1694.

Na osnovu člana 95 tačka 3 Ustava Crne Gore donosim

UKAZ

O PROGLAŠENJU ZAKONA O INFORMACIONOJ BEZBJEDNOSTI

("Službeni list Crne Gore", br. 113/24 od 27.11.2024)

Proglašavam Zakon o informacionoj bezbjednosti, koji je donijela Skupština Crne Gore na Trećoj sjednici Drugog redovnog (jesenjeg) zasijedanja u 2024. godini, dana 19. novembra 2024. godine.

Broj: 011/24-1825/2-01

Podgorica, 25. novembar 2024. godine

Predsjednik Crne Gore,

Jakov Milatović, s.r.

Na osnovu člana 82 stav 1 tačka 2 i člana 91 stav 1 Ustava Crne Gore, Skupština Crne Gore 28. saziva, na Trećoj sjednici Drugog redovnog (jesenjeg) zasijedanja u 2024. godini, dana 19. novembra 2024. godine, donijela je

ZAKON

O INFORMACIONOJ BEZBJEDNOSTI

I. OSNOVNE ODREDBE

Predmet

Član 1

Ovim zakonom propisuju se mjere informacione bezbjednosti za postizanje najvišeg nivoa informacione bezbjednosti mrežnih i informacionih sistema, uključujući sajber bezbjednost, određivanje ključnih i važnih subjekata, upravljanje sajber bezbjednošću, kao i druga pitanja od značaja za informacionu bezbjednost.

Obaveza primjene

Član 2

Po ovom zakonu obavezni su da postupaju državni organi, ministarstva i drugi organi uprave, organi jedinica lokalne samouprave, organi lokalne uprave i službe obrazovane u skladu sa zakonom kojim se uređuje lokalna samouprava, pravna lica koja vrše javna ovlašćenja (u daljem tekstu: organi), privredna društva i druga pravna lica i fizička lica koja ostvaruju pristup ili postupaju sa podacima i koji koriste i upravljaju mrežnim i informacionim sistemom (u daljem tekstu: drugi subjekti).

Informaciona bezbjednost

Član 3

Informaciona bezbjednost podrazumijeva stanje povjerljivosti, cjelovitosti, dostupnosti i zaštite podatka, kao i sajber bezbjednost.

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 sprečavaju neovlašćene izmjene podataka.

Dostupnost podatka podrazumijeva da ovlašćeni korisnici mogu da pristupe podatku kad god za tim imaju potrebu.

Ključni i važni subjekti

Član 4

Ključni subjekti su organi i drugi subjekti koji primjenjuju informaciono-komunikacione tehnologije i pružaju usluge od posebnog značaja za život, zdravlje, bezbjednost građana i funkcionisanje države i od čijeg funkcionisanja zavisi vršenje djelatnosti od javnog interesa, a čijim prekidom rada ili uništenjem bi došlo do ugrožavanja života, zdravlja, bezbjednosti građana i funkcionisanja države, bez obzira na veličinu u smislu zakona kojim se uređuje računovodstvo, a naročito operatori kritične infrastrukture u skladu sa zakonom kojim se uređuje određivanje i zaštita kritične infrastrukture.

Važni subjekti su organi i drugi subjekti koji primjenjuju informaciono-komunikacione tehnologije i pružaju usluge od značaja za život, zdravlje, bezbjednost građana i funkcionisanje države i od čijeg funkcionisanja zavisi vršenje djelatnosti od javnog interesa, a čijim prekidom rada ili uništenjem bi došlo do otežanog funkcionisanja države, bez obzira na veličinu u smislu zakona kojim se uređuje računovodstvo, a naročito operatori kritične infrastrukture u skladu sa zakonom kojim se uređuje određivanje i zaštita kritične infrastrukture.

CIRT državne uprave i jedinstvena nacionalna kontakt tačka za informacionu bezbjednost

Član 5

Zaštitu mrežnih i informacionih sistema organa državne uprave od sajber prijetnji, ozbiljnih sajber prijetnji i incidenata vrši organ državne uprave nadležan za razvoj informacionog društva i elektronske uprave (u daljem tekstu: Ministarstvo) preko posebne organizacione jedinice (u daljem tekstu: CIRT državne uprave).

Ministarstvo predstavlja jedinstvenu nacionalnu kontakt tačku za informacionu bezbjednost i sarađuje sa jedinstvenim nacionalnim kontakt tačkama drugih država.

Agencija za sajber bezbjednost

Član 6

Zaštitu mrežnih i informacionih sistema organa i drugih subjekata, a naročito ključnih i važnih subjekata, osim organa državne uprave od sajber prijetnji, ozbiljnih sajber prijetnji i incidenata, kao i stručni nadzor nad primjenom mjera informacione bezbjednosti kod tih organa i drugih subjekata vrši Agencija za sajber bezbjednost (u daljem tekstu: Agencija).

Izuzeće od primjene

Član 7

Ovaj zakon ne primjenjuje se na organ državne uprave nadležan za poslove odbrane, Vojsku Crne Gore, Agenciju za nacionalnu bezbjednost, organizacionu jedinicu organa državne uprave nadležnog za unutrašnje poslove koja vrši policijske poslove, Skupštinu Crne Gore i Centralnu banku Crne Gore, kao i na podatke čija se informaciona bezbjednost obezbjeđuje u skladu sa propisima kojima se uređuje tajnost podataka.

Zaštita podataka o ličnosti

Član 8

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

Upotreba rodno osjetljivog jezika

Član 9

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

Značenje izraza

Član 10

Izrazi upotrijebljeni u ovom zakonu imaju sljedeća značenja:

1) mrežni i informacioni sistem podrazumijeva:

- elektronsku komunikacionu mrežu koja obuhvata sisteme 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, kao i 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 najmanje jedan programski izvršava automatsku obradu podataka u elektronskom obliku, i
- podatke u elektronskom obliku koji se čuvaju, obrađuju, dobijaju ili prenose na način iz al. 1 i 2 ove tačke, u svrhu rada, korišćenja, zaštite i održavanja tih mrežnih i informacionih sistema;

2) informaciona bezbjednost mrežnog i informacionog sistema je sposobnost mrežnog i informacionog sistema da se na određenom nivou pouzdanosti odupre svakom događaju koji može da ugrozi povjerljivost, cjelovitost i dostupnost sačuvanih, prenesenih ili obrađenih podataka ili usluga koje taj mrežni i informacioni sistem nudi ili kojima omogućava pristup;

3) podatak je svaka informacija, poruka i dokument sačinjen, poslat, primljen, zabilježen, skladišten ili prikazan elektronskim, optičkim ili sličnim sredstvom, uključujući prenos internetom;

4) kriptografska zaštita podataka je primjena programskih rješenja ili uređaja za zaštitu podataka koji obezbjeđuju povjerljivost, cjelovitost i dostupnost podataka;

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 te sajber prijetnje i incidenti utiču;

6) sajber prijetnja je svaka moguća okolnost, događaj ili djelovanje koji bi mogli oštetiti, poremetiti ili na drugi način negativno uticati na podatke ili 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 karakteristika može pretpostaviti da može ozbiljno uticati na podatke ili mrežne i informacione sisteme, korisnike tih sistema i druge organe i lica, uzrokovanjem značajne materijalne ili nematerijalne štete;

8) incident je svaki događaj koji kompromituje povjerljivost, cjelovitost i dostupnost skladištenih, prenesenih ili obrađenih podataka ili usluga koje mrežni i informacioni sistemi pružaju ili kojima omogućavaju pristup;

9) rješavanje incidenta podrazumijeva sve radnje i postupke čiji je cilj otkrivanje, analiza i zaustavljanje incidenta, kao i odgovor na njega;

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

11) rizik je bilo koja okolnost ili događaj koji ima potencijalno negativan uticaj na bezbjednost podataka i mrežnog i informacionog sistema;

12) sajber kriza je događaj ili stanje u sajber prostoru koje ugrožava nacionalnu bezbjednost, 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 nadležnih organa, kao i primjenu odgovarajućih mjera;

13) sajber prostor je zamišljeni prostor u kojem se odvija komunikacija preko interneta.

