**NACRT**

**Zakon o informacionoj bezbjednosti**

**I. OSNOVNE ODREDBE**

**Predmet Zakona**

**Član 1**

Ovim zakonom propisuju se mjere informacione bezbjednosti za postizanje visokog nivoa informacione bezbjednosti mrežnih i informacionih sistema, postupci za prepoznavanje i određivanje ključnih i važnih subjekata, nacionalni okvir za bezbjednost mrežnih i informacionih sistema, postupak upravljanja sajber bezbjednošću, nadzor nad ključnim i važnim subjektima, kao i druga pitanja od značaja za postizanje visokog nivoa informacione bezbjednosti.

**Obaveza primjene**

**Član 2**

Po ovom zakonu obavezni su da postupaju državni organi, organi državne uprave, organi jedinica lokalne samouprave, organi lokalne uprave, i službe obrazovane u skladu sa zakonom kojim se uređuje lokalna samouprava, privredna društva, pravna lica sa javnim ovlašćenjima i druga pravna i fizičkih lica koja ostvaruju pristup ili postupaju sa podacima i koji koriste i upravljaju mrežnim i informacionim sistemima (u daljem tekstu: organi) kao i ključni i važni subjekti, u smislu ovog zakona.

**Izuzeće od primjene**

**Član 3**

Ovaj zakon ne primjenjuje se na organ državne uprave nadležan za poslove odbrane, organ državne uprave nadležan za poslove policije, Vojsku Crne Gore i Agenciju za nacionalnu bezbjednost, kao i na podatke čija se informaciona bezbjednost obezbjeđuje u skladu sa propisima kojima se uređuje tajnost podataka.

**Upotreba rodno osjetljivog jezika**

**Član 4**

Izrazi koji se u ovom zakonu koriste za fizička lica u muškom rodu podrazumijevaju iste izraze u ženskom rodu.

**Značenje izraza**

**Član 5**

Izrazi upotrijebljeni u ovom zakonu imaju sledeća značenja:

1. **mrežni i informacioni sistem podrazumijeva:**
* elektronsku komunikacionu mrežu koja obuhvata sisteme za prenos koji omogućavaju prenos signala žičnim, radio, optičkim ili drugim elektromagnetnim sredstvima, koja obuhvataju satelitske mreže, zemaljske fiksne (sa prebacivanjem kanala, komutacijom paketa podataka, uključujući internet) i mobilne mreže, sisteme električnih kablova, u mjeri u kojoj se koriste za prenos signala, mreže koje se koriste za radio i televizijsko emitovanje i kablovske televizijske mreže, bez obzira na vrstu informacija koje prenose;
* svaki uređaj ili skup povezanih ili sličnih uređaja, od kojih jedan ili više njih programski izvršava automatsku obradu digitalnih podataka; ili
* digitalne podatake koji se čuvaju, obrađuju, dobijaju ili prenose na način opisan u alineji 1 i 2 ove tačke, u svrhu njihovog rada, korišćenja, zaštite i održavanja;
1. **bezbjednost mrežnih i informacionih sistema** je sposobnost mrežnih i informacionih sistema da na određenom nivou pouzdanosti odolijevaju svim radnjama koje mogu ugroziti dostupnost, autentičnost, cjelovitost ili povjerljivost dostupnost sačuvanih, prenesenih ili obrađenih podataka ili usluga koje ti mrežni i informacioni sistemi nude ili kojima omogućavaju pristup;
2. **podatak** je svaka informacija, poruka i dokument sačinjen, poslat, primljen, zabilježen, skladišten ili prikazan elektronskim, optičkim ili sličnim sredstvom, uključujući prenos internetom i elektronsku poštu;
3. **kriptovana zaštita** podataka je primjena programskih rješenja ili uređaja za zaštitu podataka koji osiguravaju cjelovitost, povjerljivost i dostupnost podataka;
4. **informaciona bezbjednost** podrazumijeva stanje povjerljivosti, cjelovitosti, dostupnosti i zaštite podatka, uključujući i sajber bezbjednost;
5. **sajber bezbjednost** podrazumijeva sve aktivnosti koje su nužne za zaštitu od sajber prijetnji i incidenata kojima su izloženi mrežni i informacioni sistemi, korisnici tih sistema i drugi organi i lica na koje oni utiču;
6. **sajber prijetnja** je svaka moguća okolnost, događaj ili djelovanje koji bi mogli oštetiti, poremetiti ili na drugi način negativno uticati na podatke i mrežne i informacione sisteme, korisnike tih sistema i druge organe i lica;
7. **ozbiljna sajber prijetnja** je sajber prijetnja za koju se na osnovu njenih tehničkih obilježja može pretpostaviti da može imati ozbiljan uticaj na mrežne i informacione sisteme nekog subjekta ili korisnika usluga subjekta uzrokovanjem značajne materijalne ili nematerijalne štete;
8. **incident** je svaki događaj koji ugrožava povjerljivost, cjelovitost i dostupnost skladištenih, prenesenih ili obrađenih podataka ili usluga koje mrežni i informacioni sistemi nude ili kojima omogućavaju pristup;

10) **rešavanje incidenta** podrazumijeva sve radnje i postupke čiji je cilj otkrivanje, analiza i zaustavljanje incidenta, kao i odgovor na njega;

11) **ranjivost** je slabost, osjetljivost ili nedostatak nekog resursa, sistema, procesa ili kontrole koji sajber prijetnja može iskoristiti;

12) **rizik** je bilo koja okolnost ili događaj koji ima potencijalan negativan uticaj na bezbjednost podataka i mrežnih i informacionih sistema;

13) **sajber kriza** je događaj ili stanje koje ugrožava nacionalnu sigurnost, zdravlje i život većeg broja građana, značajno narušava životnu sredinu ili uzrokuje značajnu ekonomsku štetu, a odgovor na takav događaj ili stanje zahtijeva učešće više organa kao i primjenu odgovarajućih mjera;

14) **nadležni sektorski organ** je ministarstvo koje je u skladu sa zakonom nadležno za određene sektore;

15) **sektor** je oblast u kojoj se vrši identifikacija i određivanje ključnih i važnih subjekata;

16) **ključni subjekti** su subjekti koji su kroz postupak prepoznavanja i određivanja određeni kao ključni subjekti.

17) **važni subjekti** su subjekti koji su kroz postupak prepoznavanja i određivanja određen kao važni subjekti.

**II. MJERE INFORMACIONE BEZBJEDNOSTI**

**Mjere informacione bezbjednosti**

**Član 6**

Informaciona bezbjednost obezbjeđuje se primjenom mjera u cilju zaštite povjerljivosti, cjelovitosti i dostupnosti podatka, i zaštite od sajber prijetnji i incidenata mrežnih i informacionih sistema, korisnika tih sistema i drugih lica na koje one utiču u skladu sa ovim zakonom.

**Zaštita podataka**

**Član 7**

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

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

Dostupnost podatka podrazumijeva da ovlašćeni korisnici mogu da pristupe podatku uvijek kada za tim imaju potrebu.

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

Zaštita iz stava 4 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 od sajber prijetnji i incidenata**

**Član 8**

Zaštita od sajber prijetnji i incidenata mrežnih i informacionih sistema podrazumjeva:

1) fizičku zaštitu;

2) zaštitu mrežnih i informacionih sistema;

3) upravljanje sajber bezbjednosnim rizicima.

**Fizička zaštita**

**Član 9**

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

**Zaštita mrežnog i informacionog sistema**

**Član 10**

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

**Upravljanje sajber bezbjednosnim rizicima**

**Član 11**

Upravljanje sajber bezbjednosnim rizicima odnosi se na primjenu mjera kojima se obezbjeđuje zaštita od sajber prijetnji i incidenata mrežnih i informacionih sistema, korisnika tih sistema i drugih lica na koje one utiču.

Mjere iz stava 1 ovog člana podrazumijevu:

1. politiku analize rizika i bezbjednosti mrežnih i informacionih sistema;
2. politiku postupanja sa incidenatima (sprečavanje, otkrivanje i odgovor na incidente);
3. plan kontinuiteta poslovanja i postupanja u sajber krizama;
4. politiku bezbjednosti kojom se uređuje bezbjednost lanca snabdijevanja između subjekta koji upravlja mrežnim i informacionim sistemom i dobavljača ili pružaoca usluga;
5. akte kojima se uređuje upostavljanje, razvoj i održavanje mrežnih i informacionih sistema, uključujući bezbjednosne aspekte;
6. politike i postupke za procjenu efikasnosti mjera upravljanja sajber bezbjednosnim rizicima;
7. primjenu kriptovane zaštite podataka, ukoliko priroda posla to zahtjeva.

Bliži način utvrđivanja mjera informacione bezbjednosti iz čl. 6 do 11 ovog Zakona propisuje Vlade Crne Gore (u daljem tekstu: Vlada).

**Obaveze organa u primjeni mjera informacione bezbjednosti**

**Član 12**

Organi su dužni da primjenjuju mjere informacione bezbjednosti od čl. 6 do 10 ovog Zakona, osim mjera iz člana 8, stav 1, tačka 3 ovog zakona.

**III. KLJUČNI I VAŽNI SUBJEKTI**

**Sektori za prepoznavanje ključnih i važnih subjekata**

**Član 13**

Nadležni sektorski organ dužan je da izvrši prepoznavanje ključnih i važnih subjekata u okviru sektora, za koji je nadležan i to:

Ključne subjekte u sektorima, odnosno podsektorima:

1. energetika (električna energija; centralizovano grijanje i hlađenje; nafta; plin; vodonik),
2. transport (vazdušni; željeznički; vodeni i putni transport),
3. bankarstvo,
4. Infrastrukture finansijskog tržišta,
5. zdravlje,
6. voda za piće,
7. otpadne vode,
8. digitalna infrastruktura,
9. upravljanje uslugama informaciono-komunikacionih tehnologija,

10) javna uprava,

11) svemir;

Važne subjekte u sektorima, odnosno podsektorima:

1. poštanske i kurirske usluge,
2. upravljanje otpadom,
3. izrada, proizvodnja i distribucija hemikalija,
4. proizvodnja, prerada i distribucija hrane,
5. proizvodnja drugih važnih stvari (proizvodnja medicinskih proizvoda i in vitro dijagnostičkih medicinskih proizvoda; proizvodnja računara, elektronskih i optičkih proizvoda; proizvodnja električne opreme; proizvodnja mašina i uređaja; proizvodnja motornih vozila, prikolica i poluprikolica; proizvodnja ostale opreme za transport),
6. pružaoci digitalnih usluga.

Svi subjekti iz stava 2 ovog člana za koje se tokom postupka prepoznavanja utvrdi da nijesu ključni subjekti mogu se smatrati važnim subjektima.

