

Na temelju članka 40. Statuta Agencije za društveno poticanu stanogradnju Grada Rijeke od 31.01.2006. g., Izmjene i dopune Statuta Agencije za društveno poticanu stanogradnju Grada Rijeke od 08.07.2010. g., te temeljem čl. 32. Opće uredbe o zaštiti podataka (EU) 2016/679, ravnatelj Agencije za društveno poticanu stanogradnju Grada Rijeke (u daljnjem tekstu: Agencija) uz prethodnu suglasnost Upravnog vijeća Agencije donosi:

## **PRAVILNIK o zaštiti osobnih podataka**

### **I. OPĆE ODREDBE**

#### **Članak 1.**

Ovim pravilnikom se određuju organizacijski, tehnički i logično tehnički postupci i mjere za zaštitu osobnih podataka Agencije s ciljem da se spriječi slučajno ili namjerno neovlašteno uništavanje podataka, njihova izmjena ili gubitak, kao i neovlašten pristup, obrada, uporaba ili posredovanje osobnih podataka.

Zaposlenici i vanjski suradnici, koji pri svojem radu obrađuju i upotrebljavaju osobne podatke, moraju biti upoznati sa Zakonom o provedbi Opće uredbe o zaštiti podataka (ZPOUZP), Općom uredbom o zaštiti podataka (EU) 2016/679 (u nastavku: Uredba), s područnim zakonodavstvom koje uređuje pojedinačno područje njihovog rada i sa sadržajem ovog pravilnika.

U slučaju sumnje ili kontradiktornosti u objašnjenju stupnja, opsega i načina zaštite osobnih podataka smisleno se upotrebljavaju standardi ISO/IEC 27001, ISO/IEC 27002 ili drugi međunarodno priznati standardi zaštite informacija.

#### **Članak 2.**

U ovom pravilniku upotrijebljeni izrazi imaju jednako značenje kako je određeno čl. 4. Uredbe.

### **II. ZAŠTITA PROSTORA I RAČUNALNE OPREME**

#### **Članak 3.**

Prostorije u kojima se nalaze nositelji osobnih podataka, strojna i programska oprema (zaštićeni prostori), moraju biti osigurani organizacijskim i fizičkim i/ ili tehničkim mjerama, koje onemogućuju neovlaštenim osobama pristup podacima.

Nadležna služba zadužena za informacijsku sigurnost izrađuje nacrt sigurnosnih zona za sve fizičke lokacije društva i njih određuje uzimajući u obzir količinu i osjetljivost podataka koji se nalaze u pojedinoj sigurnosnoj zoni. Na temelju izrađenog nacrta, navedena služba određuje pisana pravila postupanja s osobnim podacima po pravilima koja propisuje ovaj pravilnik te pritom uzima u obzir prirodu posla zaposlenih odnosno njihove radne zadatke.

Nadležna služba, zadužena za informacijsku sigurnost periodično, najmanje jednom u 3 (tri) mjeseca, provjerava ispravnost pristupa do sigurnosnih zona i o eventualnim odstupanjima obavještava Službenika za zaštitu osobnih podataka.

Pristup je moguć samo u redovnom radnom vremenu, izvan toga samo na temelju odobrenja ravnatelja Agencije.

Ključevi osiguranih prostora se koriste i čuvaju u skladu s kućnim redom. Ključevi se ne ostavljaju u bravi vrata s vanjske strane, ili na drukčiji način koji bi omogućavao pristup neovlaštenim osobama.

Osigurani prostori ne smiju ostajati bez nadzora, odnosno moraju se zaključavati u odsutnosti zaposlenika koji ih nadziru.

Izvan radnog vremena ormari i pisaći stolovi s nositeljima osobnih podataka moraju biti zaključani, računala i druga strojna oprema isključeni i fizički ili programski zaključani.

