Na osnovu člana 82 stav 1 tačka 2 i člana 91 stav 1 Ustava Crne Gore, Skupština Crne Gore 28. saziva, na sjednici Prvog vanrednog zasijedanja u 2026. godini, dana 2. februara 2026. godine, donijela je

ZAKON

O DIGITALNOJ OPERATIVNOJ OTPORNOSTI FINANSIJSKOG SEKTORA*

I. OSNOVNE ODREDBE

Predmet

Član 1

Ovim zakonom utvrđuju se zahtjevi, postupci i mjere za obezbjeđivanje visokog nivoa digitalne operativne otpornosti finansijskog sektora, uključujući zahtjeve za bezbjednost mrežnih i informacionih sistema koji podržavaju poslovanje finansijskih subjekata, kao i druga pitanja od značaja za digitalnu operativnu otpornost finansijskog sektora.

Primjena

Član 2

(1) Ovaj zakon primjenjuje se na subjekte finansijskog sektora (u daljem tekstu: finansijski subjekt), i to:

1) kreditnu instituciju;
2) platnu instituciju sa sjedištem u Crnoj Gori;
3) registrovanog pružaoca usluge informacija o računu sa sjedištem u Crnoj Gori;
4) instituciju za elektronski novac sa sjedištem u Crnoj Gori;
5) investiciono društvo;
6) centralno klirinško depozitarno društvo;
7) centralnu drugu ugovornu stranu;
8) mjesto trgovanja;
9) trgovinski repozitorij;
10) društvo za upravljanje alternativnim investicionim fondom;
11) društva za upravljanje otvorenim investicionim fondom sa javnom ponudom;
12) instituciju za profesionalnu penzionu štednju;
13) pružaoca usluga dostave podataka;
14) administratora ključnih referentnih vrijednosti;
15) društvo za osiguranje;
16) društvo za reosiguranje;
17) podružnicu stranog društava za osiguranje;
18) podružnicu stranog društava za reosiguranje;
19) društvo za posredovanje u osiguranju;
20) sporednog posrednika u osiguranju;
21) preduzetnika posrednika u osiguranju;
22) društvo za zastupanje u osiguranju;
23) sporednog zastupnika u osiguranju;
24) preduzetnika zastupnika u osiguranju;
25) agenciju za pružanje drugih usluga u osiguranju;
26) pružaoca usluga povezanih sa kriptoimovinom;
27) izdavaoca tokena vezanih za imovinu.

(2) Ovaj zakon ne primjenjuje se na:

1) Razvojnu banku Crne Gore;
2) društva za osiguranje i društva za reosiguranje iz člana 3 i 4 Zakona o osiguranju ("Službeni list CG", broj 33/25);

3) posrednike u osiguranju, posrednike u reosiguranju i sporedne posrednike u osiguranju koji su klasifikovani kao mikro, mali ili srednji finansijski subjekti;

4) institucije za profesionalnu penzionu štednju koje upravljaju penzionim šemama sa ukupno najviše 15 članova, a koje su uređene zakonom kojim se uređuju dobrovoljni penzioni fondovi.

(3) Ovaj zakon ne utiče na odredbe zakona kojim se uređuju nadležnosti državnih organa u vezi sa zaštitom javne bezbjednosti, nacionalne bezbjednosti i odbrane.

Nadležni organ

Član 3

(1) Nadležni organ, u smislu ovog zakona, je organ koji je u skladu sa zakonom kojim se uređuje osnivanje i poslovanje finansijskog subjekta iz člana 2 stav 1 ovog zakona nadležan za kontrolu, superviziju, odnosno nadzor tog subjekta, i to:

1) za finansijski subjekt iz člana 2 stav 1 tač. 1 do 4 ovog zakona, Centralna banka Crne Gore (u daljem tekstu: Centralna banka);

2) za finansijski subjekt iz člana 2 stav 1 tač. 5 do 14 ovog zakona, Komisija za tržište kapitala Crne Gore (u daljem tekstu: Komisija);

3) za finansijski subjekt iz člana 2 stav 1 tač. 15 do 25 ovog zakona, Agencija za nadzor osiguranja (u daljem tekstu: Agencija);

4) za finansijski subjekt iz člana 2 stav 1 tač. 26 i 27 ovog zakona, organ utvrđen posebnim zakonom.

(2) Nadležni organi iz stava 1 ovog člana dužni su da međusobno sarađuju i razmjenjuju informacije i podatke potrebne za sprovođenje ovog zakona.

(3) Protiv rješenja nadležnog organa koje se donosi u skladu sa odredbama ovog zakona može se tužbom pokrenuti upravni spor.

(4) U upravnom sporu protiv rješenja nadležnog organa iz stava 3 ovog člana, nadležni sud ne može meritorno odlučivati o predmetu upravnog spora za čije rješavanje je ovim zakonom utvrđena nadležnost nadležnog organa.

Digitalna operativna otpornost

Član 4

Digitalna operativna otpornost, u smislu ovog zakona, je sposobnost finansijskog subjekta da izgradi, obezbijedi i preispituje svoj operativni integritet i pouzdanost, na način da, direktno ili indirektno kroz korišćenje usluga koje pružaju treće strane, odnosno pružaoci usluga informaciono komunikacionih tehnologija (u daljem tekstu: IKT), stvara uslove za primjenu svih IKT kapaciteta neophodnih za bezbjednost mrežnih i informacionih sistema koje koristi i koji podržavaju kontinuirano pružanje finansijskih usluga tog subjekta i očuvanje njihovog kvaliteta, uključujući i u slučaju poremećaja.

Princip proporcionalnosti

Član 5

(1) Finansijski subjekt je dužan da primjenjuje odredbe ovog zakona srazmjerno svojoj veličini, ukupnom rizičnom profilu, prirodi, obimu i složenosti svojih usluga, aktivnosti i poslovanja, na način utvrđen ovim zakonom.

