azop
Agencija za zaštitu osobnih podataka

Sufinancira
Europska unija

ARC
GDPR AWARENESS RAISING CAMPAIGN FOR SMEs

**Online radionica**

https://arc-rec-project.eu/

**5.7.2023.**

# „Zaštita osobnih podataka i usklađivanje s GDPR-om u turizmu”

Croatian Personal Data Protection Agency
azop
Agencija za zaštitu osobnih podataka

GPDP | GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

foi

UNIVERSITÀ DEGLI STUDI FIRENZE

VUB VRIJE UNIVERSITEIT BRUSSEL

# ZAŠTO NAM TREBA GDPR I NA KOGA SE PRIMJENJUJE?

Opća uredba o zaštiti podataka: https://eur-lex.europa.eu/legal-content/HR/TXT/HTML/?uri=CELEX:02016R0679-20160504

Zakon o provedbi Opće uredbe o zaštiti podataka: https://narodne-novine.nn.hr/clanci/sluzbeni/2018_05_42_805.html

- ✓ **Ciljevi: zaštititi osobne podatke fizičkih osoba, pružiti kontrolu građanima nad njihovim osobnim podacima te stvoriti visoku i ujednačenu razinu zaštite osobnih podataka u Europskoj uniji**

- ✓ **Olakšati poduzećima poslovanje na jedinstvenom digitalnom tržištu te olakšati prekogranični protok osobnih podataka i korištenje usluga informacijskog društva**

- ✓ Sve organizacije u Republici Hrvatskoj (mikro, mala, srednja, velika poduzeća, obrti, društva, tvrtke, tijela javne vlasti, državna tijela, udruge, nevladine organizacije, fizičke osobe itd.) koje obrađuju osobne podatke građana pojedinaca dužne su poštovati odredbe GDPR-a i Zakona o provedbi Opće uredbe o zaštiti podataka


**Voditelj obrade nije osoba npr. direktor hotela!Izvršitelj obrade nije npr. tajnica/računovotkinja zaposlena u hotelu!**

**Voditelj obrade je hotel, a izvršitelj obrade npr. IT poduzeće kojeg je hotel angažirao za izradu web stranice i održavanje inofrmacijskih sustava, marketinška agencija koju je hotel angažirao za provođenje promotivnih aktivnosti, zaštitarska tvrtka koju je angažirao za održavanje sustava videonadzora itd.**

Voditelj obrade može biti i fizička osoba, npr. iznajmljivač apartmanskog smještaja.

Ispitanici su vaši gosti, klijenti, vaši zaposlenici dakle osobe čije osobne podatke obrađujete.

Postoje situacije kad voditelj obrade **(npr. hotel) određuje kako i zašto će se osobni podaci obrađivati zajedno s drugim voditeljem obrade (npr. online platformom za oglašavanje). U toj situaciji su hotel i online platforma za oglašavanje zajednički voditelji obrade.**

azop
Agencija za zaštitu osobnih podataka

Sufinancira
Europska unija

ARC
GDPR AWARENESS RAISING CAMPAIGN FOR SMEs

# 10 KLJUČNIH KORAKA ZA USKLAĐIVANJE S GDPR-om

1. NAPRAVITI ANALIZU OSOBNIH PODATAKA KOJE OBRAĐUJETE
2. PRONAĆI ODGOVARAJUĆU PRAVNU OSNOVU ZA OBRADU OSOBNIH PODATAKA
3. POŠTOVATI NAČELA OBRADE OSOBNIH PODATAKA
4. PODUZETI ODGOVARAJUĆE TEHNIČKE I ORGANIZACIJSKE MJERE ZA ZAŠTITU OSOBNIH PODATAKA
5. POŠTOVATI PRAVA ISPITANIKA (OSOBA ČIJE OSOBNE PODATKE OBRAĐUJETE) I OMOGUĆITI IM DA OSTVARE SVOJA PRAVA
6. OSIGURATI MINIMUM DOKUMENTACIJE POTREBNE ZA DOKAZIVANJE USKLAĐENOSTI S GDPR-om
7. INFORMIRATI POJEDINCE O OBRADI NJIHOVIH OSOBNIH PODATAKA
8. VODITI EVIDENCIJE AKTIVNOSTI OBRADE (AKO JE PRIMJENJIVO)
9. IMENOVATI SLUŽBENIKA ZA ZAŠTITU PODATAKA (AKO JE PRIMJENJIVO)
10. PROVESTI PROCJENU UČINKA NA ZAŠTITU PODATAKA (AKO JE PRIMJENJIVO)

# VILLA ANAMARIA & IVA

EN HR IT

O NAMA SOBE REZERVACIJE ORGANIZACIJA EVENATA PONUDE

Sadržaji Rezervacije Politika privatnosti Kolačići Kontakti Newsletter Blog

SOCIAL MEDIA

## (PRIMJER USKLAĐIVANJA S GDPR-om IZ PRAKSE : VILLA ANAMARIA&IVA)


✓ **Prvo je potrebno utvrditi čije i koje osobne podatke prikupljate/čuvate, gdje se nalaze i zašto vam trebaju**

- **Villa ANAMARIA&IVA** je hotel s 50 soba, nalazi se u Istri, radi tijekom cijele godine, osim usluge smještaja, pruža i usluge organizacije evenata (rođendani, kongresi, vjenčanja i sl.), gosti dolaze uglavnom iz EU, ali iz ostalih zemalja izvan EU, ima 10 zaposlenika
- **Hotel prikuplja osobne podatke gostiju** (ime, prezime, broj identifikacijske isprave, spol, prebivalište, datum rođenja, državljanstvo **u svrhu prijave u E-visitor**, **e-mail adresu u svrhu ostvarivanja komunikacije s gostom i promotivne svrhe**. Osobni podaci unose se u sustav E-visitor, hotelsku evidenciju gostiju i čuvaju se u digitalnom obliku.
- **Hotel obrađuje osobne podatke zaposlenika/kandidata za posao** u svrhu provedbe natječaja za posao, obračuna plaća, prijave na HZMO,HZZO te zbog poštivanja zakonskih i podzakonskih propisa o radu i računovodstvu. Osobni podaci zaposlenika čuvaju se u digitalnom i papirnatom obliku (dosje zaposlenika koji sadrži domovnicu, doznake o bolovanjima, diplome, životopise, broj tekućeg računa i dr).

- **Hotel objavljuje komentare i slike gostiju na web stranici i društvenim mrežama u svrhu promocije svojih usluga** (hotel je zajednički voditelj obrade s Instagramom, Yotubeom i Metom (FB).
- **Šalje gostima newslettere** (ime, prezime, e-mail adresa), hotel koristi software za slanje newslettera, pohrana u osobnih podataka u digitalnom obliku
- Hotel pruža usluge organizacije evenata. **Fizičke i pravne osobe koje organiziraju evente dostavljaju hotelu popis gostiju** (imena i prezimena)
- **Hotel prikuplja osobne podatke putem videonadzornog sustava** (angažirana zaštitarska tvrtka, pohrana osobnih podataka u digitalnom obliku)
- **Hotel obrađuje osobne podatke posjetitelja svoje web stranice putem kolačića, između ostalog, i u marketinške svrhe**
- Putem **web forme na web stranici hotela, hotel prikuplja podatke o gostima koji rezerviraju smještaj** (ime, prezime, datum dolaska, datum odlaska, spol)
- Hotel iz primjera za obradu financijskih podataka (**broj kartice, CVV kreditne kartice**) koristi sigurni **sustav za online autorizaciju kreditnih kartica u realnom vremenu**. Tvrtka koja pruža usluge obrade plaćanja je izvršitelj obrade.

# 1 NAPRAVITI ANALIZU OSOBNIH PODATAKA KOJE OBRAĐUJETE

## (PRIMJER USKLAĐIVANJA S GDPR-om IZ PRAKSE : VILLA ANAMARIA&IVA)

- Hotel koristi usluge **računovodstvenog servisa za obračun plaća** (izvršitelja obrade)
- **Hotel se oglašava na Booking.com –u,** preko kojeg gosti mogu izvršiti rezervaciju smještaja i platiti uslugu smještaja (Booking. com i hotel su zajednički voditelji obrade)
- **Hotel se oglašava na platformama za oglašavanje**, gdje je moguće kupiti i platiti ponudu (oglašavačka platforma i hotel su zajednički voditelji obrade)

**UKRATKO:** Hotel prikuplja **direktno od pojedinaca (ispitanika)** sljedeće vrste osobnih podataka: identifikacijske podatke (ime i prezime, spol, način oslovljavanja, datum rođenja, broj osobne iskaznice, broj putovnice, adresu i druge osobne podatke koje je sukladno zakonskog obvezi potrebno unijeti u sustav E-visitor), kontakt podatke (e-mail adresa, broj telefona), financijske podatke (brojevi kreditnih kartica), podatke o transakcijama (konzumacije hrane i pića, welness usluge tijekom boravka u hotelu), podaci o zdravlju (alergije na hranu), tehnički podaci (IP adresa, lokacija, vrsta preglednika i operativni sustav), podaci o preferencijama (preferirani tip smještaja, hrane, zabavnih sadržaja, interesi)

- **Hotel prikuplja osobne podatke pojedinaca (ispitanika) direktno od pojedinca i indirektno**, od platforma za oglašavanje i pružatelja usluga plaćanja, od drugih pojedinaca koji umjesto gosta izvrše rezervaciju smještaja i od fizičkih i pravnih osoba koje organiziraju događanja u hotelu

## Osnovna pitanja na koja biste trebali odgovoriti su:

1) U koju svrhu prikupljate osobne podatke? **Rezervacije smještaja, pružanja i naplate usluga, promotivne svrhe, postupanja u skladu s pravnim obvezama, poboljšavanja i unapređenja usluga, izvršavanje ugovora, personalizacija usluga, zaštita sigurnosti ljudi i imovine, održavanje sigurnosti IT sustava).**

2) Jesu li vam ti podaci neophodni za poslovanje? **DA, svi prethodno navedeni podaci su Hotelu neophodni za poslovanje.**

3) Koji je pravni temelj za obradu osobnih podataka**? Pravna obveza, ugovor, legitimni interes, privola.**

4) **Gdje se osobni podaci nalaze?** U informacijskom sustavu hotela (bazi podataka) i u papirnatom obliku, spremljeno u zaključani ormarić u uredu administrativne tajnice u hotelu.

5) Tko ima pristup osobnim podacima? **Pristup imaju samo ovlaštene osobe**: direktor hotela, recepcioneri i administrativna tajnica (službenik za zaštitu podataka). S izvršiteljima obrade su sklopljeni ugovori iz članka 28. Opće uredbe o zaštiti podataka.

6) Koliko se dugo osobni podaci čuvaju? **Onoliko koliko propisuju zakonski propisi ili onoliko koliko je potrebno da se ispuni svrha. U slučaju legitimnog interesa ispitanik se ima pravo usprotiviti obradi, u tom slučaju osobne podatke brišemo. U slučaju da ispitanik povuče privolu, tad prestajemo s obradom i brišemo osobne podatke.**

7) **Prosljeđujete li osobne podatke trećim stranama?** Da, pružateljima plaćanja usluga, pružateljima IT usluga, zaštitarskoj tvrtki, e-Visitoru, u slučaju zaposlenika računovodstvenom servisu, HZMO-u, HZZO-u, Poreznoj upravi.

**8) Koji je izvor osobnih podataka (npr. pojedinac, treće strane, javno dostupni izvori)?**

Izvor je većinom ispitanik, ali i treće strane (druge osobe koje izvrše rezervaciju umjesto ispitanika, oglašavačke platforme i servisi za naplatu usluga).

**9) Jesu li podaci adekvatno zaštićeni?** Da, poduzete su adekvatne tehničke mjere (korištenje sigurnih lozinki, svaki zaposlenik koristi svoju sigurnu lozinku i username za pristup osobnim podacima, antivirusna zaštita, enkripcija, osobni podaci su osigurani od neovlaštenog kopiranja, izmjene i brisanja, SSL protokol i organizacijske mjere (pravilnici o obradi osobnih podataka, politika privatnosti, izjave o povjerljivosti, redovita edukacija zaposlenika o zaštiti podataka, službenik za zaštitu podataka, evidencije aktivnosti obrade) .

**10) Što se događa s osobnim podacima nakon isteka svrhe za koju su prikupljeni?** Podaci se anonimiziraju ili brišu.

# 2 PRONAĆI ODGOVARAJUĆU PRAVNU OSNOVU ZA OBRADU OSOBNIH PODATAKA


- ✓ **ZAKONSKA OBVEZA**
- ✓ **UGOVOR**
- ✓ **LEGITIMNI INTERES**
- ✓ **PRIVOLA**

- ✓ **Članak 6 GDPR-a**

- ✓ **PRIVOLA JE SAMO JEDAN OD 6 PRAVNIH TEMELJA I AKO IMATE DRUGI PRAVNI TEMELJ NE TREBA VAM PRIVOLA!!!**

- ✓ **Npr. privola ne treba za prijaviti novog zaposlenika na HZMO, privola vam ne treba za unos osobnih podataka u e-Visitor, privola vam ne treba za videonadzor hodnika u hotelu, recepcije i sl.**

## PRIMJER: ZAKONSKE OBVEZE

**Ključno je da ste dobro upoznati s tzv. strukovnim propisima koji uređuju djelatnost kojom se bavite u kojima se vrlo često nalaze odredbe koje reguliraju obradu osobnih podataka.**

- Propisi iz turizma: https://mint.gov.hr/pristup-informacijama/propisi/propisi-iz-turizma/107
- Propisi iz područja radnih odnosa, računovodstveni propisi
- Npr. sukladno Pravilniku o sadržaju i načinu vođenja evidencije o radnicima poslodavac ima pravo i dužnost prikupljanje sljedećih podataka o radnicima i te podatke čuvati trajno:
- ime i prezime, osobni identifikacijski broj, spol, dan,mjesec i godinu rođenja, državljanstvo, prebivalište,odnosno boravište, dozvolu za boravak i rad ili potvrdu o prijavi rada,ako ih je strani radnik obvezan imati,stručno obrazovanje te posebne ispite i tečajeve koji su uvjet za obavljanje posla (uključujući licence, certifikate i slično)
- sukladno čl.10 Zakona o računovodstvu NN 78/15, 134/15, 120/16, 116/18, 42/20, 47/20, 114/22, isplatne liste i analitička evidencija o plaćama za koje se plaćaju obvezni doprinosi čuvaju se trajno
- Sukladno Pravilniku o sustavu e-Visitor propisuje da je pružatelj usluge smještaja u ugostiteljskom objektu registriranom za pružanje usluga smještaja da je dužan prikupiti i u jedinstveni sustav prijave i odjave turista eVisitor unijeti sljedeće osobne podatke osobe koja koristi uslugu smještaja (gost/turist): prezime i ime, mjesto, država i datum rođenja, državljanstvo, vrsta i broj isprave o identitetu, prebivalište (boravište) i adresa, datum i vrijeme dolaska i odlaska iz objeka, spol, temelj za oslobođenje od plaćanja boravišne pristojbe odnosno za umanjenje plaćanja boravišne pristojbe.

# PRIMJER: TEST RAZMJERNOSTI (DOKAZIVANJE LEGITIMNOG INTERESA), https://arc-rec-project.eu/wp-content/uploads/2022/01/primjer-Test-razmjernosti-.docx

## TEST RAZMJERNOSTI

*Primjer: Hotel Villa ANAMARIA&IVA d.o.o. **(voditelj obrade) bave se pružanjem usluga smještaja i organizacijom događanja**. U svrhu prodaje svojih usluga i smještaja, voditelj obrade želi uspostaviti novi marketinški kanal, koji bi obuhvatio dosadašnje goste/korisnike usluga. Obrada bi se sastojala u slanju newslettera s ponudom usluga na e-mail adrese ispitanika čije je osobne podatke hotel prikupio prilikom boravka gostiju u hotelu i/ili korištenjem nekih od usluga koje hotel pruža.*

### KORAK 1: POSTOJI LI LEGITIMNI INTERES?

U uvodnoj izjavi 47. GDPR-a, propisano je da se može smatrati da 'postoji legitiman interes kod obrade osobnih podataka za potrebe izravnog marketinga'.

Hotel namjerava korisititi osobne podatke (e-mail adrese) gostiju hotela/korisnika svojih usluga s ciljem slanja ponuda usluga koje hotel nudi odnosno hotel namjerava obrađivati osobne podatke za potrebe direktnog marketinga, slijedom čega se može smatrati da ima legitiman interes za obradu dosadašnjih gostiju/klijenata s kojima već ima prethodno uspostavljen poslovni odnos te su isti upoznati s takvom obradom i svojim pravima putem politike privatnosti.

### KORAK 2: JE LI OBRADA NUŽNA ZA POSTIZANJE SVRHE U KOJU SE OBRAĐUJU OSOBNI PODACI?

Svrha aktivnosti obrade podataka gostiju je slanje newslettera s ponudama za usluge,. Hotelu je nužna ovakva obrada osobnih podataka kako bi ostvario kontakt s potencijalnim gostima svojih usluga, prezentirao im svoje usluge koje bi mu mogle biti od interesa s obzirom da je već boravio u hotelu/koristio usluge koje hotel nudi. Hotelu je ovo najučinkovitija i financijski najisplativija metoda, a istodobno najmanje invanzivna metoda, kako bi ostvario kontakt s svojom ciljanom publikom koja je zainteresirana za njegove usluge.

