

# Zakon o informacionoj bezbjednosti

Zakon je objavljen u "Službenom listu CG", br. [14/2010](#) i [40/2016](#).

## I. OSNOVNE ODREDBE

### Predmet

#### Član 1

Informaciona bezbjednost obezbjeđuje se primjenom mjera i standarda informacione bezbjednosti, u skladu sa ovim zakonom.

### Pojam

#### Član 2

Informaciona bezbjednost podrazumijeva stanje povjerljivosti, cjelovitosti i dostupnosti podataka.

Podatak, u smislu ovog zakona, je informacija, poruka i dokument sačinjen, poslat, primljen, zabilježen, skladišten ili prikazan elektronskim, optičkim ili sličnim sredstvom, uključujući prenos internetom i elektronsku poštu.

Povjerljivost podataka podrazumijeva da je podatak dostupan samo licima koja su ovlašćena da ostvare pristup ili postupe sa tim podatkom.

Cjelovitost podataka podrazumijeva očuvanje postojanja, tačnosti i kompletnosti podataka, kao i zaštitu procesa ili programa koji sprječavaju neovlašćeno mijenjanje podataka.

Dostupnost podataka podrazumijeva da ovlašćeni korisnici mogu da pristupe podatku uvijek kada za to imaju potrebu.

### Obaveza primjene

#### Član 3

Po ovom zakonu obavezni su da postupaju državni organi, organi državne uprave, organi jedinica lokalne samouprave, pravna lica sa javnim ovlašćenjima (u daljem tekstu: organi) i druga pravna i fizička lica koja ostvaruju pristup ili postupaju sa podacima.

### Ograničenje primjene

#### Član 4

Ovaj zakon ne primjenjuje se na podatke čija se informaciona bezbjednost obezbjeđuje u skladu sa propisima kojima se uređuje tajnost podataka.

## II. MJERE I STANDARDI INFORMACIONE BEZBJEDNOSTI

### Osnovna zaštita

#### Član 5

Mjere informacione bezbjednosti su opšta pravila kojima se obezbjeđuje osnovna zaštita podataka na fizičkom, tehničkom i organizacionom nivou.

Mjere iz stava 1 ovog člana sprovode se u skladu sa standardima informacione bezbjednosti.

### Utvrđivanje mjera

#### Član 6

Mjere informacione bezbjednosti utvrđuju se u skladu sa vrstom podataka, rizicima za njegovu bezbjednost i vrstom zaštite. Informaciona bezbjednost obuhvata mjere za:

- 1) fizičku zaštitu;
- 2) zaštitu podataka;
- 3) zaštitu informacionog sistema.

### Fizička zaštita

#### Član 7

Fizička zaštita obuhvata zaštitu objekta, prostora i uređaja u kojem se nalaze podaci.

## **Zaštita podataka**

### **Član 8**

Zaštita podatka obuhvata prevenciju i otklanjanje štete od gubitka, otkrivanja ili neovlašćene izmjene podataka.

Zaštita iz stava 1 ovog člana odnosi se na:

- 1) pravila za postupanje sa podacima;
- 2) sadržaj i način vođenja evidencije o izvršenim pristupima podacima;
- 3) nadzor bezbjednosti podataka.

## **Zaštita informacionog sistema**

### **Član 9**

Zaštita informacionog sistema obuhvata zaštitu podataka koji se obrađuju, skladište ili prenose u informacionom sistemu, kao i zaštitu povjerljivosti, cjelovitosti i dostupnosti informacionog sistema u procesu planiranja, projektovanja, izgradnje, upotrebe, održavanja i prestanka rada tog sistema.

## **Nadležnost za utvrđivanje mjera i standarda**

### **Član 10**

Mjere informacione bezbjednosti iz člana 5 stav 1 ovog zakona utvrđuje Vlada Crne Gore.

Aktom organa državne uprave nadležnog za informaciono društvo utvrđuje se koji se standardi informacione bezbjednosti primjenjuju za sprovođenje mjera iz stava 1 ovog člana, u skladu sa zakonom.

## **III. SISTEM ZAŠTITE OD RAČUNARSKIH BEZBJEDNOSNIH INCIDENATA**

### **Koordinacija prevencije i zaštite**

#### **Član 11**

Koordinaciju prevencije i zaštite od računarskih bezbjednosnih incidenata na internetu i drugih rizika bezbjednosti informacionih sistema organa i drugih pravnih i fizičkih lica iz člana 3 ovog zakona vrši organ državne uprave nadležan za informaciono društvo, preko posebne organizacione jedinice (u daljem tekstu: CIRT).