(2) Nadležni organ razmatra primjenu principa proporcionalnosti iz stava 1 ovog člana prilikom procjene konzistentnosti sistema finansijskog subjekta za upravljanje IKT rizicima, uzimajući u obzir izvještaje koji se dostavljaju na zahtjev nadležnog organa u skladu sa članom 11 stav 3 ovog zakona, odnosno članom 21 ovog zakona.

Klasifikacija finansijskih subjekata prema veličini

Član 6

(1) U smislu ovog zakona, u zavisnosti od prosječnog broja zaposlenih, ukupnog prihoda na godišnjem nivou i ukupne aktive, finansijski subjekti se klasifikuju kao:

1) mikro finansijski subjekti, ako:

- imaju prosječan broj zaposlenih u poslovnoj godini manji od deset; i
- ostvaruju ukupan prihod na godišnjem nivou i/ili ukupnu aktivu do 2.000.000,00 eura;

2) mali finansijski subjekti, ako:

- imaju prosječan broj zaposlenih u poslovnoj godini u rasponu od deset do 49; i

- ostvaruju ukupan prihod na godišnjem nivou i/ili ukupnu aktivu u rasponu od 2.000.000,01 eura do 10.000.000,00 eura;

3) srednji finansijski subjekti, ako:

- imaju prosječan broj zaposlenih u poslovnoj godini manji od 250; i

- ostvaruju ukupan prihod na godišnjem nivou do 50.000.000,00 eura i/ili ukupnu aktivu do 43.000.000,00 eura;

4) ostali finansijski subjekti, koji se ne mogu klasifikovati kao mikro, mali ili srednji finansijski subjekti, u skladu sa tač. 1 do 3 ovog stava.

(2) Klasifikaciju u skladu sa kriterijumima iz stava 1 ovog člana, vrši finansijski subjekt na dan sastavljanja finansijskih iskaza i podatke na osnovu kojih je izvršena klasifikacija koristi za narednu poslovnu godinu.

(3) Izuzetno od stava 2 ovog člana, novoosnovani finansijski subjekt klasifikuje se na osnovu podataka iz finansijskih iskaza tekuće poslovne godine i broja mjeseci poslovanja, a utvrđeni podaci koriste se za tekuću i narednu poslovnu godinu.

(4) Prosječan broj zaposlenih iz stava 1 ovog člana, izračunava se na način da se ukupan broj zaposlenih krajem svakog mjeseca, uključujući i zaposlene u inostranstvu, podijeli sa brojem mjeseci u poslovnoj godini, odnosno brojem mjeseci poslovanja finansijskog subjekta.

(5) Ako na dan sastavljanja bilansa stanja, u dvije uzastopne finansijske godine dođe do odstupanja od graničnih vrijednosti iz stava 1 ovog člana, finansijski subjekt dužan je da izvrši klasifikaciju u odgovarajuću kategoriju za narednu poslovnu godinu.

(6) Izuzetno od stava 1 tačka 1 ovog člana, finansijski subjekt koji je mjesto trgovanja, centralna druga ugovorna strana, trgovinski repozitorij ili centralno klirinško depozitarno društvo i ispunjava uslove da bude klasifikovan kao mikro finansijski subjekt, klasifikuje se kao ostali finansijski subjekt.

Upotreba rodno osjetljivog jezika

Član 7

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

Značenje izraza

Član 8

Izrazi upotrijebljeni u ovom zakonu imaju sljedeća značenja:

1) mrežni i informacioni sistem je:

- elektronska komunikaciona mreža, odnosno sistem prenosa koji se zasniva na stalnoj infrastrukturi ili centralizovanom upravljačkom kapacitetu i obuhvata, gdje je primjenljivo, uređaje za komutaciju ili usmjeravanje i druga sredstva, uključujući pasivne mrežne elemente, koji omogućavaju prenos signala pomoću žičanih, radio, optičkih ili drugih elektromagnetnih sistema, uključujući satelitske mreže, fiksne (sa komutacijom kola i paketa, uključujući internet) i mobilne mreže, elektroenergetske kablovske sisteme, u dijelu koji se koristi za prenos signala, mreže koje se koriste za prenos i distribuciju radijskih i televizijskih programa bez obzira na vrstu informacije koja se prenosi;

- svaki uređaj ili skup povezanih ili međuzavisnih uređaja, od kojih najmanje jedan programski izvršava automatsku obradu podataka u elektronskom obliku; ili

- podaci 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) zastarjeli IKT sistem je IKT sistem koji je dostigao kraj svog životnog ciklusa, a koji zbog tehnoloških ili komercijalnih razloga nije pogodan za nadogradnje ili popravke ili za koji njegov dobavljač ili treća strana koja pruža IKT usluge prestane da pruža podršku, ali je i dalje u upotrebi i podržava funkcije finansijskog subjekta;

3) bezbjednost mrežnih i informacionih sistema je sposobnost mrežnih i informacionih sistema da se, na određenom nivou pouzdanosti, odupru svakom događaju koji može da ugrozi dostupnost, autentičnost, integritet ili povjerljivost podataka koji se čuvaju, prenose ili obrađuju, kao i usluga koje ti sistemi nude ili kojima se preko njih pristupa;

4) IKT rizik je svaka razumno prepoznatljiva okolnost koja se odnosi na korišćenje mrežnih i informacionih sistema, a koja, ukoliko nastane, može da dovede do negativnih uticaja u digitalnom ili fizičkom okruženju i

ugrozi bezbjednost mrežnih i informacionih sistema, bilo kog tehnološki zavisnog alata ili procesa, poslovnih operacija i procesa ili pružanja usluga;

5) informaciona imovina je skup materijalnih ili nematerijalnih informacija, koje je potrebno zaštititi;

6) IKT imovina je softverska ili hardverska imovina u mrežnim i informacionim sistemima koje koristi finansijski subjekt;

