PRAVILNIK O POSTUPANJU S OSOBNIM PODACIMA

(„Pravilnik“)

Ovaj Pravilnik definira pravila i smjernice o tome na koji način KRIŠTO TURIZAM d.o.o., sa sjedištem u Zagrebu, Prosenička ulica 14, OIB: 74581693165 (dalje u tekstu: „**KRIŠTO TURIZAM**“) prikuplja, pohranjuje, analizira, koristi, briše te vrši sve druge radnje u svezi obrade osobnih podataka unutar svog poslovanja.

Svrha Pravilnika je osigurati usklađenost s pravilima Opće uredbe za zaštitu osobnih podataka („**GDPR**“) koja je na snazi od 25. svibnja 2018. i hrvatskim Zakonom o provedbi Opće uredbe o zaštiti podataka (NN 42/2018), te ispuniti zahtjeve transparentnosti obrade osobnih podataka i zajamčiti sigurnost.

1. VODITELJ OBRADE

Za pravilnu obradu osobnih podataka odgovornost kao voditelj obrade jamči:

KRIŠTO TURIZAM

Adresa e-pošte: delminivm@hotel-delminivm.hr

2. EVIDENCIJA AKTIVNOSTI OBRADE (čl. 30. GDPR)

KRIŠTO TURIZAM ispunjava obvezu iz čl. 30. GDPR-a i vodi te redovito ažurira evidenciju obrade osobnih podataka.

Evidencija aktivnosti obrade vodi se u obliku Word dokumenta te sadrži sljedeće informacije: podaci o aktivnostima i svrhama obrade koje KRIŠTO TURIZAM vrši u sklopu svog poslovanja; podaci koji se obrađuju u sklopu tih svrha; podaci o pravnim osnovama obrada podataka; podaci o izvršiteljima obrade i zajedničkim voditeljima, podaci o primateljima i prijenosu osobnih podataka te o lokacijama pohrane i roku čuvanja osobnih podataka.

3. SLUŽBENIK ZA ZAŠTITU OSOBNIH PODATAKA (čl. 37. – 39. GDPR)

GDPR predviđa imenovanje službenika za zaštitu osobnih podataka, koja obveza postoji u određenim slučajevima propisanim u čl. 37. GDPR-a.

KRIŠTO TURIZAM je proveo analizu postojanja obveze i potrebe imenovanja službenika za zaštitu osobnih podataka, te je zaključio kako nije obvezan imenovati osobu za službenika za zaštitu osobnih podataka.

4. TRANSPARENTNOST OBRADE I INFORMIRANJE ISPITANIKA (čl. 13. i 14. GDPR)

GDPR kao temeljnu obvezu voditelja obrade nameće obvezu transparentne obrade osobnih podataka i obvezu informiranja ispitanika o svim informacijama sadržanim u čl. 13. i 14. GDPR-a.

KRIŠTO TURIZAM osigurava da su svi njegovi ispitanici pravilno i pravovremeno obavješteni o svim obradama njihovih podataka koje KRIŠTO TURIZAM i njegovi suradnici/izvršitelji vrše. Informiranost ispitanika osigurava se na sljedeće načine:

- Web pravila privatnosti: XY;
- Obavijest o obradi osobnih podataka radnika (uručena i dostupna na uvid zaposlenicima);
- Obavijest o obradi osobnih podataka gostiju;

- Obavijest o obradi osobnih podataka poslovnih partnera.

5. PROCJENE LEGITIMNOG INTERESA (čl. 6. (1) (f) i čl. 35. GDPR)

GDPR kao jednu od pravnih osnova za obradu osobnih podataka predviđa postojanje legitimnog interesa. Međutim, obrada osobnih podataka na temelju legitimnog interesa dopuštena je samo u slučaju ako je konkretan legitiman interes jači od interesa ili temeljnih prava i sloboda ispitanika koji zahtijevaju zaštitu osobnih podataka.

KRIŠTO TURIZAM jamči da za svaku svrhu obrade koja se temelji na postojanju legitimnog interesa, legitiman interes KRIŠTO TURIZAM-a prevladava nad interesima ispitanika. U tu svrhu, u slučaju obrade koja se temelji na legitimnom interesu, provodit će se analize legitimnog interesa u kojima se ispituje i utvrđuje njegovo **postojanje**, **nužnost** (odnosno, nepostojanje drugog načina ostvarenja interesa) te **proporcionalnost** u odnosu na interese i prava ispitanika.

