Procedura obavještavanja u slučaju

povrede osobnih podataka

Zagreb, rujan 2018.

Sadržaj:

[1. UVOD 3](#_Toc524893813)

[2. OSNOVNI POJMOVI 3](#_Toc524893814)

[3. PROCEDURA OBAVJEŠTAVANJA U SLUČAJU POVREDE OSOBNIH PODATAKA 4](#_Toc524893815)

[4. ŠKOLA KAO VODITELJ OBRADE 4](#_Toc524893816)

[4.1. OBAVJEŠTAVANJE NADZORNOG TIJELA 4](#_Toc524893821)

[4.1.1. Odluka da li obavijestiti nadzorno tijelo 4](#_Toc524893826)

[4.1.2. Način obavještavanja nadzornog tijela 5](#_Toc524893827)

[4.2. OBAVJEŠTAVANJE ISPITANIKA 5](#_Toc524893833)

[4.2.1. Odluka da li obavijestiti ispitanika 5](#_Toc524893837)

[4.2.2. Način obavještavanja ispitanika 5](#_Toc524893838)

[5. ŠKOLA KAO IZVRŠITELJ OBRADE 5](#_Toc524893839)

## UVOD

Ovom Procedurom uređuje se postupanje u slučajevima kada dođe do incidenta koji je rezultirao povredom osobnih podataka ili se vjeruje da je doveo do toga. Dokument treba koristiti u kombinaciji s poduzimanjem potrebnih mjera za otklanjanje posljedica povrede i sprječavanje budućih povreda te s njima čini sveukupni proces reagiranja na incidente koji utječu na informacijsku sigurnost Škole.

Općom uredbom o zaštiti osobnih podataka (dalje u tekstu: Uredba) propisano je da voditelj obrade podataka mora incidente povrede podataka koji bi mogli dovesti do rizika za prava i slobode ispitanika prijaviti nadzornom tijelu za zaštitu podataka (u R. Hrvatskoj je to Agencija za zaštitu osobnih podataka) bez nepotrebnih kašnjenja i gdje je to moguće, u roku od 72 sata nakon otkrivanja povrede. Ako prijava nije podnesena u roku od 72 sata, moraju se navesti razlozi za kašnjenje.

U slučaju da se Škola nalazi u položaju izvršitelja obrade, obvezno je bez nepotrebne odgode obavijestiti voditelja obrade o nastaloj povredi osobnih podataka.

Ako se dogodila povreda osobnih podataka za koje je Škola voditelj obrade, potrebno je donijeti odgovarajuće odluke glede razine, trenutka i sadržaja komunikacije s ispitanicima. Zahtjev je Uredbe da se komunikacija mora dogoditi bez odgode ako je vjerojatno da će povreda rezultirati visokim rizikom za prava i slobode fizičkih osoba.

Postupci izloženi u ovom dokumentu se trebaju koristiti isključivo kao preporuke glede odgovaranja na nastalu povredu osobnih podataka. Točna priroda i učinak incidenta ne mogu se predvidjeti i važno je da se odlučivanju o radnjama koje je potrebno poduzeti pristupi razumno uz uvažavanje svih relevantnih okolnosti.

## OSNOVNI POJMOVI

|  |  |
| --- | --- |
| Osobni podaci | 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; |
| Povreda osobnih podataka | 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 | Agencija za zaštitu osobnih podataka; |
| Ispitanik | fizička osoba čiji se osobni podaci po bilo kojoj osnovi nalaze u informacijskom sustavu Škole; |
| Voditelj obrade | fizička ili pravna osoba, tijelo javne vlasti, agencija ili drugo tijelo koje određuje svrhe i sredstva obrade osobnih podataka; |
| Izvršitelj obrade | fizička ili pravna osoba, tijelo javne vlasti, agencija ili drugo tijelo koje obrađuje osobne podatke u ime voditelja obrade. |