7) IKT incident je jedan ili više povezanih događaja koje finansijski subjekt nije planirao, a koji narušavaju bezbjednost mrežnih i informacionih sistema i negativno utiču na dostupnost, autentičnost, integritet ili povjerljivost podataka, ili na usluge koje finansijski subjekt pruža;

8) operativni ili sigurnosni incident povezan sa plaćanjem je jedan ili više povezanih događaja, bez obzira da li su povezani sa IKT-om, koje finansijski subjekt iz člana 2 stav 1 tač. 1 do 4 ovog zakona nije planirao, a koji negativno utiču na dostupnost, autentičnost, integritet ili povjerljivost podataka povezanih sa plaćanjem, ili na usluge povezane sa plaćanjem koje finansijski subjekt pruža;

9) značajan IKT incident je IKT incident koji ima visok nivo negativnog uticaja na mrežne i informacione sisteme koji podržavaju kritične ili važne funkcije finansijskog subjekta;

10) značajan operativni ili sigurnosni incident povezan sa plaćanjem je operativni ili sigurnosni incident povezan sa plaćanjem koji ima visok nivo negativnog uticaja na usluge povezane sa plaćanjem koje se pružaju;

11) sajber prijetnja je svaka moguća okolnost, događaj ili djelovanje koji bi mogli oštetiti, poremetiti ili na drugi način negativno uticati na mrežne i informacione sisteme, korisnike tih sistema i druga lica;

12) ozbiljna sajber prijetnja je sajber prijetnja čije tehničke karakteristike ukazuju na to da bi mogla dovesti do značajnog IKT incidenta ili značajnog operativnog ili sigurnosnog incidenta povezanog sa plaćanjem;

13) sajber napad je zlonamjerni IKT incident izazvan pokušajem bilo kojeg aktera da uništi, razotkrije, izmijeni, onemogući, ukrade imovinu, stekne neovlašćeni pristup imovini ili je neovlašćeno koristi;

14) saznanja o prijetnjama su informacije koje su agregirane, prilagođene, analizirane, protumačene ili dopunjene radi utvrđivanja potrebe donošenja odluka i omogućavanja adekvatnog i dovoljnog razumijevanja u cilju ublažavanja posljedica IKT incidenta ili sajber prijetnje, uključujući informacije o tehničkim detaljima sajber napada, licima odgovornim za napad, njihovom načinu djelovanja i motivima;

15) ranjivost je slabost, podložnost ili nedostatak resursa, sistema, procesa ili kontrole koju sajber prijetnja može iskoristiti;

16) penetraciono testiranje vođeno prijetnjama (TLPT) je kontrolisano, prilagođeno testiranje kritičnih produkcionih sistema koje finansijski subjekt koristi, zasnovano na saznanjima o prijetnjama, odnosno testiranje crvenog tima, koje se sprovodi u skladu sa okvirom koji oponaša taktike, tehnike i postupke stvarnih zlonamjernih aktera za koje se vjeruje da predstavljaju realnu sajber prijetnju;

17) TLPT organ druge države članice je:

- jedinstveni javni organ u finansijskom sektoru sa sjedištem u drugoj državi članici, koji je imenovan u skladu sa članom 26 stav 9 Regulative (EU) br. 2022/2554;

- nadležni organ sa sjedištem u drugoj državi članici kojem je povjereno izvršavanje pojedinih ili svih zadataka u vezi sa sprovođenjem TLPT-a, u skladu sa članom 26 stav 10 Regulative (EU) br. 2022/2554;

- nadležni organ iz člana 46 Regulative (EU) br. 2022/2554, sa sjedištem u drugoj državi članici.

18) zajednički TLPT je TLPT, koji nije objedinjeni TLPT iz člana 30 stav 2 ovog zakona, a kojim je obuhvaćeno više finansijskih subjekata koji koriste IKT usluge koje pruža grupni pružalac IKT usluga ili pripadaju istoj grupi i zajednički koriste IKT sisteme;

19) IKT rizik povezan sa trećim stranama je IKT rizik kojem finansijski subjekt može biti izložen zbog korišćenja IKT usluga koje pružaju treće strane ili njihovi podizvođači, uključujući i na osnovu ugovora o eksternalizaciji;

20) treća strana koja pruža IKT usluge je pravno ili fizičko lice koje pruža IKT usluge;

21) grupni pružalac IKT usluga je pravno lice koje je dio finansijske grupe i koje pruža IKT usluge pretežno finansijskim subjektima koji su dio iste grupe ili finansijskim subjektima koji pripadaju istom institucionalnom sistemu zaštite, uključujući i njihova matična pravna lica, zavisna pravna lica, filijale i druge subjekte koji su u zajedničkom vlasništvu ili pod zajedničkom kontrolom;

22) IKT usluge su digitalne usluge i usluge vezane za podatke koje se pomoću IKT sistema, kontinuirano pružaju jednom ili više internih ili eksternih korisnika, uključujući usluge iznajmljivanja IKT opreme ("hardver kao usluga") i hardverske usluge koje uključuju pružanje tehničke podrške od strane pružaoca hardvera putem ažuriranja softvera ili firmvera, osim tradicionalnih analognih telefonskih usluga;

23) kritična ili važna funkcija je funkcija čiji bi poremećaj značajno narušio finansijske rezultate finansijskog subjekta, pouzdanost, kontinuitet njegovih usluga i aktivnosti, ili funkcija čiji bi prekidi, neispravno ili neuspješno izvršavanje značajno narušili sposobnost tog subjekta da kontinuirano ispunjava uslove i obaveze utvrđene dozvolom za rad ili druge obaveze u skladu sa propisima kojima se uređuje pružanje finansijskih usluga;

24) kritična treća strana koja pruža IKT usluge je treća strana koja pruža IKT usluge i koja je određena kao kritična u skladu sa članom 31 Regulative (EU) br. 2022/2554;

