućem položaju te njemu podređeni poduzetnici.

„**Obvezujuća korporativna pravila**” - znači politike zaštite osobnih podataka kojih se voditelj obrade ili izvršitelj obrade s poslovnim nastanom na državnom području države članice pridržava za prijenose ili skupove prijenosa osobnih podataka voditelju obrade ili izvršitelju obrade u jednoj ili više trećih zemalja unutar grupe poduzetnika ili grupe poduzeća koja se bave zajedničkom gospodarskom djelatnošću.

„**Nadzorno tijelo**” znači neovisno tijelo javne vlasti koje je osnovala država članica u skladu s člankom 51. GDPR-OUZP Uredbe.

„**Predmetno nadzorno tijelo**” znači nadzorno tijelo koje je povezano s obradom osobnih podataka zato što:

(a) voditelj obrade ili izvršitelj obrade ima poslovni nastan na državnom području države članice tog nadzornog tijela;

(b) obrada bitno utječe ili je izgledno da će bitno utjecati na ispitanike koji borave u državi članici tog nadzornog tijela; ili

(c) podnesena je pritužba tom nadzornom tijelu.

„**Prekogranična obrada**” - znači ili:

(a) obrada osobnih podataka koja se odvija u Uniji u kontekstu aktivnosti poslovnih nastana u više od jedne države članice voditelja obrade ili izvršitelja obrade, a voditelj obrade ili izvršitelj obrade ima poslovni nastan u više od jedne države članice; ili

(b) obrada osobnih podataka koja se odvija u Uniji u kontekstu aktivnosti jedinog poslovnog nastana voditelja obrade ili izvršitelja obrade, ali koja bitno utječe ili je izgledno da će bitno utjecati na ispitanike u više od jedne države članice.

„**Relevantni i obrazloženi prigovor**” - znači prigovor na nacrt odluke kao i na to je li došlo do kršenja GDPR-OUZP Uredbe, ili je li djelovanje predviđeno u vezi s voditeljem obrade ili izvršiteljem obrade u skladu s ovom Uredbom, koji jasno pokazuje važnost rizika koje predstavlja nacrt odluke u pogledu temeljnih prava i sloboda ispitanika i, ako je primjenjivo, slobodnog protoka osobnih podataka unutar Unije.

„**Usluga informacijskog društva**” znači usluga kako je definirana člankom 1. stavkom 1. točkom 2. Direktive 2015/1535 Europskog parlamenta i Vijeća (1).

„**Međunarodna organizacija**” znači organizacija i njezina podređena tijela uređena međunarodnim javnim pravom ili bilo koje drugo tijelo koje su sporazumom ili na osnovi sporazuma osnovale dvije ili više zemalja.

(2) Značenje načela

Načela obrade osobnih podataka trebaju poštovati temeljna prava i slobode pojedinca, a posebno pravo pojedinca na zaštitu osobnih podataka bez obzira na nacionalnost ili boravište pojedinca.

Čl. 5. GDPR-OUZP Uredbe, u obradi osobnih podataka, obvezuje na sljedeća načela:

a) zakonitost, poštenje i transparentnost, pri čemu je obrada zakonita samo ona u kojoj je ispunjeno najmanje jedno od sljedećih načela:

- Ispitanik je dao privolu za obradu svojih osobnih podataka u jednu ili više posebnih svrha,
- Obrada je nužna za izvršavanje ugovora u kojem je ispitanik stranka ili kako bi se poduzele radnje prije sklapanja ugovora,
- Obrada je nužna radi poštivanja 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 i temeljna prava i slobode ispitanika koji zahtijevaju zaštitu osobnih podataka, osobito ako je ispitanik dijete.