6. SIGURNOST PODATAKA – tehničke i organizacijske mjere (čl. 36. GDPR)

KRIŠTO TURIZAM poduzima sve potrebne tehničke i organizacijske mjere kako bi se osigurala sigurnost osobnih podataka. Tehničke i organizacijske mjere se poduzimaju u svrhu osiguranja razine sigurnosti razmjerne riziku, a u skladu sa zahtjevima koje nameće GDPR u članku 36.

Svrha tehničkih i organizacijskih mjera je osiguranje **povjerljivosti** (informacije su dostupne samo ovlaštenom osoblju), **integriteta** (informacije su točne i ažurne) i **dostupnosti** (podaci su dostupni ovlaštenim osobama samo kada je to potrebno) obrade osobnih podataka.

Sigurnosne i tehničke mjere koje provodi KRIŠTO TURIZAM su sljedeće:

(i) Povjerljivost:

- Kontrola ulaza

KRIŠTO TURIZAM osigurava da nema neovlaštenog pristupa uređajima za obradu podataka, putem: *ključeva, odnosno 0-24 recepcije, videouređaja*;

- Kontrola pristupa

KRIŠTO TURIZAM osigurava da nema neovlaštene upotrebe sustava i to putem: *(sigurne) lozinke, dvostruka provjera identiteta*;

- Kontrola upotrebe

KRIŠTO TURIZAM osigurava da nema neovlaštenog čitanja, kopiranja, izmjene ili uklanjanja unutar sustava, a kontrola se osigurava: *koncept autorizacije ili prikladne kontrole upotrebe, evidencija upotrebe;*

- Kontrola odvajanja

KRIŠTO TURIZAM osigurava odvojenu obradu podataka koji su prikupljeni u različite svrhe;

(ii) Cjelovitost:

- Kontrola prijenosa

KRIŠTO TURIZAM osigurava da nema neovlaštenog čitanja, kopiranja, izmjene ili uklanjanja pri elektroničkom prijenosu ili transferu i to upotrebom: enkripcije*;*

- Kontrola unosa

KRIŠTO TURIZAM utvrđuje ako se unose i kome pripadaju osobni podaci koji se unose u sustav obrade podataka ili ako se oni mijenjaju ili uklanjaju putem: *upravljanja dokumentacijom*;

(iii) Dostupnost i otpornost:

- Provjera dostupnosti

KRIŠTO TURIZAM osigurava provođenje zaštite od slučajnog ili namjernog uništenja ili gubitka osobnih podataka pomoću: *strategija sigurnosnih kopija (online/offline; on-site/off-site).*

(iv) Proces za redovno testiranje, ocjenjivanje i procjenjivanje

- Upravljanje zaštitom podataka;
- Upravljanje odgovorima na povrede (vidi poseban odjeljak);
- Postavke koje su primjerene za zaštitu podataka (čl. 25 (2) GDPR-a).

7. IZVRŠITELJI OBRADE (čl. 28. GDPR).

U sklopu svog poslovanja i pružanja usluga, KRIŠTO TURIZAM surađuje s brojnim poslovnim partnerima, bez koje suradnje ne bi bilo moguće pružati određene usluge (npr. održavanje IT sustava, računovodstvo, itd.).

Navedeni pružatelji usluga su izvršitelji obrade te postupaju prema uputi KRIŠTO TURIZAM koji osigurava pravilnu obradu osobnih podataka. U tu svrhu KRIŠTO TURIZAM ima sklopljene ugovore o obradi osobnih podataka sa svim izvršiteljima obrade. Ugovori su sklopljeni sukladno članku 28. GDPR-a te sadrže sve što je njime propisano.

8. PRIMATELJI I PRIJENOS OSOBNIH PODATAKA (čl. 44. – 50 GDPR)

U pojedinim situacijama, osobni podaci ispitanika KRIŠTO TURIZAM prenose se trećim stranama. GDPR dopušta prijenos osobnih podataka samo ako za taj prijenos postoji valjana pravna osoba.

KRIŠTO TURIZAM osigurava da za svaki pojedini prijenos osobnih podataka postoji valjana pravna osnova, da su primijenjene mjere zaštite osobnih podataka te da je ispitanik o prijenose obavješten. To se posebno odnosi na situacije kada se podaci prenose pružateljima usluga koji se nalaze izvan prostora EU/EEA.

Sigurnost prijenosa i postojanje valjane pravne osnove zajamčeno je, između ostalog, ugovorima između KRIŠTO TURIZAM kao voditelja obrade i pružatelja usluga kao izvršitelja (vidi gore). U situacijama kada se podaci prenose trećim osobama koje nisu izvršitelje obrade (a niti javna ili druga tijela kod kojih postoji zakonska obveza prijenosa podataka), sigurnost osobnih podataka zajamčena je sklapanjem ugovora o povjerljivosti podataka s trećim osobama.