25) treća strana koja pruža IKT usluge sa sjedištem u trećoj zemlji je pravno lice sa sjedištem u trećoj zemlji koje je zaključilo ugovor sa finansijskim subjektom za pružanje IKT usluga;

26) treća zemlja je strana država koja nije država članica i država članica do pristupanja Crne Gore Evropskoj uniji;

27) država članica je država članica Evropske unije i država potpisnica Ugovora o Evropskom ekonomskom prostoru;

28) zavisno pravno lice je pravno lice koje je pod kontrolom matičnog pravnog lica, uključujući i bilo koje pravno lice koje je pod kontrolom krajnjeg matičnog pravnog lica;

29) grupa je matično pravno lice i sva njegova zavisna pravna lica;

30) matično pravno lice ima značenje utvrđeno zakonom kojim se uređuje računovodstvo;

31) IKT podizvođač sa sjedištem u trećoj zemlji je IKT podizvođač koji je pravno lice sa sjedištem u trećoj zemlji koje je zaključilo ugovor sa trećom stranom koja pruža IKT usluge, bez obzira na sjedište treće strane koja pruža IKT usluge;

32) rizik IKT koncentracije je izloženost prema jednoj ili više povezanih trećih strana koje pružaju IKT usluge, kojom se stvara zavisnost od tih trećih strana na način da njihova nedostupnost, propast ili druga vrsta nedostatka može potencijalno da ugrozi sposobnost finansijskog subjekta da obavlja kritične ili važne funkcije, ili prouzrokuje druge vrste negativnih uticaja, uključujući značajne gubitke, ili ugrozi finansijsku stabilnost tržišta kao cjeline;

33) organ upravljanja je:

- jedan ili više organa finansijskog subjekta, koji su u skladu sa propisima ovlašćeni da utvrđuju strategiju, ciljeve i opšte usmjerenje tog finansijskog subjekta i koji vrše nadzor i prate odlučivanje u vezi sa upravljanjem i uključuje lica koja stvarno upravljaju poslovanjem tog finansijskog subjekta; ili

- lica koja imaju ovlašćenja jednaka ovlašćenjima iz alineje 1 ove tačke i koja, u skladu sa propisima, vode poslove finansijskog subjekta ili imaju ključne funkcije;

34) kreditna institucija ima značenje utvrđeno zakonom kojim se uređuje poslovanje kreditnih institucija;

35) platna institucija sa sjedištem u Crnoj Gori ima značenje utvrđeno zakonom kojim se uređuje platni promet;

36) registrovani pružalac usluge informacija o računu sa sjedištem u Crnoj Gori ima značenje utvrđeno zakonom kojim se uređuje platni promet;

37) institucija za elektronski novac sa sjedištem u Crnoj Gori ima značenje utvrđeno zakonom kojim se uređuje platni promet;

38) investiciono društvo ima značenje utvrđeno zakonom kojim se uređuje tržište kapitala;

39) malo i nepovezano investiciono društvo ima značenje utvrđeno zakonom kojim se uređuje tržište kapitala;

40) centralno klirinško depozitarno društvo ima značenje utvrđeno zakonom kojim se uređuje tržište kapitala;

41) centralna druga ugovorna strana ima značenje utvrđeno zakonom kojim se uređuje tržište kapitala;

42) mjesto trgovanja ima značenje utvrđeno zakonom kojim se uređuje tržište kapitala;

43) trgovinski repozitorij ima značenje utvrđeno zakonom kojim se uređuje tržište kapitala;

44) društvo za upravljanje alternativnim investicionim fondom ima značenje utvrđeno zakonom kojim se uređuje poslovanje alternativnih fondova;

45) društvo za upravljanje otvorenim investicionim fondom sa javnom ponudom ima značenje utvrđeno zakonom kojim se uređuje poslovanje otvorenih investicionih fondova sa javnom ponudom;

46) institucija za profesionalnu penzionu štednju ima značenje utvrđeno zakonom koji uređuje dobrovoljne penzione fondove;

47) mala institucija za profesionalnu penzionu štednju je institucija za profesionalnu penzionu štednju koja upravlja penzionim programima koji ukupno imaju manje od 100 članova;

48) pružalac usluga dostave podataka ima značenje utvrđeno zakonom kojim se uređuje tržište kapitala;

49) administrator ključnih referentnih vrijednosti ima značenje utvrđeno zakonom kojim se uređuju referentne vrijednosti;

50) društvo za osiguranje ima značenje utvrđeno zakonom kojim se uređuje osiguranje;

51) društvo za reosiguranje ima značenje utvrđeno zakonom kojim se uređuje osiguranje;

52) podružnica stranog društava za osiguranje ima značenje utvrđeno zakonom kojim se uređuje osiguranje;

53) podružnica stranog društava za reosiguranje ima značenje utvrđeno zakonom kojim se uređuje osiguranje;

54) društvo za posredovanje u osiguranju ima značenje utvrđeno zakonom kojim se uređuje osiguranje;

55) sporedni posrednik u osiguranju ima značenje utvrđeno zakonom kojim se uređuje osiguranje;

56) preduzetnik posrednik u osiguranju ima značenje utvrđeno zakonom kojim se uređuje osiguranje;

57) društvo za zastupanje u osiguranju ima značenje utvrđeno zakonom kojim se uređuje osiguranje;

58) sporedni zastupnik u osiguranju ima značenje utvrđeno zakonom kojim se uređuje osiguranje;

59) preduzetnik zastupnik u osiguranju ima značenje utvrđeno zakonom kojim se uređuje osiguranje;

60) agencija za pružanje drugih usluga u osiguranju ima značenje utvrđeno zakonom kojim se uređuje osiguranje;

61) pružalac usluga povezanih sa kriptoimovinom ima značenje utvrđeno propisom kojim se uređuje poslovanje ovog finansijskog subjekta;

62) izdavalac tokena vezanih za imovinu ima značenje utvrđeno propisom kojim se uređuje poslovanje ovog finansijskog subjekta;

63) javni organ je svaki organ državne uprave, drugi državni organ ili organ sa javnim ovlašćenjima, uključujući Centralnu banku Crne Gore;

64) ECB je Evropska centralna banka;

65) EBA je Evropski bankarski regulator;

66) EIOPA je Evropski nadzorni organ za osiguranje i profesionalno penzijsko osiguranje;

67) ESCB je Evropski sistem centralnih banaka;

68) ESMA je Evropski nadzorni organ za hartije od vrijednosti i tržište kapitala.