II. MJERE INFORMACIONE BEZBJEDNOSTI

Vrste mjera informacione bezbjednosti

Član 11

Mjere informacione bezbjednosti su:

1) zaštita podataka i

2) zaštita od sajber prijetnji i incidenata.

Zaštita podataka

Član 12

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

Zaštita iz stava 1 ovog člana obuhvata:

1) pravila za postupanje sa podacima;

2) vođenje evidencije o izvršenim pristupima podacima;

3) nadzor nad bezbjednošću podataka.

Zaštita od sajber prijetnji i incidenata

Član 13

Zaštita od sajber prijetnji i incidenata obuhvata:

1) fizičku zaštitu;

2) zaštitu mrežnog i informacionog sistema;

3) upravljanje rizicima u oblasti sajber bezbjednosti.

Fizička zaštita

Član 14

Fizička zaštita obuhvata zaštitu objekta, prostora i uređaja u kojem se nalazi mrežni i informacioni sistem.

Zaštita mrežnog i informacionog sistema

Član 15

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 podataka u procesu planiranja, projektovanja, izgradnje, upotrebe, održavanja i prestanka rada tog sistema.

Upravljanje rizicima u oblasti sajber bezbjednosti

Član 16

Upravljanje rizicima u oblasti sajber bezbjednosti obuhvata:

1) izradu analize rizika i bezbjednosti mrežnog i informacionog sistema;

2) donošenje pravila postupanja sa incidentima (sprečavanje, otkrivanje i odgovor na incidente);

3) donošenje plana kontinuiteta poslovanja i postupanja u sajber krizama;

4) donošenje akta kojim se uređuje bezbjednost lanca snabdijevanja između organa, odnosno drugog subjekta koji upravlja mrežnim i informacionim sistemom i dobavljača ili pružaoca usluga;

5) donošenje akata kojima se uređuje uspostavljanje, razvoj i održavanje mrežnih i informacionih sistema, kao i informacionu bezbjednost mrežnih i informacionih sistema;

6) primjenu kriptografske zaštite podataka, ako priroda poslova iz nadležnosti organa, odnosno drugog subjekta to zahtijeva;

7) donošenje pravila postupanja prilikom procjene efikasnosti mjera iz tač. 1 do 6 ovog člana.

Bliži sadržaj mjera informacione bezbjednosti

Član 17

Bliži sadržaj mjera informacione bezbjednosti iz čl. 11 do 16 ovog zakona propisuje Vlada Crne Gore (u daljem tekstu: Vlada).

Obaveza primjene mjera informacione bezbjednosti

Član 18

Organi i drugi subjekti koji su u skladu sa ovim zakonom određeni kao ključni i važni subjekti dužni su da primjenjuju mjere informacione bezbjednosti iz čl. 11 do 16 ovog zakona.

Organi i drugi subjekti koji nijesu u skladu sa ovim zakonom određeni kao ključni i važni subjekti dužni su da primjenjuju mjere informacione bezbjednosti iz čl. 11 do 15 ovog zakona.

Organi i drugi subjekti dužni su da odrede zaposleno lice za praćenje primjene mjera informacione bezbjednosti u skladu sa st. 1 i 2 ovog člana.

Radi sprovođenja mjera informacione bezbjednosti, organi i drugi subjekti koji su u skladu sa ovim zakonom određeni kao ključni subjekti moraju da ispunjavaju uslove u skladu sa važećim crnogorskim standardom za upravljanje informacionom bezbjednošću MEST ISO/IEC 27001.

O ispunjenosti uslova iz stava 4 ovog člana ključnim subjektima akreditovano pravno lice izdaje certifikat.

Ključni subjekti dužni su da od akreditovanog pravnog lica zahtijevaju periodičnu provjeru ispunjenosti uslova u skladu sa standardom iz stava 4 ovog člana.

III. ODREĐIVANJE KLJUČNIH I VAŽNIH SUBJEKATA

Sektori i podsektori u kojima se određuju ključni i važni subjekti

Član 19

Ključni subjekti određuju se u okviru sljedećih sektora, odnosno podsektora:

1) energetika (električna energija, daljinsko grijanje i hlađenje, nafta, gas i vodonik);

2) saobraćaj (vazdušni, željeznički, pomorski i drumski);

3) bankarstvo (kreditne institucije);

4) infrastruktura finansijskog tržišta (mjesta trgovanja i centrlne druge ugovorne strane utvrđeni zakonom kojim se uređuje tržište kapitala);

5) zdravlje (pružanje zdravstvene zaštite na primarnom, sekundarnom i tercijarnom nivou, rad nacionalnih referentnih laboratorija, registracija i istraživanje ljekova);

6) voda za piće (snabdijevanje i distribucija vode namijenjene za ljudsku potrošnju);

7) otpadne vode (sakupljanje, odvođenje ili prečišćavanje komunalnih otpadnih voda i otpadnih voda privrede);

8) digitalna infrastruktura (pružaoci usluga za razmjenu internet saobraćaja, pružaoci DNS usluga osim operatora korijenskih servera naziva, registar naziva domena najvišeg nivoa, pružaoci usluge računarstva u oblaku, pružaoci usluga data centara, pružaoci mreže za isporuku sadržaja, pružaoci kvalifikovanih elektronskih usluga povjerenja, pružaoci javnih elektronskih komunikacionih mreža i javno dostupnih elektronskih komunikacionih usluga);

9) upravljanje uslugama informaciono-komunikacionih tehnologija (pružaoci usluga informaciono-komunikacionih tehnologija);

10) javna uprava (organi državne uprave i organi lokalne samouprave);

11) svemir.

Važni subjekti određuju se u okviru sljedećih sektora, odnosno podsektora:

1) poštanske i kurirske usluge (pružaoci univerzalnih poštanskih usluga i pružaoci komercijalnih poštanskih usluga);

2) upravljanje otpadom (sakupljanje, odnosno transport otpada, prerada i zbrinjavanje otpada);

3) izrada, proizvodnja i distribucija hemikalija (proizvodnja i snabdijevanje hemikalijama u skladu sa zakonom kojim se uređuju hemikalije);

4) proizvodnja, prerada i distribucija hrane (veleprodaja, industrijska proizvodnja i prerada);

5) proizvodnja (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 i proizvodnja ostale opreme za transport);

6) pružaoci elektronskih usluga (pružaoci usluga na internet tržištu);

7) istraživačka djelatnost (subjekti koji imaju za primarni cilj da sprovedu primijenjena istraživanja ili eksperimentalni razvoj kako bi se rezultati tih istraživanja koristili u komercijalne svrhe).

