

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

Usklađivanje poslovnih procesa s GDPR-om: u čemu poduzetnici najviše griješe i kako prestati griješiti?

Slavonski Brod, Vinkovci, Antunovac 5.-7.rujna 2023.



Croatian Personal Data Protection Agency

azap
Agencija za zaštitu osobnih podataka



GPDP

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

foi



UNIVERSITÀ
DEGLI STUDI
FIRENZE

VUB

VRIJE
UNIVERSITEIT
BRUSSEL



**„U čemu
poduzetnici
griješe i kako
tome
doskočiti?“**

PROBLEM 1. - PODUZETNICI NE ZNAJU GDJE SU OSOBNI PODACI KOJE OBRAĐUJU

Primjer:

Slastičarnica prodaje kolače i torte na (1) fizičkim prodajnim mjestima i putem (2) webshopa.

Aktivno koristi društvene mreže i ima službene profile na Facebook-u i Instagramu putem kojih ponekad organizira nagradne natječaje s odličnim odazivom.

Prije prve kupnje u prodavaonici ili prilikom registracije u webshop, kupcima se nudi učlanjenje u program vjernosti (loyalty) gdje skupljanjem bodova ostvaruju popuste na buduće kupnje i informira ih se o akcijama i proizvodima koji bi ih mogli zanimati putem newslettera.

Kupci kolače i torte za različite prigode mogu i unaprijed naručiti telefonom ili online, a preuzeti ih mogu osobno ili im se šalju dostavnom službom.

U organizaciji poslovanja tvrtka koristi interni CRM sustav te poznati knjigovodstveni program.

Poslovni prostori su u zakupu, a za zaštitu pojedinih poslovnica od provala koristi se videonadzor sa sustavom pohrane koji je u njenom vlasništvu.

Pitanje za raspravu: Gdje su osobni podaci?

RJEŠENJE – KAKO DOSKOČITI PROBLEMU BROJ 1.

A. MAPIRANJE PODATAKA (3 KLJUČNA PITANJA)

✓ Čije osobne podatke obrađujete?

npr. zaposlenika, klijenata, korisnika usluga

✓ koje osobne podatke prikupljate?

npr. ime i prezime, OIB, broj osobne iskaznice, adresa, e-mail, fotografija, videosnimke, IP adresa, podaci o lokaciji, podaci o plaći itd.

✓ Gdje se ti osobni podaci nalaze?

u papirnatom i digitalnom obliku

RJEŠENJE – KAKO DOSKOČITI PROBLEMU BROJ 1.

B . EVIDENCIJA AKTIVNOSTI OBRADE (VODIČ LINK NA: <https://arc-rec-project.eu/wp-content/uploads/2022/11/ARC-vodic-za-popunjavanje-evidencije-aktivnosti-obrade.pdf>)

OBVEZA:

- ✓ Više od 250 zaposlenika
- ✓ Neovisno o broju zaposlenika:
 - Ako će obrada vjerojatno prouzročiti visoki rizik za prava i slobode ispitanika (primjerice: 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 (primjerice: obrada osobnih podataka zaposlenika u svrhu isplate plaća od strane poslodavca),
 - Ako obrada uključuje posebne kategorije podataka (primjerice: zdravstveni podaci, biometrijski podaci, genetski podaci),
 - Ako obrada uključuje osobne podatke u vezi s kaznenim osudama i kažnjivim djelima

Svakako vam preporučamo da ipak vodite evidenciju aktivnosti obrada!