9. POSTUPAK U SLUČAJU POVREDE OSOBNIH PODATAKA (čl. 32. – 35 GDPR)

Povreda osobnih podataka je, kako ju definira GDPR u članku 4. (12), 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.

Uzrok povrede osobnih podataka može biti interni (npr. slanje e-pošte koja sadrži osobne podatke trećim osobama koje ne bi smjele imati pristup tim podacima), te eksterni (npr. smetnje u IT sustavu, hakiranje, virusi,…).

KRIŠTO TURIZAM provodi postupak u svrhu saniranja (potencijalnih) povreda osobnih podataka, a kako bi ispunio zahtjeve koje nameće GDPR u člancima 33. i 34. Svrha postupka u slučaju povrede osobnih podataka je:

- Osiguranje zaštite prava ispitanika i njihovih osobnih podataka;
- Unaprjeđenje usluga i efikasnog upravljanja procesima obrade osobnih podataka koje one uključuju;
- Sprječavanje rizika i štete za podatke do kojih može doći ljudskim djelovanjem ili drugim faktorima;
- Informirati ispitanike i Agenciju za zaštitu osobnih podataka („**AZOP**“).

Postupak u slučaju povrede provodi se prema sljedećoj shemi:

- **Identifikacija povrede i razine rizika**

  Ovaj korak uključuje procjenu različitih faktora, kao što su vrsta povrede, priroda i opseg povrede, osjetljivost osobnih podataka o kojima je riječ, ozbiljnost (potencijalnih) posljedica i sl.;

- **Identifikacija i provođenje odgovarajućih tehničkih i organizacijskih mjera za efikasan pristup povredi i njenom saniranju;**
- **Dokumentacija svih povreda osobnih podataka, uključujući svih činjenica povrede, učinaka/posljedice povrede i usvojenih i provedenih sigurnosnih mjera;**
- **Izvješćivanje AZOP-a o povredi (bez nepotrebnog odgađanja i, kada je to moguće, unutar 72 sata od saznanja za povredu);**
- **Izvješćivanje ispitanika o povredi njegovih osobnih podataka.**

KRIŠTO TURIZAM osigurava da je ispitanik obavješten o povredi njegovih osobnih podataka bez nepotrebnog odgađanja. KRIŠTO TURIZAM će ispitanika, kada je to moguće, obavijestiti o prirodi, vrsti i opsegu povrede, (potencijalnim) posljedicama povrede te o svim mjerama koje je poduzeo/namjerava poduzeti u svrhu sprječavanja svih negativnih učinaka.

Osoba odgovorna za upravljanje postupkom povrede osobnih podataka je Jopsipa Krišto. Isključivo odgovorna osoba ima pravo i dužnost donositi odluke i provoditi postupak u slučaju povrede osobnih podataka. Svaka osoba koja sazna za (potencijalnu) povredu osobnih podataka dužna je o tome obavijestiti odgovornu osobu.

10. ČUVANJE I BRISANJE OSOBNIH PODATAKA (čl. 5. (1) (e) GDPR)

Rokovi čuvanja osobnih podataka za pojedine svrhe mogu biti propisani zakonom (npr. evidencije o radnicima, porezni i knjigovodstveni podaci) ili određeni interno (npr. čuvanje životopisa potencijalnih kandidata).

U svakom slučaju, KRIŠTO TURIZAM ne čuva osobne podatke duže nego što je to potrebno za ostvarenje svrhe obrade osobnih podataka, osim u sljedećim slučajevima:

- Obrada podataka potrebna je u svrhu provođenja aktualnog ili potencijalnog pravnog postupka/spora, u kojem slučaju KRIŠTO TURIZAM čuva podatke do pravomoćnog okončanja tog postupka/spora, odnosno do isteka zastarnog roka;

- Čuvanje podataka potrebno je u svrhu ispunjenja pravne obveze KRIŠTO TURIZAM-a, u kojem slučaju se podaci čuvaju dok je to potrebno za ispunjenje te obveze.

Bez obzira na rok čuvanja podataka, pristup podacima imaju samo ovlaštene osobe. To se odnosi i na osobne podatke u papirnatom obliku i na digitalne podatke pohranjene unutar IT sustava.