### KORAK 3: PREVLADAVAJU LI PRAVA I SLOBODEGOSTIJU NAD LEGITIMNIM INTERESOM VODITELJA OBRADE?

Voditelj obrade smatra kako gosti koji su boravili u njihovom hotelu i korisnici njihovih usluga mogu razumno očekivati da će ih hotel kontaktirati, ponuditi im svoje usluge odnosno koristiti njihovu e-mail adresu u marketinške svrhe. S tim u vezi, hotel smatra kako legitimni interes voditelja obrade prevladava nad interesom za zaštitu osobnih podaaka pojedinaca koje će kontaktirati.

### 4. KORAK: ZAŠTITNE MJERE

Hotel je uspostavio zaštitne mjere kako bi ograničio neprimjereni učinak obrade podataka na prava vezano za zaštitu podataka pojedinaca. Prvenstveno, omogućeno je izjavljivanje prigovora na obradu podataka u marketinške svrhe te gosti/klijenti imaju mogućnost odjave iz newsletter baze. Ako se pojedinac odluči odjaviti iz baze, njegovi osobni podaci se brišu s liste za newsletter i više neće zaprimati newslettere.

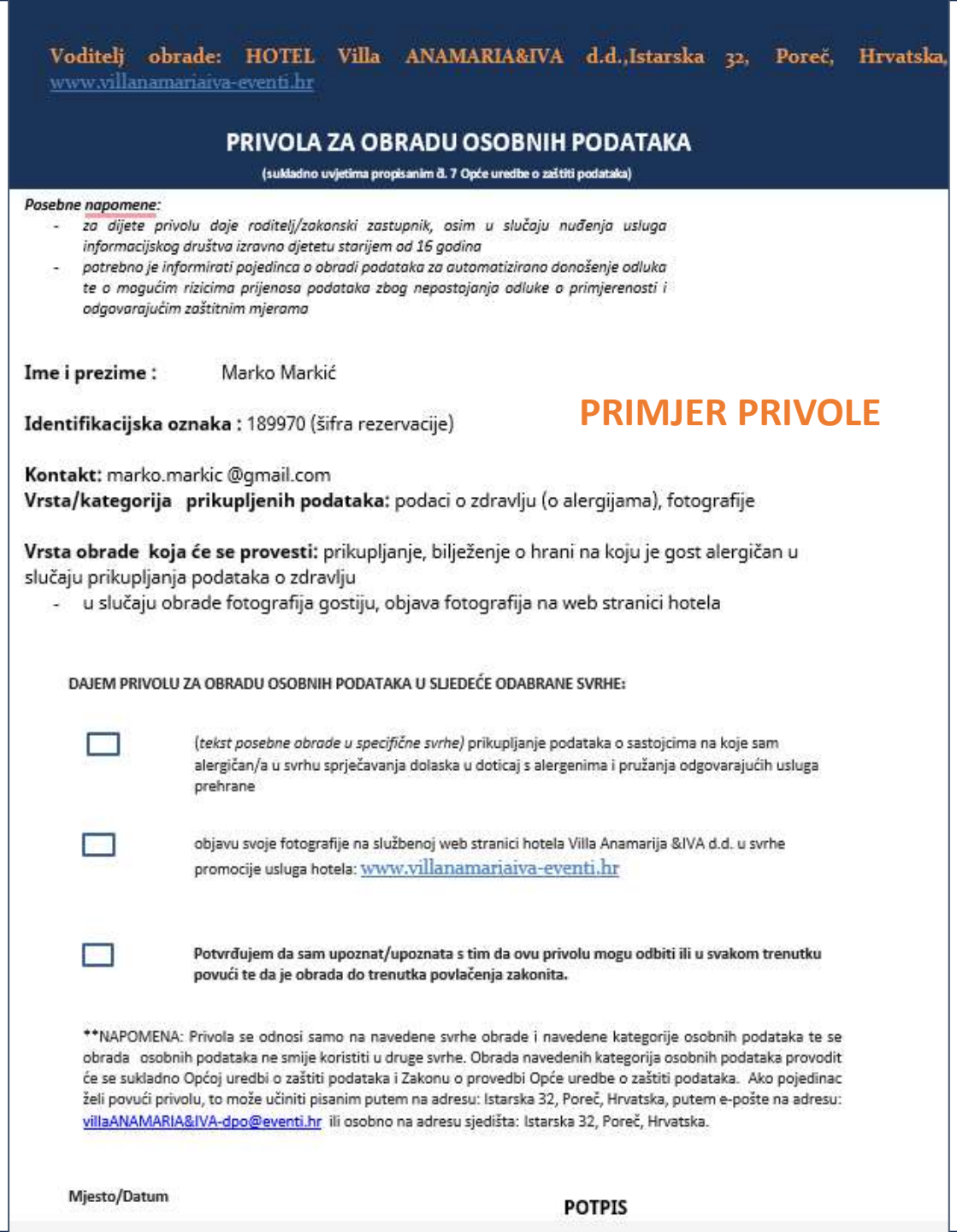
Također, provodeći načelo smanjenja (minimizacije) podataka ne pohranjuju se dodatne informacije o gostu osim e-mail adrese.

### 5. KORAK: TRANSPARENTNOST

Voditelj obrade (hotel) opisao je predmetnu obradu u politici privatnosti koja je objavljena na njegovoj web stranici, a dostupna je na recepciji hotela te u sobama. Recepcionari u hotelu goste/korisnike usluga informiraju da će se njihove e-mail adrese koristiti u svrhe direktnog marketinga te ih informiraju da se mogu odjaviti na vrlo jednostavan način s liste primatelja takvog sadržaja.

### 6. KORAK: PRAVO NA PRIGOVOR

Hotel je omogućio izjavljivanje prigovora na obradu podataka u marketinške svrhe i to na način da je pojedincima ponuđena opcija odjave iz newsletter baze. Postupak odjave iz liste primatelja je vrlo jednostavan, u tijelu e-maila nalazi se opcija „ne želim više primati ove



Voditelj obrade: HOTEL Villa ANAMARIA&IVA d.d.,Istarska 32, Poreč, Hrvatska, www.villanamariaiva-eventi.hr

**PRIVOLA ZA OBRADU OSOBNIH PODATAKA**

(sukladno uvjetima propisanim čl. 7 Opće uredbe o zaštiti podataka)

*Posebne napomene:*

- *za dijete privolu daje roditelj/zakonski zastupnik, osim u slučaju nuđenja usluga informacijskog društva izravno djetetu starijem od 16 godina*
- *potrebno je informirati pojedinca o obradi podataka za automatizirano donošenje odluka te o mogućim rizicima prijenosa podataka zbog nepostojanja odluke o primjerenosti i odgovarajućim zaštitnim mjerama*

**Ime i prezime :** Marko Markić

**Identifikacijska oznaka :** 189970 (šifra rezervacije)

**Kontakt:** marko.markic @gmail.com
**Vrsta/kategorija prikupljenih podataka:** podaci o zdravlju (o alergijama), fotografije

**Vrsta obrade koja će se provesti:** prikupljanje, bilježenje o hrani na koju je gost alergičan u slučaju prikupljanja podataka o zdravlju

- u slučaju obrade fotografija gostiju, objava fotografija na web stranici hotela

**DAJEM PRIVOLU ZA OBRADU OSOBNIH PODATAKA U SLJEDEĆE ODABRANE SVRHE:**

☐ *(tekst posebne obrade u specifične svrhe)* prikupljanje podataka o sastojcima na koje sam alergičan/a u svrhu sprječavanja dolaska u doticaj s alergenima i pružanja odgovarajućih usluga prehrane

☐ objavu svoje fotografije na službenoj web stranici hotela Villa Anamarija &IVA d.d. u svrhe promocije usluga hotela: www.villanamariaiva-eventi.hr

☐ **Potvrđujem da sam upoznat/upoznata s tim da ovu privolu mogu odbiti ili u svakom trenutku povući te da je obrada do trenutka povlačenja zakonita.**

**NAPOMENA: Privola se odnosi samo na navedene svrhe obrade i navedene kategorije osobnih podataka te se obrada osobnih podataka ne smije koristiti u druge svrhe. Obrada navedenih kategorija osobnih podataka provodit će se sukladno Općoj uredbi o zaštiti podataka i Zakonu o provedbi Opće uredbe o zaštiti podataka. Ako pojedinac želi povući privolu, to može učiniti pisanim putem na adresu: Istarska 32, Poreč, Hrvatska, putem e-pošte na adresu: villaANAMARIA&IVA-dpo@eventi.hr ili osobno na adresu sjedišta: Istarska 32, Poreč, Hrvatska.

**Mjesto/Datum** **POTPIS**

**PRIMJER PRIVOLE**

https://arc-rec-project.eu/wp-content/uploads/2022/01/Obrazac-privole.docx

Kad se mora dobiti **privola** za obradu osobnih podataka, da bi ta privola bila valjana, nekoliko sljedećih uvjeta mora biti zadovoljeno:

- mora biti **dobrovoljno dana;**
- mora biti **informirana;**
- mora biti dana za **specifičnu svrhu;**
- svi razlozi za obradu moraju biti jasno navedeni;
- **izričita** je i dana pozitivnim činom (primjer: elektronički okvir za označavanje koji pojedinac mora izričito označiti na internetu ili potpis na obrascu);
- **Upotrebljava jasan i jednostavan jezik** te je jasno vidljiva;
- moguće je i **povući privolu** i ta činjenica je objašnjena

Da bi privola bila **dobrovoljna**, pojedinac mora imati slobodan izbor i mora moći odbiti dati ili povući privolu, a da zbog toga ne trpi štetu. Npr. tražite gosta privolu da fotografirate njegovu osobnu iskaznicu. Što u slučaju ako to odbije, odbit ćete mu pružiti uslugu? Takva privola ne udovoljava zahtjevima iz GDPR-a.

**Članak 7. GDPR-a**

PRIMJER DOBRE PRAKSE

Ugovor: 4436 MONUG 1 2022

Broj rezervacije: 75895

Zagreb, 27.12.2022

Za: Toskana, San Gimignano, Siena i Firenza - Nova godina, 4 dana premium

**DATUM BORAVKA**

29.12.2022 - 01.01.2023

**VRSTA USLUGE**

Aranžman inozemni (CIJENA ARANŽMANA UKLJUČUJE: OSNOVNA cijena - prijevoz turističkim autobusom prema programu putovanja 3 noćenja s buffet doručkom u hotelu 3* u dvokrevetnim sobama tuš/WC/TV u pokrajini Pistoia (Montecatini terme ili slično, regija Toskana) razglede prema programu voditelja putovanja na hrvatskom jeziku jamčevno osiguranje, troškove organizacije i prodaje) (x2)

Prvi obrok: Zadnji obrok:

| R. br. | Korisnik usluge | Dob |
|---|---|---|
| 1. | Ivan Ivić | 29.03.1985 |
| 2. | Iva Ivić | 22.01.1980 |

PUTNO OSIGURANJE

| | |
|---|---|
| Zdravstveno osiguranje | - |
| Osiguranje od nezgode | - |
| Osiguranje prtljage | - |
| Osiguranje otkaza putovanja | - |

| OBRAČUN ARANŽMANA | | UPLATE | |
|---|---|---|---|
| Aranžman inozemni | 3.198,00 | Potvrda o uplati 5666 MONPOU 1 2022 | 3.198,00 |
| **UKUPNO** | 3.198,00 KN | **UKUPNO** | 3.198,00 KN |

**Ukupno EUR (1 EUR = 7.53450) 424,45 EUR**

UGOVARATELJ PUTOVANJA: Mladinić Anamarija, 095 818 9834, anamarija.mladinic@azop.hr

POTPIS I PEČAT

SUGLASAN/A S UVJETIMA ARANŽMANA I OPĆIM UVJETIMA PUTOVANJA

**OSOBNI PODACI KOJE PRIKUPLJATE NA TEMELJU UGOVORNE OBVEZE TREBAJU BITI NUŽNI! PRIKUPLJANJE PRESLIKA DOKUMENATA, OIB-OVA I SL. SMATRA SE PREKOMJERNIM I NIJE U SKLADU S GDPR-OM!**

# 3 POŠTOVATI NAČELA OBRADE OSOBNIH PODATAKA

## Članak 5. GDPR-a utvrđuje sedam ključnih načela povezanih s obradom osobnih podataka:

1) **Zakonitost, poštenost i transparentnost:** obrada osobnih podataka ne smije biti nezakonita, za svaku obradu osobnih podataka potrebno je odrediti pravnu osnovu, svaka obrada osobnih podataka mora biti poštena te ne smije biti štetna ili obmanjujuća za pojedinca, voditelj obrade dužan je pojedinca informirati u koje svrhe prikuplja njegove/njezine osobne podatke, koje osobne podatke prikuplja, s kime ih dijeli i dr. (članci 12, 13. i 14. GDPR-a)

2) **Ograničavanje svrhe:** osobni podaci smiju se obrađivati samo u svrhu za koju su prikupljeni, s iznimkom daljnje obrade u svrhe arhiviranja u javnom interesu, u svrhe znanstvenog ili povijesnog istraživanja ili u statističke svrhe

3) **Smanjenje količine podataka**: organizacije bi trebale prikupljati samo osobne podatke koji su im nužni za poslovanje

# POLITIKA PRIVATNOSTI

- ✓ Svaka organizacija koja obrađuje osobne podatke dužna je pojedince informirati o vrstama osobnih podataka koje prikuplja i njihovim pravima iz GDPR-a, u koju svrhu i po kojoj pravnoj osnovi obrađuje osobne podatke, na koji način i tko koristi osobne podatke te koje mjere zaštite osobnih podataka provodi i dr. (članci 12., 13. i 14. GDPR-a). Svaki voditelj obrade je pritom dužan koristiti jednostavan i lako razumljiv jezik te pružiti osobama navedene informacije u sažetom obliku
- ✓ U tu svrhu potrebno je izraditi politiku privatnosti/izjave o obradi osobnih podataka i objavite je na službenoj web stranici. U slučaju da u svom poslovanju ne koristite web stranicu, politiku privatnosti dužni ste učiniti javno dostupnom na drugi način, npr. na vidljivom mjestu u svojim poslovnim prostorijama (npr. hostel ili iznajmljivač apartmana nema web stranicu, isprintani primjerci politike bit će gostima dostupni na recepciji ili u sobama)

- ✓ PREPORUKA: IMATI POLITIKU PRIVATNOSTI I NA ENGLESKOM JEZIKU (I PO MOGUĆNOSTI DRUGIM STRANIM JEZICIMA)

- ✓ Obrazac politike privatnosti koji možete ispuniti i prilagoditi svojim aktivnostima obrade: https://arc-rec-project.eu/wp-content/uploads/2022/01/politika-privatnosti_obrazac.docx

**POLITIKA PRIVATNOSTI** - PRIMJER: **HOTEL Villa ANAMARIA&IVA**

Ovaj predložak izrađen je kako bi Vam se olakšalo izraditi vlastitu politiku/izjavu/obavijesti o privatnosti. Predmetne korake potrebno je prilagoditi vlastitim obradama osobnih podataka, imajući u vidu činjenicu da se ne radi o dokumentu koji može biti jednak za sve subjekte (voditelje obrade).

## 1. PODACI O VODITELJU OBRADE:

*U ovom dijelu potrebno je informirati pojedince čije osobne podatke obrađujete o:*

- **Villa ANAMARIA&IVA d.d., web adresa:** www.villanamariaiva-eventi.hr
- Istarska 32, Poreč
- **villaANAMARIA&IVA@eventi.hr, br. telefona: 098/345123**

Podaci o službenik za zaštitu podataka: **villaANAMARIA&IVA-dpo@eventi.hr**

## 2. VRSTE OSOBNIH PODATAKA KOJE OBRAĐUJEMO:

*U ovom dijelu potrebno je informirati pojedince čije osobne podatke obrađujete o vrsti osobnih podataka koje ste prikupili/pohranjujete/dostavljate/bilježite/strukturirate ili na drugi način obrađujete*[1].

- Ime i prezime
- Poštanska adresa, adresa e-pošte, telefonski broj
- Datum rođenja, dob pojedinca, državljanstvo, spol, datum i vrijeme odlaska i dolaska u objekt
- broj osobne iskaznice
- IP adresa računala putem kojih su pojedinci posjetili našu web stranicu
- Broj kreditne kartice, CVV kod, datum valjanosti
- Podaci o zdravlju
- Prikaz pojedinca na videonadzornim snimkama i fotografijama
- Podaci o preferencijama (aktivnostima, interesima, prehrambenim zahtjevima i sl.)

[1] obrada znači svaki postupak ili skup postupaka koji se obavljaju na osobnim podacima ili na skupovima osobnih

## 3. SVRHE OBRADE, PRAVNI TEMELJI ZA OBRADU I KOLIKO DUGO ČUVAMO VAŠE PODATKE:

*U ovom dijelu potrebno je prilagoditi odgovor Vašim razlozima obrade, međutim primjera radi stavili smo određene moguće razloge:*

- Temeljem ugovorne obveze, u svrhu izrade rezervacije hotelskog smještaja i predautorizacije kreditne kartice prikupljamo osobne podatke ime, prezime, spol, podatke s kreditne kartice koje čuvamo 30 dana.

- Temeljem ugovorne obveze, u svrhe sklapanja kupoprodajnog ugovora prikupljamo ime, prezime, datum i godina rođenja koje čuvamo 6 mjeseci.

- U slučaju plaćanja naših usluga kreditnom karticom, čuvamo vaše osobne podatke sukladno računovodstvenim propisima 11 godina.