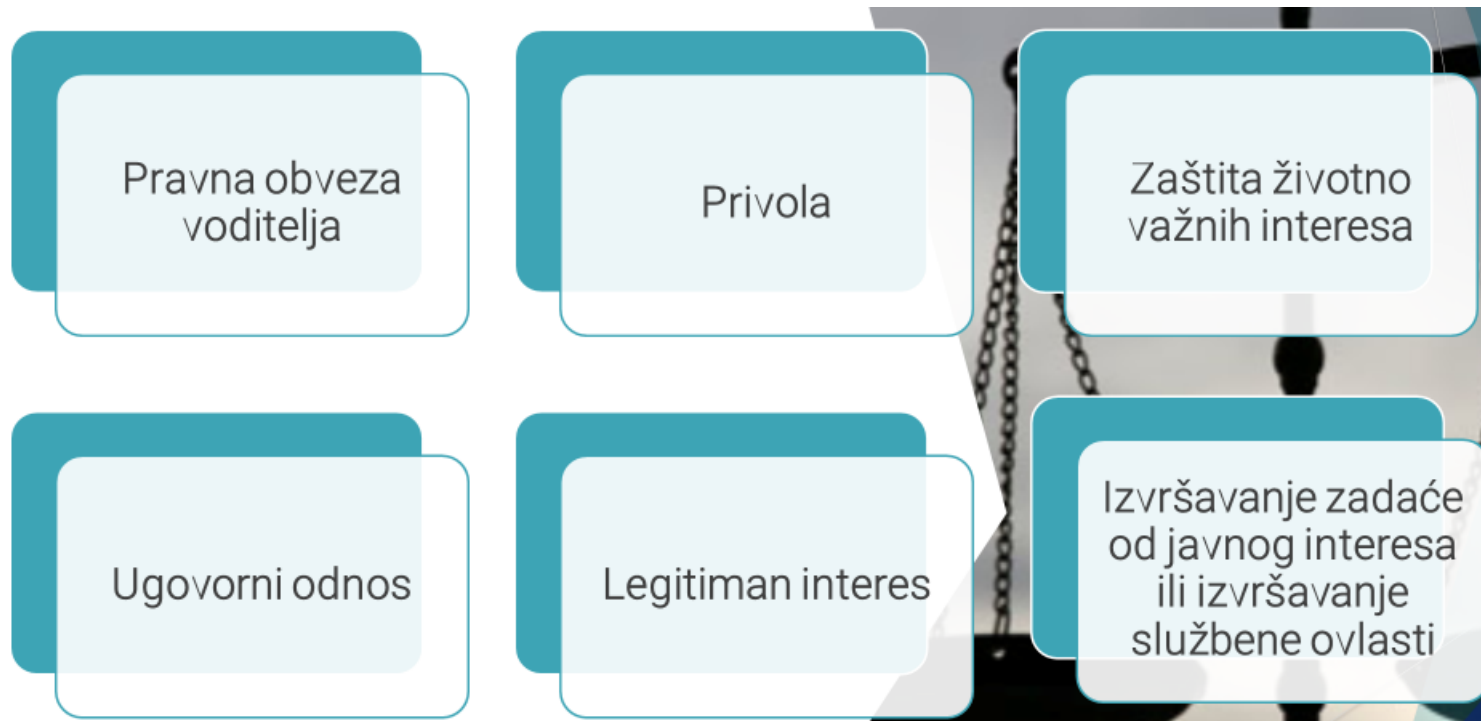
A	B	C	D	E	F	G	H	I
NAZIV OBRADE	KATEGORIJE ISPITANIKA	IZVRŠITELJ OBRADE	SVRHA OBRADE	IT SERVIS ili FIZIČKO MJESTO POHRANE (LOKACIJA OSOBNIH PODATAKA)	PRAVNA OSNOVA OBRADE (Članak 6. GDPR-a)	Prava dostupna ispitaniku	POVEZNICA NA DOKAZ O PRIVOLI	KATEGORIJE OSOBNIH PODATAKA
Naziv pod kojim je obrada prepoznatljiva	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, z...
Primjer: 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) Zakon o radu (NN 93/2014, 127/2017, 98/2019, 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 O OSOBNOSTI (ime, prezime, rođenje, spol, prebivalište, boravište), PODACI O OBRADOVANOJ OBRADI (stručno obrazovanje, radni staž, radni odnos, datum prestanka radnog odnosa, datum prestanka radnog odnosa, datum prestanka radnog odnosa, datum prestanka radnog odnosa)
Primjer: 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		Nije primjenjivo	IDENTIFIKACIJSKI PODACI O OSOBNOSTI (ime, prezime, rođenje, spol, prebivalište, boravište), PODACI O OBRADOVANOJ OBRADI (stručno obrazovanje, radni staž, radni odnos, datum prestanka radnog odnosa, datum prestanka radnog odnosa, datum prestanka radnog odnosa, datum prestanka radnog odnosa)
Primjer: EVIDENCIJA KANDIDATA ZA ZAPOSŁJAVANJE	Kandidati za posao	Agencija za zapošljavanje	Provođenje selekcijskog postupka i zapošljavanje	mapa pod nazivom kandidati za zapošljavanje u ERP-u, zaštićena šifrom	Prethodne radnje za sklapanje ugovora (Čl. 6. st. 1. t. b) GDPR-a)/Privola (Čl. st. 1. t. a) GDPR-a)		Nije primjenjivo	IDENTIFIKACIJSKI PODACI O OSOBNOSTI (ime, prezime, rođenje, spol, prebivalište, boravište), PODACI O OBRADOVANOJ OBRADI (stručno obrazovanje, radni staž, radni odnos, datum prestanka radnog odnosa, datum prestanka radnog odnosa, datum prestanka radnog odnosa, datum prestanka radnog odnosa)