Pored subjekata iz stava 2 ovog člana, kao važni subjekti mogu biti određeni i subjekti u okviru sektora, odnosno podsektora iz stava 1 ovog člana, koji nijesu određeni kao ključni subjekti, ako se ispune kriterijumi iz člana 4 stav 2 ovog zakona.

Prikupljanje podataka od značaja za određivanje ključnih i važnih subjekata

Član 20

Ministarstvo nadležno za sektor, odnosno podsektor u kojem se određuju ključni, odnosno važni subjekti (u daljem tekstu: nadležno ministarstvo) sačinjava listu svih organa i drugih subjekata u tom sektoru, odnosno podsektoru i dostavlja im zahtjev za prikupljanje podataka od značaja za određivanje ključnih i važnih subjekata.

Podaci od značaja za određivanje ključnih i važnih subjekata su:

1) naziv organa, odnosno drugog subjekta;

2) sjedište, odnosno adresa organa, odnosno drugog subjekta;

3) poreski identifikacioni broj organa, odnosno drugog subjekta;

4) ime i prezime odgovornog lica u organu, odnosno drugom subjektu;

5) jedinstvena službena adresa za elektronsku komunikaciju organa, odnosno drugog subjekta;

6) kontakt telefon odgovornog lica u organu, odnosno drugom subjektu;

7) podaci o nadležnosti, odnosno djelatnosti organa, odnosno drugog subjekta;

8) podaci kojem sektoru, odnosno podsektoru iz člana 19 st. 1 i 2 ovog zakona pripada organ, odnosno drugi subjekat.

Organi i drugi subjekti iz stava 1 ovog člana dužni su da nadležnom ministarstvu podatke iz stava 2 ovog člana dostave u roku od sedam dana od dana prijema zahtjeva.

U slučaju promjene podataka iz stava 2 ovog člana, organi i drugi subjekti dužni su da o tome obavijeste nadležno ministarstvo, u roku od 14 dana od dana nastanka promjene.

Predlog sektorske liste ključnih i važnih subjekata

Član 21

Na osnovu podataka iz člana 20 stav 2 ovog zakona, nadležno ministarstvo sačinjava predlog sektorske liste ključnih i važnih subjekata.

Predlog sektorske liste iz stava 1 ovog člana nadležno ministarstvo dostavlja Ministarstvu.

Lista ključnih i važnih subjekata

Član 22

Nakon dobijanja predloga sektorskih lista od nadležnih ministarstava, Ministarstvo sačinjava objedinjeni predlog liste ključnih i važnih subjekata i dostavlja ga Vladi.

Vlada, na predlog Ministarstva, utvrđuje Listu ključnih i važnih subjekata.

Lista iz stava 2 ovog člana sadrži sljedeće podatke o ključnim i važnim subjektima, i to:

1) naziv;

2) sjedište, odnosno adresu;

3) poreski identifikacioni broj.

Obavještavanje ključnih i važnih subjekata

Član 23

U roku od sedam dana od dana utvrđivanja Liste ključnih i važnih subjekata, nadležno ministarstvo obavještava ključne i važne subjekte u sektoru, odnosno podsektoru za koji je nadležno da su određeni kao ključni, odnosno važni subjekti.

Sektorski registar ključnih i važnih subjekata

Član 24

Na osnovu Liste ključnih i važnih subjekata, nadležno ministarstvo vodi Sektorski registar ključnih i važnih subjekata, koji sadrži podatke iz člana 20 stav 2 tač. 1 do 7 ovog zakona koji se odnose na ključne i važne subjekte u sektoru, odnosno podsektoru za koji je nadležno.

Podatke iz stava 1 ovog člana nadležno ministarstvo dostavlja Ministarstvu radi vođenja registra iz člana 25 ovog zakona.

Zbirni registar ključnih i važnih subjekata

Član 25

Na osnovu Liste ključnih i važnih subjekata i podataka koje nadležna ministarstva dostave saglasno članu 24 ovog zakona, Ministarstvo vodi Zbirni registar ključnih i važnih subjekata.

Zbirni registar ključnih i važnih subjekata sadrži podatke iz člana 20 stav 2 tač. 1 do 7 ovog zakona koji se odnose na sve ključne i važne subjekte.

Ažuriranje registara i Liste ključnih i važnih subjekata

Član 26

Ključni i važni subjekti dužni su da nadležnom ministarstvu dostave obavještenje o promjeni podataka iz člana 20 stav 2 tač. 1 do 7 ovog zakona, odmah nakon nastanka promjene.

Na osnovu obavještenja iz stava 1 ovog člana, nadležno ministarstvo ažurira Sektorski registar ključnih i važnih subjekata i o promjeni podataka obavještava Ministarstvo.

Na osnovu obavještenja iz stava 2 ovog člana, Ministarstvo ažurira Zbirni registar ključnih i važnih subjekata.

Ako, na osnovu obavještenja iz stava 1 ovog člana, utvrdi da je potrebno izvršiti izmjene, odnosno dopune Liste ključnih i važnih subjekata, Ministarstvo sačinjava predlog izmjena, odnosno dopuna Liste ključnih i važnih subjekata i dostavlja ga Vladi radi utrđivanja tih izmjena, odnosno dopuna.

Tajnost podataka, registara i listi ključnih i važnih subjekata

Član 27

Podaci iz člana 20 stav 2 ovog zakona i obavještenje iz člana 20 stav 4 ovog zakona, predlog sektorske liste iz člana 21 ovog zakona, predlog liste i Lista ključnih i važnih subjekata iz člana 22 ovog zakona, obavještenje iz člana 23 ovog zakona, Sektorski registar iz člana 24 ovog zakona, Zbirni registar iz člana 25 ovog zakona, obavještenja iz člana 26 st. 1 i 2 ovog zakona, kao i predlog izmjena, odnosno dopuna Liste ključnih i važnih subjekata iz člana 26 stav 4 ovog zakona označavaju se odgovarajućim stepenom tajnosti, u skladu sa zakonom kojim se uređuje tajnost podataka.

IV. PROCJENA UTICAJA SAJBER PRIJETNJE, OZBILJNE SAJBER PRIJETNJE I INCIDENTA I RJEŠAVANJE INCIDENTA I SAJBER KRIZE

Kriterijumi za procjenu uticaja sajber prijetnje, ozbiljne sajber prijetnje i incidenta

Član 28

U slučaju nastanka sajber prijetnje, ozbiljne sajber prijetnje, odnosno incidenta na mrežnom i informacionom sistemu, organi i drugi subjekti dužni su da vrše procjenu uticaja tih sajber prijetnji, odnosno incidenta na kontinuitet pružanja usluga.

Procjena iz stava 1 ovog člana vrši se na osnovu sljedećih kriterijuma:

1) broj korisnika koji nijesu mogli da ostvare pristup usluzi;
2) broj korisnika koji su imali značajne teškoće u ostvarivanju pristupa usluzi;
3) vrijeme trajanja sajber prijetnje, ozbiljne sajber prijetnje, odnosno incidenta;
4) geografska zastupljenost sajber prijetnje, ozbiljne sajber prijetnje, odnosno incidenta (ako je moguće utvrditi).