Načelo zakonitosti obrade - zakonska obaveza obrade osobnih podataka za koju nije potrebna posebna privola ispitanika (npr. evidencije o radnicima koje je poslodavac dužan voditi prema odredbama Zakona o radu te ostalih evidencija u koje se unose podatci koje propisuju važeći zakoni Republike Hrvatske poput: podataka za ostvarivanje prava pojedinaca na mirovinsko i zdravstveno osiguranje, podataka kojima se utvrđuju porezna i druga davanja i sl.).

b) **Ograničavanje svrhe**, načelo je koje znači da osobni podaci moraju biti prikupljeni u posebne, izričite i zakonite svrhe te se dalje ne smiju obrađivati na način koji nije u skladu s tim svrhama.

c) **Smanjenje količine podataka**, načelo je koje znači da osobni podaci trebaju biti primjereni, relevantni i ograničeni na ono što je nužno u odnosu na svrhe u koje se obrađuju.

d) **Točnost i ažurnost**, načelo je koje znači da se mora poduzeti svaka razumna mjera radi osiguravanja da se osobni podaci koji nisu točni, uzimajući u obzir svrhe u koje se obrađuju, bez odlaganja izbrišu i isprave.

e) **Ograničenje pohrane**, osobni podaci trebaju biti čuvani u obliku koji omogućuje identifikaciju ispitanika samo onoliko dugo koliko je potrebno u svrhe radi kojih se osobni podaci obrađuju. Osobni podaci se mogu pohraniti na dulja razdoblja ako će se obrađivati isključivo u svrhu javnog interesa, znanstvenog ili povijesnog istraživanja ili u statističke svrhe, što podliježe provedbi primjerenih tehničkih i organizacijskih mjera propisanih GDPR-OUZP Uredbom radi zaštite prava i sloboda ispitanika.

f) **Cjelovitost i povjerljivost**, osobni podaci trebaju biti obrađivani na način kojim se osigurava odgovarajuća sigurnost osobnih podataka, uključujući zaštitu od neovlaštene ili nezakonite obrade te od slučajnog gubitka, uništenja ili oštećenja primjenom odgovarajućih tehničkih ili organizacijskih mjera.

g) **Pouzdanost** je načelo koje znači da je Voditelj obrade odgovoran za usklađenost sa svim navedenim načelima te biti u mogućnosti to i dokazati.

Članak 3.

Prava ispitanika

Ispitanik ima pravo uvida u zbirku osobnih podataka. Najvažnija prava ispitanika su sljedeća:

- **transparentnost** (čl.12 – 14. GDPR-OUZP Uredbe): pružanje informacija prilikom prikupljanja osobnih podatak kada voditelj obrade mora među ostalim informacijama obavijestiti ispitanika i o svojem

identitetu i kontakt podacima, svrhama obrade i pravnoj osnovi za obradu podataka, primateljima, iznošenju u treće zemlje, razdoblju pohrane, mogućnosti povlačenja privole, brisanju i uništavanju podataka,

- pristup podacima (čl. 15 GDPR-OUZP Uredbe): dobiti od voditelja obrade potvrdu obrađuju li se osobni podaci koji se odnose na njega te ako se takvi osobni podaci obrađuju, pristup osobnim podacima i informacije, među ostalim, o obrađenim osobnim podacima, o svrsi obrade, roku pohrane, iznošenju u treće zemlje, brisanju i uništavanju podataka,
- pravo na ispravak (čl.16. GDPR-OUZP Uredbe): ispitanik ima pravo zahtijevati ispravak netočnih osobnih podataka koji se na njega odnose, a uzimajući u obzir svrhe obrade, ispitanik ima pravo dopuniti nepotpune osobne podatke, među ostalim i davanjem dodatne izjave;
- brisanje - pravo na zaborav (čl.17. GDPR-OUZP Uredbe): ispitanik ima pravo od voditelja obrade ishoditi brisanje osobnih podataka koji se na njega odnose bez nepotrebnog odgađanja te voditelj obrade ima obvezu obrisati osobne podatke bez nepotrebnog odgađanja ako, među ostalim, osobni podaci više nisu nužni u odnosu na svrhu obrade, ispitanik je povukao privolu za obradu, osobni podaci su nezakonito obrađeni i sl.
- pravo na ograničenje obrade (čl.18. GDPR-OUZP Uredbe): u pojedinim situacijama (na primjer kada je točnost podataka osporavana ili kada pravo na brisanje ispitanik želi da voditelj obrade zadrži njegove podatke) ispitanik ima pravo zahtijevati da se obrada ograniči uz iznimku pohrane i nekih drugih vrsta obrade;
- pravo na prenosivost (čl.20. GDPR-OUZP Uredbe): ispitanik ima pravo zaprimiti svoje osobne podatke, a koje je prethodno pružio voditelju obrade, u strukturiranom obliku te u uobičajeno upotrebljavanom i strojno čitljivom formatu te ima pravo prenijeti te podatke drugom voditelju obrade bez ometanja od strane voditelja obrade kojem su osobni podaci pruženi, ako se obrada provodi automatiziranim putem i temelji na privoli ili ugovoru;
- pravo na prigovor (čl.21. GDPR-OUZP Uredbe): ispitanik ima pravo uložiti prigovor na obradu osobnih podataka ako se ista temelji na zadaće od javnog interesa, na izvršavanje službenih ovlasti voditelja obrade ili na legitimne interesa voditelja obrade (uključujući i profiliranje), tada voditelj obrade ne smije više obrađivati osobne podatke ispitanika osim ako dokaže da njegovi legitimni razlozi za obradu nadilaze interese ispitanika te radi zaštite pravnih zahtjeva, također ako se ispitanik protivi obradi za potrebe izravnog marketinga, osobni podaci više se ne smiju obrađivati;
- pravo usprotiviti se donošenju automatiziranih pojedinačnih odluka - profiliranje (čl.22. GDPR-OUZP Uredbe): ispitanik ima pravo da se na njega ne odnosi odluka koja se temelji isključivo na automatiziranoj obradi, uključujući izradu profila, koja proizvodi pravne učinke koji se na njega odnose ili na sličan način značajno na njega utječu, osim ako je takva odluka potrebna za sklapanje ili izvršenje ugovora između ispitanika i voditelja obrade podataka, ako je dopuštena pravom EU-a ili nacionalnim pravom koji se propisuju odgovarajuće mjere zaštite prava i sloboda te legitimnih interesa ispitanika ili temeljena na izričitoj privoli ispitanika.