PROBLEM 2. - PODUZETNICI NE ZNAJU ODREDITI PRAVNI TEMELJ ZA OBRADU PODATAKA

Primjer:

- ✓ Novog zaposlenika traži se privola kako bi se osobni podaci mogli obraditi u svrhe obvezne prijave na mirovinsko i zdravstveno osiguranje
- ✓ Obrada se „definira” legitimnim interesom poduzeća, bez da se proveo test legitimnog interesa (dokazivanje legitimnog interesa)
- ✓ Obrada je temeljena na ugovoru, makar stranka ugovora nije ispitanik (primjerice, dvije pravne osobe razmjenjuju podatke o ispitaniku)

PROBLEM 2. - PODUZETNICI NE ZNAJU ODREDITI PRAVNI TEMELJ ZA OBRADU PODATAKA



RJEŠENJE – KAKO DOSKOČITI PROBLEMU BROJ 2.

Poduzeća **MORAJU** poznavati propise koji uređuju djelatnost kojom se bave!

Primjer:

a. Poduzeće je hotel

Hotel upisuje sljedeće podatke u sustav eVisitor: prezime i ime, mjesto, država i datum rođenja, državljanstvo, vrsta i broj isprave o identitetu, prebivalište (boravište) i adresa, datum i vrijeme dolaska u object, predviđeni datum odlaska iz objekta, datum i vrijeme odlaska iz objekta, spol.

Pravni temelj je pravna obveza sukladno Pravilnik o sustavu eVisitor (NN 43/20)

b. Poduzeće je knjigovodstveni ured

Ured čuva: isplatne liste, analitička evidencija o plaćama za koje se plaćaju obvezni doprinosi – trajno, isprave na temelju kojih su podaci uneseni u dnevnik i glavnu knjigu – najmanje jedanaest godina, isprave na temelju kojih su podaci uneseni u pomoćne knjige – najmanje jedanaest godina.

Pravni temelj je pravna obveza sukladno Zakonu o računovodstvu (NN NN 78/15, 134/15, 120/16, 116/18, 42/20, 47/20, 114/22, 82/23)

PRIVOLA KAO PRAVNI TEMELJ ZA OBRADU PODATAKA

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.

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

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

LEGITIMAN INTERES KAO KAO PRAVNI TEMELJ ZA OBRADU PODATAKA

Primjeri obrada koje se mogu temeljiti na legitimnom interesu:

- izravni marketing i drugi oblici marketinga ili oglašavanja
- Videonadzor

Provjeriti jesu li interesi ispitanika ili njihova temeljna prava jača u odnosu na naš ravnoteže

legitimni interes – provođenjem testa

<https://arc-rec-project.eu/obraci/>

- Prigovor

PRIMJER: TEST RAZMJERNOSTI (DOKAZIVANJE LEGITIMNOG INTERESA)

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 koristiti 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 OBRADUJU 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: PREVLAĐAVAJU LI PRAVA I SLOBODE GOSTIJU 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 legitiman interes voditelja obrade prevladava nad interesom za zaštitu osobnih podataka 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 primiti ove

PROBLEM 3. - PODUZETNICI NISU DOVOLJNO TRANSPARENTNI PREMA OSOBAMA ČIJE OSOBNE PODATKE OBRAĐUJU

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.