Sajber prijetnja, ozbiljna sajber prijetnja i incident koji nemaju uticaj na kontinuitet pružanja usluga

Član 29

U slučaju da se, na osnovu kriterijuma iz člana 28 stav 2 ovog zakona, procijeni da sajber prijetnja, ozbiljna sajber prijetnja, odnosno incident nemaju uticaj na kontinuitet pružanja usluga, izvještaj o tim sajber prijetnjama i incidentima, jednom mjesečno, organi i drugi subjekti, osim organa državne uprave dostavljaju Agenciji, a organi državne uprave CIRT-u državne uprave.

U slučaju iz stava 1 ovog člana, organi i drugi subjekti sajber prijetnje, ozbiljne sajber prijetnje, odnosno incidente rješavaju bez učešća Agencije, odnosno CIRT-a državne uprave.

Sajber prijetnja, ozbiljna sajber prijetnja i incident koji negativno utiču na kontinuitet pružanja usluga

Član 30

U slučaju da se, na osnovu kriterijuma iz člana 28 stav 2 ovog zakona, procijeni da bi sajber prijetnja, ozbiljna sajber prijetnja, odnosno incident mogli u značajnoj mjeri negativno da utiču na kontinuitet pružanja usluga, o tim sajber prijetnjama i incidentima, organi i drugi subjekti, osim organa državne uprave dostavljaju početno obavještenje Agenciji, a organi državne uprave CIRT-u državne uprave.

Početno obavještenje dostavlja se najkasnije u roku od 24 časa od trenutka saznanja za sajber prijetnju, ozbiljnu sajber prijetnju, odnosno incident, na propisanom obrascu.

Izgled i sadržaj obrasca početnog obavještenja propisuje Ministarstvo.

Određivanje nivoa negativnog uticaja sajber prijetnje, ozbiljne sajber prijetnje i incidenta na kontinuitet pružanja usluga

Član 31

Po prijemu početnog obavještenja Agencija, odnosno CIRT državne uprave sprovodi analizu uticaja sajber prijetnje, ozbiljne sajber prijetnje, odnosno incidenta na kontinuitet pružanja usluga i mogućih načina reagovanja na te sajber prijetnje, odnosno incident i utvrđuje nivo incidenta koji može biti niski, srednji ili visoki.

Bliži način sprovođenja analize i kriterijume za utvrđivanje nivoa incidenta iz stava 1 ovog člana propisuje Vlada.

Incident niskog nivoa

Član 32

Ako, po prijemu početnog obavještenja, utvrdi da je incident niskog nivoa, Agencija, odnosno CIRT državne uprave, u roku od 24 časa od prijema tog obavještenja, organu, odnosno drugom subjektu može, ako je to potrebno, dati smjernice za reagovanje na nastali incident.

Incident srednjeg nivoa

Član 33

Ako, po prijemu početnog obavještenja, utvrdi da je incident srednjeg nivoa, Agencija, odnosno CIRT državne uprave, odmah, a najkasnije u roku od 24 časa od prijema tog obavještenja, daje smjernice za reagovanje na nastali incident i učestvuje u rješavanju tog incidenta.

U toku trajanja incidenta iz stava 1 ovog člana, organi i drugi subjekti dužni su da, u roku od 72 časa od podnošenja početnog obavještenja, Agenciji odnosno CIRT-u državne uprave dostave prvi izvještaj o trajanju incidenta i mjerama koje su preduzete za rješavanje tog incidenta, na propisanom obrascu.

Ako tokom trajanja incidenta iz stava 1 ovog člana organi i drugi subjekti saznaju za nove podatke ili okolnosti koje mogu biti od uticaja na taj incident, dužni su da, o tome Agenciji, odnosno CIRT-u državne uprave, bez odlaganja, dostave poseban izvještaj na propisanom obrascu.

Ako incident iz stava 1 ovog člana traje i nakon isteka roka iz stava 2 ovog člana, organi i drugi subjekti dužni su da, svakih 72 časa, dostavljaju Agenciji, odnosno CIRT-u državne uprave kontinuirane izvještaje o trajanju incidenta i mjerama koje su preduzete za rješavanje tog incidenta, na propisanom obrascu.

Nakon rješavanja incidenta iz stava 1 ovog člana, a najkasnije u roku od 30 dana od dana rješavanja tog incidenta, organi i drugi subjekti dužni su da Agenciji, odnosno CIRT-u državne uprave dostave završni izvještaj o tom incidentu, na propisanom obrascu.

Izgled i sadržaj obrazaca izvještaja iz st. 2 do 5 ovog člana propisuje Ministarstvo.

Incident visokog nivoa

Član 34

Ako, po prijemu početnog obavještenja, utvrdi da je incident visokog nivoa, Agencija je dužna o tome da obavijesti CIRT državne uprave, odnosno CIRT državne uprave Agenciju, bez odlaganja, u pisanoj formi.

U slučaju iz stava 1 ovog člana, Agencija i CIRT državne uprave zajedno učestvuju u rješavanju incidenta i organu i drugom subjektu daju smjernice za reagovanje na nastali incident.

Tokom trajanja incidenta iz stava 1 ovog člana, organi i drugi subjekti dužni su da u roku od 72 časa od podnošenja početnog obavještenja Agenciji, odnosno CIRT-u državne uprave dostave prvi izvještaj o trajanju incidenta i mjerama koje su preduzete za rješavanje tog incidenta, na propisanom obrascu.

Ako tokom trajanja incidenta iz stava 1 ovog člana organi i drugi subjekti saznaju za nove podatke ili okolnosti koje mogu biti od uticaja na taj incident, dužni su da o tome Agenciji, odnosno CIRT-u državne uprave, bez odlaganja, dostave poseban izvještaj na propisanom obrascu.

Ako incident iz stava 1 ovog člana traje i nakon isteka roka iz stava 3 ovog člana, organi i drugi subjekti dužni su da, svakih 24 časa, Agenciji, odnosno CIRT-u državne uprave dostavljaju kontinuirane izvještaje o trajanju incidenta i mjerama koje su preduzete za rješavanje tog incidenta, na propisanom obrascu.

Nakon rješavanja incidenta iz stava 1 ovog člana, a najkasnije u roku od 30 dana od dana rješavanja tog incidenta, organi i drugi subjekti dužni su da Agenciji, odnosno CIRT-u državne uprave dostave završni izvještaj o tom incidentu, na propisanom obrascu.

Izgled i sadržaj obrazaca izvještaja iz st. 3 do 6 ovog člana propisuje Ministarstvo.

Sajber kriza

Član 35

Ako Agencija i CIRT državne uprave ne mogu da riješe incident visokog nivoa u skladu sa članom 34 ovog zakona, u roku od deset dana od dana dostavljanja početnog obavještenja, Ministarstvo, uz prethodno pribavljeno mišljenje Agencije, dostavlja Vladi predlog za proglašenje sajber krize.

Predlog iz stava 1 ovog člana sadrži podatke o incidentu, preduzetim mjerama, razloge za proglašenje sajber krize i predlog mjera za rješavanje te krize.

