

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 odredbi Opće uredbe o zaštiti podataka (EU) 2016/679 i Zakona o provedbi Opće uredbe o zaštiti osobnih podataka (NN 42/18), ravnatelj Agencije za društveno poticanu stanogradnju Grada Rijeke (u daljnjem tekstu: Agencija) uz prethodnu suglasnost Upravnog vijeća Agencije donosi:

PROCEDURU u slučaju povrede osobnih podataka

1. Svrha, opseg i korisnici

Svrha ove Procedure u slučaju povrede osobnih podataka (u nastavku: Procedura) je uređenje postupaka, rokova i odgovornosti glede ispunjavanja obveza voditelja obrade u slučaju povrede zaštite osobnih podataka.

Ista se primjenjuje u opsegu kako je propisano važećim zakonodavstvom na području zaštite osobnih podataka, i koji je nužan kako bi ispitanicima u slučaju povrede zaštite njihovih osobnih podataka bilo omogućeno adekvatno i zakonito ispitivanje njihova zahtjeva, kao i poduzimanje odgovarajućih mjera za sanaciju povrede.

Korisnici su sve osobe (u nastavku: ispitanici) koje smatraju da im je povrijeđeno neko pravo zajamčeno Zakonom o provedbi Opće uredbe o zaštiti osobnih podataka (NN 42/18) i Općom uredbom o zaštiti podataka.

2. Izvori

Izvori za uređenje Procedure su:

- Uredba (EU) 2016/679 Europskog parlamenta i Vijeća o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka (GDPR uredba) te o stavljanju izvan snage Direktive 95/46/EZ (u nastavku: Opća uredba o zaštiti podataka);
- Zakon o provedbi Opće uredbe o zaštiti podataka ("Narodne novine", broj 42/18);
- Politika privatnosti Agencije, objavljena i javno dostupna na oglasnoj ploči u poslovnim prostorijama Agencije i na web stranicama Agencije
- Pravilnik o zaštiti osobnih podataka

3. Definicije

Prema čl. 4. Opće uredbe o zaštiti podataka, značenje pojmova je kako slijedi:

- **„osobni podaci“** znači svi podaci koji se odnose na pojedinca čiji je identitet utvrđen ili se može utvrditi („ispitanik“); pojedinac čiji se identitet može utvrditi jest osoba koja se može identificirati izravno ili neizravno, osobito uz pomoć identifikatora kao što su ime, identifikacijski broj, podaci o lokaciji, mrežni identifikator ili uz pomoć jednog ili više čimbenika svojstvenih za fizički, fiziološki, genetski, mentalni, ekonomski, kulturni ili socijalni identitet tog pojedinca;
- **„obrada“** znači svaki postupak ili skup postupaka koji se obavljaju na osobnim podacima ili na skupovima osobnih podataka, bilo automatiziranim bilo neautomatiziranim sredstvima kao što

su prikupljanje, bilježenje, organizacija, strukturiranje, pohrana, prilagodba ili izmjena, pronalaženje, obavljanje uvida, uporaba, otkrivanje prijenosom, širenjem ili stavljanjem na raspolaganje na drugi način, usklađivanje ili kombiniranje, ograničavanje, brisanje ili uništavanje;