**Obaveze nadležnog sektorskog organa**

**Član 14**

U postupku prepoznavanja ključnih i važnih subjekata nadležni sektorski organ dužan je da:

1. sačini listu svih organa u sektoru za koje je nadležan;
2. pokrene postupak prikupljanja informacija o potencijalnim ključnim i važnim subjektima iz sektora za koji je nadležan;
3. utvrdi sektorske kriterijume i kriterijumske pragove za prepoznavanje ključnih i važnih subjekata, u saradnji sa određenim podsektorom;
4. utvrdi listu potencijalnih ključnih i važnih subjekata primjenom opštih kriterijuma iz člana 15 ovog zakona, sektrorskih kriterijuma i kriterijumskih pragova iz tačke 3 ovog člana;
5. vodi Registar ključnih i važnih subjekata iz sektora za koji je nadležan (u daljem tekstu: Sektorski registar);
6. jednom godišnje vrši provjeru potrebe ažuriranja Sektorskog registra.

Nadležni sektorski organ određuje sektorske kriterijume iz stava 1 tačka 3 ovog člana uzimajući u obzir karakteristike tih sektora, vrstu i značaj usluga koje taj sektor, odnosno podsektor pruža.

Nadležni sektorski organ određuje kriterijumske pragove iz stava 1 tačka 3 na osnovu procjene uticaja sajber prijetnje i incidenta na pružanje usluga, posebno uzimajući u obzir gubitke, ekonomske posljedice, uticaj na nacionalnu bezbjednost, uticaj na javnost i drugo.

**Opšti kriterijumi za prepoznavanje ključnih i važnih subjekata**

**Član 15**

Nadležni sektorski organ u postupku prepoznavanja ključnih i važnih subjekata primjenjuje sljedeće opšte kriterijume, i to:

1. da li je pružanje usluga koje vrši od opšteg interesa za Crnu Goru;
2. da li se pružanje takvih usluga vrši preko mrežnih i informacionih sistema; i
3. kakav bi negativan uticaj sajber prijetnja i incident imali na pružanje usluga, uzimajući u obzir:
* broj i vrstu korisnika kojima subjekt pruža uslugu;
* postojanje zavisnosti pružanja usluge od drugih djelatnosti ili područja pružanja usluge;
* mogući uticaj sajber prijetnje i incidenta, s obzirom na njegovu težinu i trajanje, na privredne i društvene aktivnosti, kao i na javnu bezbjednost;
* tržišni udio subjekta koji pruža uslugu;
* geografsku raširenost subjekta u pogledu pružanja usluge i područja na koje bi incident mogao uticati;
* važnost poslovanja subjekta za održavanje neophodnog nivoa pružanja usluge, uzimajući u obzir i raspoloživost alternativnih sredstava za pružanje te usluge.

Nadležni sektorski organ u postupku prepoznavanja ključnih i važnih subjekata osim opštih kriterijuma iz stava 1 ovog člana primjenjuje i druge sektorske kriterijume i kriterijumske pragove iz člana 14 stav 1 tačka 3 ovog zakona.

**Postupak prikupljanja informacija o potencijalnim ključnim i važnim subjektima**

**Član 16**

Na zahtjev nadležnog sektorskog organa potencijalni ključni i važni subjekti u roku od sedam dana od dana dostavljanja zahtjeva, moraju dostaviti sljedeće podatke:

1. naziv subjekta;
2. adresu subjekta;
3. poreski identifikacioni broj subjekta;
4. ime i prezime odgovornog lica;
5. jedinstvenu službenu adresa za prijem elektronske pošte;
6. kontakt telefon odgovornog lica subjekta;
7. podatke o vrsti djelatnosti koju taj subjekt vrši;
8. sektor, odnosno podsektor, u skladu sa članom 13 ovog zakona.

**Usvajanje liste kritičnih i važnih subjekata**

**Član 17**

Nadležni sektorski organ na osnovu dostavljenih podataka iz člana 16 ovog zakona, procjene ispunjenosti opštih kriterijuma iz člana 15 ovog zakona, kao i sektorskih kriterijuma i kriterijumskih pragova iz člana 14 stav 1 tačka 3 ovog zakona, sačinjava predlog liste za određivanje ključnih i važnih subjekata i dostavlja organu državne uprave nadležnom za poslove informacionog društva i elektronske uprave (u daljem tekstu: Ministarstvo).

Ministarstvo objedinjeni predlog liste iz stava 1 ovog člana dostavlja Vladi.

Na osnovu objedinjenog predloga liste iz stava 2 ovog člana, Vlada određuje Listu ključnih i važnih subjekata, koja sadrži sljedeće podatke:

1. naziv subjekta;
2. adresu subjekta;
3. poreski identifikacioni broj subjekta.

Podaci iz člana 16 ovog zakona, predlog iz stava 2 i Lista iz stava 3 ovog člana označavaju se odgovarajućim stepenom tajnosti, u skladu sa zakonom kojim se uređuje tajnost podataka.

**Sektorski registar**

**Član 18**

Na osnovu Liste ključnih i važnih subjekata iz člana 17 stav 3 ovog zakona, nadležni sektorski organ vodi Sektorski registar, koji sadrži podatke iz člana 16 stav 1 ovog zakona.

Ključni i važni subjekat dužan je da, najmanje jednom godišnje, nadležnom sektorskom organu dostavlja obavještenje o promjeni podataka iz člana 16 stav 1. ovog zakona.

Na osnovu dostavljenog obavještenja o promjeni podataka iz stava 2 ovog člana nadležni sektorski organ, dužan je da ažurira Sektorski registar.

Na osnovu obavještenja iz stava 2 ovog člana, nadležni sektorki organ utvrđuje da li je potrebno izvršiti izmjene, odnosno dopune u pogledu određivanja Liste ključnih i važnih subjekata.

Ako utvrdi da je potrebno izvršiti izmjene, odnosno dopune Liste ključnih i važnih subjekata nadležni sektorski organ sačinjava predlog izmjena, odnosno dopuna za za određivanje Liste ključnih i važnih subjekata koji dostavlja Ministarstvu.

Predlog iz stava 4 ovog člana Ministarstvo dostavlja Vladi, radi izmjena, odnosno dopuna Liste iz člana 17 stav 3 ovog zakona.

Registar iz stava 1, obavještenje iz stava 2 ovog člana i predlog izmjena iz stava 5 ovog člana označava se odgovarajućim stepenom tajnosti, u skladu sa zakonom kojim se uređuje tajnost podataka.

**Nacionalni registar**

**Član 19**

Na osnovu Liste iz člana 17 stav 3 ovog člana i podataka iz sektorskih registara Ministarstvo vodi Nacionalni registar ključnih i važnih subjekata (u daljem tekstu: Nacionalni registar).

Nadležni sektorski organ dužan je da Ministarstvu dostavi podatke iz Sektorskog registra, kao i da ga redovno obavještava o svim promjenama podataka iz Sektorskog registra.

Nacionalni registar iz stava 1 ovog člana i obavještenje iz stava 2 ovog člana označava se odgovarajućim stepenom tajnosti, u skladu sa zakonom kojim se uređuje tajnost podataka.

**Obaveze ključnih i važnih subjekata**

**Član 20**

Ključni i važni subjekti dužni su da primjenjuju mjere informacione bezbjednosti od čl. 6 do čl. 11 ovog Zakona.

Ključni i važni subjekti dužni su da odrede zaposleno lice za praćenje primjene mjera informacione bezbjednosti.

Ključni subjekti dužni su da primjenjuju međunarodni standard ISO/IEC 27001 za upravljanje informacionom bezbjednošću.

**IV. NACIONALNI OKVIR ZA BEZBJEDNOST MREŽNIH I INFORMACIONIH SISTEMA**

**AGENCIJA ZA SAJBER BEZBJEDNOST**

**Član 21**

Za sprovođenje i unapređenje mjera informacione bezbjednosti, vršenja nadzora nad primjenom tih mjera, kao i za uspostavljanje sistema za rano otkrivanje i odbranu od sajber prijetnji i incidenata, osniva se Agencija za sajber bezbjednost (u daljem tekstu: Agencija), koja ima svojstvo pravnog lica.

Agencija ima status državne agencije i za svoj rad odgovara Vladi Crne Gore (u daljem tekstu: Vlada).

**Statut Agencije**

**Član 22**

Statutom Agencije uređuju se sjedište, adresa i organizacija Agencije, način odlučivanja organa Agencije i druga pitanja od značaja za rad Agencije.

Na statut Agencije saglasnost daje Vlada.

**Djelokrug rada**

**Član 23**

Agencija:

* 1. priprema stručne osnove za izradu strategijskih dokumenata i akcionih planova, kao i Zakona i podzakonskih akata iz djelokruga rada Agencije;
	2. prati i analizira uporednu zakonsku regulativu i praksu EU i NATO saveznika i predlaže implementaciju najbolje prakse;
	3. donosi uputstva i procedure za postupak testiranja i procjene bezbjednosti mrežnih i informacionih sistema;
	4. daje predloge i preporuke za unaprjeđenje mjera informacione bezbjednosti;
	5. pruža rana upozorenja, najave i informiše o rizicima i incidentima;
	6. sprovodi zaštitu od sajber prijetnji i incidenata na mrežnom i informacionom sistemu ključnih i važnih subjekata osim organa državne uprave, na način iz tač.3, 4 i 5 ovog člana;
	7. postupa po prijavljenim incidentima ključnih i važnih subjekata i vrši analizu istih, osim organa državne uprave;
	8. sprovodi operativnu koordinaciju tokom rješavanja sajber krize u saradnji sa Ministarstvom;
	9. sarađuje sa Ministarstvom, odnosno Vladinim CIRT-om, u cilju jačanja informacione bezbjednosti, razmjene informacija o incidentima i načinu njihovog rješavanja;
	10. prati stanje incidenata u oblasti informacione bezbjednosti;

10) kontinuirano izrađuje analize rizika i incidenata;

11) vodi Registar o prijavljenim incidentima;

12) najmanje jednom godišnje izvještava Vladu o stanju incidenata u saradnji sa Ministarstvom;

13) vrši edukaciju organa, nadležnih sektorskih organa i ključnih i važnih subjekata kroz savjetovanja i obuke u cilju jačanja informacione bezbjednosti;

14) sarađuje sa privatnim i civilnim sektorom, nacionalnim i međunarodnim organizacijama i ključnim i važnim subjektima;

15) učestvuje u razvoju i implementaciji međunarodnih projekata;

16) vrši stručni nadzor nad radom ključnih i važnih subjektima;

17) vrši stručni nadzor nad primjenom mjera informacione bezbjednosti od čl. 6 do 11 kod ključnih i važnih subjekata;

18) vrši stručni nadzor nad primjenom mjera informacione bezbjednosti propisanih međunarodnim standardom ISO/IEC 27001 za upravljanje informacionom bezbjednošću, kod ključnih subjekata;

19) obavlja i druge poslove, u skladu sa ovim zakonom.

**Organi Agencije**

**Član 24**

Organi Agencije su: Savjet Agencije i direktor Agencije.

**Savjet**

**Član 25**

Savjet Agencije (u daljem tekstu: Savjet) imenuje i razrješava Vlada.