- Radi ispunjavanja pravnih obveza sukladno pravilniku o e-visitoru prikupljamo podatke
- 1. Prezime i ime
- 2. Mjesto, država i datum rođenja
- 3. Državljanstvo
- 4. Vrsta i broj isprave o identitetu
- 5. Prebivalište (boravište) i adresa
- 6. Datum i vrijeme dolaska, odnosno odlaska iz objekta
- 7. Spol
- 8. Temelj za oslobođenje od plaćanja boravišne pristojbe odnosno za umanjenje plaćanja boravišne pristojbe koje čuvamo 10 godina

Predmetni podaci se prikupljaju od strane pružatelja usluga smještaja te se obrađuju od strane pružatelja usluga smještaja u ugostiteljskom objektu, turističkih zajednica i tijela javne vlasti Republike Hrvatske u sljedeće zakonite svrhe:

1. praćenja izvršenja obveze prijave i odjave turista od strane obveznika prijave i odjave (pružatelja usluga smještaja) na temelju Zakona o boravišnoj pristojbi (NN 152/08, 59/09, 97/13, 158/13 i 30/14) i Pravilnika o načinu vođenja popisa turista te o obliku i sadržaju obrasca prijave turista turističkoj zajednici (NN 126/15);

2. evidencije, obračuna i naplate boravišne pristojbe na temelju Zakona o boravišnoj pristojbi (NN 152/08, 59/09, 97/13, 158/13 i 30/14) i Zakona o carinskoj službi (NN 68/13, 30/14 i 115/16);

3. vođenja knjige ili popisa gostiju od strane pružatelja usluga smještaja te praćenja izvršenja navedene obveze od strane inspekcijskih tijela vođenja na temelju Zakona o ugostiteljskoj

sadržaju i načinu vođenja knjige gostiju i popisa gostiju (NN 140/15) i Zakona o Državnom inspektoratu (NN 115/18, 117/21, 67/23)

4. prijave stranaca Ministarstvu unutarnjih poslova te praćenja izvršenja navedene obveze od strane inspekcijskih tijela na temelju Zakona o strancima (NN 133/20, 114/22, 151/22) i Zakona o policijskim poslovima i ovlastima (NN76/09, 92/14, 70/19);

5. vođenja popisa turista od strane turističkih zajednica te korištenje podataka za potrebe praćenja turističkog prometa, istraživanja i turističkih analiza, razvoja turističke ponude, planiranja marketinških aktivnosti i upravljanja posjetiteljimaZakon o turističkoj pristojbi (NN 52/19, 32/20, 42/20) i Zakona o turističkim zajednicama i promicanju hrvatskog turizma (NN 52/19, 42/20);

6. nadzora nad poslovanjem pružatelja usluge smještaja u dijelu koji se odnosi na zakonitost obavljanje djelatnosti odnosno pružanja registriranih usluga te poštivanja poreznih i drugih propisa o javnim davanjima na temelju Zakona o carinskoj službi (NN NN 68/13, 30/14, 115/16, 39/19, 98/19), Općeg poreznog zakona (NN 115/16, 106/18, 121/19, 32/20, 42/20, 114/22) te Zakona o inspekciji cestovnog prometa i cesta (NN 22/14,) 98/19, 114/22). Rok čuvanja podataka je 10 godina.

- U svrhu realizacije radnog odnosa obrađujemo osobne podatke zaposlenika koje čuvamo trajno. Pravni temelji za obradu su izvršenje sklopljenog ugovora o radu, te poštivanje zakonskih obveza kao što su Zakon o radu, Pravilnik o sadržaju i načinu vođenja evidencije o radnicima, Zakon o računovodstvu.

- U svrhe provedbe natječajnog postupka, temeljem ugovora ili kako bi se poduzele radnje prije sklapanja ugovora, prikupljamo osobne podatke kandidata za posao: ime, prezime, životopis, domovnica, dokaz o stručnoj spremi i radnom iskustvu koje čuvamo do ispunjenja svrhe (okončanja postupka zapošljavanja) te ih nakon toga brišemo odnosno uništavamo.

- Na temelju legitimnog interesa i privole, u svrhu promocije svojih usluga javno objavljujemo fotografije s događanja koje organiziramo na društvenim mrežama i web stranici hotela. Fotografije su dostupne trajno, a uklanjaju odnosno brišu na siguran način u slučaju prigovora ispitanika ili povlačenja privole.

- Na temelju legitimnog interesa, u svrhe direktnog marketinga i promocija naših usluga šaljemo gostima newslettere (e-mailove) s našim ponudama i uslugama. Osobni podaci se čuvaju dok se ispitanik ne odjavi s liste primatelja newslettera, a kad se korisnik odjavi s liste primatelja, njegovi osobni podaci se brišu na siguran način, trajno i nepovratno.

- Na temelju legitimnog interesa, a u svrhu registracije sudionika, obrađujemo osobne podatke gostiju koji posjećuju događanja koje treće strane organiziraju u našem

- Na temelju Vaše privole i ako ste nas na to upozorili, prikupljamo podatke o zdravlju (podaci o alergijama, posebnim potrebama) kako bismo spriječili da dođete u doticaj s hranom na koju ste alegrični i kako bismo vam gostu pružili prilagođene usluge u slučaju npr. invaliditeta ili bolesti.

- **Obrada osobnih podataka putem kolačića:** na službenim internetskim stranicama www.villanamariaiva-eventi.hr koriste se tzv. kolačići (cookies) – tekstualne datoteke koje na računalo korisnika smješta internetski poslužitelj (server), putem kojeg davatelj usluge pristupa Internetu (ISP) prikazuje web stranicu.
- kolačići nastaju kada preglednik na uređaju korisnika učita posjećeno mrežno odredište, koje potom šalje podatke pregledniku te izrađuje tekstualnu datoteku (kolačić). Preglednik dohvaća i šalje kolačić na poslužitelj internetske stranice prilikom povratka korisnika na njega.
- na našim stranicma koriste se tehnički kolačići (obavezni kolačići, ne mogu se isključiti) koji su nužni za funkcioniranje Internet mjesta, analitički i marketinški kolaćići u svrhe poboljšanja i promocije naših usluga, poboljšanje učnikovitosti našeg internetskog mjesta te unapređenja poslovanja.
- više o kolačićima saznajte na: www.villanamariaiva.eventi-kolacici.hr

- U svrhu zaštite imovine i ljudi obrađujemo podatke putem videonadzornog sustava temeljem legitimnog interesa, a snimke čuvamo 2 mjeseca.

Na nekima od naših stranica prikazuju se sadržaji vanjskih pružatelja usluga, kao što su YouTube, Facebook, Twitter i Instagram. Također, hotel koristi društvene mreže u svrhu promocije svojih usluga.

Kako biste vidjeli te vanjske sadržaje i pratili naš sadržaj na društvenim mrežama, prvo morate prihvatiti njihove uvjete korištenja. To uključuje njihova pravila o kolačićima, koja mi ne kontroliramo.

Ako ne otvarate taj sadržaj, kolačići treće strane neće biti pohranjeni na vaš uređaj.

Osobne podatke prikupljamo **izravno od pojedinaca** prilikom rezervacija smještaja, prijave i odjave, plaćanja, kad imaju dodatne zahtjeve ili pritužbe, prilikom komunikacije na društvenim mrežama, putem e-maila i kad se pretplate na naš newsletter. Osobne podatke prikupljamo **i indirektno, od drugih osoba** koje izvrše rezervaciju, od pružatelja usluga plaćanja i pružatelja usluga oglašavanja. Također, osobne podatke prikupljamo i od trećih strana (fizičkih i pravnih osoba) koje organiziraju događanja u našem hotelu (lista gostiju).

*Uputa:*

***Rok pohrane osobnih podataka često je propisan strukovnim zakonima koji uređuju Vašu djelatnost. Primjerice, odvjetnici čuvaju spise najmanje deset godina po***

*Ako predmetno nije određeno, vodite se načelom „**ograničenja razdoblja pohrane“ koji određuju da se osobni podaci čuvaju onoliko dugo koliko je potrebno u svrhe radi kojih se osobni podaci obrađuju**, a pohraniti se mogu na dulja razdoblja ako će se osobni podaci obrađivati isključivo u svrhe arhiviranja u javnom interesu, u svrhe znanstvenog ili povijesnog istraživanja ili u statističke svrhe.*

**Koliko je dugo potrebno pohranjivati osobne podatke za svrhe u koje se obrađuju znate Vi sami, a predmetno argumentirajte i uredite internim pravilima. Ako je moguće navedite kriterije kojim ste odredili rok pohrane.*

## 4. SIGURNOST OSOBNIH PODATAKA

<u>Uputa</u>

*Opišite pojedincima (koliko je moguće da ne ugrozite vlastite sigurnosne procese) Vaše mjere tehničke i organizacijske zaštite.*

- Pridržavamo se strogih sigurnosnih postupaka kako bismo umanjili rizik uništenja podataka, neovlaštenog otkrivanja podataka, neovlaštenog pristupa Vašim podacima i drugih povreda.
- Oprema/prostorije na/u koju pohranjujemo osobne podatke smještena je u sigurno okruženje s ograničenim fizičkim pristupom.
- Koristimo vatrozide, snažne lozinke, antivirusne programe i druge mjere za zaštitu osobnih podataka, a hard diskovi na našim računalima su enkriptirani. Svi računalni programi su redovito ažurirani. Redovito radimo sigurnosne kopije podataka koje će nam omogućiti nesmetano funkcioniranje i mogućnost nastavka rada i u slučaju nepredviđenih okolnosti.
- Pristup osobnim podacima imaju samo ovlaštene osobne u našem subjektu, a isto smo regulirali internim aktima. Svaki zaposlenik ima svoj username i password za pristup informacijskim sustavima i bazama podataka.
- Naši računalni programi imaju automatizirani sustav zapisa za evidentiranje pristupa osobnim podacima (tzv. logove) u kojima se evidentiraju podaci o korisnicima koji su pristupali osobnim podacima, vremenu kada su pristupali te što su s tim podacima radili (unosili nove podatke, ažurirali postojeće, brisali podatke, vršili uvid u podatke, pohranjivali podatke izvan programa, ispisivali podatke itd).
- Kad nam osobni podaci više nisu potrebni, anonimiziraju se ili uklanjaju se sigurnim brisanjem medija za pohranu podataka i fizičkim uništavanjem medija za pohranu, a osobni podaci u papirnatom obliku se uništavaju u uređaju za rezanje papira.
- Obvezali smo naše zaposlenike na povjerljivost svih podataka koje saznaju u obavljaju
- Redovito održavamo edukacije našim zaposlenicima kako bi razina svijesti našeg društva o zaštiti osobnih podataka bila zadovoljavajuća.

## 5. PRAVA ISPITANIKA ČIJE OSOBNE PODATKE OBRAĐUJEMO:

**Pravo na pristup osobnim podacima**

Imate pravo na pristup svojim osobnim podacima koje obrađujemo o Vama i možete zatražiti detaljne informacije osobito o njihovoj svrsi obrade, o vrsti/kategorijama osobnih podataka koji se obrađuju uključujući i uvid u svoje osobne podatke, o primateljima ili kategorijama primatelja te o predviđenom razdoblju u kojem će osobni podaci biti pohranjeni. Pristup osobnim podacima može biti ograničen samo u slučajevima propisanim pravom Unije ili našim nacionalnim zakonodavstvom odnosno kada se takvim ograničenjem poštuje bit temeljnih prava i sloboda drugih.

**Pravo na ispravak osobnih podataka**

Imate pravo zatražiti ispravljanje ili dopunjavanje osobnih podataka ako Vaši podaci nisu točni, potpuni i ažurni. Da biste to učinili, pošaljite svoj zahtjev nama kao voditelju obrade pisanim putem, uključujući i elektronički oblik komunikacije.Napominjemo kako je u zahtjevu potrebno specificirati što konkretno nije točno, potpuno ili ažurno i u kojem smislu bi navedeno trebalo ispraviti te dostaviti potrebnu dokumentaciju u prilog svojih navoda.

**Pravo na brisanje**

Imate pravo tražiti brisanje osobnih podataka koje se na Vas odnose ako je ispunjen jedan od sljedećih uvjeta: Vaši osobni podaci više nisu nužni u odnosu na svrhu u koje smo ih prikupili ili obradili; povukli ste privolu na kojoj se obrada temelji u skladu s člankom 6. stavkom 1. točkom (a) ili člankom 9. stavkom 2. točkom (a) i ako ne postoji druga pravna osnova za obradu; uložili ste prigovor na obradu svojih osobnih podataka u skladu sa člankom 21. stavkom 1. Opće uredbe o zaštiti podataka te ako ne postoje naši jači legitimni razlozi za obradu;osobni podaci nezakonito su obrađeni;osobni podaci moraju se brisati radi poštivanja pravne obveze iz prava Unije ili prava države kojoj podliježe voditelj obrade, osobni podaci prikupljeni su u vezi s ponudom usluga informacijskog društva iz članka 8. stavka 1.

<u>Navedena prava nisu primjenjiva u mjeri u kojoj je obrada nužna:</u> radi ostvarivanja prava na slobodu izražavanja i informiranja; radi poštovanja pravne obveze kojom se zahtijeva obrada u pravu Unije ili pravu države članice kojem podliježe voditelj obrade ili za izvršavanje zadaće od javnog interesa ili pri izvršavanju službene ovlasti voditelja obrade; u svrhe arhiviranja u javnom interesu, u svrhe znanstvenog ili povijesnog istraživanja ili u statističke svrhe u skladu s člankom 89. stavkom 1. u mjeri u kojoj je vjerojatno da se pravom iz stavka 1. može

**Pravo na ograničavanje obrade osobnih podataka**

Imate pravo ishoditi ograničenje obrade ako: osporavate njihovu točnost; ako je obrada nezakonita, a protivite se njihovom brisanju; ako voditelj obrade više ne treba osobne podatke ali ste ih zatražili radi postavljanja, ostvarivanja ili obrane pravnih zahtjeva;nako ste uložili prigovor na obradu Vaših osobnih podataka.

**Pravo na prigovor**

Ako se osobni podaci obrađuju na temelju legitimnog interesa ili u svrhe direktnog marketinga možete podnijeti prigovor protiv takve obrade.

**Pravo na prenosivost osobnih podataka**

Imate pravo zaprimiti svoje osobne podatke koje ste prethodno pružili voditelju obrade, u strukturiranom obliku te u uobičajeno upotrebljavanom i strojno čitljivom formatu. Imate 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.

Za ostvarivanje svojih prava možete nam se obratiti pisanim putem ili putem elektroničke pošte koristeći naše kontakt podatke koji su navedeni na sljedećoj poveznici: https://azop.hr/wp-content/uploads/2020/12/ZAHTJEV-ZA-OSTVARIVANJE-PRAVA-ISPITANIKA.docx . Potrebno je ispuniti obrazac te ga dostaviti na e-mail adresu službenika za zaštitu podataka: **villaANAMARIA&IVA@eventi.hr**.

**Također, upućujemo Vas da se za sva pitanja u vezi obrade svojih osobnih podataka obratite na navedenu e-mail adresu. Službenik za zaštitu osobnih podataka odgovorit će na Vaš prigovor/zahtjev/upit u roku od mjesec dana.**

Ukoliko želite povući privolu za davanje svojih osobnih podataka, imate na to pravo u svakom trenutku te isto možete učiniti upućivanjem e-maila na: **villaANAMARIA&IVA@eventi.hr**. **Isto tako možete uputiti prigovor ukoliko se obrada temelji na legitimnom interesu.**

## 6. INFORMACIJE O PRIMATELJIMA[2] PODATAKA/KATEGORIJAMA PRIMATELJA

Vaše osobne podatke prosljeđujemo na korištenje pružateljima informatičko-komunikacijskih rješenja i usluga koji djeluju kao izvršitelji obrade. Vaše osobne podatke dijelimo s tvrtkom za sustav za online autorizaciju kreditnih kartica u realnom vremenu i pružanje usluge obrade plaćanja. S navedenim izvršiteljima obrade sklopili smo ugovore u kojima je detaljno propisano postupanje s osobnim podacima, stoga isti nisu u mogućnosti obrađivati Vaše osobne podatke bez našeg naloga i prosljeđivati ih trećim stranama. Osobne podatke gostiju dijelimo sa sustavom e-Visitor, u skladu s propisima o pružanju usluge ugostiteljskog smještaja te načina vođenja popisa i prijave turista.

Vaše osobne podatke ne prenosimo u treće zemlje i ne izrađujemo profile niti se obrađujemo vaše podatke u svrhu automatiziranog donošenja odluka. Vaše osobne podatke dijelimo s trećim stranama (prosljeđujemo društvenim mrežama i platformama za online oglašavanje) u marketinške svrhe isključivo na temelju vaše privole. Osobne podatke zaposlenika sukladno zakonskim propisima prosljeđujemo HZMO-u, HZZO-u, Poreznoj upravi. Osobne podatke možemo podijeliti i sa sudskim, poreznim, revizorskim i drugim nadležnim tijelima, kada imamo razloga vjerovati da smo na temelju zakona i drugih propisa dužni podijeliti takve podatke (primjerice, na temelju zahtjeva poreznog tijela ili u vezi s očekivanim sudskim sporom).