- **„voditelj obrade“** znači fizička ili pravna osoba, tijelo javne vlasti, agencija ili drugo tijelo koje samo ili zajedno s drugima određuje svrhe i sredstva obrade osobnih podataka; kada su svrhe i sredstva takve obrade utvrđeni pravom Unije ili pravom države članice, voditelj obrade ili posebni kriteriji za njegovo imenovanje mogu se predvidjeti pravom Unije ili pravom države članice;
- **„izvršitelj obrade“** znači fizička ili pravna osoba, tijelo javne vlasti, agencija ili drugo tijelo koje obrađuje osobne podatke u ime voditelja obrade;
- **„primatelj“** znači fizička ili pravna osoba, tijelo javne vlasti, agencija ili drugo tijelo kojem se otkrivaju osobni podaci, neovisno o tome je li on treća strana. Međutim, tijela javne vlasti koja mogu primiti osobne podatke u okviru određene istrage u skladu s pravom Unije ili države članice ne smatraju se primateljima; obrada tih podataka koju obavljaju ta tijela javne vlasti mora biti u skladu s primjenjivim pravilima o zaštiti podataka prema svrhama obrade;
- **„treća strana“** znači fizička ili pravna osoba, tijelo javne vlasti, agencija ili drugo tijelo koje nije ispitanik, voditelj obrade, izvršitelj obrade ni osobe koje su ovlaštene za obradu osobnih podataka pod izravnom nadležnošću voditelja obrade ili izvršitelja obrade;
- **„privola“** ispitanika znači svako dobrovoljno, posebno, informirano i nedvosmisleno izražavanje želja ispitanika kojim on izjavom ili jasnom potvrdnom radnjom daje pristanak za obradu osobnih podataka koji se na njega odnose;
- **„povreda osobnih podataka“** znači kršenje sigurnosti koje dovodi do slučajnog ili nezakonitog uništenja, gubitka, izmjene, neovlaštenog otkrivanja ili pristupa osobnim podacima koji su preneseni, pohranjeni ili na drugi način obrađivani;
- **„nadzorno tijelo“** znači neovisno tijelo javne vlasti koje je osnovala država članica u skladu s člankom 51. Opće uredbe o zaštiti podataka – u Hrvatskoj je to Agencija za zaštitu osobnih podataka (u nastavku: AZOP).

4. Dužnosti osobe ovlaštene za provedbu postupka u slučaju povrede osobnih podataka

Osoba ovlaštena za provedbu postupka u slučaju povrede osobnih podataka kod voditelja obrade odnosno Službenik za zaštitu osobnih podataka (**u nastavku: Službenik**) dužna je odmah po zaprimanju obavijesti odnosno zahtjeva ispitanika za zaštitu prava radi povrede osobnih podataka proučiti stvarno činjenično stanje i o cjelovitim zaključcima informirati prvo ravnatelja Agencije, potom Agenciju za zaštitu osobnih podataka kao Središnje nadzorno tijelo (dalje tekstu: AZOP), kako to propisuje zakonodavstvo. Službenik postupuje samo u slučaju kada je zaprimio zahtjev koji je razumljiv i potpun, te sadržava sljedeće osnovne podatke:

- ime, prezime/ naziv i adresa – podaci su potrebni radi provođenja postupka i dostave odgovora,
- navod u čemu se sastoji povreda prava.

Službenik je odgovoran za osiguranje potpune, pravovremene i zakonite provedbe procedure, koordinaciju na relaciji voditelj obrade - izvršitelj obrade (ako je to primjenjivo) – ispitanik - AZOP.

Po provedbi propisanog postupka obrade zahtjeva, službenik je dužan sačiniti Izvješće o povredi osobnih podataka te osigurati da isto u zakonskom roku bude poslano AZOP-u.

Ukoliko AZOP utvrdi da su povrijeđene odredbe Zakona, Agencija ima pravo upozoriti ili opomenuti voditelja/izvršitelja obrade o nezakonitosti u obradi osobnih podataka te rješenjem:

- narediti da se nepravilnosti uklone u određenom roku,
- privremeno zabraniti prikupljanje, obradu i korištenje osobnih podataka koji se prikupljaju, obrađuju ili koriste suprotno odredbama zakona,
- narediti brisanje osobnih podataka prikupljenih bez pravne osnove,
- zabraniti iznošenje osobnih podataka iz RH ili davanje na korištenje osobnih podataka drugim korisnicima ako se osobni podaci iznose iz RH ili se daju na korištenje drugim korisnicima suprotno odredbama Zakona,
- zabraniti povjeravanje poslova prikupljanja i obrade osobnih podataka izvršiteljima obrade ako izvršitelj obrade ne ispunjava uvjete u pogledu zaštite osobnih podataka, ili je povjeravanje navedenih poslova provedeno suprotno odredbama Zakona.

Službenik je dužan pobrinuti se da voditelj obrade postupi po rješenju AZOP-a.