Na osnovu predloga iz stava 1 ovog člana, Vlada donosi odluku o proglašenju sajber krize, sa mjerama za rješavanje sajber krize i zadužuje organe koji su dužni da učestvuju u rješavanju sajber krize.

Ministarstvo koordinira radom organa iz stava 3 ovog člana u rješavanju sajber krize i najmanje jednom nedeljno izvještava Vladu o svim aktivnostima.

Agencija u saradnji sa Ministarstvom sprovodi operativnu koordinaciju rješavanja sajber krize u skladu sa Nacionalnim planom za odgovor na sajber prijetnju, ozbiljnu sajber prijetnju, incidente i sajber krizu.

Nakon rješavanja sajber krize, Ministarstvo u saradnji sa Agencijom sačinjava završni izvještaj o sajber krizi i predlog za proglašenje da je sajber kriza završena, koje dostavlja Vladi.

Na osnovu izvještaja i predloga iz stava 6 ovog člana, Vlada donosi odluku o proglašenju završetka sajber krize.

Pomoć u rješavanju incidenta i sajber krize

Član 36

U rješavanju incidenta srednjeg, odnosno visokog nivoa i sajber krize Agencija i CIRT državne uprave mogu koristiti ekspertsku pomoć domaćih i međunarodnih institucija i organizacija, kao i razmjenjivati informacije sa tim instutucijama i organizacijama.

Tajnost obavještenja, izvještaja i smjernica

Član 37

Izvještaj iz člana 29 stav 1 ovog zakona, početno obavještenje iz člana 30 stav 1 ovog zakona, smjernice iz člana 32 i člana 33 stav 1 ovog zakona, izvještaji iz člana 33 st. 2 do 5 ovog zakona, obavještenje iz člana 34 stav 1 ovog zakona, smjernice iz člana 34 stav 2 ovog zakona, izvještaji iz člana 34 st. 3 do 6 ovog zakona, predlog i mišljenje iz člana 35 stav 1 ovog zakona, odluka iz člana 35 stav 3 ovog zakona, izvještaj iz člana 35 stav 4 ovog zakona, kao i izvještaj i predlog iz člana 35 stav 6 ovog zakona označavaju se odgovarajućim stepenom tajnosti u skladu sa zakonom kojim se uređuje tajnost podataka.

V. MINISTARSTVO I CIRT DRŽAVNE UPRAVE

Nadležnosti Ministarstva

Član 38

Ministarstvo:

1) predlaže Vladi strategije i akcione planove, kao i propise iz oblasti informacione bezbjednosti;
2) izrađuje Nacionalni plan za odgovor na sajber prijetnju, ozbiljnu sajber prijetnju, incidente i sajber krizu, u saradnji sa Agencijom;
3) vrši skeniranje mrežnih i informacionih sistema organa državne uprave, u cilju otkrivanja ranjivosti tih sistema;
4) donosi uputstva i procedure koje se sprovode prilikom procjene informacione bezbjednosti mrežnih i informacionih sistema organa državne uprave;
5) daje upozorenja, najave i informacije o rizicima i incidentima organima državne uprave;
6) postupa po prijavljenim incidentima na mrežnim i informacionim sistemima organa državne uprave;
7) vodi evidenciju o prijavljenim incidentima na mrežnim i informacionim sistemima organa državne uprave;

8) sarađuje sa Agencijom radi razmjene informacija o sajber prijetnjama, ozbiljnim sajber prijetnjama i incidentima i rješavanja tih prijetnji, incidenata i sajber krize, u skladu sa ovim zakonom;

9) u cilju unapređenja informacione bezbjednosti sarađuje sa domaćim i međunarodnim institucijama i organizacijama, kao i privatnim i civilnim sektorom;

10) dostavlja Vladi izvještaj o stanju informacione bezbjednosti mrežnih i informacionih sistema organa državne uprave, najmanje jednom godišnje;

11) dostavlja Vladi i druge izvještaje, u skladu sa ovim zakonom;

12) vrši i druge poslove, u skladu sa ovim zakonom.

CIRT državne uprave

Član 39

Poslove iz člana 38 stav 1 tač. 3 do 9 ovog zakona vrši CIRT državne uprave.

CIRT državne uprave mora da ispunjava tehničke i druge uslove, i to da:

1) posjeduje sredstva komunikacije koja neće izazvati prekide, na način da u svakom trenutku ima na raspolaganju više sredstava za dvosmjernu komunikaciju;

2) posjeduje prostorije za rad i informacione sisteme, smještene na sigurnim lokacijama;

3) posjeduje adekvatan sistem za prijavljivanje i upravljanje incidentima;

4) obezbijedi povjerljivost i pouzdanost procesa rada;

5) posjeduje redundantne sisteme i rezervne radne prostorije kako bi se obezbijedio kontinuitet rada;

6) ima dovoljan broj zaposlenih kako bi se obezbijedio kontinuitet rada 24 časa.

Redundantni sistemi, u smislu stava 2 tačka 5 ovog člana, su rezervni sistemi koji zamjenjuju primarni sistem, ako je došlo do prekida rada primarnog sistema.

VI. AGENCIJA ZA SAJBER BEZBJEDNOST

Poslovi Agencije

Član 40

Agencija:

1) prati i analizira primjenu propisa, strategija i akcionih planova u oblasti informacione bezbjednosti i daje predloge i preporuke za unapređenje informacione bezbjednosti;

2) prati i analizira propise Evropske unije i država članica Sjevernoatlantskog saveza u oblasti informacione bezbjednosti;

3) vrši proaktivno skeniranje mrežnih i informacionih sistema ključnih i važnih subjekata koji nijesu organi državne uprave, uz njihovu prethodnu saglasnost;

4) donosi uputstva i procedure koje se sprovode prilikom procjene informacione bezbjednosti mrežnih i informacionih sistema organa i drugih subjekata, osim organa državne uprave;

5) daje upozorenja, najave i informacije o rizicima i incidentima organima i drugim subjektima, osim organa državne uprave;

6) postupa po prijavljenim incidentima na mrežnim i informacionim sistemima organa i drugih subjekata, osim organa državne uprave;

7) vodi evidenciju o prijavljenim incidentima na mrežnim i informacionim sistemima organa i drugih subjekata, osim organa državne uprave;

8) vrši stručni nadzor nad primjenom mjera informacione bezbjednosti kod organa i drugih subjekata, osim organa državne uprave;

9) vrši stručni nadzor utvrđivanjem da li ključni subjekti posjeduju certifikat o ispunjenosti uslova u skladu sa važećim crnogorskim standardom za upravljanje informacionom bezbjednošću MEST ISO/IEC 27001 i da li su zahtijevali periodičnu provjeru ispunjenosti uslova u skladu sa tim standardom;

10) učestvuje u implementaciji međunarodnih projekata u oblasti informacione bezbjednosti;

11) vrši edukaciju zaposlenih u organima i drugim subjektima u cilju jačanja informacione bezbjednosti;

12) sarađuje sa Ministarstvom radi razmjene informacija o sajber prijetnjama, ozbiljnim sajber prijetnjama i incidentima i rješavanja tih prijetnji, incidenata i sajber krize, u skladu sa ovim zakonom;

13) u cilju unapređenja informacione bezbjednosti sarađuje sa domaćim i međunarodnim institucijama i organizacijama, kao i privatnim i civilnim sektorom;

14) dostavlja Vladi izvještaj o stanju informacione bezbjednosti mrežnih i informacionih sistema organa i drugih subjekata, a naročito ključnih i važnih subjekata koji nijesu organi državne uprave, najmanje jednom godišnje.