Savjet ima pet članova, i to:

* 1. jednog člana kojeg predlaže Ministarstvo;
	2. jednog člana kojeg predlaže Univerzitet Crne Gore;
	3. jednog člana kojeg imenuje Privredna komora Crne Gore;
	4. jednog člana kojeg predlaže Crnogorska akademija nauka i umjetnosti;
	5. jednog člana iz reda zaposlenih u Agenciji.

Predsjednik Savjeta imenuje se iz reda članova Savjeta.

Predsjednik i članovi Savjeta imaju pravo na naknadu za rad u skladu sa zakonom.

**Mandat članova Savjeta**

**Član 26**

Mandat članova Savjeta traje četiri godine.

U slučaju da član Savjeta podnese ostavku ili bude razriješen prije isteka mandata, novi član Savjeta bira se na način i po postupku propisanim ovim zakonom.

Mandat novoizabranog člana Savjeta u slučaju iz stava 2 ovog člana traje do isteka mandata člana Savjeta umjesto kojeg je imenovan.

**Poslovi Savjeta**

**Član 27**

Savjet:

* 1. donosi statut Agencije i druga akta, u skladu sa zakonom;
	2. donosi godišnji program rada i finansijski plan Agencije;
	3. podnosi Vladi izvještaj o radu i finansijski izvještaj Agencije;
	4. imenuje i razrješava direktora Agencije;
	5. usvaja program osnovne obuke za stručno usavršavanje zaposlenih u Agenciji;
	6. utvrđuje predlog zahtjeva za obezbjeđenje budžetskih sredstava Agencije za narednu fiskalnu godinu;
	7. usvaja godišnji izvještaj o radu i finansijski izvještaj Agencije;
	8. donosi plan javnih nabavki Agencije;
	9. donosi Etički kodeks; i
	10. odlučuje o drugim pitanjima u skladu sa zakonom, statutom i drugim aktima Agencije.

**Prestanak mandata**

**Član 28**

Članu Savjeta prestaje mandat:

* 1. istekom vremena na koji je imenovan;
	2. ostavkom; i
	3. razrješenjem.

Član Savjeta iz stava 1 ovog člana razješava se ako:

* 1. je osuđen na bezuslovnu kaznu zatvora;
	2. je osuđen za krivično djelo koje ga čini nedostojnim za vršenje dužnosti;
	3. postupa suprotno zakonu ili aktima Agencije; i
	4. nestručno ili nesavjesno obavlja poslove za koje je imenovan i time nanese štetu Agenciji.

**Direktor Agencije**

**Član 29**

Direktora Agencije (u daljem tekstu: direktor) imenuje Savjet, na osnovu javnog konkursa.

Za direktora može biti imenovano lice, koje pored opštih uslova za zasnivanje radnog odnosa u državnim organima ima visoku stručnu spremu, tri godine radnog iskustva u oblasti informacione bezbjednosti ili sedam godina radnog iskustva u državnim organima ili deset godina radnog iskustva.

Mandat direktora traje pet godina.

**Poslovi direktora**

**Član 30**

Direktor:

* 1. predstavlja Agenciju, rukovodi i organizuje rad u Agenciji;
	2. odgovara za zakonitost i kvalitet rada Agencije;
	3. predlaže Savjetu statut, godišnji program rada i finansijski plan, izvještaj o radu, predlog za obezbjeđenje budžetskih sredstava Agencije za narednu fiskalnu godinu i finansijski izvještaj, kao i druge odluke;
	4. izvršava odluke Savjeta;
	5. upravlja ljudskim i finansijskim resursima;
	6. stara se o obezbjeđivanju javnosti rada Agencije;
	7. utvrđuje akt o unutrašnjoj organizaciji i sistematizaciji radnih mjesta Agencije;
	8. predlaže program osnovne obuke za stručno usavršavanje zaposlenih u Agenciji;
	9. ostvaruje saradnju sa privatnim i civilnim sektorom, nacionalnim i međunarodnim organizacijama i odlučuje o angažovanju domaćih ili stranih stručnjaka, radi ostvarivanja poslova iz svoje nadležnosti;

10) obrazuje radna tijela Agencije; i

11) vrši druge poslove utvrđene zakonom, statutom i drugim aktima Agencije.

**Prestanak mandata**

**Član 31**

Na prestanak mandata direktora primjenjuju se odredbe zakona kojima se uređuju prava i obaveze državnih službenika i namještenika, a koje se odnose na starješine organa uprave.

**Finansiranje**

**Član 32**

Sredstva za rad Agencije obezbjeđuju se u Budžetu Crne Gore.

Odobrena sredstva za funkcionisanje i rad Agencije ne mogu biti manja od 0.2% tekućeg budžeta Crne Gore.

O raspolaganju finansijskim sredstvima iz stava 2 ovog člana Agencija odlučuje samostalno.

**Primjena drugih propisa**

**Član 33**

Na prava, obaveze i odgovornost zaposlenih u Agenciji primjenjuju se propisi o državnim službenicima i namještenicima.

Zaposleni u Agenciji imaju mjesečni dodatak na zaradu u iznosu od 45%.

Direktor Agencije ima pravo na zaradu u visini koja je određena za direktora Agencije za sprječavanje korupcije.

Ovlašćenja iz zakona kojim se uređuju zarade državnih službenika i namještenika vrši direktor, u skladu sa raspoloživim budžetom.

**Savjet za informacionu bezbjednost**

**Član 34**

Radi praćenja razvoja i predlaganja mjera za unaprjeđenje informacione bezbjednosti, praćenja rada i predlaganja aktivnosti Agenciji i Ministarstvu na uspostavljanju sistema zaštite od sajber prijetnji i incidenata, kao i razmatranja stručnih pitanja u oblasti informacione bezbjednosti, Vlada će obrazovati 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 državnog uprave nadležnog za vanjske poslove, organa uprave nadležnog za tajne podatke, Ministarstva, Agencije i Agencije za nacionalnu bezbjednost, a po potrebi i predstavnici drugih organa i institucija.

Savjet za informacionu bezbjednost se obrazuje na vrijeme od četiri godine.

Stručne i administrativno-tehničke poslove za potrebe Savjeta za informacionu bezbjednost obavlja Ministarstvo.

Predsjednik, članovi i sekretar Savjeta za informacionu bezbjednost imaju pravo na naknadu za rad u skladu sa zakonom.

Aktom o obrazovanju Savjeta iz stava 5 ovog člana utvrđuju se zadaci, način rada, i druga pitanja od značaja za rad Savjeta.

**Nadležnosti Ministarstva**

**Član 35**

Ministarstvo:

1. izrađuje strategijska dokumenta i akcione planove, kao i propise iz oblasti informacione bezbjednosti;
2. sarađuje s privatnim i civilnim sektorom, nacionalnim i međunarodnim organizacijama i ključnim i važnim subjektima;
3. predstavlja jedinstvenu nacionalnu kontaktnu tačku za informacionu bezbjednost i sarađuje s jedinstvenim nacionalnim kontakt tačkama drugih država;
4. sarađuje sa Agencijom u cilju jačanja informacione bezbjednost i razmjene informacija o incidentima i načinu njihovog rješavanja;
5. izrađuje nacionalni plan za odgovor na sajber prijetnju, incidente i sajber krizu, u kojem se utvrđuje način upravljanja sajber prijetnjama, incidentima i sajber krizama, u saradnji sa Agencijom;
6. sprovodi zaštitu od sajber prijetnji i incidenata na mrežnom i informacionom sistemu organa državne uprave;
7. postupa po prijavljenim incidentima organa državne uprave i koordinira procesom rješavanja incidenata;
8. vodi Registar o prijavljenim incidentima;
9. obavlja i druge poslove, u skladu sa ovim zakonom.

Poslove iz stava 1, tač. 4 do 9 ovog člana Ministarstvo obavlja preko posebne organizacione jedinice (u daljem tekstu: Vladin CIRT).

Zaposleni u Vladinom CIRT-u imaju mjesečni dodatak na zaradu u iznosu od 45%.

**Tehnički i drugi uslovi za Agenciju i Vladin CIRT**

**Član 36**

Agencija i Vladin CIRT moraju ispunjavati sljedeće tehničke i druge zahtjeve:

1. posjedovati sredstva komunikacije koja neće izazvati prekide, na način da u svakom trenutku imaju na raspolaganju više sredstava za dvosmjernu komunikaciju;
2. posjedovati prostorije i informacione sisteme smještene na sigurnim lokacijama;
3. posjedovati adekvatan sistem za prijavljivanje i upravljanje incidenatima;
4. obezbijediti povjerljivost i pouzdanost svojih operacija;
5. moraju biti opremljeni redundantnim sistemima i rezervnim radnim prostorom kako bi se obezbjedio kontinuitet rada;
6. imati dovoljan broj zaposlenih kako bi se obezbijedila dostupnost 24 sata.

**V. UPRAVLJANJE SAJBER BEZBJEDNOŠĆU**

**Procjena uticaja sajber prijetnje i incidenta i obaveza obavještavanja**

**Član 37**

Organi i ključni i važni subjekti vrše procjenu uticaja svih sajber prijetnji i incidenata u cilju prepoznavanja incidenata koji imaju značajan uticaj na kontinuitet pružanja usluga, u skladu sa kriterijumima iz člana 38 ovog zakona.

Organi i ključni i važni subjekti osim organa državne uprave, dužni su da Agenciji jednom mjesečno dostave izvještaj o svim sajber prijetnjama i incidentima za koje utvrde da nemaju uticaj na kontinuitet pružanja usluga.

Ključni i važni subjekti koji su organi državne uprave dužni su da Vladinom CIRT-u jednom mjesečno dostave izvještaj o svim sajber prijetnjama i incidentima za koje utvrde da nemaju uticaj na kontinuitet pružanja usluga.

Ključni i važni subjekti, osim organa državne uprave dužni su da o svim ozbiljnim sajber prijetnjama koje bi mogle dovesti do incidenta koji ima značajan uticaj na kontinuitet pružanja usluga, i o incidentima koji imaju značajan uticaj na kontinuitet usluga koje pružaju, u skladu sa kriterijumima iz člana 38 ovog zakona, kao i o svim mjerama koje preduzimaju ili planiraju da preduzmu kao odgovor na sajber prijetnju, odnosno incident, obavijeste Agenciju.

Ključni i važni subjekti koji su organi državne uprave dužni su da o svim ozbiljnim sajber prijetnjama i incidentima iz stava 4 ovog člana obavijeste Vladin CIRT.

Ključni i važni subjekti dužni su da obavijeste primaoce svojih usluga o svim ozbiljnim sajber prijetnjama i incidentima iz stava 4 ovog člana, koji bi mogli negativno da utiču na pružanje njihovih usluga, kao i o svim mjerama koje bi ti primaoci usluga trebalo da preduzmu kao odgovor na sajber prijetnje i incidente.

Organi su dužni da o svim ozbiljnim sajber prijetnjama i incidentima iz stava 4 ovog člana obavijeste Agenciju.