Ovim Pravilnikom Voditelj obrade upoznaje ispitanika s opsegom prikupljanja i svrhama obrade osobnih podataka, s rizicima, načelima obrade osobnih podataka, pravilima, zaštitnim mjerama i pravima u vezi s obradom osobnih podataka i načinom ostvarenja svojih prava u vezi s obradom.

Članak 4.

Voditelj obrade, svi njegovi radnici, fizičke i pravne osobe koje rade za i u ime, obvezuju se na poštivanje GDPR-OUZP uredbe i ovog Pravilnika koji se odnose na sve aktivnosti koje uključuju obradu osobnih podataka uključujući podatke o korisnicima roba i usluga, klijentima, zaposlenicima, dobavljačima i ostalim partnerima, kao i sve druge podatke koje obrađuje voditelj obrade iz bilo kojeg izvora.

Treća strana ne može pristupiti osobnim podacima koje se obrađuju bez prethodno sklopljenog ugovora/izjave o povjerljivosti.

Voditelj obrade može odabrati Izvršitelja obrade sa kojim je dužan sklopiti ugovor o obradi osobnih podataka u kojem su jasno definirane obaveze Izvršitelja obrade i koji je u skladu sa GDPR-OUZP Uredbom.

Članak 5.

Opseg prikupljanja osobnih podataka

Osobni podaci se prikupljaju isključivo **po načelu ograničavanja svrhe i legitimnom pravu** Voditelja obrade te se ne smiju prikupljati i obrađivati na način koji nije u skladu s tim svrhama.

Osobni podaci koji se obrađuju biti će korišteni u isključivo u sljedeće svrhe:

- Obračun plaće, evidencije o radnicima, knjigovodstvene, računovodstvene i porezne svrhe,
- Izvršenja ugovora,
- Legitimni interes, i
- Privola.

Posebne kategorije podataka nije potrebno niti dopušteno prikupljati.

Članak 6.

Obrada osobnih podataka podrazumijeva **identificiranje zakonske osnove** prije same obrade osobnog podatka. Obrada je zakonita ako i u onoj mjeri u kojoj je ispunjeno najmanje jedno od sljedećega:

- Ispitanik je dao privolu za obradu svojih osobnih podataka u jednu ili više posebnih svrha,
- 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 poštivanja pravnih obaveza Voditelja obrade**,
- Obrada je **nužna kako bi se zaštitili ključni interesi ispitanika ili druge fizičke osobe**,
- 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.

Članak 7.