Organi Agencije

Član 41

Organi Agencije su: Savjet Agencije i direktor Agencije.

Savjet Agencije

Član 42

Savjet Agencije ima predsjednika i četiri člana koje imenuje i razrješava Vlada.

Predsjednika Savjeta Agencije predlaže Ministarstvo, a po jednog člana Savjeta Agencije predlažu:

1) Univerzitet Crne Gore;

2) Privredna komora Crne Gore;

3) Generalni sekretarijat Vlade Crne Gore;

4) Agencija iz reda zaposlenih.

Predsjednik i članovi Savjeta Agencije imenuju se na period od četiri godine.

Poslovi Savjeta Agencije

Član 43

Savjet Agencije:

1) donosi statut Agencije;

2) donosi godišnji program rada i finansijski plan Agencije;

3) usvaja i podnosi Vladi godišnji izvještaj o radu i finansijski izvještaj Agencije;

4) imenuje i razrješava direktora Agencije;

5) utvrđuje plan obuka za stručno usavršavanje zaposlenih u Agenciji;

6) donosi Etički kodeks zaposlenih u Agenciji;

7) vrši i druge poslove u skladu sa zakonom i statutom Agencije.

Finansijski plan Agencije donosi se uz prethodnu saglasnost organa državne uprave nadležnog za poslove finansija.

Prestanak mandata predsjednika i člana Savjeta Agencije

Član 44

Predsjedniku, odnosno članu Savjeta Agencije prestaje mandat:

1) istekom vremena na koje je imenovan;

2) ostavkom;

3) razrješenjem.

Predsjednik, odnosno član Savjeta Agencije razrješava 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;

4) nestručno ili nesavjesno vrši poslove za koje je imenovan.

Direktor Agencije

Član 45

Direktor Agencije imenuje se osnovu javnog konkursa koji raspisuje Savjet Agencije.

Za direktora Agencije može biti imenovano lice koje, pored opštih uslova za zasnivanje radnog odnosa u državnim organima, ispunjava sljedeće uslove, i to da ima:

1) najmanje VII1 nivo kvalifikacije obrazovanja, i

2) radno iskustvo, i to:

- pet godina radnog iskustva u oblasti informacione bezbjednosti ili
- sedam godina radnog iskustva u državnim organima ili organima državne uprave ili deset godina radnog iskustva, od čega pet godina radnog iskustva na poslovima rukovođenja.

Mandat direktora Agencije traje pet godina.

Poslovi direktora Agencije

Član 46

Direktor Agencije:

1) predstavlja i rukovodi Agencijom;

2) zastupa Agenciju i odgovara za zakonitost i kvalitet rada Agencije;

3) organizuje rad u Agenciji;

4) predlaže Savjetu Agencije statut Agencije, godišnji program rada i finansijski plan Agencije, godišnji izvještaj o radu i finansijski izvještaj Agencije, kao i druge odluke;

5) izvršava odluke Savjeta Agencije;

6) upravlja ljudskim i finansijskim resursima;

7) utvrđuje akt o unutrašnjoj organizaciji i sistematizaciji Agencije;

8) stara se o obezbjeđivanju javnosti rada Agencije;

9) predlaže plan obuka za stručno usavršavanje zaposlenih u Agenciji;

10) sarađuje sa domaćim i međunarodnim organizacijama, kao i privatnim i civilnim sektorom u cilju unapređenja informacione bezbjednosti;

11) vrši druge poslove u skladu sa zakonom i statutom Agencije.

Akt o unutrašnjoj organizaciji i sistematizaciji Agencije utvrđuje se uz prethodnu saglasnost organa državne uprave nadležnog za poslove finansija.

Prestanak mandata direktora Agencije

Član 47

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

Status Agencije

Član 48

Agencija ima svojstvo pravnog lica i status državne agencije.

Agencija za svoj rad odgovara Vladi.

Odluku o osnivanju Agencije donosi Vlada.

Statut Agencije

Član 49

Agencija ima statut.

Statutom Agencije uređuju se sjedište Agencije, unutrašnja organizacija Agencije, način rada, odlučivanja i nadležnosti organa Agencije, javnost rada i druga pitanja od značaja za rad Agencije.

Na statut Agencije saglasnost daje Vlada.

Finansiranje Agencije

Član 50

Sredstva za rad Agencije obezbjeđuju se u budžetu Crne Gore.

Agencija je dužna da svoje finansijsko poslovanje organizuje i vodi u skladu sa propisima kojima se uređuje oblast budžetskog sistema i budžetskog računovodstva.

Primjena drugih propisa

Član 51

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

Zaposleni koji rade na poslovima informacione bezbjednosti u Agenciji zasnivaju radni odnos bez postupka javnog oglašavanja, a koji poslovi moraju biti prepoznati aktom o unutrašnjoj organizaciji i sistematizaciji.

VII. STRUČNI NADZOR

Nadzornik

Član 52

Agencija vrši stručni nadzor u skladu sa ovim zakonom preko zaposlenih lica u Agenciji, koja su ovlašćena za obavljanje poslova stručnog nadzora u skladu sa aktom o unutrašnjoj organizaciji i sistematizaciji Agencije (u daljem tekstu: nadzornik).

Nadzornik može biti lice koje, pored opštih uslova za zasnivanje radnog odnosa u državnim organima, ispunjava sljedeće uslove, i to da ima:

1) najmanje VII1 nivo kvalifikacije obrazovanja, i

2) pet godina radnog iskustva u oblasti informacione bezbjednosti.

Ovlašćenja nadzornika

Član 53

U postupku stručnog nadzora, nadzornik ima ovlašćenje da kod organa i drugih subjekata, osim organa državne uprave vrši kontrolu primjene mjera informacione bezbjednosti iz čl. 11 do 15 ovog zakona.

Pored ovlašćenja iz stava 1 ovog člana, u postupku stručnog nadzora, nadzornik ima ovlašćenje da kod ključnih i važnih subjekata, osim organa državne uprave vrši i kontrolu primjene mjera informacione bezbjednosti iz člana 16 ovog zakona.

Pored ovlašćenja iz st. 1 i 2 ovog člana, u postupku stručnog nadzora, nadzornik ima ovlašćenje da kod ključnih subjekata, osim organa državne uprave vrši kontrolu da li ti subjekti posjeduju certifikat o ispunjenost uslova u skladu sa važećim crnogorskim standardom za upravljanje informacionom bezbjednošću MEST ISO/IEC 27001 i da li su zahtijevali periodičnu provjeru ispunjenosti uslova u skladu sa tim standardom.

Obaveze ključnih i važnih subjekata prilikom vršenja stručnog nadzora

Član 54

Radi vršenja stručnog nadzora, organi i drugi subjekti, osim organa državne uprave dužni su da 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.

Zapisnik

Član 55

O izvršenom stručnom nadzoru nadzornik sačinjava zapisnik i dostavlja ga organu, odnosno drugom subjektu kod kojeg je vršen stručni nadzor, u roku od tri dana od dana izvršenog nadzora.