II. UPRAVLJANJE IKT RIZICIMA

Korporativno upravljanje i organizacija

Član 9

(1) Organ upravljanja finansijskog subjekta dužan je da obezbijedi da finansijski subjekt postupa u skladu sa odredbama ovog zakona.

(2) Finansijski subjekt dužan je da uspostavi sistem upravljanja i sistem interne kontrole kojima se obezbjeđuje efikasno i pouzdano upravljanje IKT rizicima, u skladu sa članom 10 st. 5 i 6 ovog zakona, radi postizanja visokog nivoa digitalne operativne otpornosti.

(3) Organ upravljanja finansijskog subjekta dužan je da utvrdi, odobri i nadzire sva pravila, postupke, procese, mehanizme, mjere i resurse povezane sa sistemom upravljanja IKT rizicima iz člana 10 stav 1 ovog zakona i da obezbijedi njihovu primjenu, i u tom cilju naročito da:

1) uspostavlja politike sa ciljem održavanja visokog nivoa dostupnosti, autentičnosti, integriteta i povjerljivosti podataka;

2) jasno utvrđuje ovlašćenja, zaduženja i odgovornosti za obavljanje svih poslova povezanih sa IKT i uspostavlja odgovarajuće mehanizme upravljanja kako bi se, na svim organizacionim nivoima, obezbijedila efikasna i blagovremena komunikacija, saradnja i koordinacija u vezi sa obavljanjem tih poslova;

3) utvrđuje strategiju digitalne operativne otpornosti iz člana 12 stav 1 ovog zakona, uključujući i odgovarajući nivo tolerancije finansijskog subjekta prema IKT riziku iz člana 12 stav 2 tačka 2 ovog zakona;

4) usvaja i periodično preispituje IKT politiku kontinuiteta poslovanja iz člana 17 stav 1 ovog zakona i planove za odgovor i oporavak u IKT oblasti iz člana 17 stav 4 ovog zakona i nadzire njihovu primjenu;

5) odobrava i periodično preispituje planove interne revizije u IKT oblasti, njihove značajne izmjene i da redovno razmatra rezultate revizija u IKT oblasti;

6) donosi i periodično preispituje odgovarajući plan raspodjele finansijskih sredstava za ispunjavanje svih potreba finansijskog subjekta u pogledu digitalne operativne otpornosti, uključujući i sprovođenje relevantnih

programa za podizanje svijesti o IKT bezbjednosti i obuka o digitalnoj operativnoj otpornosti iz člana 19 stav 10 ovog zakona i sticanje znanja i vještina u IKT oblasti za sve zaposlene;

7) usvaja i periodično preispituje politiku o korišćenju IKT usluga koje pružaju treće strane koje pružaju IKT usluge;

8) na nivou cijele organizacije uspostavlja mehanizme izvještavanja za blagovremeno i adekvatno informisanje u vezi sa:

- zaključenim ugovorima sa trećim stranama koje pružaju IKT usluge;

- svim planiranim značajnim promjenama u vezi sa trećim stranama koje pružaju IKT usluge;

- potencijalnim uticajem promjena iz alineje 2 ove tačke na kritične ili važne funkcije, uključujući rezime analize rizika za procjenu uticaja tih promjena;

- IKT incidentima, a najmanje o značajnim IKT incidentima i njihovom uticaju, kao i o odgovoru, oporavku i korektivnim mjerama.

(4) Finansijski subjekt, koji nije klasifikovan kao mikro finansijski subjekt, dužan je da odredi organizacioni dio odgovoran za praćenje realizacije ugovora zaključenih sa trećim stranama koje pružaju IKT usluge, ili da imenuje člana višeg rukovodstva koji će biti odgovoran za nadzor izloženosti prema povezanom riziku i pripadajuće dokumentacije.

(5) Članovi organa upravljanja dužni su da aktivno unapređuju znanje i vještine potrebne za razumijevanje i procjenu IKT rizika i njegovog uticaja na poslovanje finansijskog subjekta, uključujući i kroz redovne posebne obuke, srazmjerno prirodi rizika kojim se upravlja.

Sistem upravljanja IKT rizicima

Član 10

(1) Finansijski subjekt je dužan da uspostavi pouzdan, sveobuhvatan i dobro dokumentovan sistem upravljanja IKT rizicima, kao dio opšteg sistema upravljanja rizicima, kojim se omogućava brzo, efikasno i sveobuhvatno tretiranje IKT rizika i obezbjeđuje visok nivo digitalne operativne otpornosti.

(2) Sistem upravljanja IKT rizicima iz stava 1 ovog člana, najmanje obuhvata strategije, politike, procedure, IKT protokole i alate potrebne za pravilnu i adekvatnu zaštitu cjelokupne informacione imovine i IKT imovine, uključujući softver, servere i ostali hardver i zaštitu svih relevantnih fizičkih komponenti i infrastrukture, kao što su prostorije, računarski centri i posebna osjetljiva područja, kako bi se obezbijedilo da je sva informaciona imovina i IKT imovina adekvatno zaštićena od rizika, uključujući oštećenja, neovlašćen pristup ili korišćenje.

(3) Finansijski subjekt je dužan da, u skladu sa sistemom upravljanja IKT rizicima, svede na najmanju moguću mjeru uticaj IKT rizika, primjenom odgovarajućih strategija, politika, procedura, IKT protokola i alata iz stava 2 ovog člana.