CIRT preduzima mjere za:

- 1) uspostavljanje sistema zaštite od računarskih bezbjednosnih incidenata na internetu i drugih rizika bezbjednosti informacionih sistema organa i drugih pravnih i fizičkih lica iz člana 3 ovog zakona;
- 2) prevenciju računarsko-bezbjednosnih incidenata;
- 3) otklanjanje posljedica u slučaju bezbjednosnih incidenata na internetu koji prelaze okvire djelovanja informacionih sistema organa i drugih pravnih i fizičkih lica iz člana 3 ovog zakona.

### **Organizovanje zaštite pojedinačnih informacionih sistema**

#### **Član 12**

Organi i druga pravna i fizička lica iz člana 3 ovog zakona mogu organizovati prevenciju i zaštitu svojih informacionih sistema od računarskih bezbjednosnih incidenata na internetu i drugih rizika bezbjednosti tih sistema.

### **Usklađivanje postupanja u slučaju računarskih incidenata**

#### **Član 13**

U slučaju nastanka bezbjednosnih računarskih incidenata na informacionim sistemima organa i drugih pravnih i fizičkih lica iz člana 3 ovog zakona, CIRT koordinira radom tih organa u primjeni mjera informacione bezbjednosti.

Organi i druga pravna lica iz člana 3 ovog zakona, dužni su da odrede lica zadužena za uspostavljanje sistema zaštite od računarskih i bezbjednosnih incidenata na internetu i drugih rizika bezbjednosti tih sistema, koji će neposredno sarađivati sa CIRT-om radi usklađivanja postupanja tih organa i pravnih lica u primjeni mjera informacione bezbjednosti u slučaju iz stava 1 ovog člana.

### **Savjet za informacionu bezbjednost**

#### **Član 13a**

Radi unaprjeđenja mjera informacione bezbjednosti, kao i praćenja rada i predlaganja aktivnosti CIRT-u na uspostavljanju sistema zaštite od računarskih i bezbjednosnih incidenata na internetu, Vlada Crne Gore obrazuje Savjet za informacionu bezbjednost.

Savjet iz stava 1 ovog člana, čine predstavnici organa državne uprave nadležnog za unutrašnje poslove, organa državne uprave nadležnog za poslove odbrane, organa državne uprave nadležnog za poslove pravosuđa, organa uprave nadležnog za informaciono društvo, organa uprave nadležnog za tajne podatke i Agencije za nacionalnu bezbjednost, a po potrebi i predstavnici drugih organa i institucija.

Zadaci Savjeta za informacionu bezbjednost utvrdiće se aktom o njegovom obrazovanju.

## **Propis o načinu koordinacije prevencije i zaštite**

### **Član 14**

Bliži način koordinacije prevencije i zaštite iz čl. 11, 12 i 13 ovog zakona propisuje organ državne uprave nadležan za informaciono društvo.

## **Kritična informatička infrastruktura**

### **Član 14a**

U cilju zaštite kritične informatičke infrastrukture, organ državne uprave nadležan za informaciono društvo preduzima mjere zaštite te infrastrukture.

Kritičnu informatičku infrastrukturu čine informacioni sistemi organa čijim bi se prekidom rada ili uništenjem ugrozili život, zdravlje, bezbjednost građana i funkcionisanje države i od čijeg funkcionisanja zavisi vršenje djelatnosti od javnog interesa.

Kritičnu informatičku infrastrukturu i način njene zaštite propisuje Vlada Crne Gore.

## **IV. NADZOR**

### **Vršenje nadzora**

### **Član 15**

Nadzor nad sprovođenjem ovog zakona vrši organ državne uprave nadležan za informaciono društvo, preko inspektora, u skladu sa zakonom.

Radi vršenja nadzora, organi i druga pravna i fizička lica iz člana 3 ovog zakona dužni su da inspektoru omoguće pristup prostoru, računarskoj opremi i uređajima, kao i da bez odlaganja stave na uvid ili dostave potrebne podatke i dokumentaciju u vezi sa predmetom nadzora.

## **V. PRELAZNE I ZAVRŠNA ODREDBA**

### **Član 16**

Propis iz člana 10 stav 1 ovog zakona donijeće se u roku od 30 dana od dana stupanja na snagu ovog zakona.

### **Član 17**

Propisi iz člana 10 stav 2 i člana 14 ovog zakona donijeće se u roku od šest mjeseci od dana stupanja na snagu propisa iz člana 16 ovog zakona.

### **Član 17a**

Propis iz člana 14a stav 3 ovog zakona, donijeće se u roku od šest mjeseci od dana stupanja na snagu ovog zakona.

### **Član 18**

Ovaj zakon stupa na snagu osmog dana od dana objavljivanja u "Službenom listu Crne Gore".