Službenik je dužan voditi i redovno ažurirati Registar povreda osobnih podataka kod voditelja obrade, te o istome izvještavati ravnatelja voditelja obrade prilikom svake promjene.

5. Postupak odgovora na povredu osobnih podataka

Ispitanik pisanim zahtjevom poslanim na adresu: **Agencija za društveno poticanu stanogradnju Grada Rijeke, Rijeka, Titov trg 3**, s naznakom »za Službenika za zaštitu osobnih podataka«, može zahtijevati pristup, dopunu, ispravak, blokiranje odn. ograničenje obrade ili brisanje (»pravo na zaborav«) osobnih podataka, prigovoriti obradi podataka koji se obrađuju s njim u svezi, te zahtijevati prijenos podataka. Službenik u ime voditelja obrade pisanim putem obavještava ispitanika o podnošenju službenog Izvješća o povredi osobnih podataka AZOP-u, te prilaže opis mjera koje je voditelj obrade donio odn. predložio za sanaciju povrede zaštite osobnih podataka, kao i mjera za ublažavanje eventualnih štetnih učinaka povrede, ako je to primjenjivo.

Detalnije je postupak odgovora na povredu osobnih podataka ispitaniku obrazložen u točki 8. ove Procedure.

6. Obavijest o povredi osobnih podataka: izvršitelj obrade voditelju obrade

U slučaju povrede zaštite osobnih podataka koja proizlazi iz sfere djelovanja izvršitelja obrade, isti se potpisom ugovora o obradi osobnih podataka s voditeljem obrade (u nastavku: Ugovor) obvezuje odmah obavijestiti ovlaštenu osobu – Službenika za zaštitu osobnih podataka voditelja obrade, i to najkasnije u roku 24 sata po saznanju o povredi. Izvršitelj obrade će o povredi obavijestiti voditelja obrade, a opis povrede kojeg izvršitelj obrade posreduje voditelju obrade mora sadržavati sve propisane elemente, najmanje sljedeće:

- a) opis vrste povrede zaštite osobnih podataka, po mogućnosti i kategorije i približan broj obuhvaćenih ispitanika na koje se odnose osobni podaci, kao i vrste i približan broj obuhvaćenih evidencija osobnih podataka;
- b) opis vjerojatnih posljedica povrede zaštite osobnih podataka;
- c) opis mjera koje izvršitelj obrade donese odn. predlaže za sanaciju povrede zaštite osobnih podataka, kao i mjera za ublažavanje eventualnih štetnih učinaka povrede, ako je to primjenjivo.

Izvršitelj obrade je prema Ugovoru dužan dokumentirati svaku povredu zaštite osobnih podataka, uključujući radnje u svezi povreda zaštite osobnih podataka, njene učinke i donesene mjere. Navedenu dokumentaciju se izvršitelj obrade obvezuje posredovati voditelju obrade u roku kojeg mu isti odredi.

7. Obavijest o povredi osobnih podataka: voditelj obrade nadzornom tijelu

Sukladno čl. 33. Opće uredbe o zaštiti podataka, u slučaju povrede osobnih podataka voditelj obrade bez nepotrebnog odgađanja i, ako je izvedivo, najkasnije 72 sata nakon saznanja o toj povredi, izvješćuje nadzorno tijelo nadležno u skladu s člankom 55. o povredi osobnih podataka, 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.

U izvješćivanju iz stavka 1. mora se barem:

a) opisati priroda povrede osobnih podataka, uključujući, ako je moguće, kategorije i približan broj dotičnih ispitanika te kategorije i približan broj dotičnih evidencija osobnih podataka;

b) navesti ime i kontaktne podatke službenika za zaštitu podataka ili druge kontaktne točke od koje se može dobiti još informacija;

c) opisati vjerojatne posljedice povrede osobnih podataka;

d) opisati mjere koje je voditelj obrade poduzeo ili predložio poduzeti za rješavanje problema povrede osobnih podataka, uključujući prema potrebi mjere umanjivanja njezinih mogućih štetnih posljedica.