## 7. OBJASNITE POJEDINCIMA DA IMAJU PRAVO PODNIJETI PRITUŽBU AGENCIJI ZA ZAŠTITU OSOBNIH PODATAKA:

U slučaju da smatrate da Vam je povrijeđeno Vaše pravo na zaštitu podataka te smatrate da se obradom osobnih podataka krše propisi odnosni na zaštitu osobnih možete podnijeti pritužbu Agenciji za zaštitu osobnih podataka kao nadležnom nadzornom tijelu za područje zaštite osobnih podataka: https://azop.hr/zahtjev-za-utvrdivanje-povrede-prava/.

## 8. PROMJENE POLITIKE PRIVATNOSTI

Politiku privatnosti redovito ažuriramo kako bi ista bila točna i ažurna te zadržavamo pravo promjene sadržaja iste ako smatramo da je to nužno. O svim izmjenama i dopunama biti ćete pravovremeno informirani putem naše internetske stranice , u našem objektu te putem newslettera u skladu s načelom transparentnosti.

**4) Točnost:** osobni podaci koji se prikupljaju moraju biti točni, a netočni podaci moraju se ispraviti

**5) Ograničenje pohrane**: osobni podaci smiju se čuvati samo onoliko koliko je potrebno, odnosno onoliko dugo koliko je zakonski propisano

**6) Cjelovitost i povjerljivost**: organizacije su dužne poduzeti sve tehničke i organizacijske mjere kako bi zaštitile osobne podatke od neovlaštene ili nezakonite obrade, od slučajnog gubitka, uništenja ili oštećenja

**7) Pouzdanost**: morate biti u mogućnosti dokazati usklađenost s GDPR-om (primjerice dokumentirane tehničke i organizacijske mjere, politika privatnosti, evidencije aktivnosti obrade, službenik za zaštitu podataka koji udovoljava zahtjevima iz članka 37.-39. GDPR-a).

ARC
GDPR AWARENESS RAISING CAMPAIGN FOR SMEs

# AEPD (Spain) - PS/00499/2022



The Spanish DPA imposed a total fine of €75,000 on an accommodation company for requiring excessive data for guests' check-in and for not providing them with complete information about the processing of their data.

## Contents



## English Summary 

### Facts 

The data subject booked an apartment from Marketing Accomodantion Solutions, the controller, for a period of vacation in Catalonia. To check in, the data subject had to fill in an online form and provide personal data of all guests, including emails, telephone numbers and addresses, as well as photos of both sides of the identity cards of each of them.

The data subject filed a complaint with the Spanish DPA claiming that the data requested was excessive. In response, the controller argued that it was obliged by law to register its guests and to transfer their data to the Catalan police. Not satisfied with the response, the data subject filed a complaint twith the Spanish DPA, which proceeded to investigate the facts.

**AEPD - PS/00499/2022**

| | |
|---|---|
| Authority: | AEPD (Spain) |
| Jurisdiction: | Spain |
| Relevant Law: | Article 5(1)(c) GDPR<br>Article 13 GDPR |
| Type: | Complaint |
| Outcome: | Upheld |
| Started: | 27.10.2021 |
| Decided: | |

**ŠPANJOLSKO NADZORNO TIJELO KAZNILO JE JEDNO PODUZEĆE KOJE IZNAJMLJUJE APARTMANSKI SMJEŠTAJ S 75 000 EUR:**

- ✓ DA BI REZERVIRAO SMJEŠTAJ ZA SEBE I SVOJE PRIJATELJE, GOST KOJI SE PRITUŽIO NADZORNOM TIJELU MORAO JE ISPUNITI ONLINE OBRAZAC S SVOJIM OSOBNIM PODACIMA TE UZ TO PRILOŽITI OBOSTRANE PRESLIKE SVOJE OSOBNE I OSOBNE ISKAZNICE SVOJIH PRIJATELJA

- ✓ ŠPANJOLSKO NADZORNO TIJELO KAZNILO JE IZNAJMLJIVAČA APARTMANA ZBOG:

- **KRŠENJA ČLANKA 5. TOČKA C) (25 000 EUR):**

**Osobni podaci moraju biti:**

(c) **primjereni, relevantni i ograničeni na ono što je nužno u odnosu na svrhe u koje se obrađuju („smanjenje količine podataka”);**

- **KRŠENJA ČLANKA 13. GDPR-a (50 00 EUR) JER ISPITANICI U TRENUTKU PRIKUPLJANJA OSOBNIH PODATAKA NISU BILI U POTPUNOSTI INFORMIRANI O OBRADI SVOJIH OSOBNIH PODATAKA, TOČNIJE NISU BILI INFORMIRANI O TOME TKO JE VODITELJ OBRADE I O KONTAKT PODACIMA VODITELJA OBRADE, KONTAKT PODACIMA SLUŽBENIKA ZA ZAŠTITU PODATKA, PRAVNOM TEMELJU ZA OBRADU OSOBNIH PODATAKA, PRIMATELJIMA I KATEGORIJAMA PRIMATELJA OSOBNIH PODATAKA I RAZDOBLJU ČUVANJA OSOBNIH PODATAKA.**

**1) DAKLE, SMIJEMO LI KOPIRATI OSOBNU ISKAZNICU/PUTOVNICU/DOKUMENTE GOSTIJU KAD STIGNU U NAŠ HOTEL/APARTMANSKI SMJEŠTAJ?**

**NE, TAKVA OBRADA SE SMATRA PREKOMJERNOM I KOPIRANJE OSOBNE ISKAZNICE NIJE NUŽNO** DA BI SE ISPUNILA SVRHA (REZERVACIJA SMJEŠTAJA, UPIS U E-VISITOR), ČAK I U SLUČAJU AKO STE DOBILI PRIVOLU ISPITANIKA. Dovoljno je da goste zatražite osobnu iskaznicu na uvid i s nje prepišete osobne podatke koji su nužni za unos u e-Visitor.

**2) SMIJEMO LI KOPIRATI OSOBNU ISKAZNICU/PUTOVNICU/KREDITNU KARTICU GOSTIJU I TRAŽITI DA NAM ISTO POŠALJU E-MAILOM?**

NE, TAKVA OBRADA SE SMATRA PREKOMJERNOM TE NIJE U SKLADU S **ČLANKOM 5. TOČKOM C)** , ČAK I U SLUČAJU AKO STE DOBILI PRIVOLU ISPITANIKA. DODATNO UKAZUJEMO KAKO JE RAZMJENA OSOBNIH PODATAKA PUTEM ELEKTRONIČKE POŠTE (BEZ PRIMJENE DODATNIH MJERA ZAŠTITE) S ASPEKTA ZAŠTITE OSOBNIH PODATAKA VRLO NESIGURAN NAČIN KOMUNIKACIJE I RAZMJENE PODATAKA IZ RAZLOGA ŠTO ELEKTRONIČKA POŠTA OD POŠILJATELJA DO PRIMATELJA PUTUJE U LAKO ČITLJIVOM OBLIKU I PROLAZI KROZ NIZ TOČAKA U KOMUNIKACIJSKOM KANALU ELEKTRONIČKE POŠTE NAD KOJIMA NITI POŠILJATELJ NITI PRIMATELJ NEMAJU KONTROLU.


## 3) AKO NE SMIJEMO TRAŽITI GOSTE DA NAM ŠALJU PRESLIKE SVOJIH KREDITNIH KARTICA I CVV BROJEVE, KAKO MOŽEMO GARANTIRATI REZERVACIJU?

**MOŽETE KORISTITI PODATKE O KREDITNOJ KARTICI U SVRHU GARANCIJE REZERVACIJE NA NAČIN DA KORISTITE USLUGE POUZDANIH TVRTKI KOJE PRUŽAJU USLUGE ONLINE REZERVACIJE I PLAĆANJA SMJEŠTAJA ODNOSNO PREDAUTORIZACIJE KREDITNIH KARTICA. TAKOĐER AKO IMATE WEB STRANICU, MOŽETE PREDAUTORIZACIJU I REZERVACIJU IZVRŠITI PUTEM WEB FORME NA SVOJOJ WEB STRANICI. KLJUČNO JE DA JE WEB STRANICA IMA SSL CERTIFIKAT, DA JE STRANICA REDOVITO AŽURIRANA, DA SE REDOVITO PROVODI SIGURNOSNO SKENIRANJE STRANICE TE DA JE ZAŠTIĆENA OD HAKERSKIH NAPADA I VIRUSA.**

**4) Suprug i ja vlasnici smo kuće za odmor i iznajmljujemo je kao fizička osoba.**

**Ponekad nismo u mogućnosti dočekati goste, a ponekad i njima bolje odgovara self check-in. Zanima me koje je najispravnije postupanje s osobnim podacima u toj situaciji?**

Ako ih zamolimo da napišu svoje osobne podatke, ne možemo provjeriti točnost istih. Ako ih tražimo sliku osobne, mi smo u prekršaju. Što je najispravnije napraviti?

U ovom slučaju najispravnije je tražiti da vam napišu osobne podatke koji su vam potrebni za unos u e-Visitor. Osobne podatke možete provjeriti kad gosti stignu u kuću za odmor/tijekom boravka u kući za odmor. Slanje preslike/fotografije osobne iskaznice unaprijed putem e-maila smatra se prekomjernom obradom osobnih podataka i nije u skladu s Općom uredbom o zaštiti podataka.

UKOLIKO IZ NEKOG RAZLOGA NIJE MOGUĆE DA UNESETE IMENA GOSTIJU U E-VISITOR NA LICU MJESTA I DA KORISITITE ONLINE SUSTAVE ZA PREDAUTORIZACIJU I REZERVACIJU, U TOM SLUČAJU POSTOJI MOGUĆNOST DA NA TEMELJU PRIVOLE KOJA MORA UDOVOLJAVATI SVIM ZAHJTEVIMA IZ GDPR-a, TRAŽITE GOSTA DA VAM PUTEM E-MAILA POŠALJE SVOJE OSOBNE PODATKE (osobne podatke kao što su ime, prezime, datum rođenja itd. a ne i presliku dokumenata), **ALI SAMO ONE KOJI SU VAM NUŽNI U SVRHU REZERVACIJE SMJEŠTAJA I/ILI UNOSA U E-VISITOR. PREPORUČAMO DA SE OSOBNI PODACI ŠALJU U DATOTECI ZAŠTIĆENOJ LOZINKOM, A LOZINKU UPUTITI PRIMATELJU PUTEM NPR. SMS PORUKE. KAD GOST DOĐE U VAŠ OBJEKT, TAD JE POTREBNO DA GA TRAŽITE UVID U NJEGOVU OSOBNU ISKAZNICU I PROVJERITE TOČNOST OSOBNIH PODATAKA KOJE VAM JE POSLAO E-MAILOM. ONO ŠTO JE KLJUČNO DA SAMO OVLAŠTENE OSOBE IMAJU PRISTUP E-MAILU ODNOSNO OSOBNIM PODACIMA GOSTIJU TE DA SE OSOBNI PODACI NAKON ŠTO JE ISPUNJENA SVRHA RADI KOJE SE PRIKUPLJAJU ODMAH BRIŠU/UNIŠTAVAJU NA SIGURAN NAČIN. U PRAKSI SMO SE SUSRETALI SA SITUACIJAMA GDJE HOTELI/IZNAJMLJIVAČI ZAPRIMAJU NA E-MAIL PRESLIKE OSOBNIH ISKAZNICA/KREDITNIH KARTICA ZAJEDNO S CVV BROJEVIMA. TAKVI E-MAILOVI DOSTUPNI SU NEOGRANIČENOM KRUGU OSOBA, PRIVITCI KOJI SADRŽE PRESLIKE SE PRINTAJU I POTOM STAVLJAJU NA VIDLJIVA MJESTA GDJE SU VRLO LAKO DOSTUPNE SVIMA. NAKON ŠTO VIŠE NISU POTREBNE PRESLIKE SE NE BRIŠU/UNIŠTAVAJU.**

**OVAKVE POSLOVNE PRAKSE VRLO SU RIZIČNE ZA GOSTE KOJE SE IZLAŽE MOGUĆNOSTI ZLOUBORABE NJIHOVIH OSOBNIH PODATAKA I KRAĐE IDENTITETA, A I ZA VODITELJE OBRADE KOJI RISKIRAJU VISOKE NOVČANE KAZNE.**

## 5) Razmjenjujemo osobne podatke gostiju s drugom firmom s kojom organiziramo evente. Smijemo li listu gostiju (imena, prezimena) slati e-mailom?

Pod pretpostavkom da imate pravni temelj za ovakvu razmjenu osobnih podataka (npr. dokumentirani legitimni interes i da su ispitanici s time upoznati, osobne podatke možete razmijenjivati. Kako je razmjena osobnih podataka putem elektroničke pošte (bez primjene dodatnih mjera zaštite) s aspekta zaštite osobnih podataka vrlo nesiguran način komunikacije i razmjene podataka iz razloga što elektronička pošta od pošiljatelja do primatelja putuje u lako čitljivom obliku i prolazi kroz niz točaka u komunikacijskom kanalu elektroničke pošte nad kojima niti pošiljatelj niti primatelj nemaju kontrolu. Stoga za dostavu osobnih podataka (liste gostiju jednog voditelja obrade drugome) preporučamo da sve privitke/datoteke, odnosno popratnu dokumentaciju koja se želi slati putem elektroničke pošte prvo „zapakirate“, odnosno upotrijebiti neki od programa za sažimanje, a koji u sebi ima mogućnosti enkripcije svog sadržaja putem lozinke velike složenosti i algoritma za enkripciju velike složenosti te se tek tako „zapakirane“ i enkriptirane datoteke stavljaju kao privitak u elektroničku poštu (listu gostiju s imenima i prezimenima).

- Sigurna lozinka treba sadržavati velika i mala slova (az, AZ);znamenke (0-9); specijalne znakove ( @ # $% ^ * () _ + | ~ – = `{} []:”; ‘, /?.), najmanje 10 znakova; sigurna lozinka ne bi trebala sadržavati riječi; Sigurna lozinka ne bi trebala sadržavati osobne informacije poput imena, datuma rođenja i sl.

- Lozinku kojom je enkriptiran privitak elektroničke pošte preporučljivo je dostaviti primatelju različitim kanalom od kanala kojim se dostavlja elektronička pošta, tj. nije preporučljivo dostaviti lozinku za dekriptiranje sadržaja privitka čke pošte, jer se onda gubi smisao enkripcije (mogući neželjeni/neovlašteni primatelj poruke potencijalno ima mogućnost uvida u sadržaj enkriptiranog privitka bez ikakvih prepreka), već dostaviti putem npr. SMS poruke, izdiktirati telefonom itd.

## 6) Na recepciji je često gužva i gosti su nervozni ako moraju čekati da prepišemo osobne podatke s iskaznice. Iz tog razloga lakše nam je napraviti presliku osobne ili uzeti od gosta osobnu iskaznicu/putovnicu pa mu je vratiti kad upišemo podatke u e-visitor. Jel to u redu?

**Ne, izrada preslike osobne iskaznice je prekomjerna obrada koja nije nužna. Gostu ne smijete uzeti osobnu iskaznicu, već ju možete samo dobiti na uvid. Postoje ID skeneri koji automatski obrađuju samo one podatke s osobne iskaznice koje je potrebno unijeti u e-Visitor. Potrebno je voditi računa da su takv skeneri/aplikacije usklađeni s GDPR-om.**

**Ubrzajte vaš proces check-ina uz ID skener za hotele**
Registrirajte više gostiju u kraćem vremenu uz Skaner ID koji koristi tehnologiju čitanja za brzo izdvajanje podataka. Jednostavno skenirajte putovnicu ili osobnu iskaznicu kako biste automatski unijeli podatke o gostima u polja za prijavu – više nema ručnog unosa!

Postavite putovnicu u bijeli okvir i kliknite na gumb za snimanje; osobni će dokument biti skeniran.

Podaci o gostima poput imena i prezimena, zemlje podrijetla, datuma rođenja i broja osobnog dokumenta odmah se popunjavaju. Radi zaštite osobnih podataka, osobni podaci s putovnice nisu pohranjeni u sustavu.

# 4 PODUZETI ODGOVARAJUĆE TEHNIČKE I ORGANIZACIJSKE MJERE ZA ZAŠTITU OSOBNIH PODATAKA

Članak 32. GDPR-a

- ✓ Jedna od glavnih obveza prema GDPR-u je osigurati odgovarajuću sigurnost osobnih podataka, uključujući zaštitu od neovlaštenih ili nezakonitih obrada (uključujući krađu, uništavanje, oštećenje i otkrivanje) osobnih podataka. Kako biste zaštitili osobe podatke svojih klijenata/korisnika usluga/zaposlenika (ukratko pojedinaca čijim osobnim podacima raspolažete), **dužni ste provoditi odgovarajuće tehničke i organizacijske mjere.** Na ovaj način svest ćete mogućnost nezakonite obrade osobnih podataka i povreda osobnih podataka na minimum.

- ✓ Neke od **tehničkih mjera za zaštitu osobnih podataka** su pseudonimizacija, enkripcija, korištenje korisničkih imena i snažnih lozinki za pristup računalima i računalnoj opremi, postavljanje adekvatnih programa na računala koji sprječavaju neovlaštene pristupe, redovito izrađivanje sigurnosnih kopija podataka itd. Papirnata dokumentacija koja sadrži osobne podatke trebala bi se nalaziti u zaključanim ormarićima i prostorijama, sefovima ili bi trebala biti zaštićena protuprovalnim sustavom. Također, trebali biste koristiti provjerene/certificirane uređaje, programe i tehničku opremu te redovito nadograđivati operativni sustav računala, mobilnih uređaja i računalnih programa.