Izvještaje iz st. 2 i 3 ovog člana i obavještenja iz st. 4 do 7 ovog člana označavaju se odgovarajućim stepenom tajnosti, u skladu sa zakonom kojim se uređuje tajnost podataka.

Agencija i Vladin CIRT, nakon prijema obavještenja iz st. 4, 5 i 7 ovog člana u obavezi su da obavijeste nadležne organe, u skladu sa posebnim propisima.

**Incidenti sa značajnim uticajem na kontinuitet pružanja usluga**

**Član 38**

Incident sa značajnim uticajem na kontinuitet pružanja usluga utvrđuje se prema sljedećim kriterijumima:

1) broju korisnika pogođenih prekidom pružanja usluge, odnosno značajnih teškoća u pružanju te usluge;

2) trajanju incidenta;

3) geografskoj raširenosti incidenta;

4) utvrđenim sektorskim kriterijumima i kriterijumskim pragovima iz člana 14 stav 1 tačka 3 ovog zakona.

**Vrste obaviještenja**

**Član 39**

Ključni i važni subjekti dužni su da o svim incidentima sa značajnim uticajem na kontinuitet pružanja usluga, Agenciji, odnosno Vladinom CIRT-u dostave:

1. početno obavještenje o incidentu sa značajnim uticajem na kontinuitet pružanja usluga;
2. prvi izvještaj i dodatne izvještaje tokom trajanja incidenta;
3. završni izvještaj o incidentu.

**Početno obavještenje o incidentu sa značajnim uticajem**

**Član 40**

Početno obavještenje o incidentu sa značajnim uticajem na kontinuitet pružanja usluga dostavlja se odmah, a najkasnije u roku od 24 sata od trenutka otkrivanja tog incidenta.

Početno obavještenje o incidentu sa značajnim uticajem na kontinuitet pružanja usluga mora da sadrži opis incidenta i njegove očekivane posljedice, zasnovane na svim podacima koji su ključnom i važnom subjektu dostupni tokom procjene uticaja incidenta, u skladu sa kriterijumima iz člana 38 ovog zakona i podacima dostupnim nakon otkrivanja tog incidenta.

**Izvještaj tokom trajanja incidenta**

**Član 41**

Prvi izvještaj tokom trajanja incidenta sa značajnim uticajem na kontinuitet pružanja usluga dostavlja se najkasnije u roku od 72 sata od podnošenja početnog obavještenja o incidentu i mora sadržati detaljan opis incidenta i njegovih nastalih i mogućih posljedica, u skladu sa kriterijumima iz člana 38 ovog zakona.

Ključni i važni subjekti dužni su da tokom trajanja incidenta sa značajnim uticajem na kontinuitet pružanja usluga dostavljaju i dodatne izvještaje o tom incidentu ako saznaju za nove podatke ili nove okolnosti koje su od uticaja na sami incident.

**Završni izvještaj o incidentu**

**Član 42**

Ključni i važni subjekti dužni su podnijeti završni izvještaj o incidentu sa značajnim uticajem na kontinuitet pružanja usluga, najkasnije u roku od 30 dana od dana rješavanja nastalog incidenta.

Završni izvještaj o incidentu mora sadržati sljedeće:

1. podatke o incidentu prema kriterijumima iz člana 38;
2. analizu uzroka incidenta;
3. mjere koje su primijenjene za reagovanje na incident;
4. mjere koje su primijenjene za sprečavanje ponovnog incidenta.

Obavještenje iz člana 40 i izvještaji iz čl. 41 i 42 ovog zakona označavaju se odgovarajućim stepenom tajnosti, u skladu sa zakonom kojim se uređuje tajnost podataka.

**Rješavanje incidenata**

**Član 43**

Organi i ključni i važni subjekti sajber prijetnje i incidente koji nemaju značajan uticaj na kontinuitet pružanja usluga rješavanju bez učešća Agencije, odnosno Vladinog CIRT-a.

Agencija se po prijemu obavještenja iz člana 37 stav 7 ovog zakona o incidentu sa značajnim uticajem na kontinuitet pružanja usluga, može uključiti u rješavanje, po svojoj procjeni, u skladu sa mogućnostima i raspoloživim kapacitetom.

Agencija, odnosno Vladin CIRT po prijemu obavještenja iz člana 40 ovog zakona o incidentu sa značajnim uticajem na kontinuitet pružanja usluga sprovodi analizu i prema nivou značaja i načinu reagovanja na incident vrši klasifikaciju incidenta koji može biti niskog, srednjeg ili visokog nivoa.

Ako je incident sa značajnim uticajem na kontinuitet pružanja usluga niskog nivoa, Agencija, odnosno Vladin CIRT će nakon prijema obavještenja o incidentu, u roku od 24 sata dati odgovor podnosiocu obavještenja o početnim informacijama o incidentu i, na njegov zahtjev, smjernice o primjeni mjera za reagovanje na nastali incident.

Agencija, odnosno Vladin CIRT se u rješavanje incidenta niskog nivoa uključuje u zavisnosti od potrebe i po svojoj procjeni.

Ako je incident sa značajnim uticajem na kontinuitet pružanja usluga srednjeg nivoa, Agencija, odnosno Vladin CIRT će nakon prijema obavještenja o incidentu, u roku od 24 sata dati odgovor podnosiocu obavještenja o početnim informacijama o incidentu i, na njegov zahtjev, smjernice o primjeni mjera za reagovanje na nastali incident.

Agencija, odnosno Vladin CIRT uključuje se u rješavanje incidenta srednjeg nivoa.

Ako je incident sa značajnim uticajem na kontinuitet pružanja usluga visokog nivoa koji je doveo do značajnog oštećenja, poremećaja i negativnih uticaja na podatke i mrežne i informacione sisteme, korisnike tih sistema i druge ključne i važne subjekte i organe, Agencija i Vladin CIRT uključuju se zajednički u rješavanje incidenta.

Agencija i Vladin CIRT u rješavanju incidenata iz stava 8 ovog člana mogu koristiti ekspertsku i stručnu pomoć nacionalnih i međunarodnih institucija i organizacija.

Ako Agencija i Vladin CIRT ne mogu samostalno da riješe incident visokog nivoa iz stava 8 ovog člana, Ministarstvo u saradnji sa Agencijom priprema predlog akta Vladi za proglašenje sajber krize, uz obrazloženje o razlozima za proglašenje sajber krize, kao i predlogom mjera za rješavanje te krize.

Bliži način određivanja nivoa incidenta iz stava 3 ovog član prema nivou značaja i način reagovanja na incidente, na predlog Agencije, uređuje Vlada.

Obavještenja iz čl. 2, 3,4, 6, 8 ovog člana , kao i predlog akta Vladi iz stava 10 ovog člana označavaju se odgovarajućim stepenom tajnosti, u skladu sa zakonom kojim se uređuje tajnost podataka.

**Rješavanje sabjer krize**

**Član 44**

Na osnovu predloga akta iz člana 43 stav 10 ovog zakona, Vlada cijeni razloge za proglašenje sajber krize.

Ako Vlada procijeni da su razlozi za proglašenje sajber krize opravdani donosi akt o proglašenju sajber krize, sa mjerama za rješavanje te krize i zadužuje organe koji su dužni da učestvuju u rješavanju sajber krize.

Ministarstvo u ime Vlade sprovodi stratešku koordinaciju rješavanja sajber krize i redovno izvještava Vladu o svim aktivnostima.

Agencija u saradnji sa Ministarstvom sprovodi operativnu koordinaciju rješavanja sajber krize.

Vlada po završetku sajber krize donosi akt kojim proglašava da je sajber kriza završena.

**Informisanje javnosti o incidentu**

**Član 45**

Ako je za sprečavanje ozbiljne sajber prijetnje i incidenta ili rješavanje incidenta iz člana 37 ovog zakona koji je u toku, neophodno obavijestiti javnost ili ako je otkrivanje incidenta u javnom interesu zbog nekog drugog razloga, Agencija u saradnji sa Ministarstvom, nakon savjetovanja sa ključnim, odnosno važnim subjektom ili organom koji je izložen incidentu, obaviještava javnost o incidentu ili zahtijeva od ključnog, odnosno važnog subjekta ili organa da to učini.

**VI. NADZOR**

**Član 46**

Upravni nadzor nad sprovođenjem ovog zakona, drugih propisa i akata donijetih na osnovu ovog zakona, vrši Ministarstvo.

**Inspekcijski i stručni nadzor**

**Član 47**

Inspekcijski nadzor nad primjenom ovog zakona vrši organ uprave nadležan za inspekcijske poslove, preko inspektora za usluge informacionog društva (u daljem tekstu: inspektor).

Stručni nadzor nad primjenom ovog zakona vrši Agencija, preko zaposlenog lica koje je ovlašćeno za vršenje nadzora (u daljem tekstu: nadzornik).

Inspektor, odnosno nadzornik prilikom inspekcijskog, odnosno stručnog nadzora, svojstvo organa nadzora dokazuje službenom legitimacijom.

Organi koji vrše inspekcijski i stručni nadzor, dužni su u poslovima nadzora ostvarivati potrebnu koordinaciju, komunikaciju i saradnju.

Radi vršenja nadzora, organi i ključni i važni subjekti iz člana 2 ovog zakona dužni su da inspektoru, odnosno nadzorniku 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.

**Inspekcijski nadzor**

**Član 48**

Poslove inspekcijskog nadzora iz člana 47 ovog zakona inspektor vrši u skladu sa ovim zakonom i posebnim zakonima kojima se uređuju inspekcijski nadzor.

Oblik i sadržaj službene legitimacije za obavljanje poslova inspekcijskog nadzora propisuje Ministarstvo.

**Nadležnost i ovlašćenja inspektora**

**Član 49**

Pored ovlašćenja utvrđenih posebnim zakonom kojim se uređuje oblast inspekcijskog nadzora, inspektor ima ovlašćenja da ključnim i važnim subjektima:

1. naloži donošenje politike analize rizika i bezbjednosti mrežnih i informacionih sistema;
2. naloži donošenje politike postupanja sa incidentima (sprječavanje, otkrivanje i odgovor na incidente);
3. naloži donošenje plana kontinuiteta poslovanja i postupanja u sajber krizama;
4. naloži donošenje politike bezbjednosti kojom se uređuje bezbjednost lanca snadbijevanja između subjekta koji upravlja mrežnim i informacionim sistemom i dobavljača ili pružaoca usluga;
5. naloži donošenje akata kojima se uređuje upostavljanje, razvoj i održavanje mrežnih i informacionih sistema, uključujući bezbjednosne aspekte;
6. naloži donošenje politike i postupke za procjenu efikasnosti mjera upravljanja sajber bezbjednosnim rizicima;
7. naloži primjenu kriptovane zaštite podataka, ukoliko priroda posla to zahtjeva;
8. da upozorenje da su dužni ispunjavati obaveze obavještavanja iz ovog zakona na propisan način i u propisanom roku;
9. naloži da obavijeste primaoce svojih usluga o sajber prijetnjama i incidentima koji bi mogli negativno uticati na pružanje njihovih usluga, kao i o svim mjerama koje bi trebali preduzeti kao odgovor na sajber prijetnje i incidente;

10) naloži da imenuju zaposleno lice za praćenje primjene mjera informacione bezbjednosti;

11) privremeno zabrani rad i pružanje usluga koje mogu predstavljati sajber prijetnju i incident, koji mogu imati negativan uticaj na podatke i mrežne i informacione sisteme, korisnike tih sistema i druge ključne i važne subjekte i organe.