Zaposlenici ne smiju puštati nositelje osobnih podataka (uključujući papire) na stolovima u prisutnosti osoba koje nemaju ovlaštenja uvida u iste. Svaki puta kada zaposlenik napusti svoje radno mjesto mora osigurati da se na stolu ili drugoj radnoj površini ne nalaze osobni podaci (politika »čistog stola«).

Nositelji osobnih podataka koji se nalaze izvan osiguranih prostora (hodnici, prostorije za okupljanje) moraju stalno biti zaključani.

Posebne vrste osobnih podataka se ne smiju čuvati izvan zaštićenih prostorija.

Zaposlenici mogu obrađivati samo one osobne podatke za obradu koji ih zaduži ovlašteni nadređeni ili odgovorna osoba za pojedinačnu zbirku osobnih podataka.

#### **Članak 4.**

U prostorijama koje su namijenjene poslovanju sa strankama, nositelji osobnih podataka i računalni prikazi namješteni tako da stranke nemaju uvida u iste.

#### **Članak 5.**

Održavanje i popravak strojne računalne i druge opreme je dozvoljeno samo uz znanje ovlaštene osobe, izvode ga samo ovlašteni servisi i održavatelji koji s **Agencijom** imaju zaključen odgovarajući ugovor.

#### **Članak 6.**

Održavatelji prostorija, strojne i programske opreme, posjetitelji i poslovni partneri se smiju kretati u osiguranim prostorijama samo uz znanje ovlaštene osobe. Zaposlenici kao što su čistačice, zaštitari i sl. se izvan radnog vremena kreću samo u onim zaštićenim prostorijama gdje je onemogućen uvid u osobne podatke (nositelji podataka su pohranjeni u zaključanim ormarima i pisaćim stolovima, računala i druga strojna oprema su isključeni ili na neki drugi način fizički ili programski zaključani).

### III. ZAŠTITA SISTEMSKE I APLIKATIVNO PROGRAMSKE RAČUNALNE OPREME TE PODATAKA KOJI SE OBRAĐUJU S RAČUNALNOM OPREMOM

#### Članak 7.

##### ***Pristup računalnom operativnom sistemu (logiranje na računalo)***

Na svakom računalu u Agenciji definiran je jedan korisnički profil ne personaliziranog korisničkog imena kojim se služe zaposlenici ovlaštene za pristup pojedinom računalu. Svaki zaposlenik u Agenciji ima svoje personalizirano korisničko ime s kojim se može prijaviti na bilo koje računalo u Agenciji i pristupiti svojem poštanskom sandučiću (pošti).

Korisnički profil zaštićen je korisničkom šifrom koju znaju osobe koje su ovlaštene za rad s računalom.

Svaki zaposlenik Agencije mora znati svoju korisničku šifru koja otvara njegov korisnički profil i ne smije je davati drugima.

Šifra ne smije biti zapisana na način da je npr. zalijepljena na monitor ili na bilo koji način lako dostupna neovlaštenom korisniku. Šifra se sastoji od minimalno 7 (sedam) znakova, velikih i malih slova, brojeva i simbola sukladno Pravilniku. Unutar korisničkog profila na računalu ne smiju se nalaziti osobni podaci koji su predmet zaštite GDPR-a, nego se isti isključivo nalaze unutar specijaliziranih aplikacija za poslovanje Agencije kojima je pristup strogo personaliziran.

#### Članak 8.

##### ***Antivirusni sustav***

Na svim računalima AGENCIJE instaliran je antivirusni sustav Symantec Endpoint Protection. Antivirusne definicije obnavljaju se svakodnevno putem interneta sa servera proizvođača softvera. Licence za cijelu ustanovu obnavljaju se jednom godišnje. Prilikom nabave novog računala ili reinstalacije postojećeg standardna je procedura instalacija i nadogradnja na trenutno najviši dostupni nivo navedenog antivirusnog softvera.