Dužnost korištenja jednostavnog i lako razumljivog jezika, sažet oblik

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

RJEŠENJE – KAKO DOSKOČITI PROBLEMU BROJ 3.

- Izrada politike privatnosti/izjave o obradi osobnih podataka + objava 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. frizerski studio nema web stranicu, isprintani primjerci izjave o privatnosti bit će gostima dostupni na recepciji ili prostoriji za čekanje)

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

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 OBRADU:

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 OBRADUJEMO:

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 obrađujete¹.

- 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 OBRADU, 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 u 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 posjetiteljima Zakon 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 šaljemostima 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 stranicama koriste se tehnički kolačići (obavezni kolačići, ne mogu se isključiti) koji su nužni za funkcioniranje Internet mjesta, analitički i marketinški kolačići u svrhe poboljšanja i promocije naših usluga, poboljšanje učinkovitosti 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

Uputa

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 osobe 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 OBRADUJEMO:

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.

Navedena prava nisu primjenjiva u mjeri u kojoj je obrada nužna: 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/ZAHTEJEV-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 PRIMATELJIMA² 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.

PROBLEM 4. - PODUZETNICI IGNORIRAJU ZAHTJEVE ZA PRAVIMA ISPITANIKA

- VAŽNO JE DA SU ISPITANICI UPOZNATI SA SVOJIM PRAVIMA
- Voditelj obrade odgovara na upite bez odgađanja, najkasnije u roku od MJESEC dana (može se produljiti)
- Poduzeće može (u određenim slučajevima) naplatiti razumnu naknadu ili odbiti rješavati po zahtjevu

PROBLEM 4. - PODUZETNICI IGNORIRAJU ZAHTJEVE ZA PRAVIMA ISPITANIKA

KOJA PRAVA POSTOJE?

- ✓ PRAVO NA PRISTUP OSOBNIM PODACIMA (KOJI SE ODNOSE NA IPITANIKA)
- ✓ PRAVO NA ISPRAVAK
- ✓ PRAVO NA BRISANJE („pravo na zaborav“)
- ✓ PRAVO NA OGRANIČENJE OBRADE
- ✓ PRAVO NA PRENOSIVOST PODATAKA („data portability“)
- ✓ PRAVO NA PRIGOVOR
- ✓ PRAVO USPROTIVITI SE DONOŠENJU AUTOMATIZIRANIH POJEDINAČNIH ODLUKA, UKLJUČUJUĆI IZRADU PROFILA

pravo na zaštitu osobnih podataka NIJE APSOLUTNA

test ravnoteže sa ostalim pravima

RJEŠENJE – KAKO DOSKOČITI PROBLEMU BROJ 4.

Ako u svom poslovanju koristite web stranicu, najbolje bi bilo da na web stranici imate dostupan obrazac putem kojeg ispitanik može ostvariti svoja prava!

ZAHTEJEV 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:

PROBLEM BROJ 5. - PODUZEĆE NE PROVODI (USPJEŠNO):

ORGANIZACIJSKE MJERE ZAŠTITE

odnose se na **dokumentirano uređenje** te **organizacijsku kulturu**, **poslovnu praksu i procese** unutar MSP na način da se internim aktima i ugovornim klauzulama uređuje područje zaštite osobnih podataka koje organizacija obrađuje te da se **aktivno procesno provodi** sukladno dokumentiranoj informaciji i da je u mogućnosti **nedvojbeno to dokazati**

TEHNIČKE MJERE ZAŠTITE

odnose se na **zaštitne mjere** koje se postavljaju na **fizička mjesta** te **IT sustave ili proizvode** koji se koriste unutar MSP ili u sklopu krajnjih proizvoda klijentima, a vezano uz ophođenje s podacima; ili tehničke mjere koje MSP **ugovorno regulira s trećim stranama** koje imaju uvid ili s kojima sudjeluje u obradi ili pohrani podataka, a da su sve od navedenih strana u mogućnosti **nedvojbeno to dokazati**



VJEŽBA: tehničke i organizacijske mjere

<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).