**Organizacijske mjere zaštite** odnose se na dokumentirano uređenje u vašoj organizaciji na način da se internim aktima uredi područje zaštite osobnih podataka koje obrađujete, odnosno da se, primjerice, vodi evidencija pristupa osobnim podacima odnosno tzv. logovi o ulascima i aktivnostima korisnika po sustavima, i odredi kojim osobnim podacima zaposlenici imaju pristup prilikom obavljanja svojih poslova.

Neki od takvih internih akata su:

- **Pravilnik o informacijskoj sigurnosti** kojim se, između ostalog, propisuju tehničke mjere zaštite koje se primjenjuju za zaštitu podataka od neovlaštenog pristupa u poslovnom subjektu.
- **Pravilnici kojima se uređuje obrada osobnih podataka:** propisuju tko obrađuje osobne podatke, u koju svrhu, koji je pravni temelj obrade, koji je opseg osobnih podataka u obradi, tko ima pravo pristupa i obrade osobnih podataka, koliko dugo se podaci čuvaju, koje su tehničke mjere zaštite provedene za taj sustav pohrane (bazu podataka) itd.
- **U ugovornim klauzulama unutar ugovora o radu** mogu biti definirani sustavi pohrane koje će zaposlenik obrađivati i koja prava će imati za obradu tih sustava pohrane (baza podataka).
- **Izjavom o povjerljivosti** zaposlenik poslovnog subjekta ili vanjski suradnik daje pisanu izjavu da će osobne podatke obrađivati u skladu sa zakonskim
- **Ugovor o obradi osobnih podataka između voditelja i izvršitelja obrade**

**NAJČEŠĆE DO POVREDE OSOBNIH PODATAKA DOLAZI ZBOG LJUDSKOG FAKTORA ODNOSNO NEZNANJA ZAPOSLENIKA! EDUCIRAJTE SVOJE ZAPOSLENIKE I NA TAJ NAČIN UMANJITE ŠANSE ZA POVREDE OSOBNIH PODATAKA, PHISHING NAPADE, RANSOMWARE NAPADE!**

**Investicija u informacijsku sigurnost više nije nešto što je poželjno, nego je u današnje digitalno doba nužno.**

Saznajte više na: https://arc-rec-project.eu/wp-content/uploads/2021/01/Vodic-za-informacijsku-sigurnost.pdf, https://arc-rec-project.eu/wp-content/uploads/2022/08/ARC-Kratki-vodic-phishing-i-socijalni-inzenjering.pdf, https://arc-rec-project.eu/wp-content/uploads/2022/06/ARC-Sigurnost-podataka.pdf, https://arc-rec-project.eu/wp-content/uploads/2022/06/ARC-Pet-koraka-do-sigurnog-Cloud-okruzenja.pdf , https://arc-rec-project.eu/wp-content/uploads/2022/06/ARC-Smjernice-za-organizacije-koje-angaziraju-pruzatelje-usluga-u-Cloudu.pdf

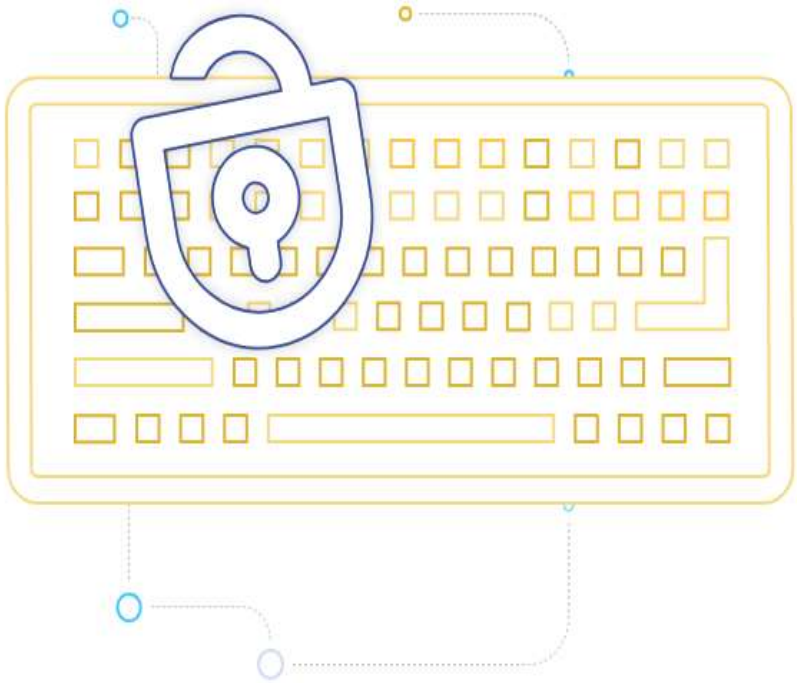
NO MORE RANSOM

# TREBATE LI POMOĆ pri otključavanju vašeg digitalnog života, a ne želite platiti osobama odgovornim za napad?

DA NE

Trenutačno nemamo rješenja za sve tipove ransomware virusa. Provjeravajte ovu stranicu u budućnosti zbog novih ključeva i rješenja koji će naknadno biti dodani.





Ransomware je malware (zlćudni računalni program) koji zaključa vaše računalo i mobilne uređaje i kriptira vaše elektroničke datoteke. Ako se to dogodi, vaši podaci su nedostupni ako ne platite otkupninu.

**Nemate jamstvo da će vam podatci biti dekriptirani, stoga otkupninu nikad ne plaćajte!**

Novi dekriptor za

Poduzeće ima otvoren poslovni račun u jednoj banci. Na e-mail poduzeća pristigla je elektronička pošta s nazivom te banke, a u poruci je pisalo da banka moli ažuriranje nove verzije mobilnog bankarstva. Za to se trebalo prijaviti na link koji se nalazio u elektroničkoj pošti. Ulaskom na link zatražen je korisnički broj za ulaz u mobilno bankarstvo, pin i jednokratna zaporka koja je pristigla SMS porukom s broja banke. Zaposlenica poduzeća je otvorila zlonamjernu poruku, kliknula na poveznicu, unijela tražene podatke i s poslovnog računa poduzeća je nestalo nekoliko tisuća eura.


**ZAŠTO VAM TREBA SSL CERTIFIKAT (HTTPS PROTOKOL)?**

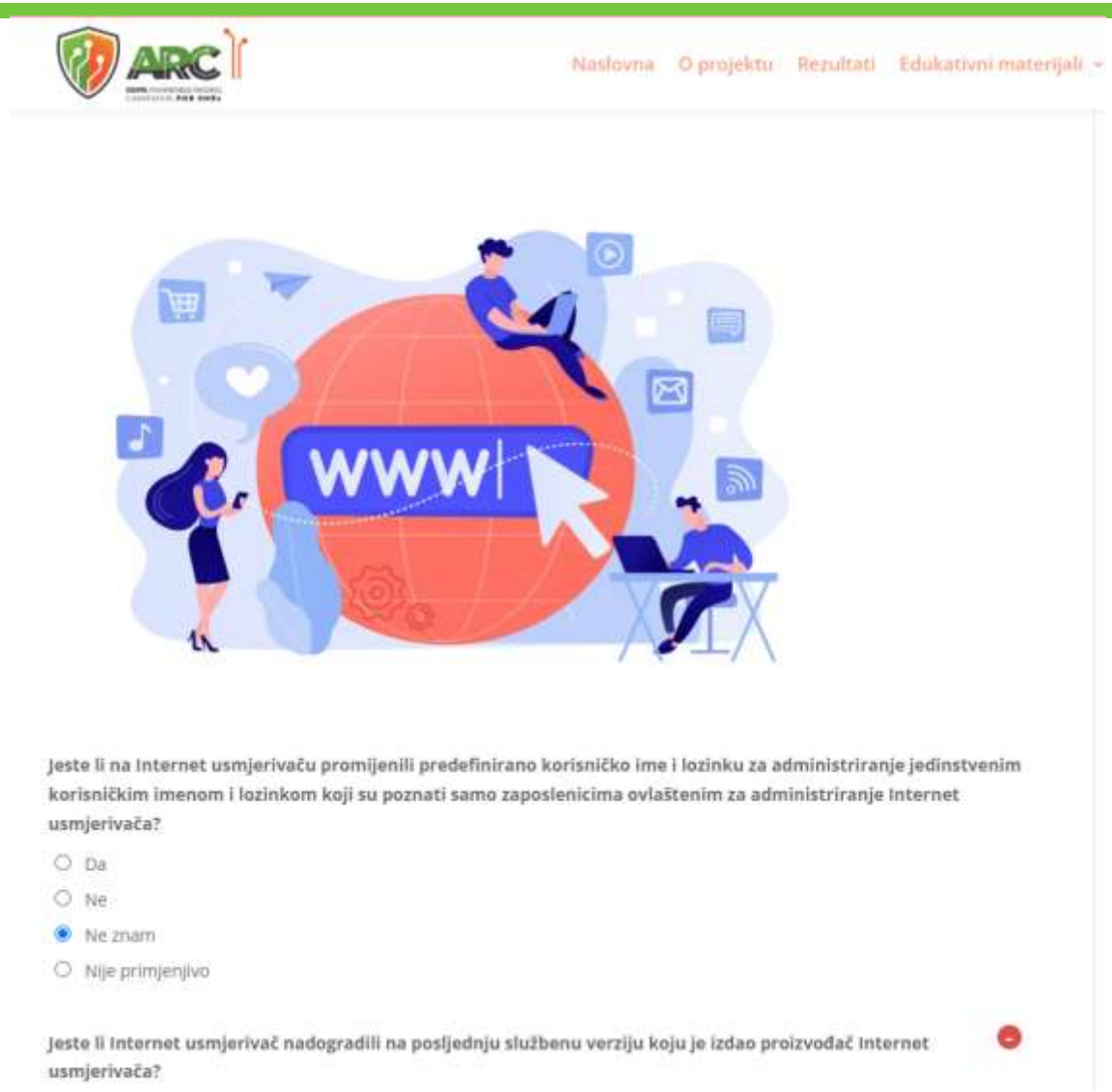
Možda mislite da niste dovoljno zanimljivi da bi bili žrtva hakerskog napada, ali ističemo da se napadi provode putem raznih zlonamjernih softvera (botova) koji automatski prolaze kroz razne web adrese i napadaju nasumično sve. Uz nedostatak SSL protokola, vaši i podaci vaših korisnika mogu vrlo lako biti kompromitirani jer takvi zlonamjerni softveri prvenstveno vrebaju slabo zaštićene stranice.

## BRITANSKO NADZORNO TIJELO IZREKLO HOTELU MARRIOTT KAZNU IZNOSU OD 20,4 milijuna eura ZBOG NEPODUZIMANJA ADEKVATNIH TEHNIČKIH I ORGANIZACIJSKIH MJERA

- ✓ Mariott je kažnjen sa oko 20,4 milijuna eura zbog povrede osobnih podataka (*data breacha*) 339 milijuna svojih gostiju

- ✓ 2018. Godine Marriot dolazi do saznanja da su im sustavi od 2014. godine cijelo vrijeme kompromitirani

- ✓ Osobni podaci kojima su napadači ostvarili pristup uključuju imena, adrese elektroničke pošte, telefonske brojeve, brojeve putovnica, informacije o dolascima i odlascima, VIP status gosta i korisnički broj u loyalty programu




**VJEŽBA: ispunjavanje upitnika:**

https://arc-rec-project.eu/upitnik-tehnicke-i-organizacijske-mjere-zastite-osobnih-podataka/

Ovaj upitnik za samoprocjenu voditeljima i izvršiteljima obrade služi isključivo u svrhu ukazivanja na neke od osnovnih tehničkih i organizacijskih mjera koje bi trebali poduzeti kako bi zaštitili osobne podatke svojih gostiju/klijenata/zaposlenika.

**Odgovori na sva pitanja trebali bi biti DA, osim u slučajevima kad neka od mjera nije primjenjiva na Vaše poslovanje (npr. ako u poslovanju ne koristite pametne telefone ili tablet računala, u tom slučaju ćete na pitanje odgovoriti NIJE PRIMJENJIVO).**

# 5 POŠTOVATI PRAVA ISPITANIKA (OSOBA ČIJE OSOBNE PODATKE OBRAĐUJETE) I OMOGUĆITI IM DA OSTVARE SVOJA PRAVA

- ✓ Svaka organizacija koja obrađuje osobne podatke pojedinaca, dužna je poštovati njihova prava zagarantirana GDPR-om i Zakonom o provedbi Opće uredbe o zaštiti podataka, informirati pojedince o njihovim pravima (**npr. putem politike privatnosti**) te im omogućiti da ostvaruju svoja prava.

- ✓ Ukoliko u svom poslovanju koristite web stranicu, preporuka Agencije je da na web stranici objavite obrazac zahtjeva putem kojeg ispitanik može ostvariti svoja prava. Primjer takvog obrasca dostupan je na: https://azop.hr/wp-content/uploads/2020/12/ZAHTJEV-ZA-OSTVARIVANJE-PRAVA-ISPITANIKA.docx

- ✓ Na zahtjeve pojedinaca za ostvarivanje njihovih prava iz GDPR-a dužni ste odgovoriti bez nepotrebnog odgađanja, **a najkasnije u roku od mjesec dana od primitka zahtjeva**. Rok za odgovor je moguće produžiti za još dva mjeseca ako je zahtjev složen, no u tom slučaju morate obavijestiti pojedinca u roku od mjesec dana o razlozima zbog kojeg i koliko će taj rok biti produžen.

- ✓ Prava ispitanika: Članci 12.-23. GDPR-a

## ZAHTJEV ZA OSTVARIVANJE PRAVA ISPITANIKA

**PODACI O ISPITANIKU KOJI ŽELI OSTVARITI PRAVA:**

Ime i prezime:_____

Ulica i broj:_____

Mjesto:_____

Broj telefona (opcionalno):_____

e-mail (opcionalno):_____

OIB (ako je primjenjivo ili za strane državljane - nacionalni ID broj/broj ID isprave) :_____

**VRSTE PRAVA KOJE ISPITANIK MOŽE OSTVARITI:**

(potrebno je označiti željeno pravo ili više njih)

- Pravo na pristup osobnim podacima
- Pravo na ispravak osobnih podataka
- Pravo na dopunu osobnih podataka
- Pravo na brisanje („zaborav“) osobnih podataka
- Pravo na ograničenje obrade osobnih podataka
- Pravo na prenosivost osobnih podataka
- Pravo na podnošenje/ulaganje prigovora

**OBRAZLOŽENJE ISPITANIKA ZA OSTVARIVANJE ŽELJENIH PRAVA:**

_____
_____
_____
_____
_____
_____
_____
_____
_____

_____ _____

**Mjesto i datum** **Potpis ispitanika**

| | |
|---|---|
| **PRAVO NA INFORMIRANJE** | Kada obrađuju Vaše osobne podatke, voditelji obrade (organizacije/društva/državna tijela) Vas trebaju na jasan i sažet način informirati o uporabi Vaših podataka. |
| **PRAVO NA PRISTUP OSOBNIM PODACIMA** | PRIMJER: imate pravo zatražiti presliku ugovora o Vašem bankovnom kreditu ili presliku Vašeg medicinskog kartona. |
| **PRAVO NA ISPRAVAK OSOBNIH PODATAKA** | PRIMJER: Ugovarate policu životnog osiguranja i doznajete da osiguravajuća kuća raspolaže s netočnim podatkom da ste pušač, što povećava iznos premije životnog osiguranja. Imate pravo tražiti osiguravajuću kuću ispravak tog netočnog podatka. |
| **PRAVO NA BRISANJE OSOBNIH PODATAKA ("PRAVO NA ZABORAV")** | PRIMJER: Ne želite više imati profil na društvenoj mreži te ste isti deaktivirali. Imate pravo zatražiti od društvene mreže brisanje osobnih podataka koje posjeduje o Vama. |
| **PRAVO NA PRIGOVOR** | PRIMJER: Prijavili ste se na nagradnu igru i dali privolu za obradu Vaših osobnih podataka te na Vaš email neprestano pristižu promotivne ponude. Imate pravo uložiti prigovor te organizacija mora prestati sa slanjem neželjenim promotivnim materijalom. |
| **PRAVO NA PRENOSIVOST PODATAKA** | PRIMJER: Niste zadovoljni uslugom trenutnog teleoperatera i želite ga promijeniti. Od teleoperatera čije usluge više ne želite koristiti imate pravo zatražiti da Vaše osobne podatke prenese direktno drugom operateru, ukoliko je to tehnički moguće. |
| **PRAVO NA OGRANIČENJE OBRADE OSOBNIH PODATAKA** | PRIMJER: Odlučili ste promijeniti banku te ste zatražili zatvaranje računa i brisanje svih Vaših osobnih podataka. Međutim, banka ima zakonsku obvezu čuvati sve podatke o bivšem klijentu u zakonski utvrđenom vremenskom razdoblju. U tom slučaju možete zatražiti ograničenje obrade svojih osobnih podataka. |
| **PRAVO U VEZI AUTOMATIZIRANOG POJEDINAČNOG DONOŠENJA ODLUKA** | PRIMJER: Zatražili ste kredit putem interneta te na temelju unesenih osobnih podataka računalni program banke „odlučuje“ hoće li kredit biti odobren te navodi predloženu kamatnu stopu. Imate pravo osporiti odluku i zatražiti uključivanje osobe u proces. |

Više o pravima ispitanika na: https://azop.hr/wp-content/uploads/2021/11/Gradani-upoznajte-svoja-prava-8.pdf,

https://arc-rec-project.eu/wp-content/uploads/2021/03/Pravo-ispitanika-na-pristup-osobnim-podacima.pdf

# Dokumentacija koju će ovlašteni službenici Agencije zatražiti prilikom provedbe nadzornih aktivnosti:

- Dokument iz kojeg je vidljivo da je fizička osoba ovlaštena od strane društva za komunikaciju s nadzornim tijelom (npr. punomoć za zastupanje ili punomoć odvjetnika , Odluka o imenovanju službenika)
- Interne akte kojima je regulirana zaštita osobnih podataka (npr. Pravilnik o zaštiti osobnih podataka, Politika privatnosti, Obavijest/informacije koje se pružaju ispitanicima o njihovim pravima)
- Akte iz kojih su vidljive ovlasti zaposlenika ili vanjskih suradnika (primjerice: Ugovor u radu ili drugi akt koji propisuje razine ovlasti kao npr. Pravilnik o ovlaštenjima)
- Izjave o povjerljivosti, obrazac: https://arc-rec-project.eu/wp-content/uploads/2022/01/zjava_o_povjerljivosti_obrazac-za-zaposlenike.docx
- Evidencije aktivnosti obrade, obrazac: https://arc-rec-project.eu/wp-content/uploads/2022/09/ARC-obrazac-Evidencija-aktivnosti-obrade.xlsx
- Ugovor o obradi osobnih podataka između voditelja i izvršitelja obrade, predložak dostupan na: https://arc-rec-project.eu/wp-content/uploads/2022/01/Ugovor-o-obradi-podataka-izmedu-voditelja-obrade-i-izvrsitelja-obrade-prema-clanku-28-OUZP-template-ARC.docx
- Dokumentaciju odnosnu na mjere zaštite (organizacijske i tehničke)
- Dokumentaciju odnosnu na određeni slučaj i pojedince, na koji način su prikupljeni određeni osobni podaci, temeljem koje pravne osnove i u koju točno svrhu (npr. obrazac privole ako se obrada temelji na privoli, test legitimnog interesa ako se obrada temelji na legitimnom interesu, pravilnik o videonadzoru itd.)