#### Članak 9.

##### ***Zaštita računalnog sustava od vanjskih upada***

Na svim računalima unutar AGENCIJE uključen je firewall koji je konfiguriran na način da omogućava izlaz na vanjske resurse koji su potrebni za rad AGENCIJE te da omogućava ulaz ovlaštenim djelatnicima i/ili partnerima (udaljenim korisnicima) u računalni sustav AGENCIJE. Povezivanje izvana u sustav AGENCIJE izvedeno je tako da korisnici Agencije trebaju biti članovi VPN grupe, imati instaliran Forticlient vpn program i konfiguriran na pravilan način tako da upisujući personalizirano korisničko ime i lozinku spajaju se u mrežu Grada i nakon toga pokreću vezu s udaljenim računalom za pristup svojem računalu u Agenciji.

## **Članak 10.**

### ***Udaljeni pristup informatičkom sustavu***

Svi korisnici udaljenog pristupa moraju imati instaliran antivirusni softver i mora im biti postavljena pristupna lozinka u skladu sa Pravilnikom. Svako računalo koje pristupa informatičkom sustavu AGENCIJE bilo direktno iz lokalne mreže (LAN) ili udaljenim pristupom (WAN) mora imati uključen i firewall na vlastitom operativnom sistemu.

## **Članak 11.**

### ***Zaštita baze podataka***

Osobni podaci korisnika koji se obrađuju od strane voditelja obrade koji je ujedno i izvršitelj obrade pohranjeni su na file server koji je u redovnom dnevnom i tjednom backupu i samo djelatnici Agencije imaju pristup tome.

O backupu se brine backup administrator i Veeam softver koji je instaliran na backup poslužitelj. Pristup poslužitelju i softveru ima samo backup administrator, a backupi se spremaju na trake koje svakih tjedan dana se fizički prenose u sef koji se nalazi na drugoj lokaciji od poslužitelja i koji je pod šifrom.

## **IV. USLUGE KOJE PRUŽAJU VANJSKE PRAVNE ILI FIZIČKE OSOBE**

### **Članak 12.**

Sa svakom vanjskom pravnom ili fizičkom osobom koja obavlja pojedinačne zadaće u svezi s prikupljanjem, obradom, pohranom ili posredovanjem osobnih podataka (izvršitelj obrade), sklapa se pisani ugovor predviđen u čl. 28. st. 3. Uredbe. Navedeno vrijedi i za vanjske osobe koje održavaju strojnu i programsku opremu te izdaju i namještaju novu strojnu ili programsku opremu.

Vanjske pravne ili fizičke osobe smiju pružati usluge obrade osobnih podataka samo u okviru od voditelja obrade izdanih ovlaštenja i određenog opsega vrste osobnih podataka te iste ne smiju obrađivati ili na drugi način koristiti ni za jednu drugu svrhu.

Ovlaštena pravna ili fizička osoba koja za **Agenciju** obavlja dogovorene usluge izvan prostorija voditelja obrade mora imati barem jednako strog način zaštite osobnih podataka kako ga predviđa ovaj pravilnik.

Prije sklapanja ugovora o obradi osobnih podataka potrebno je o tome obavijestiti Službenika za zaštitu osobnih podataka i uzeti u obzir njene preporuke.

Agencija za društveno poticanu stanogradnju Grada Rijeke vodi ažurnu evidenciju svih sklopljenih ugovora o obradi osobnih podataka.

## **V. ZAPRIMANJE I POSREDOVANJE OSOBNIH PODATAKA**

### **Članak 13.**

Zaposlenik koji je zadužen za zaprimanje i evidenciju pošte mora isporučiti poštansku pošiljku s osobnim podacima neposredno pojedinoj osobi ili službi na koju je ta pošiljka adresirana.

Zaposlenik koji je zadužen za zaprimanje i evidenciju pošte otvara i pregledava sve poštanske pošiljke i pošiljke koje na drugi način pristižu u Agenciju – donose ih stranke ili kuriri, osim pošiljaka iz stavaka 3. i 4. ovog članka.