(4) Finansijski subjekt je dužan da nadležnom organu, na njegov zahtjev, dostavi potpune i ažurne informacije o IKT rizicima i sistemu upravljanja IKT rizicima iz stava 1 ovog člana.

(5) Finansijski subjekt, koji nije klasifikovan kao mikro finansijski subjekt, dužan je da odgovornost za upravljanje i nadzor nad IKT rizikom dodijeli kontrolnoj funkciji i da obezbijedi odgovarajući nivo njene nezavisnosti, na način da se izbjegava sukob interesa.

(6) Finansijski subjekt je dužan da obezbijedi međusobnu nezavisnost i razdvajanje poslova u kojima IKT rizik nastaje, poslova kontrolnih funkcija i poslova interne revizije, u skladu sa modelom tri linije odbrane ili internim modelom za upravljanje i kontrolu rizika.

Unaprjeđivanje i revizija sistema upravljanja IKT rizicima

Član 11

(1) Finansijski subjekt je dužan da kontinuirano unaprjeđuje sistem upravljanja IKT rizicima iz člana 10 stav 1 ovog zakona na osnovu iskustava stečenih kroz njegovu praktičnu primjenu i praćenje, kao i da taj sistem preispituje i ažurira:

1) najmanje jednom godišnje;

2) u slučaju značajnog IKT incidenta;

3) na zahtjev nadležnog organa;

4) u skladu sa rezultatima testiranja digitalne operativne otpornosti;

5) u skladu sa zaključcima revizije.

(2) Izuzetno od stava 1 tačka 1 ovog člana, finansijski subjekt koji je klasifikovan kao mikro finansijski subjekt dužan je da preispituje i ažurira sistem upravljanja IKT rizicima iz stava 1 ovog člana periodično.

(3) Finansijski subjekt je dužan da izvještaj o preispitivanju i ažuriranju iz st. 1 i 2 ovog člana dostavi nadležnom organu, na njegov zahtjev.

(4) Finansijski subjekt, koji nije klasifikovan kao mikro finansijski subjekt, dužan je da obezbijedi redovne interne revizije sistema upravljanja IKT rizicima iz člana 10 stav 1 ovog zakona, u skladu sa planom revizije, od strane nezavisnih revizora koji posjeduju znanje, vještine i iskustvo u oblasti IKT rizika.

(5) Učestalost i predmet revizija iz stava 4 ovog člana moraju biti srazmjerni IKT riziku finansijskog subjekta.

(6) Finansijski subjekt je dužan da uspostavi formalan proces koji omogućava blagovremeno otklanjanje ključnih nepravilnosti i nedostataka utvrđenih revizijom iz stava 4 ovog člana, kao i adekvatnu provjeru i praćenje tog postupka.

Strategija digitalne operativne otpornosti

Član 12

(1) Finansijski subjekt je dužan da u strategiji digitalne operativne otpornosti, koja predstavlja sastavni dio sistema upravljanja IKT rizicima iz člana 10 stav 1 ovog zakona, utvrdi način primjene tog sistema.

(2) Strategija iz stava 1 ovog člana mora da obuhvati opšte kriterijume i metode za tretiranje IKT rizika i postizanje konkretnih IKT ciljeva, a najmanje mora da:

1) opisuje i objašnjava kako sistem za upravljanje IKT rizicima podržava poslovnu strategiju i ciljeve finansijskog subjekta;

2) utvrđuje nivo tolerancije prema IKT riziku, u skladu sa sklonošću finansijskog subjekta ka preuzimanju rizika, i sadrži analizu prihvatljivog uticaja IKT poremećaja;

3) definiše jasne ciljeve u oblasti informacione bezbjednosti, uključujući ključne indikatore uspješnosti i ključne metrike rizika;

4) opisuje i objašnjava referentnu, odnosno ciljanu IKT arhitekturu i sve promjene potrebne za postizanje konkretnih poslovnih ciljeva;

5) okvirno navodi različite mehanizme uspostavljene radi otkrivanja IKT incidenata, sprečavanja njihovog uticaja i obezbjeđivanja zaštite od tog uticaja;

6) jasno prikazuje postojeće stanje digitalne operativne otpornosti, na osnovu informacija o broju prijavljenih značajnih IKT incidenata i efikasnosti preventivnih mjera;

7) predviđa sprovođenje testiranja digitalne operativne otpornosti, u skladu sa odredbama čl. 27 do 32 ovog zakona;

8) utvrđuje strategiju komunikacije u slučaju IKT incidenata o kojima se informacije saopštavaju u skladu sa članom 20 ovog zakona.

(3) Finansijski subjekt može, da utvrdi sveobuhvatnu strategiju IKT nabavke od više dobavljača, na nivou grupe ili subjekta, kojom se identifikuju ključne zavisnosti od trećih strana koje pružaju IKT usluge i obrazlažu razlozi za diverzifikaciju dobavljača.

(4) Finansijski subjekt može, u skladu sa zakonom, da povjeri obavljanje poslova provjere usklađenosti sa zahtjevima za upravljanje IKT rizicima subjektima unutar grupe ili drugim subjektima.

(5) U slučaju iz stava 4 ovog člana, finansijski subjekt zadržava odgovornost za usklađenost sa zahtjevima za upravljanje IKT rizicima, kao i za provjeru te usklađenosti.