# Ugovor o obradi podataka između voditelja obrade i izvršitelja obrade prema članku 28. st. 3. Opće uredbe o zaštiti podataka sklapa se između

**izvršitelja obrade** (Ime i kontakt podaci izvršitelja)

i

**voditelja obrade** (Ime i kontakt podaci voditelja obrade)

## Uvodne odredbe

Voditelj obrade želi ugovoriti izvršenje usluga navedenih u čl. 3. ovog ugovora s Izvršiteljem. Ugovorene usluge uključuju obradu osobnih podataka. Opća uredba o zaštiti podataka (Uredba), posebice čl. 28. Uredbe postavlja određene zahtjeve u pogledu obrade osobnih podataka koje je izvršitelj dužan ispunjavati u ime voditelja obrade. Kako bi se osiguralo ispunjenje tih zahtjeva, stranke sklapaju ovaj Ugovor.

## Čl. 1. Definicije pojmova

Pojmovi korišteni u ovom Ugovoru, a koji su definirani člancima Opće uredbe o zaštiti podataka imat će značenje kako je utvrđeno primjenjivim odredbama Uredbe.

## Čl. 2 Predstavnici na području Europske unije

*(ukoliko je primjenjivo)*: Prema odredbama čl. 27. st.1. Opće uredbe, izvršitelj je za predstavnika na području Europske unije odabrao:

---

*(Ime i prezime, trgovačko društvo (ukoliko je primjenjivo), e-mail adresa i telefonski broj Predstavnika)*

## 3. Predmet ugovora

3.1. U ime voditelja obrade i temeljem glavnog ugovora sklopljenog dan/mjesec/godina („Glavni ugovor"), izvršitelj će pružati usluge voditelju obrade na sljedećim područjima:

---

U tu svrhu, voditelj obrade ustupit će potrebne osobne podatke Izvršitelju obrade koji će obrađivati te podatke isključivo u ime voditelja obrade i prema uputama koje će mu dati voditelj obrade, osim ukoliko je drukčije uređeno pravom Europske unije ili zakonskim odredbama zakonodavstva neke države članice Unije primjenjivim na Izvršitelja obrade. Svrha i opseg obrade osobnih podataka od strane izvršitelja određene su Glavnim ugovorom i uputama voditelja obrade te opisane u Dodatku 1 ovog Ugovora. Voditelj obrade odgovoran je za zakonitost obrade podataka prema čl.6.st.1. Opće uredbe o zaštiti podataka.

ZAGLAVLJE TVRTKE, MEMORANDUM

## IZJAVA O POVJERLJIVOSTI

Ovom izjavom obvezujem se da ću sukladno propisima koji uređuju područje zaštite osobnih podataka, 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) i Zakonom o provedbi Opće uredbe o zaštiti podataka, čuvati povjerljivost svih osobnih podataka kojima imam pravo i ovlast pristupa a koji se nalaze u sustavima pohrane koje vodi tijelo/društvo u kojem sam zaposlen/a te da ću iste osobne podatke koristiti isključivo u točno određenu (propisanu) svrhu.

Također se obvezujem da osobne podatke kojima imam pravo i ovlast pristupa neću dostavljati/davati na korištenje niti na bilo koji drugi način učiniti dostupnima trećim (neovlaštenim) osobama, te se obvezujem da ću povjerljivost istih osobnih podataka čuvati i nakon prestanka ovlasti pristupa osobnim podacima.

Upoznat/a sam da bilo kakvo neovlašteno raspolaganje osobnim podacima kojima imam pravo pristupa u svojem radu predstavlja povredu radne obveze.

Datum: _____

Ime i prezime: _____

Potpis: _____

VILLA ANAMARIA & IVA

INFORMIRATI POJEDINCE O OBRADI NJIHOVIH OSOBNIH PODATAKA



SOCIAL MEDIA

# 8 VODITI EVIDENCIJE AKTIVNOSTI OBRADE (AKO JE PRIMJENJIVO)

Evidencija aktivnosti obrade je obrazac koji služi kao dokaz da je obrada osobnih podataka zakonita. Ista mora sadržavati informacije **iz članka 30. GDPR-a**, a podaci sadržani u evidenciji obrade trebali bi biti na odgovarajući način zaštićeni.

- ✓ **PREPORUKA AGENCIJE!** Preporučamo da vodite evidenciju aktivnosti obrade čak i ako istu niste obvezni voditi jer je evidencija aktivnosti obrade jedan od dokumenta kojim možete dokazati usklađenost s GDPR-om.

- ✓ **NAPOMENA!** Evidencije aktivnosti obrade **NE dostavljate Agenciji za zaštitu osobnih podataka**, već ih vodite i čuvate u pisanom obliku u poslovnom prostoru, a dajete ih na uvid ako vas AZOP to zatraži.

✓ Neovisno o broju zaposlenika, bilo da ste voditelj obrade ili izvršitelj obrade, **DUŽNI** ste voditi evidenciju obrade ukoliko je ispunjen jedan od sljedećih uvjeta:

- ako će obrada vjerojatno prouzročiti visoki rizik za prava i slobode ispitanika (npr. uvođenje novih tehnologija kao što su biometrijski čitači, prepoznavanje lica, IT servisa koji obrađuju osobne podatke),
- ako obrada nije povremena, odnosno ako je obrada stalna (npr. obrada osobnih podataka zaposlenika u svrhu isplate plaća),
- ako obrada uključuje posebne kategorije podataka (npr. zdravstveni podaci, biometrijski podaci, genetski podaci),
- ako obrada uključuje osobne podatke u vezi s kaznenim osudama i kažnjivim djelima

! Evidenciju niste dužni voditi ako zapošljavate manje od 250 zaposlenika i ako nije ispunjen niti jedan od prethodno navedenih uvjeta.

# SIVA POLJA SU OBAVEZNA, A ZELENA OPCIONALNA

| | Podaci o voditelju obrade | | Službenik za zaštitu podataka (ukoliko je imenovan) | |
|---|---|---|---|---|
| | NAZIV: | Hotel Villa ANAMARIA&IVA | IME I PREZIME: | Ana Anić |
| | ADRESA: | Istarska 32, Poreč | e-mail adresa: | villaANAMARIA&IVA-dpo@eventi.hr |
| | EMAIL: | villaANAMARIA&IVA@eventi.hr | | |
| | TELEFON: | 098/345123 | | |

UPUTE ZA POPUNJAVANJE: https://arc-rec-project.eu/wp-content/uploads/2022/08/ARC-vodic-za-popunjavanje-evidencije-aktivnosti-obrade.pdf

| NAZIV OBRADE | KATEGORIJE ISPITANIKA | IZVRŠITELJ OBRADE | SVRHA OBRADE | IT SERVIS ili FIZIČKO MJESTO POHRANE (LOKACIJA OSOBNIH PODATAKA) | PRAVNA OSNOVA OBRADE (Članak 6. GDPR-a) | Prava dostupna ispitaniku | POVEZNICA NA DOKAZ O PRIVOLI | KATEGORIJE OSOBNIH PODATAKA KOJE SE OBRAĐUJU |
|---|---|---|---|---|---|---|---|---|
| Naziv pod kojim je obrada prepoznatljiva | Zaposlenici, kupci, posjetitelji, vanjski suradnici.... | Podaci o izvršitelju obrade (ako postoji) | Razlog obrade podataka | Popis IT servisa u kojima se vrši obrada podataka ili lokacija fizičkog mjesta pohrane ako podatak nije digitaliziran | Članak 6. GDPR-a: (privola, zakon, ugovor, legitimni interes voditelja obrade, zaštita prava ispitanika, izvršavanje zadaća u okviru javne ovlasti) | Pravo na pristup podacima, pravo na ispravak, pravo na brisanje, pravo na ograničenje obrade, pravo na prigovor, pravo na prijenos drugom voditelju obrade | Unijeti poveznicu na privolu ili lokaciju privole ukoliko je privola temelj ove obrade | Identifikacijski podaci, lokacijski podaci, financijski podaci, zdravstveni podaci itd. |
| EVIDENCIJA PODATAKA O ZAPOSLENICIMA | Zaposlenici | Nema | Vođenje evidencije o zaposlenicima | mapa u zaključanom ormaru u uredu vlasnika poduzeća; mapa pod nazivom zaposlenici u ERP-u, zaštićena šifrom | Obrada je nužna radi poštovanja pravnih obveza voditelja obrade (Čl. 6. GDPR-a, st. 1. točka c)<br>Zakon o radu (NN 93/2014, 127/2017, 98/2019,<br>Pravilnik o sadržaju i načinu vođenja evidencije o radnicima (NN 32/15, 97/15) | Pravo na pristup podacima, pravo na ispravak, pravo na ograničenje obrade | Nije primjenjivo | IDENTIFIKACIJSKI PODACI (Ime, prezime, OIB, datum rođenja, spol, prebivalište, boravište, državljanstvo)<br>PODACI O OBRAZOVANJU<br>PODACI O RADNOM STAŽU |
| OBRAČUN I ISPLATA PLAĆA I DRUGIH DOHODAKA | Zaposlenici | Knjigovodstveni servis xy | Obračun i isplata plaća | mapa pod nazivom zaposlenici- isplata plaća u ERP-u, zaštićena šifrom | Obrada je nužna radi poštovanja pravnih obveza voditelja obrade (Čl. 6. GDPR-a, st. 1. točka c) , Zakon o računovodstvu, Zakon o radu, Zakon o mirovinskom osiguranju | Pravo na pristup podacima, pravo na ispravak, pravo na ograničenje obrade | Nije primjenjivo | IDENTIFIKACIJSKI PODACI (Ime i prezime, adresa, OIB, Spol, dan, mjesec, godina rođenja, prebivalište/boravište)<br>PODACI O OBRAZOVANJU I RADNOM STAŽU (stručno obrazovanje, datum početka rada, naznaku radi li se o punom radnom vremenu ili nepunom radnom vremenu,<br>mjesto rada, datum prestanka radnog odnosa, razlog prestanka radnog odnosa, podaci za potrebu |

| IME I KONTAKT PODACI ZAJEDNIČKOG VODITELJA OBRADE (AKO JE PRIMJENJIVO) | LEGITIMNI INTERESI ZA OBRADU (AKO JE PRIMJENJIVO) | POSTOJANJE AUTOMATIZIRANOG DONOŠENJA ODLUKA, UKLJUČUJUĆI PROFILIRANJE (AKO JE PRIMJENJIVO) | KATEGORIJE PRIMATELJA | POVEZNICA NA UGOVOR S IZVRŠITELJEM OBRADE | ROKOVI BRISANJA (ČUVANJA) PODATAKA | JE LI POTREBNO NAPRAVITI PROCJENU UČINKA NA ZAŠTITU OSOBNIH PODATAKA? | POVEZNICA NA PROCJENU UČINKA NA ZAŠTITU OSOBNIH PODATAKA | JE LI DOŠLO DO POVREDE OSOBNIH PODATAKA? | POVEZNICA NA DOKAZ O POVREDI OSOBNIH PODATAKA | OPI O |
|---|---|---|---|---|---|---|---|---|---|---|
| Ako dvoje ili više voditelja obrade zajednički odrede svrhe i načine obrade, oni su zajednički voditelji obrade. Unijeti kontakt podatke zajedničkog voditelja, ukoliko je primjenjivo | Navesti koji su legitimni interesi temelj obrade (npr. zaštita tjelesnog integriteta i imovine, sprječavanje prijevara, osiguranje sigurnosti računalnog sustava,...) - navesti da li je proveden test legitimnog interesa (razmjernosti) i unijeti | Navesti ukoliko ova obrada rezultira automatskim donošenjem odluka vezano uz ispitanika | npr. MUP, DORH, Ministarstvo financija - Carina, HZZO, HZMO Porezna uprava, sudovi... | Ukoliko u svoj obradi postoji izvršitelj obrade, potrebno je navesti broj ugovora ili poveznicu na ugovor ili naziv ugovora ili drugi odgovarajući identifikator | Unijeti rok čuvanja podataka i temeljem čega je određen (za regulatorne obveze provjeriti točno propisani rok ovisno o pojedinom zakonu) | Ukoliko obrada može rezultirati visokim rizikom za prava i slobode pojedinca, unijeti DA, inače NE | Unijeti poveznicu na izvještaj o procjeni učinka na zaštitu osobnih podataka vezanu uz ovu obradu | Ukoliko je došlo do povrede osobnih podataka, unijeti DA, inače NE | Unijeti poveznicu na evidenciju iz Registra povreda osobnih podataka | |
| Nije primjenjivo | Nije primjenjivo | Nije primjenjivo | HZZO, HZMO, Porezna uprava | Nije primjenjivo | Trajno (Članak 5. Pravilnik o sadržaju i načinu vođenja evidencije o radnicima NN 73/2017) | Ne | Nije primjenjivo | Ne | Nije primjenjivo | |
| Nije primjenjivo | Nije primjenjivo | Nije primjenjivo | HZZO, HZMO, Porezna uprava | Poveznica na ugovor s knjigovodstvenim servisom | Trajno (sukladno čl.10 Zakona o računovodstvu NN 78/2015, isplatne liste i analitička evidencija o plaćama za koje se plaćaju obvezni doprinosi čuvaju se trajno) | Ne | Nije primjenjivo | Ne | Nije primjenjivo | |
| Nije primjenjivo | Link na dokumentirani test legitimnog interesa | Nije primjenjivo | Sustav e-Visitor; podaci o zdravlju (alergijama) prosljeđuju se s recepcije zaposlenicima iz kuhinje, te u slučaju posebnih potreba gostiju sobaricama i pomoćnom osoblju u hotelu | Nije primjenjivo | Obveza čuvanja podataka iz popisa turista te prijave i odjave turista (osobni podaci koji se unose u e-Visitor) je 10 godina. Osobni podaci iz interne evidencije gositju čuvaju se 6 mjeseci, a u slučaju odštatnih zahtjeva i sudskih postupaka do okončanja sudskog postupka. Podaci prikupljeni na temelju privole brišu se ukoliko ispitanik povuče privolu ili se brišu nakon ispunjenja | Ne | Nije primjenjivo | Ne | Nije primjenjivo | |
| | | | | | | | | | | |

| | OPIS PODUZETIH TEHNIČKIH I ORGANIZACIJSKIH MJERA | PRIJENOS U TREĆE ZEMLJE | OPIS PODUZETIH SIGURNOSNIH MJERA U SLUČAJU PRIJENOSA PODATAKA U TREĆE ZEMLJE | IZVOR PODATAKA | NAPOMENE |
|---|---|---|---|---|---|
| 8 | Procedure - politike - pravilnici - edukacija -IT rješenja - certifikati.. Unijeti reference na dokumente gdje je primjenjivo | Iznose li se podaci u treće zemlje (izvan EU)? U koje zemlje i u koje svrhe? | Npr. standardne ugovorne klauzule ili obvezujuća korporativna pravila (* članak 49. Uredbe). Ako postoji prijenost osobnih podataka u treće zemlje, staviti poveznicu na dokumente kojima su takvi prijenosi regulirani | Od koga su pribavljeni osobni podaci (od ispitanika, treće osobe, javnog tijela...) | Važne činjenice koje nisu obuhvaćene prethodnim kategorijama |
| 9 | Politika privatnosti, Pravilnik o zaštiti podataka, izjava o povjerljivosti, backup programa, antivirusni programi, evidencija pristupa osobnim podacima (logovi), edukacija zaposlenika na temu zaštite podataka, enkripcija, korištenje korisničkih imena i snažnih lozinki za pristup računalima i računalnoj opremi, antivirusni programi, redovito izrađivanje sigurnosnih kopija podataka. Papirnata dokumentacija koja sadrži osobne podatke nalazi se u zaključanom ormariću u zaključanoj prostoriji | Ne | Nije primjenjivo | Ispitanik | Nema |
| 10 | Politika privatnosti, Pravilnik o zaštiti podataka, izjava o povjerljivosti, ugovor s izvršiteljem obrade, backup programa, antivirusni programi, evidencija pristupa osobnim podacima (logovi), edukacija zaposlenika na temu zaštite podataka, enkripcija, korištenje korisničkih imena i snažnih | Ne | Nije primjenjivo | Ispitanik | Nema |
| 11 | olitika privatnosti, Pravilnik o zaštiti podataka, izjava o povjerljivosti, ugovor s izvršiteljem obrade, backup programa, antivirusni programi, evidencija pristupa osobnim podacima (logovi), edukacija zaposlenika na temu zaštite podataka, enkripcija, korištenje korisničkih imena i snažnih | Ne | Nije primjenjivo | Ispitanik | Nema |
| | Politika privatnosti, Pravilnik o zaštiti podataka, izjava o povjerljivosti, backup | | | | |