Zaposlenik koji je zadužen za zaprimanje i evidenciju pošte ne otvara one pošiljke koje su naslovljene na drugu organizaciju i greškom su dostavljene te pošiljke koje su označene kao osobni podaci.

Zaposlenik koji je zadužen za zaprimanje i evidenciju pošte ne smije otvarati pošiljke naslovljene na zaposlenike, na kojima je na omotnici navedeno da se moraju uručiti osobno adresatu, i pošiljke na kojima je prvo navedeno osobno ime zaposlenika bez oznake njegova položaja i uz to naziv Agencije.

#### **Članak 14.**

Osobne podatke je dozvoljeno prenositi informacijskim, telekomunikacijskim i drugim sredstvima samo u sklopu provedbi postupaka i mjera koje neovlaštenim osobama sprječavaju prisvajanje ili uništenje podataka te neosnovano upoznavanje s njihovim sadržajem.

Posebne vrste osobnih podataka se fizički šalju adresatima u zatvorenim omotnicama preporučenom pošiljkom s povratnicom.

Osobni podaci se šalju preporučeno s povratnicom.

Omotnica u kojoj se posreduju osobni podaci mora biti izrađena na takav način da ne omogućuje da se na normalnoj svjetlosti ili pri osvjetljavanju omotnice običnim svjetlom može vidjeti sadržaj omotnice. Isto tako omotnica mora biti takva da otvaranje iste i upoznavanje sa sadržajem nije moguće obaviti bez vidljivog slijeda otvaranja omotnice.

#### **Članak 15.**

Obrada posebnih vrsta osobnih podataka mora biti posebno označena i zaštićena. Svaki dokument, datoteka ili mapa koja sadrži posebne vrste osobnih podataka mora biti označena natpisom »Posebne vrste osobnih podataka«.

Podaci iz prijašnjeg stavka se smiju posredovati preko telekomunikacijskih mreža samo ako su posebno zaštićeni kriptografskim metodama i elektronskim potpisom tako da je osigurana nečitljivost podataka tijekom njihovog prijenosa.

#### **Članak 16.**

Osobni podaci se posreduju samo onim korisnicima koji dokažu valjani zakonski osnov ili pisani zahtjev odnosno privolu pojedinca (punomoć) na kojeg se podaci odnose.

Za svako posredovanje osobnih podataka korisnik mora podnijeti pisanu izjavu, u kojoj jasno mora biti navedena odredba zakona ili Uredbe koja korisnika ovlašćuje na pridobivanje osobnih podataka, ili prijavi mora biti priložen pisani zahtjev odnosno privola pojedinca na kojeg se podaci odnose.

Svako posredovanje osobnih podataka se bilježi u evidenciji posredovanja, iz koje mora biti razvidno koji su osobni podaci bili posredovani, kome, kada i na kojoj osnovi.

Nikada se ne posreduju originali dokumenata, osim u slučaju pisane odluke suda. Originalni dokument se u vremenu odsutnosti mora nadomjestiti kopijom.

## VI. BRISANJE PODATAKA

### Članak 17.

Po isteku roka čuvanja ili svrhe obrade, osobni podaci se brišu, uništavaju, blokiraju ili anonimiziraju, osim ako je zakonom ili drugim propisom određeno drukčije.

### Članak 18.

Za brisanje podataka iz računalnih medija upotrebljava se takva metoda brisanja sukladno kojoj je nemoguća obnova svih ili dijela brisanih podataka.

Podaci na klasičnim medijima (papiri, kartoteke, registri, popisi) se uništavaju na način koji onemogućuje čitanje svih ili dijela uništenih podataka (spaljivanje, rezanje...).

Na jednak način se uništava pomoćno gradivo (npr. matrice, podloge, izračuni, grafikoni, skice, nacrti, probni odnosno neuspješni ispisi i sl.).

Zabranjeno je bacati otpadne nositelje podataka s osobnim podacima u koševе za smeće.