IKT sistemi, protokoli i alati

Član 13

Finansijski subjekt je dužan da, radi tretiranja i upravljanja IKT rizikom, koristi i održava ažurnim IKT sisteme, protokole i alate koji moraju biti:

1) primjereni za obim operacija koje podržavaju njegovo poslovanje, u skladu sa principom proporcionalnosti iz člana 5 ovog zakona;

2) pouzdani;

3) dovoljnog kapaciteta za tačnu obradu podataka neophodnih za obavljanje aktivnosti i blagovremeno pružanje usluga, kao i kapacitet za obradu u uslovima najvećeg opterećenja u pogledu obima naloga, poruka ili transakcija, u skladu sa potrebama, uključujući i u slučaju uvođenja nove tehnologije;

4) tehnološki otporni kako bi mogli na adekvatan način odgovoriti na dodatne potrebe za obradom informacija koje nastaju usljed poremećaja na tržištu ili u drugim nepovoljnim situacijama.

Identifikacija i procjena IKT rizika, usluga, sistema i imovine

Član 14

(1) Finansijski subjekt je dužan da, u okviru sistema upravljanja IKT rizicima, identifikuje, klasifikuje i adekvatno dokumentuje sve poslovne funkcije podržane IKT-om, zaduženja i odgovornosti, informacionu imovinu i IKT imovinu koja podržava te funkcije, kao i njihove uloge i međuzavisnosti u pogledu IKT rizika.

(2) Finansijski subjekt je dužan da, po potrebi, a najmanje jednom godišnje, preispituje adekvatnost klasifikacije iz stava 1 ovog člana i cjelokupne pripadajuće dokumentacije.

(3) Finansijski subjekt je dužan da kontinuirano:

1) identifikuje sve izvore IKT rizika, a naročito izloženosti riziku prema drugim finansijskim subjektima i od drugih finansijskih subjekata;

2) procjenjuje sajber prijetnje i IKT ranjivosti koje se odnose na njegove poslovne funkcije podržane IKT-om, informacionu imovinu i IKT imovinu.

(4) Finansijski subjekt je dužan da redovno, a najmanje jednom godišnje, razmatra scenarije rizika koji mogu da utiču na funkcije i imovinu iz stava 3 tačka 2 ovog člana.

(5) Finansijski subjekt, koji nije klasifikovan kao mikro finansijski subjekt, dužan je da sprovede procjenu rizika u slučaju svake značajne promjene u:

1) infrastrukturi mrežnih i informacionih sistema;

2) procesima ili procedurama koje utiču na njegove poslovne funkcije podržane IKT-om, informacionu imovinu ili IKT imovinu.

(6) Finansijski subjekt je dužan da identifikuje svu informacionu imovinu i IKT imovinu, uključujući mrežne resurse, hardversku opremu i imovinu na udaljenim lokacijama, i da posebno evidentira informacionu imovinu i IKT imovinu koja se smatra kritičnom.

(7) Finansijski subjekt je dužan da dokumentuje konfiguraciju informacione imovine i IKT imovine i informacije o povezanosti i međuzavisnosti između različite informacione i IKT imovine.

(8) Finansijski subjekt je dužan da identifikuje i dokumentuje sve procese koji zavise od trećih strana koje pružaju IKT usluge, kao i da identifikuje međusobne povezanosti sa trećim stranama koje pružaju IKT usluge kojima se podržavaju kritične ili važne funkcije.

(9) Finansijski subjekat je dužan da, radi postupanja u skladu sa st. 1, 6, 7 i 8 ovog člana, vodi odgovarajuće registre, koje mora da ažurira redovno i u slučaju svake značajne promjene iz stava 5 ovog člana.

(10) Finansijski subjekt, koji nije klasifikovan kao mikro finansijski subjekt, dužan je da redovno, a najmanje jednom godišnje, sprovodi procjenu IKT rizika za sve zastarjele IKT sisteme, kao i vanredno prije i nakon povezivanja tehnologija, aplikacija ili sistema.

Zaštita IKT sistema i sprečavanje IKT incidenata

Član 15

(1) Radi adekvatne zaštite IKT sistema i u cilju organizovanja mjera odgovora, finansijski subjekt dužan je da kontinuirano prati i kontroliše bezbjednost i funkcionisanje IKT sistema i alata, kao i da na najmanju moguću mjeru svede uticaj IKT rizika na IKT sisteme, primjenom odgovarajućih IKT bezbjednosnih alata, politika i procedura.

(2) Finansijski subjekt je dužan da osmisli, kreira i/ili nabavi i primijeni politike, procedure, protokole i alate za IKT bezbjednost u cilju obezbjeđivanja otpornosti, kontinuiteta i dostupnosti IKT sistema, a naročito onih koji podržavaju kritične ili važne funkcije, i u cilju održavanja visokog nivoa dostupnosti, autentičnosti, integriteta i povjerljivosti podataka, bez obzira da li su u stanju mirovanja, upotrebi ili prenosu.

(3) Radi ostvarivanja ciljeva iz stava 2 ovog člana, finansijski subjekt je dužan da koristi IKT rješenja i procese koji su primjereni, u smislu člana 5 ovog zakona i kojima se:

1) omogućava bezbjednost sredstava i metoda za prenos podataka;

2) na najmanju moguću mjeru svodi rizik od oštećenja ili gubitka podataka, neovlašćenog pristupa i tehničkih nedostataka koji mogu narušiti poslovanje;

3) sprečava nedostupnost i gubitak podataka, narušavanje autentičnosti, integriteta i povjerljivosti podataka;

4) obezbjeđuje zaštita podataka od rizika koji proizilaze iz upravljanja podacima, uključujući propuste u administraciji, rizike povezane sa obradom i ljudske greške.