Evidencija aktivnosti obrada

[Poveznica na obrazac evidencije aktivnosti obrade i upute za ispunjavanje:]

https://arc-rec-project.eu/wp-content/uploads/2022/09/ARC-obrazac-Evidencija-aktivnosti-obrade.xlsx

https://arc-rec-project.eu/wp-content/uploads/2022/11/ARC-vodic-za-popunjavanje-evidencije-aktivnosti-obrade.pdf

Članak 30 GDPR-a

# 9 IMENOVATI SLUŽBENIKA ZA ZAŠTITU PODATAKA (AKO JE PRIMJENJIVO)

## Imenovanje službenika za zaštitu podataka (čl. 37 GDPR-a) obvezno je:

- ✓ **Ako obradu provodi tijelo javne vlasti ili javno tijelo** (bez obzira na to koji se podaci obrađuju);
- ✓ **Ako se osnovne djelatnosti voditelja obrade ili izvršitelja obrade sastoje od postupaka obrade koji iziskuju redovito i sustavno praćenje ispitanika u velikoj mjeri**
- ✓ **Ako se osnovne djelatnosti voditelja obrade ili izvršitelja obrade sastoje od opsežne obrade posebnih kategorija podataka ili osobnih podataka koji se odnose na kaznene osude i kažnjiva djela** (npr. poduzeće koje se bavi pružanjem usluga ugovornog obavljanja poslova zaštite na radu)

**Službenik za zaštitu podataka imenuje se na temelju stručnih kvalifikacija, a posebno stručnog znanja o pravu i praksama u području zaštite podataka te sposobnosti izvršavanja njegovih zadaća (članci 37, 38 i 39 GDPR-a).**

- ❑ Iznajmljivači apartmanskog smještaja, manji hoteli nisu u obvezi imenovanja službenika za zaštitu podataka.

- ❑ **Villa ANAMARIA&IVA ipak ima službenika za zaštitu podataka iako nije u obvezi imenovanja službenika, jer u slučaju data breacha, pritužbi ispitanika i upita nadzornog tijela ili ispitanika je važno imati osobu koja ima dovoljno znanja da može komunicirati s nadzornim tijelom, ispitanicima i odgovarati na njihove upite/zahtjeve. Radi se o administrativnoj tajnici koja nije niti pravne niti IT struke, ali je upućena na sveobuhvatnu edukaciju iz područja zaštite podataka te se kontinuirano obrazuje na radionicama koje organizira AZOP besplatno ☺**

- ✓ Ipak, preporuka Agencije da se službenika za zaštitu ipak imenuje, ali VAŽNO JE NAPOMENUTI DA SLUŽBENIK MORA POSJEDOVATI ADEKVATNA ZNANJA IZ PODRUČJA ZAŠTITE OSOBNIH PODATAKA KAKO BI MOGAO PRATITI JE LI ORGANIZACIJA USKLAĐENA S PROPISIMA O ZAŠTITI PODATAKA I SAVJETOVATI VODITELJA OBRADE! Nemojte imenovati službenika koji nema znanja, tek toliko da ga imenujete. U slučaju povrede osobnih podataka, službenik je kontakt točka za komunikaciju s nadzornim tijelom. Ako službenik nema adekvatna znanja, to će biti za vas dodatna otegotna okolnost.

Odluku o imenovanju službenika potrebno je dostaviti AZOP-u, upute na: https://azop.hr/imenovanje-sluzbenika-za-zastitu-podataka/

# 10 PROVESTI PROCJENU UČINKA NA ZAŠTITU PODATAKA (AKO JE PRIMJENJIVO)

**Procjena učinka na zaštitu podataka (članak 35. GDPR-a obvezna je u slučaju):**

(a) sustavne i opsežne procjene osobnih aspekata u vezi s pojedincima koja se temelji na automatiziranoj obradi, uključujući izradu profila i na temelju koje se donose odluke koje proizvode pravne učinke za pojedinca;
(b) opsežne obrade posebnih kategorija osobnih podataka ili podataka u vezi s kaznenim osudama i kažnjivim djelima ili
c) sustavnog praćenja javno dostupnog područja u velikoj mjeri.

Obrazac: https://arc-rec-project.eu/wp-content/uploads/2022/01/DPIA-obrazac_procjena_ucinka.docx

- ✓ Prilikom procjene koji će postupci prouzročiti vjerojatno visok rizik za prava pojedinaca, potrebno je uzeti u obzir devet kriterija koji su detaljno opisani u Vodiču za provedbu procjene učinka na zaštitu podataka, dostupnom na web stranici projekta ARC: https://arc-rec-project.eu/vodici/

- ✓ **Popis vrsta postupaka obrade koje podliježu zahtjevu za procjenu učinka na zaštitu podataka možete pronaći na web stranici AZOP-a:** https://azop.hr/odluka-o-uspostavi-i-javnoj-objavi-popisa-vrsta-postupaka-obrade-koje-podlijezu-zahtjevu-za-procjenu-ucinka-na-zastitu-podataka/

## VIDEONADZOR

Obrada osobnih podataka putem **videonadzora dodatno je uređena Zakonom o provedbi Opće uredbe (članci 25.-32.), a može se provoditi samo u svrhu koja je nužna i opravdana za zaštitu osoba i imovine**, ako ne prevladavaju interesi ispitanika koji su u suprotnosti s obradom podataka putem videonadzora. Sustav videonadzora mora biti zaštićen od pristupa neovlaštenih osoba, a odgovorne osobe koje imaju pravo pristupa osobnim podacima ne smiju koristiti snimke suprotno svrsi u koju je postavljen videonadzor.

Ukoliko planirate ili već imate postavljen **videonadzor** u vašem poslovnom prostoru, dužni ste označiti da je objekt odnosno pojedina prostorija u njemu te vanjska površina objekta pod videonadzorom, **a oznaka treba biti vidljiva najkasnije prilikom ulaska u perimetar snimanja te sadržavati jednostavnu i razumljivu sliku uz tekst kojim se osobama pružaju najmanje sljedeće informacije:** da je prostor pod videonadzorom, podatke o voditelju obrade (poduzeću/društvu/obrtu/organizaciji/tijelu jave vlasti, državnom tijelu): naziv, adresa i kontakt podaci voditelja obrade, svrhu obrade, pravnu osnovu, prava ispitanika i poveznicu na politiku privatnosti ili drugi odgovarajući dokument.


- ✓ Videonadzorom ne smiju biti obuhvaćene sobe, liftovi, toaleti, wellness prostorije, javne površine, dvorišta i nekretnine susjeda i sl.
- ✓ U primjeru **Villa ANAMARIA&IVA ,** videonazdorom je obuhvaćena recepcija, hotelski hodnici i dvorište i parking koji je u vlasništvu hotela u svrhu zaštite ljudi i imovine. Na svim mjestima gdje se nalazi videonadzor, **prije ulaska u perimetar snimanja nalazi se obavijest o videonazdoru**
- ✓ **Predložak obavijesti o videonadzoru možete preuzeti na: https://azop.hr/wp-content/uploads/2022/08/template-obavijest-videonadzor.pptx**
- ✓ **Više informacija na: https://azop.hr/videonadzor-preporuka/**
- ✓ **Videosnimka na kojoj se nalazi osoba je njezin osobni podatak. Osoba ima pravo tražiti vas kopiju snimke na kojoj se nalazi! Vi ste joj dužni tu kopiju dostaviti, uz napomenu da je potrebno zaštititi identitet drugih osoba na snimci**

## MOLIMO ISPUNITE ANKETU

**Ciljevi ankete:**

https://ec.europa.eu/eusurvey/runner/CERV_2021-2027

Informacije o obradi Vaših osobnih podataka dostupne su na: https://arc-rec-project.eu/politika-privatnosti/ .

**- dobivanje uvida u vaše zadovoljstvo našim aktivnostima, kako bi u budućnosti bile bolje i odgovarale vašim očekivanjima**

**- AZOP-ova ugovorna obveza prema Europskoj komisiji, kako bi Komisija koja je financirala projekt mogla ocijeniti uspješnost ARC2 projekta i kao dokaz da smo proveli sve aktivnosti sukladno ugovoru**

**- stjecanje dubljeg uvida u mišljenje građana o vladavini prava u njihovoj zemlji i EU**

**- promoviranje rodne ravnopravnosti i da svi pojedinci imaju jednake mogućnosti i jednak pristup sudjelovanju u društvu i gospodarstvu**

## Upute za ispunjavanje (prva stranica upitnika koju svi ispunjavate isto):

https://ec.europa.eu/eusurvey/runner/CERV_2021-2027

Izabrati u izborniku hrvatski jezik

Padajući izbornik je u gornjem desnom kutu ekrana

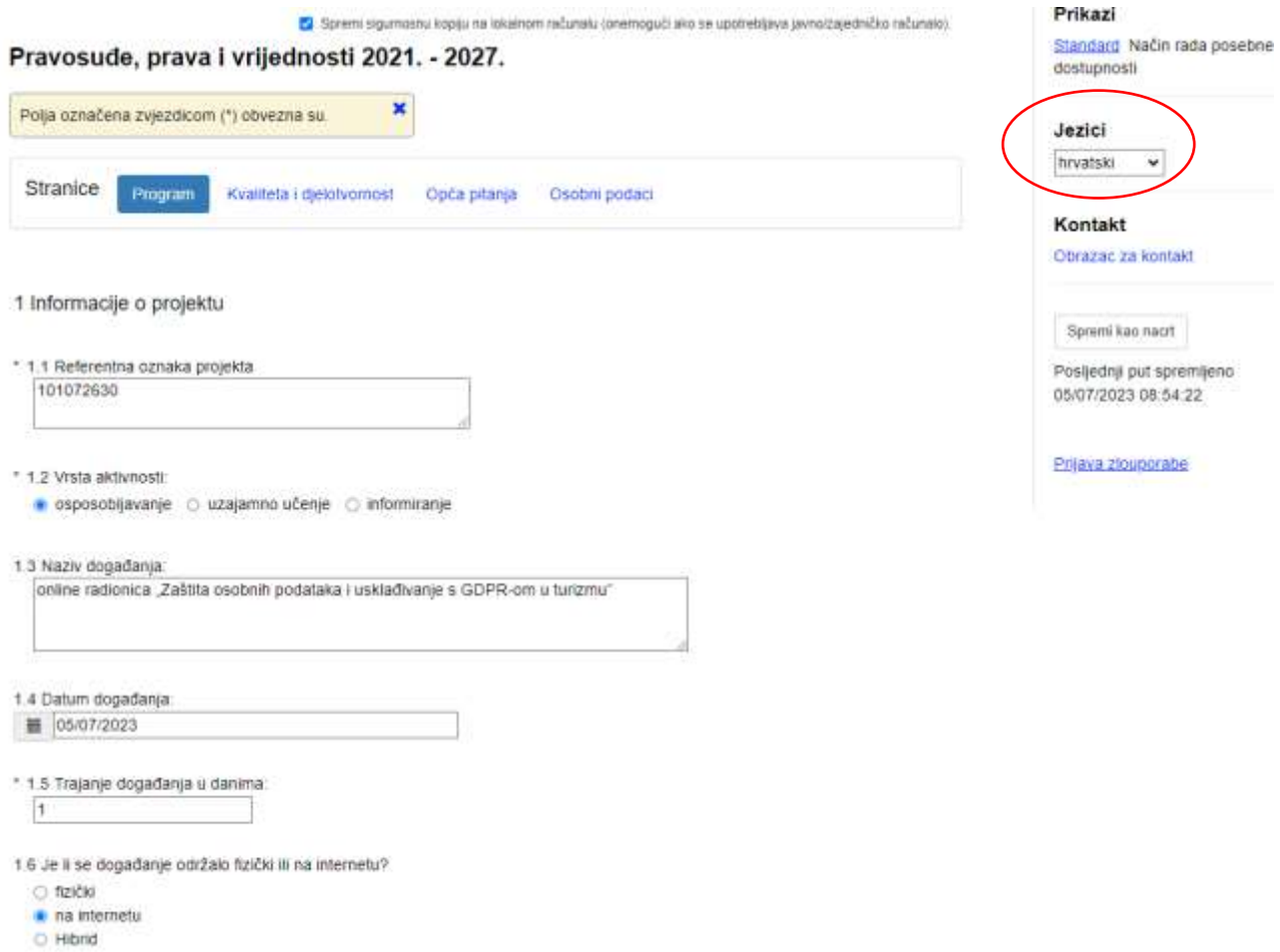
Informacije o projektu:

**Referentna oznaka:** 101072630

**Vrsta aktivnosti:** osposobljavanje

**Naziv: online radionica „Zaštita osobnih podataka i usklađivanje s GDPR-om u turizmu”**

**Datum:** 05/07/2023



# OBRADA OSOBNIH PODATAKA PUTEM KOLAČIĆA

**Kolačići (cookies) su male datoteke koje Internet preglednik (eng. Web Browser) pohranjuje na računalo, mobilni uređaj ili neki drugi uređaj kojim je korisnik posjetio neko Internet mjesto (eng. Web site).**

Kolačići se dijele prema **trajanju**, prema **izvoru kolačića** i prema **funkciji**.

Prema **trajanju** kolačići mogu biti:

- ✓ **Stalni kolačići (spremljeni)** (eng Persistent Cookies)
- ✓ **Privremeni kolačići ili kolačići sesije** (eng. Session Cookies)

Prema **izvoru** kolačići mogu biti:

- ✓ **Kolačići prve strane** (first party cookie)
- ✓ **Kolačići treće strane** (third party cookie)

Prema **funkciji** postoji više vrsta kolačića, a najčešće su:

- ✓ **Tehnički/neophodni kolačići**
- ✓ **Funkcionalni kolačići**
- ✓ **Statistički kolačići**
- ✓ **Marketinški kolačići**

Kolačići za koje **nije potrebna privola** pripadaju jednoj od sljedećih skupina kolačića:

- ✓ **Tzv. kolačići "Unos od strane korisnika"**
- ✓ **Kolačići za autentifikaciju**
- ✓ **Sigurnosni kolačići usmjereni na korisnika**
- ✓ **Kolačići sesije multimedijskog playera**
- ✓ **Sesijski kolačići za uravnotežavanje učitavanja (eng Load balancing session cookies)**
- ✓ **Kolačići za dijeljenje korisničkog sadržaja u socijalnim mrežama putem dodataka za društvene mreže (eng. Social plug-in content sharing cookies)**
- ✓ **Preporuka: Ako vam kolačići nisu neophodni za poslovanje, nemojte ih koristiti. Izbjegavajte Google Analytcs jer u tom slučaju prenosite osobne podatke u treću zemlju. Angažirajte stručnog izvršitelja obrade upoznatog s zakonskim propisima o obradi osobnih podataka putem kolačića i sklopiti s njim ugovor voditelj-izvršitelj obrade iz članka 28. GDPR-a**
- ✓ **Upute: Vodič za kolačiće, Kako uskladiti web stranicu s GDPR-om?**

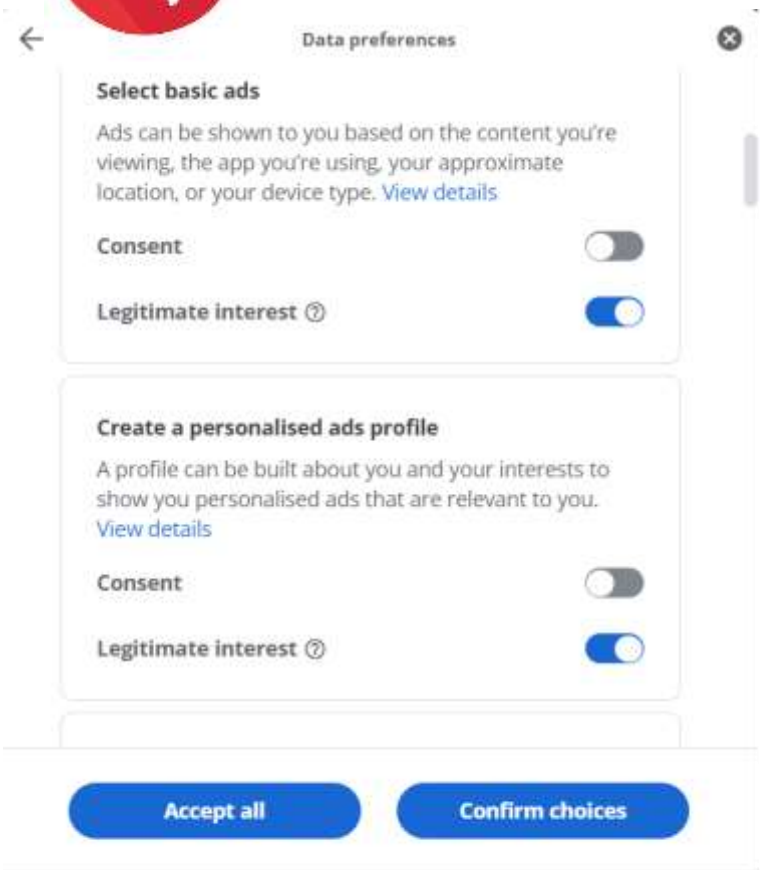
- ✓ Ukoliko u vašem poslovanju koristite web stranicu i **obrađujete osobne podatke putem kolačića,** dužni ste o tome obavijestiti posjetitelje svoje web stranice putem jasno vidljive obavijesti (skočnog prozora/bannera) te na web stranici uz politiku privatnosti morate imati objavljenu i obavijest o kolačićima. Informacije o kolačićima ispitaniku možete pružiti unutar politike privatnosti u zasebnom poglavlju na pregledan i jasno razumljiv način ili u zasebnom dokumentu. **U svakom slučaju, oba dokumenta moraju biti jasno vidljiva i najčešće se nalaze u podnožju web stranice.**

- ✓ Obavijest o kolačićima treba sadržavati sve informacije o tome što su kolačići, vrsti kolačića koji se na web stranici koriste i njihovoj funkciji. **Korisnik treba imati mogućnost na jednako jednostavan način odbiti i prihvatiti kolačiće.**

- ✓ Za obradu osobnih podataka putem kolačića, **pravni temelj NE MOŽE BITI LEGITIMAN INTERES VEĆ SAMO PRIVOLA!** I to privola koja mora udovoljavati svim uvjetima iz GDPR-a, biti informirana, dana dobrovoljno, UKRATKO: korisniku mora biti jasno i transparentno objašnjeno za kakvu obradu osobnih podataka daje privolu, u koju svrhu se njegovi osobni podaci obrađuju i s kime se dijele te mu usluga ne smije biti uskraćena zato jer nije dao privolu.