Pri prijenosu nositelja osobnih podataka na mjesto uništavanja, potrebno je osigurati adekvatno osiguranje i u trenutku prijenosa.

Prijenos nositelja podataka na mjesto uništavanja i uništavanje nositelja osobnih podataka nadzire osoba koju odredi nositelj privatne prakse i koja po provedenom uništenju sastavlja kratki zapisnik o načinu i temeljitosti uništenja.

## VII. DJELOVANJE PRILIKOM SUMNJE NA NEOVLAŠTEN PRISTUP I OBAVJEŠTAVANJE

### Članak 19.

Zaposlenici su dužni o aktivnostima koje su povezane s otkrivanjem ili neovlaštenom obradom osobnih podataka, zlonamjernom ili neovlaštenom uporabom, prisvajanjem, izmjenama ili oštećenjem odmah (najkasnije u roku 1 sat od saznanja o možebitnom incidentu ili štetnom slučaju) obavijestiti Službenika za zaštitu osobnih podataka te istovremeno sami pokušati takvu aktivnost spriječiti.

### Članak 20.

#### **(Obavještavanje ovlaštene osobe za zaštitu osobnih podataka)**

U slučaju povrede zaštite osobnih podataka, Službenik za zaštitu osobnih podataka mora najkasnije u roku 72 sata od saznanja o kršenju o tome službeno obavijestiti Središnje nadzorno tijelo – Agenciju za zaštitu osobnih podataka (dalje u tekstu: AZOP), osim ako nije vjerojatno da bi povredom zaštite osobnih podataka bila ugrožena prava i slobode pojedinaca.

Obavijest iz prethodnog stavka mora sadržavati:

- opis vrste povrede zaštite osobnih podataka, kategorije i približan broj obuhvaćenih pojedinaca na koje se odnose osobni podaci, te vrste i približan broj obuhvaćenih evidencija osobnih podataka;
- izvještaj o imenu i kontaktnim podacima ovlaštene osobe za zaštitu podataka ili drugim kontaktnim mjestima pri kojima je moguće dobiti više informacija;
- opis vjerojatnih posljedica povrede zaštite osobnih podataka;
- opis mjera koje Agencija donese ili donošenje kojih predlaže za saniranje povrede zaštite osobnih podataka, kao i mjera za ublažavanje eventualnih štetnih učinaka povrede, ako je to primjenjivo.

U slučaju da informacije iz prethodnog stavka nije moguće iznijeti u cijelosti, one se daju postupno, svakako u roku 1 sata od saznanja.

U slučaju da je do povrede zaštite osobnih podataka došlo kod izvršitelja obrade, isti je dužan najkasnije u roku 24 sata obavijestiti voditelja obrade. Takva odredba mora biti zapisana u svakom ugovoru o obradi podataka koji Agencija sklopi s izvršiteljem obrade.

Ovlaštena osoba koja ispituje incident odnosno otklanja eventualne posljedice incidenta mora dokumentirati svaku povredu zaštite osobnih podataka, uključujući radnje u svezi s povredom zaštite osobnih podataka, njene učinke i usvojene popravne mjere. Tu dokumentaciju je dužna pokazati AZOP-u, ako on to zahtijeva.

Svi zaposlenici koji rade na ispitivanju incidenta ili su na bilo koji način povezani s otklanjanjem posljedica incidenta, moraju ovlaštenu osobu za zaštitu podataka obavijestiti odmah, najkasnije u roku 1 sata, o svim informacijama povezanim s incidentom.

### **Članak 21.**

#### **(Obavještavanje ispitanika)**

Ako ovlaštena osoba za zaštitu podataka ocijeni da je vjerojatno da je povreda zaštite osobnih podataka prouzročila veliki rizik za prava i slobode pojedinaca, osoba ovlaštena za zaštitu podataka ili nadležna služba, koju ovlasti ravnatelj Agencije, mora najkasnije u roku 24 sata ispitaniku na kojeg se odnose osobni podaci dati informaciju o tome da je došlo do povrede osobnih podataka.