Čuvanje i način obrade osobnih podataka

Voditelj obrade ne smije čuvati osobne podatke koji mogu identificirati pojedinca **duže od vremena potrebnog za ispunjenje svrhe** za koju su podaci prikupljeni i vremena određenog zakonom.

Voditelj osobnih podataka će obrađene osobne podatke čuvati **sukladno zakonskoj obavezi čuvanja dokumentacije**, nakon čega će osobne podatke brisati (automatizirana obrada) i uništiti (pisani zapisi).

Način obrade može biti ručni (pisani zapis) i automatizirani (PC i informatička infrastruktura).

Članak 8.

Sigurnost obrade osobnih podataka

Voditelj osobnih podataka, u svrhu sigurnosti obrade i pohrane, poduzima odgovarajuće organizacijske i tehničke mjere.

Svi zaposlenici voditelja obrade i druge osobe koje rade za i u ime Voditelja obrade odgovorni su za sigurnost svih osobnih podataka koje voditelj obrade posjeduje i obrađuje.

Podatke treba čuvati na **sigurnom mjestu** koje onemogućava neovlašteni pristup osobnim podacima.

Iz tog razloga, svi osobni podaci moraju se čuvati:

- U **zaključanoj** prostoriji sa kontroliranim pristupom,
- U **zaključanoj** ladici ili ormaru,
- Ako se radi o digitalnim podacima, isti moraju biti **zaključani lozinkom**, i
- Pohranjeni na računalnim medijima koji su **šifrirani**.

Pisani zapisi ne smiju biti ostavljeni u prostorijama u koje mogu pristupiti neovlaštene osobe, niti na radnim stolovima te ne smiju biti uklonjeni iz sigurnog područja bez pisanog odobrenja. Hard diskovi (HD) računala koji više nisu u upotrebi moraju se uništiti.

Članak 9 .

Definiranje organizacijskih i tehničkih mjera

Odgovornost je Voditelja obrade osigurati točne i ažurne podatke ispitanika. Podaci čuvani od strane Voditelja obrade moraju se redovito ažurirati te isti ne smiju biti čuvani ukoliko nisu točni i ažurni.

Osobno podaci moraju biti prikladni svrsi, relevantni i ograničeni u skladu s okvirima nužnim za obradu prema definiranim obavezama.

Voditelj obrade ne prikuplja podatke koji nisu nužno potrebni za ispunjenje svrhe za koju su prikupljeni.

Voditelj obrade je obavezan organizacijskim i tehničkim mjerama osigurati podatke od neovlaštenog pristupa. Organizacijske mjere su postupci kojima se prikupljaju i obrađuju podaci a tehničke mjere su postupci čuvanja osobnih podataka.

Organizacijske i tehničke mjere Voditelj obrade definira i evidentira u Evidenciji aktivnosti obrade po kategorijama ispitanika nakon izvršene kategorizacije i analize rizika.

Sastavni dio ovog Pravilnika su i sljedeći dokumenti:

1. Kategorizacija i analiza postojećeg stanja,
2. Anliza rizika,
3. Popis mjera,
4. Evidencija aktivnosti obrade,
5. Obrazac privole,
6. Izjava o povjerljivosti.

1. Kategorizacije i analiza postojećeg stanja - u svrhu usklađenost sa GDPR-OUZP Uredbom, odgovorna osoba Voditelja obrade ili osoba kojoj prenese ovlasti treba izraditi kategorizaciju i analizu postojećeg stanja u kojoj treba identificirati najmanje sljedeće;

- Kategoriju obrade podataka,
- Izvor i osnovu prikupljanja podataka,
- Način evidentiranja,
- Vrstu obrade,
- Način obrade i rok čuvanja, i
- Prosljeđivanje podataka i primatelje.

2. **Analiza rizika** – dokument koji treba sadržavati pregledan opis postupaka obrade za koju voditelj obrade procijeni da mogu biti rizični.
3. **Popis mjera** – dokument je koji treba sadržavati popis rizičnih točaka obrade, ukoliko postoje, te organizacijske i tehničke mjere za svaku pojedinu kategoriju obrade podataka.
4. **Evidencija aktivnosti obrade** je ključni dokument, izveden iz prethodno opisanih postupaka 1-2-3, kojeg voditelj obrade, tijekom godine stalno prati i po potrebi dopunjuje organizacijske i tehničke mjere ukoliko procijeni da mogu biti ugrožena prava ispitanika.
5. **Obrazac privole** je dokument kojim Voditelj obrade od ispitanika dobiva pismeni pristanak za obradu njegovih podataka a odnose se na radnike, kupce i roditelje.
6. **Izjava o povjerljivosti** – dokument je kojeg izrađuje voditelj obrade za djelatnike unutar poduzeća koji izravno prikupljaju i obrađuju osobne podatke i koji izjavu potpisuju.