Pored ovlašćenja iz stava 1 ovog člana, inspektor ima ovlašćenja da ključnim subjektima naloži primjenu standarda ISO/IEC 27001 za upravljanje informacionom bezbjednošću.

Pored ovlašćenja utvrđenih posebnim zakonom kojim se uređuje oblast inspekcijskog nadzora, inspektor ima ovlašćenja da organima naloži primjenu mjera informacione bezbjednosti od čl. 6 do 10 ovog Zakona, osim mjera iz člana 8, stav 1, tačka 3 ovog Zakona.

**Stručni nadzor**

**Član 50**

Nadzornik obavlja poslove stručnog nadzora na osnovu ovlašćenja iz ovog zakona i propisa donijetih na osnovu ovog zakona.

Oblik i sadržaj službene legitimacije za obavljanje poslova stručnog nadzora propisuje Agencija.

**Nadležnost i ovlašćenja nadzornika**

**Član 51**

U postupku stručnog nadzora, nadzornik ima ovlašćenje da ključnim i važnim subjektima:

1. kontroliše politiku analize rizika i bezbjednosti mrežnih i informacionih sistema;
2. kontroliše politiku postupanja sa incidentima (sprječavanje, otkrivanje i odgovor na incidente);
3. kontroliše plan kontinuiteta poslovanja i postupanja u sajber krizama;
4. kontroliše politiku bezbjednosti kojom se uređuje bezbjednost lanca snadbijevanja između subjekta koji upravlja mrežnim i informacionim sistemom i dobavljača ili pružaoca usluga;
5. kontroliše akte kojima se uređuje upostavljanje, razvoj i održavanje mrežnih i informacionih sistema, uključujući bezbjednosne aspekte;
6. kontroliše politiku i postupke za procjenu efikasnosti mjera upravljanja sajber bezbjednosnim rizicima;
7. kontroliše upotrebu kriptovane zaštite podataka, ukoliko priroda posla to zahtjeva;
8. kontroliše da li su obavijestili primaoce svojih usluga o sajber prijetnjama i incidentima koji bi mogli negativno uticati na pružanje njihovih usluga, kao i o svim mjerama koje bi trebali preduzeti kao odgovor na sajber prijetnje i incidente;
9. kontroliše da li su ispunili obaveze obavještavanja iz ovog zakona na propisan način i u propisanom roku;

10) kontroliše da li su imenovali zaposleno lice za praćenje primjene mjera informacione bezbjednosti.

Nadzornik svoja ovlašćenja i nadležnosti sprovodi i na osnovu podataka prikupljenih u postupku nadzora ili na osnovu podataka prikupljenih u skladu sa stavom 4 ovog člana.

Nadzornik je dužan da o svim uočenim nedostacima najkasnije u roku od tri dana od dana uočavanja nedostataka obavijest inspektora.

Agencija može, osim nadzornika, ovlastiti i druga zaposlena lica da na licu mjesta, kod ključnih i važnih subjekata, izvrše kontrolu i uzimanje podataka neophodnih za izvršavanje poslova iz nadležnosti Agencije.

Nadzornik i lica iz stava 4 ovog člana dužna su da čuvaju tajnost svih informacija o radu ključnih i važnih subjekata za koje saznaju pri svom radu, u skladu sa ovim zakonom, kao i zakonom koji uređuje pitanja povjerljivosti i zaštite podataka.

Na postupak stručnog nadzora shodno se primjenjuju odredbe zakona kojim se uređuje oblast inspekcijskog nadzora.

**Međusobna saradnja**

**Član 52**

Inspektor i nadzornik u vršenju poslova inspekcijskog i stručnog nadzora međusobno sarađuju.

U vršenju inspekcijskog nadzora inspektor je dužan da o uočenim nepravilnostima obavijesti Agenciju.

U vršenju stručnog nadzora nadzornik je dužan da o uočenim nepravilnostima obavijesti inspektora, na način iz člana 51 stav 3 ovog zakona, radi preuzimanja mjera iz njegove nadležnosti.

**Zaštita podataka o ličnosti**

**Član 53**

Podaci o ličnosti koriste se i obrađuju u skladu sa zakonom kojim se uređuje zaštita podataka o ličnosti.

**VII. KAZNENE ODREDBE**

**Član 54**

Novčanom kaznom u iznosu od 500 do 20.000 eura kazniće se za prekršaj pravno lice koje je kao ključni subjekat upisano u Nacionalni registar, ako:

1. nadležnom sektorskom organu ne dostavlja podatke (član 16);
2. nadležnom sektorskom organu najmanje jednom godišnje ne dostavlja obavještenje o promjeni podataka iz člana 16 stav 1 ovog zakona (član 18 stav 2);
3. ne primjenjuje mjere informacione bezbjednosti (član 20 stav 1);
4. ne odredi zaposleno lice za praćenje primjene mjera informacione bezbjednosti (član 20 stav 2);
5. ne primjenjuje međunarodni standard ISO/IEC 27001 za upravljanje informacionom bezbjednošću (član 20 stav 3);
6. Agenciji jednom mjesečno ne dostavi izvještaj o svim sajber prijetnjama i incidentima za koje utvrdi da nemaju uticaj na kontinuitet pružanja usluga (član 37 stav 2).
7. ne obavijeste Agenciju o svim ozbiljnim sajber prijetnjama koje bi mogle dovesti do incidenta koji ima značajan uticaj na kontinuitet pružanja usluga, i o incidentima koji imaju značajan uticaj na kontinuitet usluga koje pružaju, kao i o svim mjerama koje preduzimaju ili planiraju da preduzmu kao odgovor na sajber prijetnju, odnosno incident (član 37 stav 4);
8. primaoce svojih usluga ne obavijeste o svim ozbiljnim sajber prijetnjama i incidentima koji bi mogli negativno da utiču na pružanje njihovih usluga, kao i o svim mjerama koje bi ti primaoci usluga trebalo da preduzmu kao odgovor na sajber prijetnje i incidente (član 37 stav 6);
9. početno obavještenje o incidentu sa značajnim uticajem na kontinuitet pružanja usluga ne dostavi u roku od 24 sata od trenuta otkrivanja tog incidenta (član 40 stav 1);
10. prvi izvještaj tokom trajanja incidenta sa značajnim uticajem na kontinuitet pružanja usluga ne dostavi najkasnije u roku od 72 sata od podnošenja početnog obavještenja o incidentu koji sadrži detaljan opis incidenta i njegovih nastalih i mogućih posljedica, u skladu sa kriterijumima iz člana 38 ovog zakona (član 41 stav 1);
11. tokom trajanja incidenta sa značajnim uticajem na kontinuitet pružanja usluga dostavljaju ne dostavlja dodatne izvještaje o tom incidentu ako sazna za nove podatke ili nove okolnosti koje su od uticaja na sami incident (član 41 stav 2);
12. ne podnese završni izvještaj o incidentu sa značajnim uticajem na kontinuitet pružanja usluga, najkasnije u roku od 30 dana od dana rješavanja nastalog incidenta koji mora sadržati: podatke o incidentu, analizi uzroka incidenta, mjere koje su primijenjene za reagovanje na incident i mjere koje su primijenjene za sprečavanja ponovnog incidenta (član 42);
13. inspektoru, odnosno nadzorniku ne omogući pristup prostoru, računarskoj opremi i uređajima, kao i bez odlaganja stave na uvid ili dostave potrebne podatke i dokumentaciju u vezi sa predmetom nadzora (član 47 stav 5).

Za prekršaj iz stava 1 ovog člana kazniće se fizičko lice novčanom kaznom u iznosu od 30 eura do 1.500 eura.

**Član 55**

Novčanom kaznom u iznosu od 500 do 10.000 eura kazniće se za prekršaj pravno lice koje je kao važni subjekat upisano u Nacionalni registar, ako:

1. nadležnom sektorskom organu ne dostavlja podatke (član 16);
2. nadležnom sektorskom organu ne dostavlja obavještenje o promjeni podataka iz člana 16 stav 1 ovog zaona (član 18 stav 2);
3. ne primjenjuje mjere informacione bezbjednosti (član 20 stav 1);
4. ne odredi zaposleno lice za praćenje primjene mjera informacione bezbjednosti (član 20 stav 2);
5. Agenciji jednom mjesečno ne dostave izvještaj o svim sajber prijetnjama i incidentima za koje utvrde da nemaju uticaj na kontinuitet pružanja usluga (član 37 st. 2 i 3);
6. Ne obavijesti Agenciju, odnosno Vladin CIRT o svim ozbiljnim sajber prijetnjama koje bi mogle dovesti do incidenta koji ima značajan uticaj na kontinuitet pružanja usluga, i o incidentima koji imaju značajan uticaj na kontinuitet usluga koje pružaju, kao i o svim mjerama koje preduzimaju ili planiraju da preduzmu kao odgovor na sajber prijetnju, odnosno incident, (član 37 stav 4);
7. primaoce svojih usluga ne obavijeste o svim ozbiljnim sajber prijetnjama i incidentima koji bi mogli negativno da utiču na pružanje njihovih usluga, kao i o svim mjerama koje bi ti primaoci usluga trebalo da preduzmu kao odgovor na sajber prijetnje i incidente (član 37 stav 6);
8. početno obavještenje o incidentu sa značajnim uticajem na kontinuitet pružanja usluga ne dostavi u roku od 24 sata od trenuta otkrivanja tog incidenta (član 40 stav 1);
9. početno obavještenje o incidentu sa značajnim uticajem na kontinuitet pružanja usluga ne dostavi sa opisom incidenta i njegovih očekivanih posljedica, zasnovanih na podacima koji su mu dostupni tokom procjene uticaja incidenta (član 40 stav 2);
10. prvi izvještaj tokom trajanja incidenta sa značajnim uticajem na kontinuitet pružanja usluga ne dostavi najkasnije u roku od 72 sata od podnošenja početnog obavještenja o incidentu koji sadrži detaljan opis incidenta i njegovih nastalih i mogućih posljedica, u skladu sa kriterijumima iz člana 38 ovog zakona (član 41 stav 1);
11. tokom trajanja incidenta sa značajnim uticajem na kontinuitet pružanja usluga dostavljaju ne dostavlja dodatne izvještaje o tom incidentu ako sazna za nove podatke ili nove okolnosti koje su od uticaja na sami incident (član 41 stav 2);
12. ne podnese završni izvještaj o incidentu sa značajnim uticajem na kontinuitet pružanja usluga, najkasnije u roku od 30 dana od dana rješavanja nastalog incidenta koji mora sadržati: podatke o incidentu, analizi uzroka incidenta, mjere koje su primijenjene za reagovanje na incident i mjere koje su primijenjene za sprečavanja ponovnog incidenta (član 42);
13. inspektoru, odnosno nadzorniku ne omogući pristup prostoru, računarskoj opremi i uređajima, kao i bez odlaganja stave na uvid ili dostave potrebne podatke i dokumentaciju u vezi sa predmetom nadzora (član 47 stav 5).