## PROCEDURA OBAVJEŠTAVANJA U SLUČAJU POVREDE OSOBNIH PODATAKA

Nakon što je utvrđeno da je nastala povreda osobnih podataka, Uredba propisuje da sljedeće tri strane moraju dobiti spomenutu informaciju:

1. Nadzorno tijelo;
2. Ispitanici;
3. Voditelj obrade (ako je povreda uočena od strane Izvršitelja obrade)

Svaka povreda osobnih podataka ne mora nužno biti prijavljena. Navedeno ovisi o procjeni rizika nastalog povredom, odnosno, koliki je rizik povredom nastao za prava i slobode fizičkih osoba. U nastavku ove Procedure opisuje se kako se navedeno procjenjuje i što je potrebno poduzeti ako je prijava potrebna.

## ŠKOLA KAO VODITELJ OBRADE

1.
2.
3.
4.

##  OBAVJEŠTAVANJE NADZORNOG TIJELA

Kada je Škola voditelj obrade za osobne podatke glede kojih se povreda dogodila u slučaju obavještavanja nadzornog tijela o povredi obavijest se šalje na e-mail adresu: azop@azop.hr**, odnosno, drugu e-mail adresu naznačenu na stranicama nadzornog tijela (**[www.azop.hr](http://www.azop.hr)**) za tu namjenu.**

ili poštom na:

Agencija za zaštitu osobnih podataka

Martićeva ulica 14

HR - 10000 ZAGREB

1.
2.
3.
4.

### Odluka da li obavijestiti nadzorno tijelo

Uredba propisuje da se povrede osobnih podataka prijavljuju nadzornom tijelu osim ako nije vjerojatno da će povreda prouzročiti rizik za prava i slobode fizičkih osoba (čl. 33. Uredbe). Navedene formulacija zahtijeva od Škole da procijeni rizik nastao povredom prije nego što odluči obavijestiti nadzorno tijelo.

Elementi koje je potrebno uzeti u obzir prilikom procjene uključuju:

* Osobni podaci koji su povrijeđeni (npr. adresa, financijski podaci);
* Količina podataka koja je ugrožena;
* Broj ispitanika na koje se povreda odnosi;
* Da li su osobni podaci bili kriptirani;
* Do koje mjere su podaci pseudonimizirani (ako je primjenjivo);
* Ostale podatke koje smatramo relevantnima.

Nakon provedene procjene potrebno je odabrati jednu od sljedećih opcija:

1. Povreda osobnih podataka ne zahtijeva podnošenje prijave;
2. Povreda osobnih podataka zahtijeva smo podnošenje prijave nadzornom tijelu;
3. Povreda osobnih podataka zahtijeva i prijavu nadzornom tijelu i obavještavanje ispitanika.

Odluku je potrebno dokumentirati i pohraniti. Odluka se može promijeniti u slučaju promjene okolnosti i/ili otkrića novih činjenica/mišljenja nadzornog tijela.

### Način obavještavanja nadzornog tijela

U slučaju donošenja odluke o podnošenju prijave nadzornom tijelu, prijavu je potrebno dostaviti bez nepotrebne odgode, a najkasnije u roku od 72 sata od povrede. Prijava se podnosi putem *Obrasca za podnošenje prijave o povredi podataka.*

Prijava mora sadržavati informacije o:

1. Prirodi povrede, uključujući (gdje je moguće) kategorije i približan broj ispitanika zahvaćenih povredom te kategorije i približnu količinu osobnih podataka zahvaćenih povredom;
2. Ime i kontakte podatke osobe zadužene za rad oko povrede;
3. Opis vjerojatnih posljedica povrede;
4. Opis poduzetih mjere za otklanjanje posljedica povrede;
5. Ako se prijava šalje nakon 72 sata od otkrivanja povrede, razloge za kašnjenje.
6.
7.
8.
9. 1.