Članak 10.

Politike privatnosti

Voditelj podataka se obvezuje na zaštitu osobnih podataka temeljem GDPR-OUZP Uredbe prepoznajući važnost zaštite privatnosti, sigurnosti i zaštite podataka korisnika usluga i svih osoba koje s voditeljem obrade dođu u kontakt.

Svrha prikupljanja osobnih podataka

Sukladno načelu ograničenosti svrhe, osobni podaci se prikupljaju isključivo radi osiguravanja pružanja tražene usluge ispitanika i što učinkovitijeg odgovora na upit te u svrhu poslovanja.

Podaci pokriveni sustavom Politike privatnosti

Podaci koji su pokriveni politikom privatnosti su sljedeći: Ime i prezime, datum rođenja, adresa stanovanja, e-mail, broj telefona i/ili faksa, osobni identifikacijski broj (OIB). Ostali podaci se mogu prikupiti samo uz pismenu privolu ispitanika.

Tajnost podataka

Svi osobni podaci ostaju tajni uključujući i podatke koje ispitanik dostavlja elektroničkom poštom po kojima je moguća identifikacija. Takvi se podaci koriste samo u svrhu ispunjenja zahtjeva ispitanika te ih je Voditelj obrade obavezan čuvati u sustavu pohrane kao tajne sukladno načelu ograničenja pohrane. Zaštita privatnosti podataka ispitanika je trajna.

Legitimni interes

Voditelj obrade, svoj legitimni interes, definira kao pravo prikupljanja dostupnih podataka potencijalnih kupaca sa interneta i drugih javno dostupnih izvora, poštujući načela ograničavanja svrhe i smanjenja količine podataka, pod uvjetom da interesi ili temeljna prava i slobode ispitanika nemaju prednost te uz mogućnost da, ukoliko to ispitanik zatraži, prikupljene podatke izbriše iz svoje evidencije.

Legitimni interes kojeg provodimo jest:

- Marketing i promicanje Motovuna kao turističke destinacije, i
- Obavljanje ostalih djelatnosti u svrhu povećanja receptivnih kapaciteta destinacije.

Članak 11.

Obaveze Voditelja osobnih podataka

Obaveze Voditelja osobnih podataka su sljedeće:

- Poduzeti odgovarajuće tehničke i organizacijske mjere kako bi osigurao i dokazao da se obrada provodi u skladu s GDPR-OUZP Uredbom te, u tom smislu, provesti aktivnosti iz članka 4. Ovog Pravilnika,
- Poštivati i provoditi prava ispitanika iz članka 3. Ovog Pravilnika,
- Uputiti izvršitelja obrade da postupa sukladno odredbama ovog Pravilnika, uključujući i dodatna ograničenja ukoliko postoje, posebnim pravnim aktom koji regulira odnos sa izvršiteljem obrade.
- Pridržavati se načela obrade osobnih podataka navedenih u čl. 2. st.2. ovog Pravilnika.
- Provoditi politiku privatnosti.

Članak 7.

Kaznene odredbe

Ovim Pravilnikom se reguliraju kaznene odredbe samo u dijelu koji se odnosi na kršenje odredaba Izjave o povjerljivosti koju potpisuju radnici poduzeća.

U slučaju kršenja odredaba Izjave o povjerljivosti od strane radnika, odgovorna osoba voditelja osobnih podataka može izreći novčanu kaznu radniku u visini 1/3 neto plaće.

U slučaju grubog ili višekratnog kršenja odredaba Izjave o povjerljivosti od strane djelatnika, odgovorna osoba Voditelja osobnih podataka može radniku uručiti pismeni otkaz i raskinuti ugovor o radu.

Članak 8.

Stupanje na snagu

Ovaj Pravilnik stupa na snagu 25. 05. 2018. godine.

Odgovorna osoba: _____



(potpis i pečat)