Za prekršaj iz stava 1 ovog člana kazniće se fizičko lice novčanom kaznom u iznosu od 30 eura do 1.500 eura.

**Član 56**

Novčanom kaznom u iznosu od 500 do 5.000 eura kazniće se za prekršaj pravno lice koje je organ, ako:

1. ne primjenjuje mjere informacione bezbjednosti (član 12);
2. Agenciji jednom mjesečno ne dostave izvještaj o svim sajber prijetnjama i incidentima za koje utvrde da nemaju uticaj na kontinuitet pružanja usluga (član 37 stav 2);
3. Ne obavijeste Agenciju o svim ozbiljnim sajber prijetnjama i incidentima (član 37 stav 7);
4. inspektoru, odnosno nadzorniku ne omogući 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 (član 47 stav 5).

Za prekršaj iz stava 1 ovog člana kazniće se fizičko lice novčanom kaznom u iznosu od 30 eura do 1.500 eura.

U slučaju ponavljanja povreda iz stava 1 ovog člana izreći će se zabrana obavljanja djelatnosti u trajanju od tri do šest mjeseci.

**VIII. PRELAZNE I ZAVRŠNE ODREDBE**

**Rok za donošenje podzakonskih akata**

**Član 57**

Propisi za sprovođenje ovog zakona donijeće se u roku od šest mjeseci od dana stupanja na snagu ovog zakona.

**Rok za dostavljanja Predloga Liste ključnih i važnih subjekata**

**Član 58**

Nadležni sektorski organi dužni su da predlog Liste ključnih i važnih subjekata iz člana 17 stav 1 dostave Ministarstvu, najkasnije u roku od devet mjeseci od dana stupanja na snagu ovog zakona.

**Rok za** **certifikovanje za primjenu međunarodnog standarda**

**Član 59**

Ključni subjekti dužni su da se certifikuju za primjenu međunarodnog standarda ISO/IEC 27001 za upravljanje informacionom bezbjednošću, u roku od 30 mjeseci od dana stupanja na snagu ovog zakona.

**Rok za** **izbor članova Savjeta i direktora Agencije**

**Član 60**

Izbor članova Savjeta Agencije izvršiće se u roku od 60 dana od dana stupanja na snagu ovog zakona.

Izbor direktora Agencije izvršiće se u roku od 90 dana od dana izbora Savjeta.

Do izbora direktora Agencije na način iz stava 2 ovog člana Vlada će, na predlog ministra javne uprave odrediti vršioca dužnosti direktora Agencije, u roku od 15 dana od dana stupanja na snagu ovog zakona.

Vršilac dužnosti direktora Agencije obavljaće dužnost do izbora direktora Agencije, u skladu sa ovim zakonom.

**Donošenje akata Agencije i** **preuzimanje državnih službenika**

**Član 61**

Statut Agencije, akt o unutrašnjoj organizaciji i sistematizaciji Agencije, poslovnik o radu Savjeta, i drugi akti Agencije, donijeće se u roku od 90 dana od dana izbora vršioca dužnosti direktora Agencije.

Donošenjem akta o unutrašnjoj organizaciji i sistematizaciji iz stava 1 ovog člana Agencija će od Direkcije za zaštitu tajnih podataka preuzeti državne službenike koji su vršili poslove u okviru organizacione jedinice CIRT, opremu i službenu dokumentaciju.

Državni službenici iz stava 2 ovog člana, do donošenja akta o raspoređivanju u skladu sa aktom u unutrašnjoj organizaciji i sistematizaciji iz stava 1 ovog člana, nastavljaju sa radom u zvanjima koja su stekli prije preuzimanja.

**Početak rada Agencije**

**Član 62**

Agencija će početi sa radom 01. avgusta 2023. godine.

**Rad Savjeta za informacionu bezbejdnost
Član 63**

Savjet za informacionu bezbjednost koji se obrazovan u skladu sa Zakonom o informacionoj bezbjednosti ("Službeni list CG" br. 14/10, 40/16 i 74/20) nastavlja sa radom do obrazovanja Savjeta za informacionu bezbjednost u skladu sa ovim zakonom.

**Prestanak važenja propisa**

**Član 64**

Danom početka primjene ovog zakona prestaje da važi Zakon o informacionoj bezbjednosti ("Službeni list CG" br. 14/10, 40/16 i 74/20) i odredbe člana 74 stav 1 tačka 8b, član 74a, 87d st. 2 i 3, 87e i 87f, Zakona o tajnosti podataka ("Službeni list CG" br. 14/08, 76/09, 41/10, 40/11, 38/12, 44/12, 14/13, 18/14, 48/15 i 74/20).

**Stupanje na snagu i početak primjene**

**Član 65**

Ovaj zakon stupa na snagu osmog dana od dana objavljivanja u "Službenom listu Crne Gore", a primjenjivaće se od 01. avgusta 2023. godine.

**OBRAZLOŽENJE**

**USTAVNI OSNOV ZA DONOŠENJE ZAKONA**

Ustavni osnov za donošenje ovog zakona sadržan je u odredbi člana 16 Ustava Crne Gore kojim je, između ostalog, propisano da se zakonom uređuju određena pitanja od interesa za Crnu Goru.

**RAZLOZI ZA DONOŠENJE ZAKONA**

Donošenju Zakona o informacionoj bezbjednosti pristupilo se u cilju jačanja informacione bezbjednosti u Crnoj Gori, prepoznavanjem mehanizama za jačanje informacione bezbjednosti (Agencija za sajber bezbjednost i Vladin CIRT), stvaranju jasno definisanog nacionalnog okvira za upravljanje sajber bezbjednošću, kao i potrebi usaglašavanja sa Direktivom (EU) 2022/2555 EVROPSKOG PARLAMENTA I SAVJETA od 14. decembra 2022. godine o mjerama za visoki zajednički nivo sajber bezbjednosti širom Unije, izmjeni Uredbe (EU) br. 910/2014 i Direktive (EU) 2018/1972 i o ukidanju Direktive (EU) 2016/1148 (NIS 2 Direktiva).

Naime, Crna Gora se našla na meti sajber napada visokog nivoa sofisticiranosti, koji se dogodio 20. avgusta 2022. godine. Predmetnim sajber napadom primarno je pogođena Vladina informatička infrastruktura i informaciono-komunikaciona mreža organa, koji su bili pod kontinuiranim sajber napadima velikog intenziteta i kompleksnosti. Nastali sajber napad onemogućio je nesmetan rad i funkcionisanje javne uprave, što se odrazilo i na pripredu i građane, pa se sa elektronskog poslovanja moralo preći na tradicionalni način poslovanja. Ugrožen je veliki broj informacionih sistema, od kojih je zavisio kontinuitet pružanja usluga i ostvarena značajna šteta, koja je iziskivala oporavak u više faza.

Donošenju ovog zakona pristupilo se i radi prevazilaženja problema koji su se pojavili u praktičnoj primjeni važećeg propisa, kao što su: nedostatak opštih kriterijuma za prepoznavanje ključnih i važnih subjekata od kojih zavisi vršenje djelatnosti od javnog interesa; nedostatak jasno definisanog postupka obavještavanja o sajber prijetnjama i incidentima; precizno nedefinisan postupak rješavanja incidenata i postupanje u slučaju sajber prijetnji i incidenata sa značajnim uticajem; rješavanje i postupanje u slučaju sajber krize; nepostojanje nadležnih tijela odgovornih za sajber bezbjednost i za nadzorne zadake sa propisanim nadležnostima; nepostojanje obaveze izvještavanja o incidentima na nivou subjekata; nepostojanje jasno propisanih mjera u pogledu sajber bezbjednosnih rizika; nepostojanje stručnog nadzora i nepostojanje kaznenih odredbi.

Donošenjem Zakona o informacionoj bezbjednosti značajno bi se unaprijedila ova oblast, uspostavile jasne nadležnosti i procedure u slučaju budućih eventualnih sajber prijetnji i incidenata, kao i mjere informacione bezbjednosti koje prate trendove Evropske unije. Takođe, uspostavio bi se održiv sistem za efikasno otkrivanje i odbranu od sajber prijetnji i incidenata visokog nivoa sofisticiranosti i osigurao kontinuitet pružanja usluga u slučaju budućih incidenata, čime se doprinosi efikasnijem funkcionisanju privrede i društva uopšte i jačanju povjerenja korisnika elektronske uprave u zaštitu njihovih podataka.

**USAGLAŠENOST SA PRAVNOM TEKOVINOM EVROPSKE UNIJE I POTVRĐENIM MEĐUNARODNIM KONVENCIJAMA**

Ovaj zakon usklađen je sa Direktivom (EU) 2022/2555 EVROPSKOG PARLAMENTA I SAVJETA od 14. decembra 2022. godine o mjerama za visoki zajednički nivo sajber bezbjednosti širom Unije, izmjeni Uredbe (EU) br. 910/2014 i Direktive (EU) 2018/1972 i o ukidanju Direktive (EU) 2016/1148 (NIS 2 Direktiva).

**OBJAŠNJENJE OSNOVNIH PRAVNIH INSTITUTA**

 I. OSNOVNE ODREDBE

 Kada je u pitanju poglavlje I. Nacrta zakona o informacionoj bezbjednosti **odredbom člana 1** ovog zakonadefinisan je predmet zakona,odnosno da se ovim zakonom propisuju mjere informacione bezbjednosti za postizanje visokog nivoa informacione bezbjednosti mrežnih i informacionih sistema, postupci za prepoznavanje i određivanje ključnih i važnih subjekata, nacionalni okvir za bezbjednost mrežnih i informacionih sistema, postupak upravljanja sajber bezbjednošću, nadzor nad ključnim i važnim subjektima, kao i druga pitanja od značaja za postizanje visokog nivoa informacione bezbjednosti.

**Odredbom člana 2** propisuje se obaveza primjene na državne organe, organe državne uprave, organe jedinica lokalne samouprave, organe lokalne uprave, i službe obrazovane u skladu sa zakonom kojim se uređuje lokalna samouprava, privredna društva, pravna lica sa javnim ovlašćenjima i druga pravna i fizičkih lica koja ostvaruju pristup ili postupaju sa podacima i koji koriste i upravljaju mrežnim i informacionim sistemima (organi) kao i na ključni i važni subjekti, u smislu ovog zakona.

