



CENTAR ZA NESTALU
I ZLOSTAVLJANU DECU



POLITIKA POSTUPANJA U SLUČAJU POVREDE PODATAKA (DATA BREACH)

Datum poslednje izmene: 20.04.2026.



1. Uvod

Ova politika definiše postupke u slučaju povrede bezbednosti podataka o ličnosti na internet platformi „Nestali Srbija“, kojom upravlja Centar za nestalu i zlostavljanu decu.

Cilj politike je brzo otkrivanje, ograničavanje i upravljanje incidentima koji mogu ugroziti prava i slobode lica.

2. Definicija incidenta

Povreda podataka o ličnosti uključuje svaku situaciju koja dovodi do:

- neovlašćenog pristupa podacima
- slučajnog ili nezakonitog uništenja podataka
- gubitka podataka
- neovlašćenog otkrivanja ili objave podataka
- zloupotrebe pristupnih kredencijala

3. Primeri incidenta

Incidenti mogu uključivati:

- kompromitovanje administratorskog naloga
- neovlašćeno preuzimanje baze podataka
- pogrešno javno objavljivanje podataka
- curenje fotografija ili ličnih informacija
- napad na server (malware, ransomware)

4. Detekcija i prijava incidenta

Svaki zaposleni, saradnik ili tehničko lice dužno je da:

- odmah prijavi sumnju na incident
- obavesti odgovorno lice za zaštitu podataka (DPO ili administrator)
- obezbedi relevantne informacije o incidentu

5. Prva reakcija (containment)

Nakon identifikacije incidenta preduzimaju se hitne mere:

- izolacija kompromitovanog sistema



- deaktivacija kompromitovanih naloga
- blokiranje neovlašćenog pristupa
- zaštita preostalih podataka

Cilj je sprečavanje daljeg širenja incidenta.

6. Procena rizika

Vrši se procena:

- vrste i obima podataka koji su ugroženi
- da li su uključeni podaci maloletnih lica
- da li postoji rizik po prava i slobode lica
- verovatnoće zloupotrebe podataka

7. Obaveštavanje nadležnih organa

U slučaju visokog rizika, Rukovalac obaveštava:

- Poverenika za informacije od javnog značaja i zaštitu podataka o ličnosti (u skladu sa ZZPL)
- nadležne državne organe (po potrebi, npr. policiju)

Obaveštenje se dostavlja bez nepotrebnog odlaganja, a po pravilu u zakonskom roku.

8. Obaveštavanje lica na koje se podaci odnose

Ako incident predstavlja visok rizik za prava i slobode lica, pogođena lica se obaveštavaju:

- na jasan i razumljiv način
- uz opis prirode incidenta
- uz preporuke za zaštitu

9. Dokumentovanje incidenta

Svaki incident se evidentira i uključuje:

- opis incidenta
- vreme i način otkrivanja
- obim podataka
- preduzete mere
- posledice incidenta



- korektivne mere

10. Korektivne mere

Nakon incidenta preduzimaju se mere za sprečavanje ponavljanja:

- unapređenje bezbednosnih sistema
- promena pristupnih kontrola
- dodatna obuka zaposlenih
- revizija internih procedura

11. Poseban režim za osetljive podatke

S obzirom na to da platforma obrađuje podatke koji se odnose na maloletna lica i nestale osobe:

- svaki incident se tretira kao potencijalno visokorizičan
- primenjuju se pojačane mere zaštite
- prioritet ima zaštita identiteta i privatnosti lica

12. Odgovornost

Odgovornost za upravljanje incidentima ima:

- tehnički administrator sistema
- lice zaduženo za zaštitu podataka (DPO ili ekvivalent)
- rukovalac podacima

13. Revizija politike

Ova politika se redovno ažurira u skladu sa:

- promenama sistema
- bezbednosnim rizicima
- zakonskim izmenama