## OBAVJEŠTAVANJE ISPITANIKA

Kada je Škola voditelj obrade glede podataka, ako to proizlazi iz procjene okolnosti, o povredi može biti potrebno obavijestiti ispitanike[[1]](#footnote-1).

1. 1.
	2.

### Odluka da li obavijestiti ispitanika

Uredba propisuje da će se ispitanik obavijestiti i povredi osobnih podataka kada je vjerojatno da će povreda prouzročiti visok rizik za prava i slobode fizičkih osoba. Za razliku od potrebe obavještavanja nadzornog tijela gdje se traži mogućnost nastanka rizika, u ovom slučaju se traži mogućnost nastanka **visokog** rizika.

Mogućnost nastanka visokog rizika se ocjenjuje kroz procjenu iz točke 4.1. ove Procedure. Ako su u međuvremenu poduzete mjere koje su smanjile opisani rizik, nije potrebno obavijestiti ispitanika.

Odluka se može promijeniti u slučaju promjene okolnosti i/ili otkrića novi činjenica/mišljenja nadzornog tijela.

### Način obavještavanja ispitanika

Ako je utvrđeno da razina povrede osobnih podataka opravdava obavještavanje ispitanika, Uredba zahtijeva da se to obavi bez nepotrebne odgode.

Obavijest ispitanicima zahvaćenima povredom treba biti u jednostavnom i razumljivom jeziku (zahtjev iz članka 34. Uredbe) opisati prirodu povrede te također mora sadržavati:

1. Ime i prezime i kontaktne podatke osobe zaposlene u Školi kod koje ispitanik može dobiti više informacija (službenika za zaštitu podataka);
2. Opis vjerojatnih posljedica povrede;
3. Opis poduzetih ili predloženih mjera kako bi se otklonile posljedice povrede.

Uz opisani sadržaj, može biti prikladno ponuditi ispitaniku savjete na koji način može smanjiti rizike vezane uz nastalu povredu osobnih podataka.

Za potrebe obavještavanja predlaže se ispitanika kontaktirati pisanim pute ili putem e-maila, ili na oba načina kako bi se osiguralo da je ispitanik zaprimio obavijest i da ima priliku poduzeti potrebne radnje.

## ŠKOLA KAO IZVRŠITELJ OBRADE

Ako se Škola temeljem neke pravne osnove nalazi glede obrade podataka u položaju izvršitelja obrade za jednog ili više voditelja obrade, u slučaju uočavanja povrede osobnih podataka obvezna je bez nepotrebne odgode obavijestiti svakog voditelja obrade o povredi osobnih podataka koja se na njega odnosi. Na voditelju obrade je dalje odluka da li je potrebno povredu prijaviti i poduzimanje daljnjih koraka.

Kako bi omogućio voditelju obrade da ispuni zahtjeve iz Uredbe, Škola mu treba dostaviti sljedeće informacije:

* Datum i vrijeme kada je povreda otkrivena;
* Pretpostavljeni datum i vrijeme kada se povreda dogodila;
* Koji su osobni podaci povrijeđeni (npr. adresa, financijski podaci);
* Količinu podataka koji su ugroženi;
* Broj ispitanika na koje se povreda odnosi;
* Prirodu povrede (npr. krađa, slučajno brisanje);
* Da li su osobni podaci bili kriptirani;
* Do koje mjere su podaci pseudonimizirani (ako je primjenjivo);
* Mjere koje su poduzete da se adresira povreda;
* Kontakt podaci osobe unutar Škole koja vodi postupanje oko povrede (najčešće službenik za zaštitu podataka);
* Ostale podatke koje smatraju relevantnima.

Ako ima više voditelja podataka na koje se povreda odnosi, potrebno je obavijestiti svakog pojedinačno.

1. Ako je riječ o povredi podataka djece, obavještavaju se roditelji, odnosno, nositelji roditeljske skrbi [↑](#footnote-ref-1)