Izveštaj iz prethodnog stavka mora biti napisan jasnim i jednostavnim jezikom i mora sadržavati sljedeće informacije:

- informacije o imenu i kontaktnim podacima ovlaštene osobe za zaštitu podataka ili drugim kontaktnim mjestima putem kojih je moguće dobiti više informacija;
- opis vjerojatnih posljedica povrede zaštite osobnih podataka;
- opis mjera koje Agencija donese ili donošenje kojih predlaže za saniranje povrede zaštite osobnih podataka, kao i mjera za ublažavanje eventualnih štetnih učinaka povrede, ako je to primjenjivo.

Izveštaj pojedincu iz prvog stavka nije potreban u sljedećim slučajevima:

- ovlaštena osoba za zaštitu podataka je provela odgovarajuće potrebne tehničke i organizacijske zaštitne mjere, koje su bile uporabljene za osobne podatke u svezi s kojima se dogodila povreda zaštite, posebice mjere na temelju kojih osobni podaci postaju nerazumljivi svima koji nemaju ovlaštenje za pristup istima, kao što je šifriranje;
- ovlaštena osoba za zaštitu podataka je usvojila naknadne mjere za osiguranje da se veliki rizik za prava i slobode pojedinaca na koje se odnose osobni podaci iz prvog stavka vjerojatno ne ostvari;
- u slučajevima u kojima bi takvo izvještavanje zahtijevalo nerazmjeran napor. U takvom slučaju se umjesto toga objavi javna obavijest ili izvede prikladna mjera kojom su na koje se odnose osobni podaci jednako učinkovito obavješteni.

## **VIII. SLUŽBENIK ZA ZAŠTITU OSOBNIH PODATAKA**

### **Članak 22.**

Službenik za zaštitu osobnih podataka je osoba koju u skladu s poglavljem 4 Uredbe imenuje ravnatelj ustanove.

Službenik za zaštitu osobnih podataka mora imati pristup svim informacijama koje treba pri svom radu, zaposlenici su dužni poštovati njegove preporuke na području zaštite osobnih podataka.

U slučaju obrazovanja koje organizira Službenik za zaštitu osobnih podataka, zaposlenici su se istima dužni odazvati i sudjelovati.

## **IX. ODGOVORNOST ZA PROVOĐENJE SIGURNOSNIH MJERA I POSTUPAKA**

### **Članak 23.**

Za provođenje postupaka i mjera za zaštitu osobnih podataka ravnatelj Agencije imenuje odgovorne osobe za pojedinačnu zbirku osobnih podataka.

Nadzor nad provođenjem postupaka i mjera određenih ovim pravilnikom obavlja Službenik za zaštitu osobnih podataka. Njegove preporuke su dužni poštovati svi zaposlenici.

### **Članak 24.**

Svatko tko obrađuje osobne podatke je dužan provoditi propisane postupke i mjere za zaštitu podataka i štiti podatke za koje je saznao odnosno s njima bio upoznat pri obavljanju svog posla. Obveza zaštite podataka ne prestaje prestankom radnog odnosa.

Prije stupanja na radno mjesto u sklopu kojeg se osobni podaci obrađuju, zaposlenik mora potpisati posebnu izjavu koja ga obvezuje na zaštitu osobnih podataka – obrazac izjave se nalazi u Prilogu 1 ovog pravilnika i čini njegov sastavni dio. Jednaku izjavu moraju potpisati i korisnici i izvršitelji obrade Agencije.

### **Članak 25.**

Za kršenje odredbi ovog pravilnika zaposlenici su disciplinski odgovorni, ostali na temelju ugovornih obveza.

## **X. ZAVRŠNE ODREDBE**

### **Članak 26.**

Ovaj pravilnik stupa na snagu danom donošenja.

Broj: IZ-2021-364-014

U Rijeci, 30.12.2021.g.