- ✓ Tehničke i organizacijske mjere provode se s obzirom na rizik. Procjenite rizik u vašem poduzeću za osobne podatke koje obrađujete.
- ✓ Ako se bavite visoko rizičnom djelatnošću (primjerice zdravstveni sektor, setor socijalne zaštite itd.), kada primjenjivo provedite procjenu učinka

<https://arc-rec-project.eu/wp-content/uploads/2021/10/Vodic-za-procjenu-ucinka-na-zastitu-podataka-za-SMEs.pdf>



Pauza za Anketu (10 min)

Važno!

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

Izabрати u izborniku hrvatski jezik

Padajući izbornik je u gornjem desnom kutu ekrana
Informacije o projektu:

Referentna oznaka: 101072630

Vrsta aktivnosti: osposobljavanje

Naziv: „Kako se pripremiti za nadzor AZOP-a?“

Datum: 05/09/2023

Trajanje događanja u danima: 1

Je li se događanje održalo fizički ili na internetu: fizički

Mjesto događanja: Slavonski Brod

Spremi sigurnosnu kopiju na lokalnom računalu (onemogućiti ako se upotrebljava javno/zajedničko računalo).

Pravosuđe, prava i vrijednosti 2021. - 2027.

Polja označena zvjezdicom (*) obvezna su.

Stranice **Program** Kvaliteta i djelotvornost Opća pitanja Osobni podaci

1 Informacije o projektu

* 1.1 Referentna oznaka projekta
101072630

* 1.2 Vrsta aktivnosti:
 osposobljavanje uzajamno učenje informiranje

1.3 Naziv događanja:
Kako se pripremiti za nadzor AZOP-a?

1.4 Datum događanja:
05/09/2023

* 1.5 Trajanje događanja u danima:
1

1.6 Je li se događanje održalo fizički ili na internetu?
 fizički na internetu Hibrid

1.7 Mjesto događanja:
Slavonski Brod, Velika vijećnica Brodsko-posavske županije, Petra Krešimira IV 1

Prikazi
[Standard](#) Način rada posebne dostupnosti

Jezici
hrvatski

Kontakt
[Obrazac za kontakt](#)

[Spremi kao nacrt](#)

Posljednji put spremljeno
03/09/2023 20:06:27

[Prijava zlouporabe](#)

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

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

Izabрати u izborniku hrvatski jezik

Padajući izbornik je u gornjem desnom kutu ekrana

Informacije o projektu:

Referentna oznaka: 101072630

Vrsta aktivnosti: osposobljavanje

Naziv: „Kako se pripremiti za nadzor AZOP-a?“

Datum: 06/09/2023

Trajanje događanja u danima: 1

Je li se događanje održalo fizički ili na internetu: fizički

Mjesto događanja: Vinkovci

Polja označena zvjezdicom (*) obvezna su.

Stranice Program Kvaliteta i djelotvornost Opća pitanja Osobni podaci

1 Informacije o projektu

* 1.1 Referentna oznaka projekta
101072630

* 1.2 Vrsta aktivnosti:
 osposobljavanje uzajamno učenje informiranje

1.3 Naziv događanja:
„Kako se pripremiti za nadzor AZOP-a?“

1.4 Datum događanja:
06/09/2023

* 1.5 Trajanje događanja u danima:
1

1.6 Je li se događanje održalo fizički ili na internetu?
 fizički na internetu Hibrid

1.7 Mjesto događanja:
Vinkovci

Sljedeće

Jezici
hrvatski

Kontakt
Obrazac za kontakt

Spremi kao nacrt

Posljednji put spremijeno
03/09/2023 20:06:27

[Prijava zlouporabe](#)