## PRIMJER DOBRE PRAKSE


## PRIMJER LOŠE PRAKSE



## I ZA KRAJ...

- ✓ Nemojte samo iskopirati „dokumente za usklađivanje s GDPR-om" od nekog drugog hotela ili iznajmljivača apartmanskog smještaja. To ne znači da ste usklađeni s GDPR- om. Interni akti moraju odražavati stvarne aktivnosti obrade u vašoj organizaciji. „Mrtvo slovo na papiru" vas neće zaštititi od *data breacheva* i kazni Agencije za zaštitu podataka.

- ✓ U slučaju pritužbi pojedinaca i nadzora AZOP-a, pravilnici vam neće biti od nikakve koristi ako niste doista implementirali tehničke i organizacijske mjere u svoje poslovne procese odnosno ako su te mjere samo na papiru, a u praksi se ne primjenjuju.

- ✓ U slučaju **povrede osobnih podataka, dužni ste obavijestiti Agenciju za zaštitu osobnih podataka bez odgađanja,** ako je moguće, najkasnije 72 sata nakon saznanja o toj povredi, osim ako nije vjerojatno da će povreda osobnih podataka prouzročiti rizik za prava i slobode pojedinaca. Ako izvješćivanje nije učinjeno unutar 72 sata, mora biti popraćeno razlozima za kašnjenje, obrazac za izvješćivanje: https://azop.hr/izvjescivanje-o-povredi-osobnih-podataka/

1) MVEP u postupku izdavanja D viza u svrhu rada ne želi na naše upite o statusu zahtjeva i očekivanom okončanju postupka sa nama dijeliti relevantne podatke, uz obrazloženje da su obveznici poštivanja GDPR-a. Premda je naše poduzeće subjekt iste obveze, ne dobivamo traženu informaciju premda nam je ona izrazito potrebna radi planiranja ostalih aktivnosti (organizacija putovanja, kupovina zrakoplovne karte, putnog zdravstvenog osiguranja i sl.). Molim Vas da li je takvo tumačenje MVEP-a ispravno. Ili se GDPR koristi kao izlika za neučinkovitost sustava uslijed kojeg u značajnom broju slučajeva dolazi do kašnjenja u rješavanju zahtjeva za izdavanje D viza?

Nedostaje nam više informacija kako bismo dali konkretan odgovor, ali razabire se da je ovdje u primjeni PRAVILNIK O VIZAMA (NN 109/21) koji određuje da državljanin treće zemlje osobno podnosi zahtjev za izdavanje vize. Iznimno može se prihvatiti zahtjev od drugih subjekata kao primjerice posredstvom komercijalnog posrednika (npr. turističke agencije). Stoga, ako nije riječ o zahtjevu koji je podnesen od strane posrednika, nije razvidan pravni temelj za otkrivanje statusa zahtjeva kojeg je netko osobno podnio. Ono što prvo morate znati ako želite obrađivati osobne podatke koji vam je pravni temelj i zakonita svrha za obradu osobnih podataka. Ako ne možete odrediti pravni temelj, a ne može niti MVEP obrada nije u skladu s GDPR-om.

2) U praksi postoje različita mišljenja u vezi s nužnošću potpisivanja izjave kojom gosta daje suglasnost na obradu osobnih podataka (uobičajeni naziv dokumenta na engleskom jeziku Registration form and consent). Za potrebe boravka gosta u hotelu prikupljaju se samo obvezni podaci. Međutim također je uobičajeno da gost putem hotela zatraži dodatnu uslugu kao npr. prijevoz, izlet, ugostiteljska usluga u drugom restoranu, a u kojim slučajevima je potrebno dati neke od osobnih podataka gosta trećim osobama (najčešće ugovornim partnerima hotela). S obzirom na podijeljenost mišljenja i nesigurnosti u ispravnost postupanja, najčešće se hotelijeri priklanjaju opciji prikupljanja suglasnosti gostiju.

Pitanje glasi: Je li u opisanom slučaju nužno tražiti pisanu suglasnost gosta?

Za svaku obradu osobnih podataka je potreban pravni temelj. Ukoliko je izlet, ugostiteljska usluga, prijevoz itd. dio ugovorenog aranžmana, obrada osobnih podataka temelji se na ugovornoj obvezi te privola nije potrebna. ONO ŠTO JE KLJUČNO DA JE ISPITANIK INFORMIRAN S KIME SE I KOJI OSOBNI PODACI DIJELE (npr. putem politike privatnosti). Ukoliko takvi sadržaji nisu dio ugovorne obveze, privola je potrebna. Postoji još i mogućnost legitimnog interesa kao pravnog temelja, ali ovisi o okolnostima i potrebno je dokazati legitimni interes provedbom testa razmjernosti.

3) Smijem li od gostiju unaprijed mailom traziti osobne podatke u svrhu unosa u eVisitor i nakon toga obrisati mail? Ukoliko niste iz nekog razloga na licu mjesta zatražiti gosta uvod u osobnu iskaznicu i upisati osobne podatke u e-visitor, ispitanika načelno možete zatražiti da vam pošalje osobne podatke putem e-maila (ali samo osobne podatke ne i presliku/fotografiju osobne iskaznice/putovnice). Ipak, preporuka Agencije je da to ne radite već da goste upisujete u e-visitor kad dođu u Vaš objekt, ako niste u mogućnosti gosta dočekati da korisite provjerene online platforme za obradu rezervacija.

4) Kako gostu pristupiti i objasniti zašto moramo slikati njegovu putovnicu za prijavu u sustav e-Visitor?

Slikanje putovnice je prekomjerna obrada, te nije u skladu s načelom smanjenja količine osobnih podataka. Ono što morate sukladno zakonskoj obvezi je zatražiti gosta uvid u putovnicu, upisati u sustav e-Visitor podatke i gostu vratiti putovnicu. Goste morate putem politike privatnosti informirati o obradi osobnih podataka. Ta politika privatnosti može biti dostupna na vašoj web stranici ukoliko je imate, u printanom obliku na recepciji, u sobama. Ako vas gost pita, morate znati reći zašto i u koje svrhe prikupljate njegove osobne podatke. Ukoliko vam gost odbije dati uvid u osobnu iskaznicu, imate pravo uskratiti mu uslugu.

5) Treba li biti imenovana osoba za zaštitu osobnih podataka uposlenika i gostiju, te ako treba molim Vas kakva je preporuka je li to posao za jednu osobu ili su to dva odvojena područja?

Ključna osoba koja vodi brigu o tome da je organizacija usklađena s propisima o zaštiti osobnih podataka je službenik za zaštitu podataka. Jedna osoba vodi brigu o obradi osobnih podataka svih pojedinca čiji se osobni podaci obrađuju: gostiju, klijenata zaposlenika. Postoje uvjeti kad je organizacija u obvezi imenovanja službenika za zaštitu podataka, ali čak i kad iznajmljivači apartmana/hoteli nisu u obvezi imenovanja službenika, preporuka Agencije je da istog imenuje. Taj službenik mora udovoljavati svim zahtjevima iz članaka 37.-39. Opće uredbe o zaštiti podataka, a odluka o imenovanju se mora dostaviti Agenciji. Saznajte više na: https://azop.hr/imenovanje-sluzbenika-za-zastitu-podataka/ .

6) Što je sa videonadzorom? Trebamo li tražiti dozvolu agencije? Koristiti certificirane kamere?
Videonadzor mora biti usklađen s zakonskim propisima o zaštiti podataka (GDPR-om i Zakonom o provedbi Opće uredbe o zaštiti podataka). Agencija (niti bilo koje drugo tijelo) ne izdaje dozvolu za videonadzor, niti postoje certificirane kamere niti tvrtke koje instaliraju certificirane kamere.

7) Vezano za iznajmljivače, fizičke osobe, da li je nositelj rješenja ujedno i voditelj obrade podataka?

Voditelj obrade je bilo fizička ili pravna osoba koja određuje sredstva i svrhe obrade, odnosno kako i zašto će se osobni podaci obrađivati.

Dakle, iznamljivač apartmana je voditelj obrade ako određuje koje osobne podatke će obrađivati i kako te je na njemu odgovornost da se uskladi s zakonskim propisima o zaštiti podataka. Hotel kao pravna osoba koja određuje koji osobni podaci će se obrađivati i zašto je voditelj obrade.

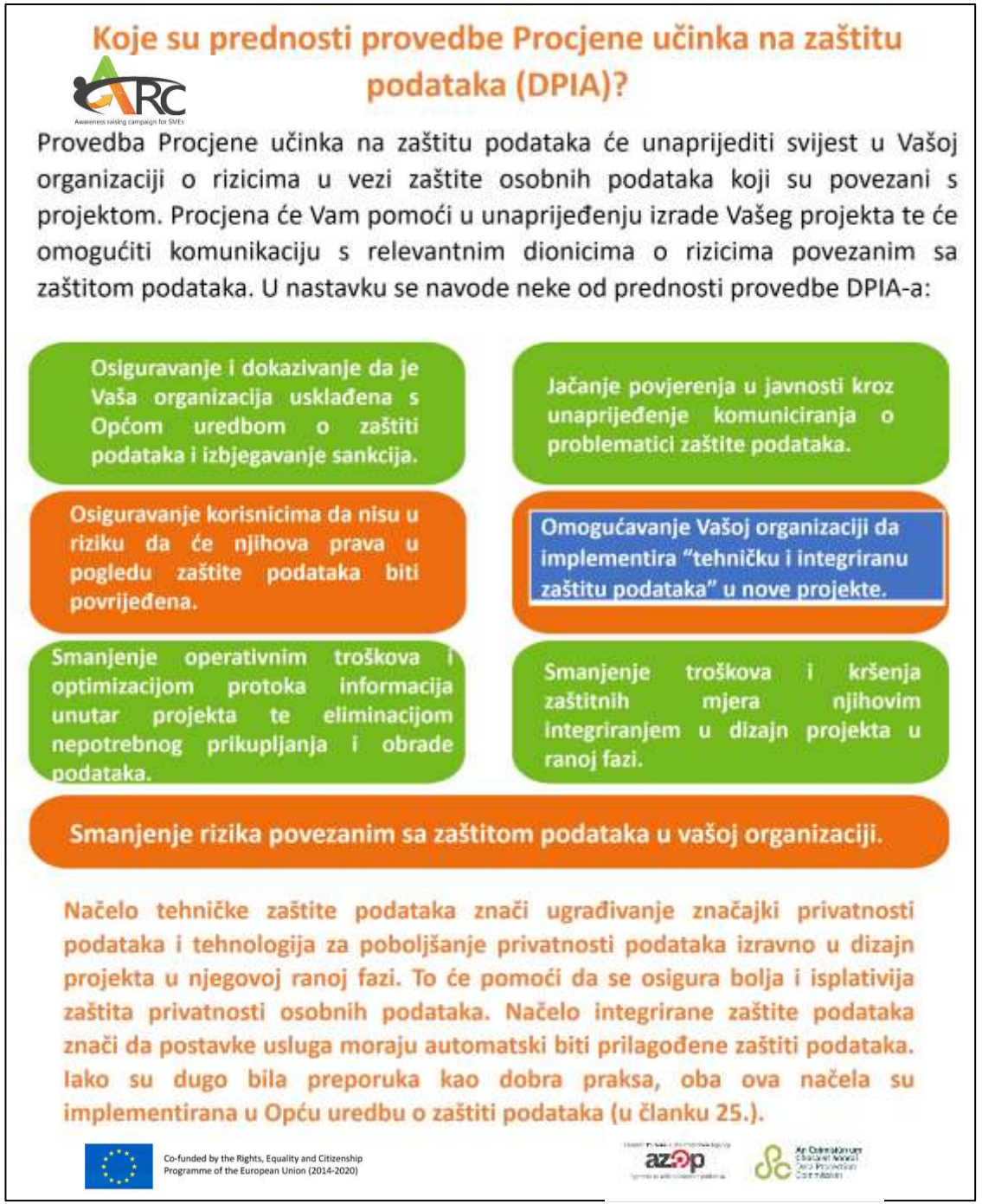
8) Kako uskladiti self check in sa GDPR-om, gost može iznajmljivaču natipkati podatke za prijavu u e-visitor, ali ako nismo na lokaciji, kako provjeriti istinitost tih podatka?

Ako niste na lokaciji, ne možete provjeriti istinitost podataka, istinitost se provjerava uvidom u osobnu iskaznicu/putovnicu. Voditelj obrade mora dokazati pouzdanost, dakle usklađenost s Općom uredbom o zaštiti podataka. Konkretan način kako će to učiniti nije propisan, ali postoje različite mogućnosti, kao što su korištenje provjerenih aplikacija i online sustava za rezervacije koji obrađuju osobne podatke u skladu s GDPR-om.

10) M visitor aplikacija bi riješila puno tih pitanja, ali je zasad ne koriste sve Turističke zajednice, zašto se ne omogući svim iznajmljivačima korištenje te aplikacije, odnosno ne pokrene inicijativa od strane HTZ-a? Agencija nadzire provedbu Opće uredbe o zaštiti podataka i Zakona o provedbi Opće uredbe o zaštiti podataka. Omogućavanje korištenje aplikacije/pokretanje inicijative nije u nadležnosti Agencije. Na web stranici M visitor nema politike privatnosti niti ikakvih informacija o tehničkim i organizacijskim mjerama poduzetim u svrhu zaštite osobnih podataka korisnika aplikacije.

11) Vaše mišljenje o korištenju inCheckin i sličnih mobilnih aplikacija za prijavu gostiju i na što iznajmljivač apartmana treba pripaziti prilikom ugovaranja takve usluge?

Ono što je bitno kod takvih aplikacija je da su usklađene s GDPR-om, da poštuju načela obrade osobnih podataka, da je obrada putem takvih aplikacija sigurna. Voditelj obrade koji koristi takve aplikacije mora poduzeti odgovarajuće tehničke i organizacijske mjere kojima se osigurava da integriranim načinom budu obrađeni samo osobni podaci koji su nužni za svaku posebnu svrhu obrade. Ta se obveza primjenjuje na količinu prikupljenih osobnih podataka, opseg njihove obrade, razdoblje pohrane i njihovu dostupnost. Točnije, takvim se mjerama osigurava da osobni podaci nisu automatski, bez intervencije pojedinca, dostupni neograničenom broju pojedinca (članak 25 GDPR-a, *privacy by design and by default*). **Voditelj obrade (iznajmljivač apartmana) koji ugovara takve usluge mora s izvršiteljem obrade sklopiti ugovor kojim će biti propisane, između ostalog, adekvatne tehničke i organizacijske mjere.**




- ✓ Razvoj aplikacija bi trebao biti napravljen na odgovoran način, s dokumentiranim svim mehanizmima ugrađene tehničke i integrirane zaštite osobnih podataka.
- ✓ Proizvođač aplikacije treba procijeniti rizike povezane s obradom podataka (provesti procjenu učinka na zaštitu podataka) i primijeniti odgovarajuće tehničke i organizacijske mjere zaštite.
- ✓ Voditelj obrade koji aplikaciju namjerava koristiti treba procijeniti je li aplikacija sigurna za korištenje, odnosno postoje li rizici za prava pojedinaca i jesu li poduzete adekvatne mjere kako bi se ti rizici sveli na najmanju moguću mjeru.