**Odredbama čl. 2 i 3** ovog zakona propisano je da se ovaj zakon ne primjenjuje se na organ državne uprave nadležan za poslove odbrane, organ državne uprave nadležan za poslove policije, Vojsku Crne Gore i Agenciju za nacionalnu bezbjednost, kao i na podatke čija se informaciona bezbjednost obezbjeđuje u skladu sa propisima kojima se uređuje tajnost podataka, te da izrazi koji se u ovom zakonu koriste za fizička lica u muškom rodu podrazumijevaju iste izraze u ženskom rodu. **Odredbom člana 5** definisani su izrazi upotrijebljeni u ovom zakonu.

II. MJERE INFORMACIONE BEZBJEDNOSTI

U poglavlju II. Nacrta zakona definisane su mjere informacione bezbjednosti i **članom 6** je propisano da se informaciona bezbjednost obezbjeđuje primjenom mjera u cilju zaštite povjerljivosti, cjelovitosti i dostupnosti podatka, i zaštite od sajber prijetnji i incidenata mrežnih i informacionih sistema, korisnika tih sistema i drugih lica na koje one utiču u skladu sa ovim zakonom, dok je u **članu 7** detaljnije definisano, šta podrazumijeva povjerljivost, cjelovitost i dostupnost podataka, kao i šta obuhvata zaštita podataka i na šta se odnosi.

**Odredbom člana 8** ovog zakonadefinisano je da zaštita od sajber prijetnji i incidenata mrežnih i informacionih sistema podrazumijeva fizičku zaštitu, zaštitu mrežnih i informacionih sistema i upravljanje sajber bezbjednosnim rizicima, dok je **odredbama čl. 9, 10 i 11** propisano šta obuhvata fizička zaštita i zaštita mrežnog i informacionog sistema, kao i na koju primjenu mjera se odnosi upravljanje sajber bezbjednosnim rizicima, odnosno šta te mjere podrazumijevaju**. Odredbom člana 12** propisano je koje mjere informacione bezbjednosti su organi, definisani u smislu ovog zakona, dužni da primjenjuju.

III. KLJUČNI I VAŽNI SUBJEKTI

U poglavlju III. definisan je postupak prepoznavanja ključnih i važnih subjekata, obaveze nadležnih sektorskih organa, kao i ključnih i važnih subjekata, u smislu ovog zakona.

Naime, **odredbama člana 13** ovog zakona propisano je da je nadležni sektorski organ dužan da izvrši prepoznavanje ključnih i važnih subjekata u okviru sektora, za koji je nadležan uz navođenje sektora, odnosno podsektora u kojima treba prepoznati ključne i važne subjekte.

Navedenom odredbom propisano je da ključne subjekte treba prepoznati u sektorima: energetika (podsektor: električna energija; centralizovano grijanje i hlađenje; nafta; plin; vodonik), transport (podsektor: vazdušni; željeznički; vodeni i putni transport), bankarstvo, infrastruktura finansijskog tržišta, zdravlje, voda za piće, otpadne vode, digitalna infrastruktura, upravljanje uslugama informaciono-komunikacionih tehnologija, javna uprava, i svemir. Istom odredbom je propisano da važne subjekte treba prepoznati u sektorima: poštanske i kurirske usluge, upravljanje otpadom, izrada, proizvodnja i distribucija hemikalija, proizvodnja, prerada i distribucija hrane, proizvodnja drugih važnih stvari (podsektor: proizvodnja medicinskih proizvoda i in vitro dijagnostičkih medicinskih proizvoda; proizvodnja računara, elektronskih i optičkih proizvoda; proizvodnja električne opreme; proizvodnja mašina i uređaja; proizvodnja motornih vozila, prikolica i poluprikolica; proizvodnja ostale opreme za transport), i pružaoci digitalnih usluga.

Nadalje, **odredbama člana 14 ovog** zakonapropisane su obaveze nadležnog sektorskog organa i to da: sačini listu svih organa u sektoru za koje je nadležan; pokrene postupak prikupljanja informacija o potencijalnim ključnim i važnim subjektima iz sektora za koji je nadležan; utvrdi sektorske kriterijume i kriterijumske pragove za prepoznavanje ključnih i važnih subjekata, u saradnji sa određenim podsektorom; utvrdi listu potencijalnih ključnih i važnih subjekata primjenom opštih kriterijuma iz člana 15 ovog zakona, sektrorskih kriterijuma i kriterijumskih pragova iz tačke 3 ovog člana; vodi Registar ključnih i važnih subjekata iz sektora za koji je nadležan (u daljem tekstu: Sektorki registar) i jednom godišnje vrši provjeru potrebe ažuriranja Sektorskog registra. Takođe je propisano i da nadležni sektorki organ određuje sektorske kriterijume uzimajući u obzir karakteristike tih sektora, vrstu i značaj usluga koje taj sektor, odnosno podsektor pruža, ako i kriterijumske pragove koje utveđuje na osnovu procjene uticaja sajber prijetnje i incidenta na pružanje usluga, posebno uzimajući u obzir gubitke, ekonomske posledice, uticaj na nacionalnu bezbjednost, uticaj na javnost i drugo.

**Članom 15** ovog zakona bliže su definisani opšti kriterijumi, koje nadležni sektorski organ primjenjuje u postupku prepoznavanja ključnih i važnih subjekata, dok je **članom 16** propisano koje podatke potencijalni ključni i važni subjekti moraju dostaviti nadležnom sektorskom organu, a to su: naziv subjekta, adresa subjekta, poreski identifikacioni broj subjekta, ime i prezime odgovornog lica, jedinstvenu službenu adresa za prijem elektronske pošte, kontakt telefon odgovornog lica subjekta, podatke o vrsti djelatnosti koju taj subjekt vrši, sektor, odnosno podsektor, u skladu sa članom 13 ovog zakona.

**Odredbama člana 17** ovog zakona propisano je da nadležni sektorski organ na osnovu prethodno dostavljenih podataka, procjene ispunjenosti opštih kriterijuma iz člana 15 ovog zakona, kao i sektorskih kriterijuma i kriterijumskih pragova sačinjava predlog liste za određivanje ključnih i važnih subjekata i dostavlja organu državne uprave nadležnom za razvoj informacionog društva i elektronske uprave (Ministarstvo). Takođe je propisano da Ministarstvo objedinjeni predlog liste iz stava 1 ovog člana dostavlja Vladi, kao i da na osnovu objedinjenog predloga liste iz stava 2 ovog člana, Vlada određuje Listu ključnih i važnih subjekat, koja podatke: naziv, adresu i poreski identifikacioni broj subjekta.

**Odredbama člana 18** ovog zakona propisano je da na osnovu Liste ključnih i važnih subjekata, nadležni sektorski organ vodi Sektorski registar, kao i koje podatke taj sektorski registar treba da sadrži. Takođe je propisana i dužnost ključnih i važnih subjekata da najmanje jednom godišnje nadležnom sektorskom organu dostavljaju obavještenje o promjeni podataka, na osnovu kog obavještenja je nadležni sektorski organ dužan da ažurira Sektorski registar. Definisano je da nadležni sektorki organ utvrđuje da li je potrebno izvršiti izmjene, odnosno dopune u pogledu određivanja Liste ključnih i važnih subjekata, te ako utvrdi da je potrebno izvršiti izmjene, odnosno dopune Liste ključnih i važnih subjekata nadležni sektorski organ sačinjava predlog izmjena, odnosno dopuna za za određivanje Liste ključnih i važnih subjekata koji dostavlja Ministarstvu, a Ministarstvo dostavlja Vladi, radi izmjena, odnosno dopuna Liste iz člana 17 stav 3 ovog zakona.

**Odredbama člana 19** ovog zakona propisano je da Ministarstvo vodi Nacionalni registar ključnih i važnih subjekata, i da je nadležni sektorski organ dužan da Ministarstvu dostavi podatke iz Sektorskog registra, kao i da ga redovno obavještava o svim promjenama podataka iz Sektorskog registra, dok su **odredbama člana 20** definisane obaveze ključnih i važnih subjekata i to da primjenjuju mjere informacione bezbjednosti od čl. 6 do čl. 11 ovog Zakona, kao i da odrede zaposleno lice za praćenje primjene mjera informacione bezbjednosti.Takođe je propisano da su ključni subjekti dužni su da primjenjuju međunarodni standard ISO/IEC 27001 za upravljanje informacionom bezbjednošću.

IV. NACIONALNI OKVIR ZA BEZBJEDNOST MREŽNIH I INFORMACIONIH SISTEMA

U poglavlju IV ovog zakona definisan je nacionalni okvir za bezbjednost mrežnih i informacionih sistema, koji čine Agencija za sajber bezbjednost (Agencija), Savjet za informacionu bezbjednost i Ministarstvo.

**Odredbama člana 21** ovog zakona definisano je osnivanje Agencije za sajber bazbjednost, koja ima svojstvo pravnog lica, status državne agencije i za svoj rad odgovara Vladi Crne Gore, dok je odredbama **člana 22** propisano da se statutom Agencije uređuju sjedište, adresa i organizacija Agencije, način odlučivanja organa Agencije i druga pitanja od značaja za rad Agencije, kao i da na statut Agencije saglasnost daje Vlada.

**Članom 23** ovog zakona definisan je djelokrug rada Agencije, i to da: priprema stručne osnove za izradu strategijskih dokumenata i akcionih planova, kao i Zakona i podzakonskih akata iz djelokruga rada Agencije, prati i analizira uporednu zakonsku regulativu i praksu EU i NATO saveznika i predlaže implementaciju najbolje prakse; donosi uputstva i procedure za postupak testiranja i procjene bezbjednosti mrežnih i informacionih sistema, daje predloge i preporuke za unaprjeđenje mjera informacione bezbjednosti, pruža rana upozorenja, najave i informiše o rizicima i incidentima, sprovodi zaštitu od sajber prijetnji i incidenata na mrežnom i informacionom sistemu ključnih i važnih subjekata osim organa državne uprave, postupa po prijavljenim incidentima ključnih i važnih subjekata, osim organa državne uprave, sprovodi operativnu koordinaciju tokom rješavanja sajber krize u saradnji sa Ministartsvom, sarađuje sa Ministarstvom, odnosno Vladinim CIRT-om, u cilju jačanja informacione bezbjednosti, razmjene informacija o incidentima i načinu njihovog rješavanja, prati stanje incidenata u oblasti informacione bezbjednosti, kontinuirano izrađuje analize rizika i incidenata, vodi Registar o prijavljenim incidentima, najmanje jednom godišnje izvještava Vladu o stanju incidenata u saradnji sa Ministarstvom, vrši edukaciju organa, nadležnih sektorskih organa i ključnih i važnih subjekata kroz savjetovanja i obuke u cilju jačanja informacione bezbjednosti, sarađuje sa privatnim i civilnim sektorom, nacionalnim i međunarodnim organizacijama i ključnim i važnim subjektima, učestvuje u razvoju i implementaciji međunarodnih projekata, vrši stručni nadzor nad radom ključnih i važnih subjektima u skladu sa zakonom, vrši stručni nadzor nad primjenom mjera informacione bezbjednosti od čl. 6 do 11 kod ključnih i važnih subjekata, vrši stručni nadzor nad primjenom mjera informacione bezbjednosti propisanih međunarodnim standardom ISO/IEC 27001 za upravljanje informacionom bezbjednošću, kod ključnih subjekata i obavlja i druge poslove, u skladu sa ovim zakonom.