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

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

Izabрати u izborniku hrvatski jezik

Padajući izbornik je u gornjem desnom kutu ekrana
Informacije o projektu:

Referentna oznaka: 101072630

Vrsta aktivnosti: osposobljavanje

Naziv: „Kako se pripremiti za nadzor AZOP-a?“

Datum: 07/09/2023

Trajanje događanja u danima: 1

Je li se događanje održalo fizički ili na internetu: fizički

Mjesto događanja: Antunovac

Polja označena zvjezdicom (*) obvezna su.

Stranice: Program | Kvaliteta i djelotvornost | Opća pitanja | Osobni podaci

1 Informacije o projektu

* 1.1 Referentna oznaka projekta
101072630

* 1.2 Vrsta aktivnosti:
 osposobljavanje uzajamno učenje informiranje

1.3 Naziv događanja:
„Kako se pripremiti za nadzor AZOP-a?“

1.4 Datum događanja:
07/09/2023

* 1.5 Trajanje događanja u danima:
1

1.6 Je li se događanje održalo fizički ili na internetu?
 fizički na internetu Hibrid

1.7 Mjesto događanja:
Antunovac

Sjedeće

Jezici
hrvatski

Kontakt
Obrazac za kontakt

Spremi kao nacrt

Posljednji put spremljeno
03/09/2023 20:06:27

[Prijava zlouporabe](#)

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

“Kako se pripremiti za nadzor AZOP-a?”

Slavonski Brod, 5. rujna 2023.



Croatian Personal Data Protection Agency



GDPD

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

foi



UNIVERSITÀ
DEGLI STUDI
FIRENZE



VRIJE
UNIVERSITEIT
BRUSSEL



**„Nadzorne i istražne
aktivnosti AZOP-a:
što morate znati i
kako se pripremiti?“**

Istražne ovlasti Agencije

- ✓ narediti voditelju obrade i izvršitelju obrade, da mu pruže sve informacije potrebne za obavljanje svojih zadaća
- ✓ provoditi istrage u obliku revizije implementacije zaštite podataka
- ✓ provoditi preispitivanje certifikata
- ✓ obavijestiti voditelja obrade ili izvršitelja obrade o mogućem kršenju Uredbe
- ✓ ishoditi, od voditelja obrade i izvršitelja obrade, pristup svim osobnim podacima i svim informacijama potrebnim za obavljanje svojih zadaća
- ✓ ishoditi pristup svim prostorijama voditelja obrade i izvršitelja obrade, uključujući svu opremu i sredstva za obradu podataka

- ✓ napraviti preslike dostupnih dokumenata, presnimiti sve sadržaje sustava pohrane i prikupiti druge relevantne informacije,
- ✓ oduzeti potrebne sustave pohrane i opremu koja sadržava druge relevantne informacije i zadržati je koliko je potrebno za izradu preslika te dokumentacije (do 15 dana / ako iz tehničkih razloga nije moguće tijekom nadzora napraviti preslike potrebne dokumentacije),
- ✓ zapečatiti sustave pohrane ili opremu za vrijeme nadzora i u opsegu prijeko potrebnom za provedbu nadzornih aktivnosti ako postoji opasnost od uništenja ili izmjena dokaza (do 15 dana),
- ✓ o istome je ovlaštena osoba dužna sastaviti službenu zabilješku sa svim relevantnim informacijama primjerak predati nadziranom subjektu.