**Ravnatelj Agencije**

**Hrvoje Šćulac, dipl. ing. el.**



## Prilog 1

**Izjava o upoznatosti sa zaštitom osobnih podataka,  
s Pravilnikom o zaštiti osobnih podataka  
AGENCIJE ZA DRUŠTVENO POTICANU STANOGRADNJU GRADA RIJEKE,  
i s mogućim posljedicama nepoštivanja**

Niže potpisani \_\_\_\_\_ potvrđujem da sam pročitao Pravilnik o zaštiti osobnih podataka Agencije za društveno poticanu stanogradnju Grada Rijeke, Rijeka, Titov trg kbr. 3, da ga razumijem i obvezujem se na njegovu eksplicitnu provedbu cijelo vrijeme trajanja mog rada odn. suradnje s Agencijom, kao i po prestanku mog rada odn. suradnje s navedenom Agencijom.

Isto tako potvrđujem da sam upoznat s odredbama zakona koji uređuje područje zaštite osobnih podataka i Uredbom, te s posljedicama eventualnog nepoštivanja pravilnika, zakona ili Uredba – a koje su disciplinska odgovornost i/ili ugovorna kazna. Upoznat sam i s time da ću biti regresno odgovoran u slučaju da Agenciji, njezinim ugovornim izvršiteljima obrade ili korisnicima zbog mojeg nezakonitog postupanja budu izrečene globe ili kazne.

Datum, \_\_\_\_\_

\_\_\_\_\_  
(vlastoručni potpis)

## IZVJEŠĆE

### *o povredi osobnih podataka*

*temeljem članka 33. UREDBE (EU) 2016/679 EUROPSKOG PARLAMENTA I VIJEĆA od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (Opća uredba o zaštiti podataka)*

\* Voditelj obrade:

---

(navesti registrirani službeni naziv Voditelja obrade)

\* Sjedište Voditelja obrade:

---

(navesti adresu, poštanski broj i mjesto sjedišta Voditelja obrade)

\* OIB Voditelja obrade:

---

(navesti OIB Voditelja obrade)

\* Službenik za zaštitu podataka (ili druga kontakt osoba):

---

(navesti ime i prezime, adresu rada službenika za zaštitu podataka, te navesti svojstvo – ukoliko se funkcija obavlja temeljem ugovora o djelu, broj telefona za kontakt i e-mail adresu za kontakt službenika za zaštitu podataka ili druge kontakt osobe)

\* Opis prirode povrede osobnih podataka:

---

---

---

(uključujući procijenjeno vrijeme nastupa povrede, kategorije i približan broj ispitanika na koje se povreda odnosi te kategorije i približan broj evidencija osobnih podataka na koje se povreda odnosi)

\* Vrijeme saznanja o povredi osobnih podataka:

---

---

---

(uključujući razloge kašnjenja ukoliko izvješćivanje nije učinjeno unutar 72 sata od saznanja o povredi osobnih podataka)

\* Vjerojatne posljedice povrede osobnih podataka:

---

---

---

---

\* Mjere koje je voditelj obrade poduzeo ili predložio poduzeti za rješavanje problema povrede osobnih podataka:

---

---

---

---

(uključujući prema potrebi mjere umanjivanja mogućih štetnih posljedica predmetne povrede)

Mjesto:

Dana:

---

\* M.P.

\*

---

(Klasa, Urbroj i ostali neobvezni podaci)

(pečat Voditelja obrade –  
ako je primjenjivo)

(potpis odgovorne osobe kod  
Voditelja obrade)

(Potrebno je u obrascu popuniti sve obvezne podatke (označeni su zvjezdicom) i izvješće s potpisom odgovorne osobe i pečatom (ako je primjenjivo) Voditelja obrade, u izvorniku, dostaviti na adresu sjedišta Agencije: Agencija za zaštitu osobnih podataka, Martićeva 14, 10000 Zagreb, te skenirano na e-mail adresu: [incidenti@azop.hr](mailto:incidenti@azop.hr))