Otklanjanje nepravilnosti

Član 56

U slučaju da su u vršenju stručnog nadzora utvrđene nepravilnosti, nadzornik upozorava organ, odnosno drugi subjekat kod kojeg je utvrđena nepravilnost i ostavlja mu primjeren rok za otklanjanje te nepravilnosti, što konstatuje u zapisniku iz člana 55 ovog zakona.

Ako organ, odnosno drugi subjekat ne otkloni nepravilnosti u skladu sa stavom 1 ovog člana, zapisnik iz člana 55 ovog zakona nadzornik dostavlja i direktoru Agencije.

U slučaju iz stava 2 ovog člana, direktor Agencije donosi rješenje kojim nalaže mjere za otklanjanje nepravilnosti.

Protiv rješenja iz stava 3 ovog člana može se pokrenuti upravni spor.

Primjena drugih propisa u vršenju stručnog nadzora

Član 57

Na postupak i način vršenja stručnog nadzora, obaveze i ovlašćenja nadzornika i druga pitanja od značaja za vršenje stručnog nadzora shodno se primjenjuju propisi kojima se uređuje inspekcijski nadzor i upravni postupak, ako ovim zakonom nije drukčije određeno.

Postupanje sa podacima

Član 58

Nadzornik je dužan da čuva i štiti podatke do kojih je došao prilikom vršenja stručnog nadzora, u skladu sa zakonima kojima se uređuju tajnost podataka, zaštita podataka o ličnosti i zaštita poslovne tajne.

Službena legitimacija nadzornika

Član 59

Nadzorniku se, radi dokazivanja svojstva nadzornika, izdaje službena legitimacija.

Službenu legitimaciju iz stava 1 ovog člana izdaje Agencija na propisanom obrascu.

U slučaju gubitka ili nestanka službene legitimacije iz stava 1 ovog člana, nadzornik o tome obavještava direktora Agencije, u roku od tri dana od dana gubitka, odnosno nestanka legitimacije i oglašava je nevažećom u "Službenom listu Crne Gore".

Danom prestanka radnog odnosa u Agenciji, odnosno prestankom svojstva nadzornika, nadzornik vraća službenu legitimaciju iz stava 1 ovog člana Agenciji.

O izdatim i vraćenim službenim legitimacijama iz stava 1 ovog člana Agencija vodi evidenciju koja sadrži: redni broj, ime i prezime nadzornika, serijski broj legitimacije, datum izdavanja, datum vraćanja, odnosno gubitka ili nestanka legitimacije, potpis nadzornika i napomenu.

Izgled i sadržaj obrasca službene legitimacije iz stava 1 ovog člana propisuje Agencija.

Tehnički i drugi uslovi

Član 60

Agencija mora da ispunjava tehničke i druge uslove iz člana 39 stav 2 ovog zakona.

VIII. SAVJET ZA INFORMACIONU BEZBJEDNOST

Obrazovanje Savjeta za informacionu bezbjednost

Član 61

Radi praćenja razvoja informacione bezbjednosti, a naročito sajber bezbjednosti u cilju obezbjeđivanja bezbjednog sajber prostora Crne Gore, Vlada obrazuje Savjet za informacionu bezbjednost.

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

Sastav Savjeta za informacionu bezbjednost

Član 62

Savjet za informacionu bezbjednost čine predstavnici Ministarstva, Agencije, organa državne uprave nadležnog za unutrašnje poslove, organa državne uprave nadležnog za poslove odbrane, organa državne uprave nadležnog za poslove pravosuđa, organa državne uprave nadležnog za vanjske poslove, organa uprave nadležnog za tajne podatke i Agencije za nacionalnu bezbjednost, a po potrebi i predstavnici drugih organa i institucija.

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

Akt o obrazovanju Savjeta za informacionu bezbjednost

Član 63

Aktom o obrazovanju Savjeta za informacionu bezbjednost utvrđuju se zadaci, način rada, kao i druga pitanja od značaja za rad tog Savjeta.

IX. INSPEKCIJSKI NADZOR

Upravni nadzor

Član 64

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

Inspekcijski nadzor

Član 65

Inspekcijski nadzor nad primjenom mjera informacione bezbjednosti kod organa državne uprave vrši inspektor za usluge informacionog društva (u daljem tekstu: inspektor) u skladu sa ovim zakonom i zakonom kojim se uređuje inspekcijski nadzor.

Posebna ovlašćenja inspektora

Član 66

U postupku inspekcijskog nadzora inspektor, pored ovlašćenja utvrđenih zakonom kojim se uređuje oblast inspekcijskog nadzora, ima ovlašćenje da kod organa državne uprave vrši kontrolu primjene mjera informacione bezbjednosti iz čl. 11 do 15 ovog zakona.

Pored ovlašćenja iz stava 1 ovog člana, u postupku inspekcijskog nadzora, inspektor ima ovlašćenje da kod organa državne uprave koji su u skladu sa ovim zakonom određeni kao ključni i važni subjekti vrši kontrolu primjene mjera informacione bezbjednosti iz člana 16 ovog zakona.

Pored ovlašćenja iz st. 1 i 2 ovog člana, u postupku inspekcijskog nadzora, inspektor ima ovlašćenje da kod organa državne uprave koji su u skladu sa ovim zakonom određeni kao ključni subjekti vrši kontrolu da li ti organi posjeduju certifikat o ispunjenost uslova u skladu sa važećim crnogorskim standardom za upravljanje informacionom bezbjednošću MEST ISO/IEC 27001 i da li su zahtijevali periodičnu provjeru ispunjenosti uslova u skladu sa tim standardom.

Obaveze organa državne uprave prilikom vršenja inspekcijskog nadzora

Član 67

Radi vršenja inspekcijskog nadzora, organi državne uprave 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.

X. KAZNENE ODREDBE

Član 68

Novčanom kaznom u iznosu od 500 do 20.000 eura kazniće se za prekršaj pravno lice - ključni subjekat, ako:

1) ne primjenjuje mjere informacione bezbjednosti iz čl. 11 do 16 ovog zakona (član 18 stav 1);
2) ne ispunjava uslove u skladu sa važećim crnogorskim standardom za upravljanje informacionom bezbjednošću MEST ISO/IEC 27001 (član 18 stav 4);
3) od akreditovanog pravnog lica ne zahtijeva periodičnu provjeru ispunjenosti uslova u skladu sa važećim crnogorskim standardom za upravljanje informacionom bezbjednošću MEST ISO/IEC 27001 (član 18 stav 6);
4) nadležnom ministarstvu ne dostavi obavještenje o promjeni podataka iz člana 20 stav 2 tač. 1 do 7 ovog zakona, odmah nakon nastanka promjene (član 26 stav 1).

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

Član 69

Novčanom kaznom u iznosu od 500 do 10.000 eura kazniće se za prekršaj pravno lice - važni subjekat, ako:

1) ne primjenjuje mjere informacione bezbjednosti iz čl. 11 do 16 ovog zakona (član 18 stav 1);

2) nadležnom ministarstvu ne dostavi obavještenje o promjeni podataka iz člana 20 stav 2 tač. 1 do 7 ovog zakona, odmah nakon nastanka promjene (član 26 stav 1).