Nadzorne ovlasti Agencije

- ✓ provedba neizravne nadzorne aktivnosti (provjera javno dostupnih podataka,...)
- ✓ traženje dostave informacija i relevantne dokumentacije
- ✓ provedba izravne nadzorne aktivnosti
 - najavljeni nadzor
 - nenajavljeni nadzor
- ✓ ako se kod provođenja nadzora očekuje njegovo ometanje pružanjem otpora, Agencija će uputiti pisani zahtjev ministarstvu unutarnjih poslova za pružanje pomoći pri provođenju tih nadzornih aktivnosti

Neizravne nadzorne aktivnosti

- ✓ provjera usklađenosti javno dostupnih podataka/usluga kojima voditelj obrade obrađuje osobne podatke s zakonskim odredbama o zaštiti osobnih podataka (npr. na Internet stranici Politika privatnosti, privola za kolačiće, tehničke mjere zaštite,...)
- ✓ provjera evidencije o dostavi izvješća o imenovanju službenika za zaštitu podataka Agenciji
- ✓ provjera evidencija o dostavi Izvješća o povredi osobnih podataka Agenciji (kod javne objave iz koje proizlazi događanje povreda osobnih podataka)
- ✓ provjera evidencija o provedenom Prethodnom savjetovanju

Po utvrđenju nesukladnosti provode se izravne nadzorne aktivnosti ili se traži dostava informacija od voditelja/izvršitelja obrade.

Kada Agencija provodi nadzorne aktivnosti

Agencija provodi nadzorne aktivnosti temeljem:

- ✓ **zahtjeva za zaštitu prava ispitanika**
- ✓ **prijave građana ili institucija o mogućoj povredi obrade osobnih podataka**
- ✓ **izvješća o povredama osobnih podataka**
- ✓ **godišnjeg plana nadzornih aktivnosti**
- ✓ **saznanja iz javno dostupnih izvora**
- ✓ **mehanizama međunarodne suradnje**

Najčešći upiti/zahtjevi/prijave povreda ispitanika

- ✓ **transparentnost, dostupnost i ažurnost informacija o obradi osobnih podataka ispitanika**
- ✓ **neadekvatni poslovni procesi upravljanja zahtjevima ispitanika (politike upravljanja privolama / prikupljanja - povlačenja istih, poštivanje rokova za postupanje po zahtjevima, brisanje podataka)**
- ✓ **neodgovarajuće tehničko organizacijske mjere**

Kako umanjiti rizik od nastupa povreda

- ✓ imenovanje službenika za zaštitu podataka (kompetencije uz prepoznati značaj istog unutar organizacije).
- ✓ detaljna analiza poslovnih procesa (data mapping, data flow, analiza rizika) – Evidencija aktivnosti obrade.
- ✓ kod donošenja novih poslovnih odluka / uvođenja novih poslovnih procesa posebnu pozornost obratiti na sveobuhvatnost utjecaja istih na prava i slobode ispitanika (risk management).

Kako se pripremiti za nadzor

- ✓ uključiti službenika za zaštitu podataka
- ✓ pripremiti/dostaviti informacije i relevantnu dokumentaciju vezanu za predmet nadzornog postupanja
- ✓ opsežnost nadzora ovisna je o opsegu utvrđenja moguće povrede zakona pa stoga po potrebi:
 - ✓ uključiti nositelja određenih poslovnih procesa
 - ✓ uključiti izvršitelja obrade kod nadzorne aktivnosti (odgovornost za pojedine poslovne procese)
- ✓ surađivati s nadzornim tijelom i poštovati zadane rokove

Što pripremiti

- ✓ odluku o zastupanju ili punomoć odvjetniku, odluku o imenovanju službenika za zaštitu podataka
- ✓ Evidencija aktivnosti obrade
- ✓ interni akti kojima je regulirana zaštita osobnih podataka – prava ispitanika / prava i obveze zaposlenika organizacije (Pravilnik o zaštiti osobnih podataka, Politika privatnosti, Obavijest/informacije koje se pružaju ispitanicima o njihovim pravima)
- ✓ akte (organizacijske mjere) iz kojih su vidljive ovlasti zaposlenika ili vanjskih suradnika i način upravljanja istima (Ugovor, Politika upravljanja/dodjele ovlaštenja) – neposredna provjera razine ovlaštenja pristupa
- ✓ Izjave o povjerljivosti