**Odredbama čl. 24 do 26** definisano je da su organi Agencije Savjet Agencije i direktor, da Savjet Agencije ima pet članova, koje imenuje i razrješava Vlada, da se predsjednik Savjeta bira iz reda članova Savjeta, kao i trajanje mandata članova Savjeta. **Odredbama čl. 27 do 31** propisani su poslovi Savjeta Agencije, prestanak mandata, imenovanje direktora Agencije, kao i poslovi direktora Agencije i predstanak mandata, dok je **odredbama čl. 32 i 33** propisano obezbjeđenje sredstava za funkcionisanje i rad Agencije, kao i primjena propisa na prava, obaveze i odgovornosti zaposlenih u Agenciji.

**Odredbama člana 34** ovog zakona propisano je da Vlada radi praćenja razvoja i predlaganja mjera za unaprjeđenje informacione bezbjednosti, praćenja rada i predlaganja aktivnosti Agenciji i Ministarstvu na uspostavljanju sistema zaštite od sajber prijetnji i incidenata, kao i razmatranja stručnih pitanja u oblasti informacione bezbjednosti, obrazuje Savjet za informacionu bezbjednost, kao i da Savjet za informacionu bezbjednost čine 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 tajne podatke, Ministarstva, Agencije i Agencije za nacionalnu bezbjednost, a po potrebi i predstavnici drugih organa i institucija.Definisano je i na koji period se taj Savjet obrazuje, kao i da se aktom o obrazovanju Savjeta utvrđuju zadaci, način rada, i druga pitanja od značaja za rad Savjeta.

**Odredbama člana 35** ovog zakona, propisane su nadležnosti Minitarstva, i to da: izrađuje strategijska dokumenta i akcione planove, kao i propise iz oblasti informacione bezbjednosti, sarađuje s privatnim i civilnim sektorom, nacionalnim i međunarodnim organizacijama i ključnim i važnim subjektima, predstavlja jedinstvenu nacionalnu kontaktnu tačku za informacionu bezbjednost i sarađuje s jedinstvenim nacionalnim kontakt tačkama drugih država, sarađuje sa Agencijom u cilju jačanja informacione bezbjednost i razmjene informacija o incidentima i načinu njihovog rješavanja, izrađuje nacionalni plan za odgovor na sajber prijetnju, incidente i sajber krizu, u kojem se utvrđuje način upravljanja sajber prijetnjama, incidentima i sajber krizama, u saradnji sa Agencijom, sprovodi zaštitu od sajber prijetnji i incidenata na mrežnom i informacionom sistemu organa državne uprave, postupa po prijavljenim incidentima organa državne uprave i koordinira procesom rješavanja incidenata, vodi Registar o prijavljenim incidentima, obavlja i druge poslove, u skladu sa ovim zakonom. Propisano je i koje poslove obavlja preko posebne organizacione jedinice Vladin CIRT. **Odredbom člana 36** propisani su tehnički i drugi uslovi koje moraju da ispunjavaju Agencija i Vladin CIRT.

 V. UPRAVLJANJE SAJBER BEZBJEDNOŠĆU

**Odredbama člana 37** ovog zakona, u poglavlju V. propisano je da organi i ključni i važni subjekti vrše procjenu uticaja svih sajber prijetnji i incidenata u cilju prepoznavanja incidenata koji imaju značajan uticaj na kontinuitet pružanja usluga, u skladu sa kriterijumima iz člana 38 ovog zakona, kao i da su organi i ključni i važni subjekti osim organa državne uprave, dužni da Agenciji jednom mjesečno dostave izvještaj o svim sajber prijetnjama i incidentima za koje utvrde da nemaju uticaj na kontinuitet pružanja usluga, kao i da su ključni i važni subjekti koji su organi državne uprave dužni da Vladinom CIRT-u jednom mjesečno dostave izvještaj o svim sajber prijetnjama i incidentima za koje utvrde da nemaju uticaj na kontinuitet pružanja usluga. Nadalje, propisana je dužnost ključnih i važnih subjekata, osim organa državne uprave da o svim ozbiljnim sajber prijetnjama koje bi mogle dovesti do incidenta koji ima značajan uticaj na kontinuitet pružanja usluga, i o incidentima koji imaju značajan uticaj na kontinuitet usluga koje pružaju, u skladu sa kriterijumima iz člana 38 ovog zakona, kao i o svim mjerama koje preduzimaju ili planiraju da preduzmu kao odgovor na sajber prijetnju, odnosno incident, obavijeste Agenciju, kao i da su ključni i važni subjekti koji su organi državne uprave dužni da o svim ozbiljnim sajber prijetnjama i incidentima obavijeste Vladin CIRT.

**Članom 38** ovog zakona propisani su kriterijumi prema kojima se utvrđuje incident sa značajnim uticajem na kontinuitet pružanja usluga, dok su **članom 39** definisane vrste obavještenja, koja su ključni i važni subjekti dužni da dostave Agenciji, odnosno Vladinom CIRT-u o svim incidentima sa značajnim uticajem na kontinuitet pružanja usluga, to: početno obavještenje o incidentu sa značajnim uticajem na kontinuitet pružanja usluga, kontinuirani izvještaji tokom trajanja incidenta i završni izvještaj o incidentu. **Odredbama čl. 40 do 42** detaljnije je definisano dostavljanje početnog obavještenja o tom incidentu, kontinuiranih izvještaja tokom trajanja incidenta i završnog izvještaja o incidentu, kao i rokovi za definisanje.

**Odredbama člana 43** ovog zakona definisano je rješavanje incidenata na način da organi i ključni i važni subjekti sajber prijetnje i incidente koji nemaju značajan uticaj na kontinuitet pružanja usluga rješavanju bez učešća Agencije, odnosno Vladinog CIRT-a. Takođe je precizno definisano učešće Agencije, odnosno Vladinog CIRT-a, po prijemu obavještenja o svim ozbiljnim sajber prijetnjama koje bi mogle dovesti do incidenta koji ima značajan uticaj na kontinuitet pružanja usluga, i o incidentima koji imaju značajan uticaj na kontinuitet usluga koje pružaju, u zavisnosti od toga da li je taj incident niskog, srednjeg ili visokog nivoa, dok je **odredbama člana 44** definisano proglašenje sajber krize od strane Vlade, kao i uloge Ministarstva i Agencije, u slučaju proglašenje sajber krize, a **odredbom člana 45** informisanje javnosti o incidentu kojem je izložen ključni ili važni subjekat.

VI. NADZOR

 U poglavlju V. **u članu 46** definisano je da upravni nadzor nad sprovođenjem ovog zakona, drugih propisa i akata donijetih na osnovu ovog zakona, vrši Ministarstvo, dok je u **odredbama člana 47** između ostalog definisano da inspekcijski nadzor nad primjenom ovog zakona vrši organ uprave nadležan za inspekcijske poslove, preko inspektora za usluge informacionog društva (inspektor), a stručni nadzor nad primjenom ovog zakona vrši Agencija, preko zaposlenog lica koje je ovlašćeno za vršenje nadzora (nadzornik), kao i da su organi koji vrše inspekcijski i stručni nadzor, dužni da u poslovima nadzora ostvarivati potrebnu koordinaciju, komunikaciju i saradnju**. Odredbama člana 48** propisano je da poslove inspekcijskog nadzora inspektor vrši u skladu sa ovim zakonom i posebnim zakonima kojima se uređuju inspekcijski nadzor, a da oblik i sadržaj službene legitimacije za obavljanje poslova inspekcijskog nadzora propisuje Ministarstvo, dok je **članom 49** propisano koja ovlašćenja ima inspektor nad ključnim i važnim subjektima, pored ovlašćenja utvrđenih posebnim zakonom kojim se uređuje oblast inspekcijskog nadzora.

**Odredbama člana 50** ovog zakona propisano je da nadzornik obavlja poslove stručnog nadzora na osnovu ovlašćenja iz ovog zakona i propisa donijetih na osnovu ovog zakona i da oblik i sadržaj službene legitimacije za obavljanje poslova stručnog nadzora propisuje Agencija, dok je **članom 51** propisano koja ovlašćenja ima nadzornik na ključnim i važnim subjektima u postupku stručnog nadzora. **Članom 52** uređena je međusobna saradnja inspektora i nadzornika, dok je u **članu 53** definisana zaštita podataka o ličnosti.

VII. KAZNENE ODREDBE

 U poglavlju VII u **čl. 54 do 56** ovog zakona propisano je u kojim slučajevima će se novčano kazniti za prekršaj pravno lice koje je kao ključni, odnosno važni subjekat upisano u Nacionalni registar , kao i pravno lice koje je organ.

VIII. PRELAZNE I ZAVRŠNE ODREDBE

**Odredbom člana 57** ovog zakona propisan je rok za donošenje podzakonskih akata, dok su **odredbama čl. 58 i 59** propisani rokovi za dostavljanja Predloga Liste ključnih i važnih subjekata od strane nadležnih sektorskih organa, kao i rok za ključne subjekte za certifikovanje međunarodnog standarda. Nadalje, **odredbama čl. 60 i 61** propisani su rokovi za izbor članova Savjeta i direktora Agencije, donošenje akata Agencije, kao i preuzimanje državnih službenika iz Direkcije za zaštitu tajnih podataka koji vrše poslove u okviru organizacione jedinice CIRT. **Članom 62** ovog zakona propisan je početak rada Agencije , dok je članom 63 propisan nastavak rada Savjeta za informacionu bezbjednost.

**Članom 64** propisano je da danom početka primjene ovog zakona prestaje da važi Zakon o informacionoj bezbjednosti ("Službeni list CG" br. 14/10, 40/16 i 74/20) i odredbe člana 74 stav 1 tačka 8b, član 74a, 87d st. 2 i 3, 87e i 87f, Zakona o tajnosti podataka ("Službeni list CG" br. 14/08, 76/09, 41/10, 40/11, 38/12, 44/12, 14/13, 18/14, 48/15 i 74/20), dok je **članom 65** propisano da ovaj zakon stupa na snagu osmog dana od dana objavljivanja u "Službenom listu Crne Gore",kao i da će se primjenjivati od 01. avgusta 2023. godine .

**FINANSIJSKA SREDSTVA ZA SPROVOĐENJE ZAKONA**

Za sprovođenje ovog zakona potrebno je obezbijediti finansijska sredstva. Finansijska sredstva za sprovođenje ovog zakona obezbijediće se iz tekuće budžetske jedinice.