Ako i u onoj mjeri u kojoj nije moguće istodobno pružiti informacije, informacije je moguće postupno pružati bez nepotrebnog daljnjeg odgađanja.

8. Obavijest o povredi osobnih podataka: voditelj obrade ispitaniku

Sukladno čl. 34. Opće uredbe o zaštiti podataka, u slučaju povrede osobnih podataka koje će vjerojatno prouzročiti visok rizik za prava i slobode pojedinaca, voditelj obrade bez nepotrebnog odgađanja obavješćuje ispitanika o povredi osobnih podataka.

Obavješćivanjem ispitanika iz stavka 1. ovog članka opisuje se priroda povrede osobnih podataka uporabom jasnog i jednostavnog jezika te ono sadržava barem informacije i mjere iz točke 7. ove Procedure, i to točaka (b), (c) i (d).

Obavješćivanje ispitanika iz stavka 1. nije obvezno ako je ispunjen bilo koji od sljedećih uvjeta:

a) voditelj obrade poduzeo je odgovarajuće tehničke i organizacijske mjere zaštite i te su mjere primijenjene na osobne podatke pogođene povredom osobnih podataka, posebno one koje osobne podatke čine nerazumljivima bilo kojoj osobi koja im nije ovlaštena pristupiti, kao što je enkripcija;

b) voditelj obrade poduzeo je naknadne mjere kojima se osigurava da više nije vjerojatno da će doći do visokog rizika za prava i slobode ispitanika iz stavka 1.;

c) time bi se zahtijevao nerazmjeran napor. U takvom slučaju mora postojati javno obavješćivanje ili slična mjera kojom se ispitanici obavješćuju na jednako djelotvoran način.

Ako voditelj obrade nije do tog trenutka obavijestio ispitanika o povredi osobnih podataka, nakon razmatranja razine vjerojatnosti da će povreda osobnih podataka prouzročiti visok rizik, nadzorno tijelo može od njega zahtijevati da to učini ili može zaključiti da je ispunjen neki od uvjeta navedenih u stavku 3.

9. Odgovornost

Voditelj obrade odgovoran je za slučaj da AZOP utvrdi da je ostvarena povreda zaštite osobnih prava ispitanika u mjeri gdje je moguće utvrditi isključivu odgovornost voditelja obrade.

Izvršitelj obrade odgovoran je sukladno sklopljenom Ugovoru o obradi osobnih podataka, kada utvrđena povreda proizlazi iz ugovornog odnosa s voditeljem obrade.

Službenik je za povredu zaštite osobnih prava ispitanika odgovoran temeljem potpisanog ugovora o radu s voditeljem obrade, ukoliko je moguće utvrditi njegovu isključivu krivnju za povredu.

10. Upravljanje spisima na temelju ovog dokumenta

Voditelj obrade vodi poseban Registar povreda, i to u elektronskom obliku, kao i u fizičkom obliku na način na koji se čuva sva povjerljiva dokumentacija kod voditelja obrade, propisano internim aktima s područja zaštite osobnih prava i zaštite informacijske sigurnosti.

Svi spisi koji proizlaze iz postupanja po ovoj Proceduri su poslovna tajna, te je pristup istima strogo ograničen, a o čemu brigu vodi Službenik u skladu sa svojim ovlaštenjima.

11. Valjanost i upravljanje dokumentima

Voditelj obrade dokumentira sve povrede osobnih podataka, uključujući činjenice vezane za povredu osobnih podataka, njezine posljedice i mjere poduzete za popravlanje štete. Ta dokumentacija nadzornom tijelu omogućuje provjeru poštovanja ovog članka.

Svi dokumenti koji proizlaze iz postupanja po ovoj Proceduri su poslovna tajna, te je pristup istima strogo ograničen, a o čemu brigu vodi Službenik u skladu sa svojim ovlaštenjima.

Ova Procedura stupa na snagu i primjenjuje se danom donošenja.

Broj: IZ-2021-182-004
U Rijeci, 01.07.2021. god.



Ravnatelj Agencije

Hrvoje Šćulac, dipl. ing. el.

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)