11. PRAVA ISPITANIKA (čl. 16. – 22. GDPR)

KRIŠTO TURIZAM osigurava svojim ispitanicima ostvarenje svih prava propisanih u člancima 16. – 22. GDPR-a.

Upiti i zahtjevi upućeni KRIŠTO TURIZAM-u obrađuju se bez nepotrebnog odgađanja i u skladu sa zakonskim obvezama. Ispitanici se informiraju o svim mjerama koje su poduzete u svrhu ispunjena njihovih zahtjeva za ostvarenjem prava.

Kontakt KRIŠTO TURIZAM-a za ostvarivanje prava: delminivm@hotel-delminivm.hr.

Prava ispitanika ostvaruju se prema niže opisanoj shemi:

Pravo na povlačenje privole	Ispitanici, ukoliko je pravna osnova obrade osobni podataka privola, imaju pravo u bilo kojem trenutku, potpuno besplatno, povući svoju privolu: Povlačenje privole ne utječe na zakonitost obrade koja se temeljila na privoli prije nego li je privola povučena.
Pravo na pristup	Ispitanici imaju pravo dobiti od KRIŠTO TURIZAM potvrdu o obradi njihovih osobnih podataka (uključujući kopiju tih podataka) te pristup informacijama o obradi (npr. svrsi obrade, kategorijama osobnih podataka, primateljima, razdoblju pohrane). U slučajevima prijenosa osobnih podataka izvan EU, ispitanici imaju pravo na informacije o odgovarajućim zaštitnim mjerama.
Pravo na brisanje	Ispitanici imaju pravo ishoditi brisanje osobnih podataka koji se na njih odnose, bez nepotrebnog odgađanja, ako ne postoji zakonit razlog za daljnju obradu (npr. ako podaci više nisu nužni u odnosu na svrhe za koje su obrađivani). Ako takav zakonit razlog ipak postoji, ispitanici će o tome biti detaljno informirani u sklopu odgovora na njihov zahtjev.
Pravo na ispravak	Ispitanici imaju pravo ishoditi ispravak u slučaju da su njihovi osobni podaci netočno navedeni, a koji je KRIŠTO TURIZAM dužan provesti bez nepotrebnog odgađanja. Uzimajući u obzir svrhe obrade, ispitanici imaju pravo dopuniti nepotpune osobne podatke, među ostalim i davanjem dodatne izjave.
Pravo na prigovor	Ako se obrada zasniva na ostvarenju legitimnih interesa KRIŠTO TURIZAM, ispitanici imaju pravo u svakom trenutku uložiti prigovor na takvu obradu u mjeri u kojoj se ona odnosi na njihove osobne podatke. U tom slučaju, KRIŠTO TURIZAM podatke neće dalje obrađivati u svrhu na koju se prigovor odnosi, osim ako dokaže da postoje uvjerljivi legitimni razlozi koji nadilaze interese, prava i slobode ispitanika ili ako je to potrebno radi ostvarivanja ili obrane pravnih zahtjeva KRIŠTO TURIZAM.
Pravo na ograničenje obrade	Ispitanici imaju pravo ishoditi ograničenje obrade njihovih osobnih podataka ako: osporavaju točnost; obrada nije zakonita, a protive se brisanju; traže ih radi postavljanja, ostvarivanja ili obrane pravnih zahtjeva, a KRIŠTO TURIZAMU nisu

	potrebni za obradu; uložili su prigovor vezano za obradu njihovih osobnih podataka i čekaju potvrdu.
Pravo na prenosivost podataka	Ispitanici imaju pravo podatke koji se odnose na njih i koje su pružili KRIŠTO TURIZAM-u, zaprimiti u strukturiranom, uobičajeno upotrebljavanom i strojno čitljivom formatu i prenijeti ih drugom pružatelju usluga. Pritom imaju pravo na izravni prijenos podataka od KRIŠTO TURIZAM drugome voditelju obrade, ako je to tehnički izvedivo.
KONTAKT ZA OSTVARIVANJE PRAVA:	Navedena prava ispitanici mogu ostvariti na sljedeći način: delminivm@hotel-delminivm.hr.
PRITUŽBA NADLEŽNOM TIJELU	Svoja prava ispitanici mogu ostvarivati i putem pritužbe nadzornom tijelu u svezi s obradom njihovih osobnih podataka. U Republici Hrvatskoj, to je **Agencija za zaštitu osobnih podataka** na čijim stranicama se mogu pronaći dodatne informacije o načinu kontaktiranja (**http://azop.hr**).

KRIŠTO TURIZAM d.o.o.
Direktorica:

_____
Josipa Krišto