Što pripremiti

- ✓ **podatke i dokumentaciju u odnosu na povezana društva koja imaju ovlaštenja pristupa sustavima pohrane osobnih podataka**
 - **ugovor s Izvršiteljem obrade**
 - **upute dane u svezi konkretne obrade osobnih podataka – nadzorno postupanje i kod izvršitelja obrade**
 - **razine ovlaštenja pristupa i načina pristupa – provjera uvidom u logove**
 - **nadzor nad provođenjem uputa voditelja obrade**
 - **dokaz da izvršitelj obrade jamči odgovarajuću razinu zaštite osobnih podataka**
- ✓ **Procjena učinka na zaštitu podataka**
- ✓ **drugu relevantnu dokumentaciju odnosnu na sam događaj**

Što pripremiti

- ✓ **interne akte odnosne na tehničke mjere zaštite (npr. Pravilnik o informacijskoj sigurnosti, Pravilnici kojima se uređuje obrada pojedinih zbirki podataka (npr. pravilnik o videonadzoru, pravilnik o evidenciji radnog vremena, Politika sigurnog korištenja Interneta,...) i sl. – neposredna provjera implementacije istih (dozvola pristupa samo ovlaštenim osobama, mogućnost korištenja USB portova, bilježenja logova prijenosa podataka, bilježenje pristupa evidencijama, alarmiranja u slučaju neovlaštenog pristupa, mogućnost udaljenog povezivanja, edukacije zaposlenika i sl.)**
- ✓ **ukoliko je nadzorno postupanje temeljem Izvješća o povredi osobnih podataka, dokumentaciju u odnosu na vrijeme saznanja, izvješćivanje ispitanika, poduzete mjere za otklanjanje rizika – evidencija povreda osobnih podataka**

Što pripremiti

- ✓ ako je nadzorno postupanje na temelju zahtjeva za utvrđivanjem povrede prava, dokumentaciju odnosnu na predmetni slučaj i ispitanika posebice u odnosu na način prikupljanja, dokazivanje pravne osnove za obradu (zakonski propisi/test razmjernosti) i svrhe prikupljanja osobnih podataka ispitanika uključivo
 - korespondenciju između društva i ispitanika uz provjeru evidencije zahtjeva ispitanika (pristup i pregled sandučiću e-pošte)
 - dokumentaciju iz koje je vidljiva zakonitost obrade uz preslike osobnih dokumenata ukoliko su isti prikupljeni
 - dokumentaciju odnosna na videonadzorni sustav ukoliko je isto predmet nadzornog postupanja

Primjeri loše prakse

- ✓ **neimenovanje / neuključenost / neadekvatan položaj službenika za zaštitu podataka**
- ✓ **donošenje / provedba poslovnih odluka bez analize rizika na prava i slobode ispitanika**
- ✓ **nakon početnog usklađenja organizacije ne ažuriraju / procjenjuju relevantnost primjenjivanih tehničko organizacijskih mjera**
- ✓ **kod početnog usklađenja nisu uzeti u obzir svi rizici niti je učinjena sveobuhvatna analiza poslovnih procesa što ima za rezultat nemogućnost adekvatnog praćenja svih okolnosti obrade osobnih podataka**
- ✓ **propisane tehničko organizacijske mjere zaštite se ne provode**

Primjeri loše prakse

- ✓ korištenje tehničkih rješenja zaštite sustava koji su neadekvatni riziku / zastarjeli (bilo od vanjske ugroze ili zlouporabe ovlaštenja unutar organizacije)
- ✓ korištenje Izvršitelja obrade biranog samo u odnosu na najbolju ponudu
- ✓ sklapanje samo poslovnog ugovora sa izvršiteljem obrade bez odredbi o obradi / zaštiti osobnih podataka ili bez davanja uputa izvršitelju obrade
- ✓ umanjivanje rizika kod procjene utjecaja određene obrade osobnih podataka na prava i slobode ispitanika
- ✓ neadekvatne politike / procedure upravljanja zahtjevima ispitanika
- ✓ neizvješćivanje nadzornog tijela o povredi osobnih podataka

Q&A

Hvala na pažnji!

Agencija za zaštitu osobnih podataka

<https://azop.hr/>
azop@azop.hr