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

Član 70

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

1) ne primjenjuje mjere informacione bezbjednosti iz čl. 11 do 15 ovog zakona (član 18 stav 2);

2) ne odredi zaposleno lice za praćenje primjene mjera informacione bezbjednosti (član 18 stav 3);

3) nadležnom ministarstvu ne dostavi podatke u roku od sedam dana od dana prijema zahtjeva (član 20 stav 3);

4) nadležno ministarstvo ne obavijesti o promjeni podataka u roku od 14 dana od dana nastanka promjene (član 20 stav 4);

5) izvještaj o sajber prijetnjama, ozbiljnim sajber prijetnjama, odnosno incidentima, jednom mjesečno ne dostavi Agenciji, odnosno CIRT-u državne uprave (član 29 stav 1);

6) ne dostavi početno obavještenje Agenciji, odnosno CIRT-u državne uprave o sajber prijetnji, ozbiljnoj sajber prijetnji odnosno incidentu koji bi mogli u značajnoj mjeri da utiču na kontinuitet pružanja usluga (član 30 stav 1);

7) ne dostavi početno obavještenje za sajber prijetnju, ozbiljnu sajber prijetnju i incident, na propisanom obrascu u roku od 24 časa od trenutka saznanja za taj incident (član 30 st. 1 i 2);

8) u roku od 72 časa od podnošenja početnog obavještenja, Agenciji odnosno CIRT-u državne uprave ne dostavi prvi izvještaj o trajanju incidenta srednjeg nivoa i mjerama koje su preduzete za rješavanje tog incidenta, na propisanom obrascu (član 33 stav 2);

9) bez odlaganja ne dostavi poseban izvještaj na propisanom obrascu, Agenciji, odnosno CIRT-u državne uprave, a tokom trajanja incidenta srednjeg nivoa sazna za nove podatke ili okolnosti koje mogu biti od uticaja na taj incident (član 33 stav 3);

10) Agenciji, odnosno CIRT-u državne uprave svakih 72 časa, ne dostavi kontinuirane izvještaje o trajanju incidenta i mjerama koje su preduzete za rješavanje incidenta srednjeg nivoa, na propisanom obrascu (član 33 stav 4);

11) Agenciji, odnosno CIRT-u državne uprave ne dostavi završni izvještaj o incidentu srednjeg nivoa, najkasnije u roku od 30 dana od dana rješavanja tog incidenta, na propisanom obrascu (član 33 stav 5);

12) u roku od 72 časa od podnošenja početnog obavještenja, Agenciji odnosno CIRT-u državne uprave ne dostavi prvi izvještaj o trajanju incidenta visokog nivoa i mjerama koje su preduzete za rješavanje tog incidenta, na propisanom obrascu (član 34 stav 3);

13) bez odlaganja ne dostavi poseban izvještaj na propisanom obrascu, Agenciji, odnosno CIRT-u državne uprave, a tokom trajanja incidenta visokog nivoa sazna za nove podatke ili okolnosti koje mogu biti od uticaja na taj incident (član 34 stav 4);

14) svakih 24 časa, Agenciji, odnosno CIRT-u državne uprave ne dostavi kontinuirane izvještaje o trajanju incidenta i mjerama koje su preduzete za rješavanje tog incidenta, na propisanom obrascu (član 34 stav 5);

15) Agenciji, odnosno CIRT-u državne uprave ne dostavi završni izvještaj o incidentu srednjeg nivoa, najkasnije u roku od 30 dana od dana rješavanja tog incidenta, na propisanom obrascu (član 34 stav 6).

Za prekršaj iz stava 1 ovog člana kazniće se i odgovorno lice u pravnom licu 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 vršenja poziva, djelatnosti ili dužnosti u trajanju od tri do šest mjeseci.

XI. PRELAZNE I ZAVRŠNE ODREDBE

Rok za donošenje podzakonskih akata

Član 71

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

Do donošenja podzakonskih akata iz stava 1 ovog člana primjenjivaće se podzakonski akti donijeti na osnovu Zakona o informacionoj bezbjednosti ("Službeni list CG", br. 14/10, 40/16 i 67/21).

Rok za dostavljanje predloga sektorskih listi

Član 72

Nadležna ministarstva dužna su da predloge sektorskih listi iz člana 21 stav 1 ovog zakona dostave Ministarstvu, najkasnije u roku od devet mjeseci od dana stupanja na snagu ovog zakona.

Rok za dobijanje certifikata

Član 73

Ključni subjekti dužni su da dobiju certifikat o ispunjenosti uslova u skladu sa važećim crnogorskim standardom za upravljanje informacionom bezbjednošću MEST ISO/IEC 27001, u roku od 30 mjeseci od dana stupanja na snagu ovog zakona.

Rok za osnivanje Agencije

Član 74

Odluka o osnivanju Agencije donijeće se u roku od 15 dana od dana stupanja na snagu ovog zakona.

Rok za imenovanje predsjednika i članova Savjeta Agencije

Član 75

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

Rok za imenovanje direktora Agencije

Član 76

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

Do imenovanja direktora Agencije, u skladu sa ovim zakonom poslove direktora Agencije obavljaće vršilac dužnosti, koga, na predlog ministra javne uprave, odredi Vlada.

Predlog iz stava 2 ovog člana dostaviće se Vladi u roku od 15 dana od dana stupanja na snagu ovog zakona.

Donošenje akata Agencije

Član 77

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.

Preuzimanje državnih službenika

Član 78

Danom donošenja akta o unutrašnjoj organizaciji i sistematizaciji Agencije, 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 1 ovog člana, do donošenja akta o raspoređivanju u skladu sa aktom o unutrašnjoj organizaciji i sistematizaciji Agencije, nastavljaju sa radom u zvanjima koja su stekli prije preuzimanja.

Državni službenici iz stava 1 ovog člana koji ne budu raspoređeni u skladu sa aktom o unutrašnjoj organizaciji i sistematizaciji Agencije ostvaruju prava u skladu sa propisima o državnim službenicima i namještenicima.

Nastavak rada Savjeta za informacionu bezbjednost

Član 79

Savjet za informacionu bezbjednost koji je obrazovan u skladu sa Zakonom o informacionoj bezbjednosti ("Službeni list CG", br. 14/10, 40/16 i 67/21) nastavlja sa radom do obrazovanja Savjeta za informacionu bezbjednost u skladu sa ovim zakonom.

Prestanak važenja propisa

Član 80

Danom stupanja na snagu ovog zakona prestaje da važi Zakon o informacionoj bezbjednosti ("Službeni list CG", br. 14/10, 40/16 i 67/21) i odredbe člana 74 stav 1 tačka 8b i člana 74a Zakona o tajnosti podataka ("Službeni list CG", br. 14/08, 76/09, 41/10, 38/12, 44/12, 14/13, 18/14, 48/15 i 74/20).

Stupanje na snagu

Član 81

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

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 u Uniji, izmjeni Regulative (EU) br. 910/2014 i Direktive (EU) 2018/1972 i prestanku važenja Direktive (EU) 2016/1148 (Direktiva NIS2).

Broj: 10-2/24-1/19
EPA 246 XXVIII
Podgorica, 19. novembar 2024. godine
Skupština Crne Gore 28. saziva
Predsjednik,
Andrija Mandić, s.r.