(4) Finansijski subjekt je dužan da, u okviru sistema upravljanja IKT rizicima:

1) razvije i usvoji politiku informacione bezbjednosti kojom se utvrđuju pravila za zaštitu dostupnosti, autentičnosti, integriteta i povjerljivosti podataka, informacione imovine i IKT imovine, uključujući podatke i imovinu njegovih klijenata, kada je to primjenljivo;

2) primjenom pristupa zasnovanog na procjeni rizika, uspostavi pouzdanu strukturu za upravljanje mrežom i infrastrukturom, korišćenjem odgovarajućih tehnika, metoda i protokola;

3) utvrdi i primjenjuje politike kojima se odobrava fizički i logički pristup informacionoj imovini i IKT imovini do nivoa koji je neophodan za obavljanje opravdanih i odobrenih poslova i aktivnosti, i u tu svrhu primjenjuje skup pravila, postupaka i kontrola za adekvatno upravljanje pravima pristupa i kontrolu pristupa;

4) utvrdi i primjenjuje politike i protokole za korišćenje pouzdanih mehanizama provjere autentičnosti, zasnovanih na relevantnim standardima i specijalizovanim sistemima kontrole, kao i mjere za zaštitu kriptografskih ključeva za šifrovanje podataka;

5) utvrdi i primjenjuje politike, procedure i kontrole za upravljanje IKT promjenama, uključujući promjene softverskih i hardverskih komponenti, firmvera, sistema i bezbjednosnih parametara, koje su zasnovane na procjeni rizika i predstavljaju sastavni dio opšteg procesa upravljanja promjenama u finansijskom subjektu, kako bi se obezbijedilo da se sve promjene IKT sistema evidentiraju, testiraju, procjenjuju, odobravaju, sprovode i provjeravaju na kontrolisan način;

6) utvrdi i primjenjuje odgovarajuće i sveobuhvatne politike za primjenu softverskih i hardverskih zakrpa i ažuriranja.

(5) Finansijski subjekt je dužan da strukturu za upravljanje mrežom i infrastrukturom iz stava 4 tačka 2 ovog člana kreira i implementira na način kojim se omogućava brzo ukidanje ili segmentiranje mrežnog pristupa, kako bi se u najvećoj mogućoj mjeri ograničilo i spriječilo širenje zaraze, a naročito u slučaju međusobno povezanih finansijskih procesa.

(6) Struktura za upravljanje mrežom i infrastrukturom iz stava 4 tačka 2 ovog člana može da obuhvati primjenu automatizovanih mehanizama za izolaciju zahvaćene informacione imovine u slučaju sajber napada.

(7) Postupak upravljanja IKT promjenama iz stava 4 tačka 5 ovog člana mora biti odobren od strane odgovarajućih linija i nivoa odlučivanja finansijskog subjekta, i mora da se sprovodi u skladu sa posebno utvrđenim protokolima finansijskog subjekta.

Praćenje, otkrivanje i analiza IKT događaja i incidenata

Član 16

(1) Finansijski subjekt je dužan da uspostavi mehanizme za brzo otkrivanje neuobičajenih aktivnosti, u skladu sa članom 22 ovog zakona, uključujući otkrivanje problema u performansama IKT mreže i IKT incidenata, kao i mehanizme za identifikovanje potencijalnih značajnih jedinstvenih tačaka prekida.

(2) Finansijski subjekt je dužan da obezbijedi redovno testiranje mehanizama iz stava 1 ovog člana na način propisan članom 28 ovog zakona.

(3) Mehanizmi iz stava 1 ovog člana moraju da omoguće kontrolu na više nivoa, utvrde pragove za dobijanje upozorenja i kriterijume za aktiviranje i započinjanje procesa odgovora na IKT incidente, što uključuje i mehanizme za automatsko obavještavanje relevantnih lica zaduženih za odgovor na IKT incidente.

(4) Finansijski subjekt je dužan da obezbijedi dovoljne resurse i kapacitete za praćenje aktivnosti korisnika, otkrivanje neuobičajnih IKT događaja i IKT incidenata, a naročito sajber napada.

(5) Pružalac usluga dostave podataka dužan je da uspostavi sisteme kojima se može efikasno provjeriti da li su izvještaji o trgovanju potpuni i kojima se mogu utvrditi propusti i očigledne greške i zahtijevati ponovni prenos tih izvještaja.

Kontinuitet poslovanja, odgovor na IKT incidente i oporavak nakon njih

Član 17

(1) Finansijski subjekt je dužan da, u okviru sistema upravljanja IKT rizicima, na osnovu rezultata postupanja u skladu sa članom 14 ovog zakona, uspostavi sveobuhvatnu IKT politiku kontinuiteta poslovanja.

(2) IKT politika kontinuiteta poslovanja iz stava 1 ovog člana predstavlja sastavni dio opšte politike kontinuiteta poslovanja finansijskog subjekta, a može se usvojiti u formi zasebnog, namjenskog akta.

(3) Finansijski subjekt je dužan da IKT politiku kontinuiteta poslovanja iz stava 1 ovog člana primjenjuje pomoću odgovarajućih, namjenskih i dokumentovanih mjera, planova, procedura i mehanizama u cilju:

1) obezbjeđivanja kontinuiteta kritičnih ili važnih funkcija finansijskog subjekta;

2) brzog, adekvatnog i efikasnog odgovora na sve IKT incidente i njihovog rješavanja, na način kojim se ograničava šteta i daje prioritet nastavku poslovanja i oporavku;

3) pokretanja, bez odlaganja, namjenskih planova kojima se, za sve vrste IKT incidenata, omogućava sprovođenje njima prilagođenih mjera, procesa i tehnologija za suzbijanje negativnih efekata i sprečavanje nastanka dalje štete, kao i posebno prilagođenih procedura za odgovor i oporavak iz člana 18 ovog zakona;

4) preliminarne procjene uticaja, štete i gubitaka;

5) utvrđivanja mjera za komunikaciju i upravljanje u kriznim situacijama kojima se obezbjeđuje dostavljanje ažurnih informacija svim relevantnim zaposlenima i eksternim zainteresovanim stranama u skladu sa članom 20 ovog zakona, i za izvještavanje nadležnog organa u skladu sa odredbama člana 24 ovog zakona.

(4) Finansijski subjekt je dužan da, u okviru sistema upravljanja IKT rizicima, utvrdi i primjenjuje odgovarajuće planove za odgovor i oporavak u IKT oblasti.

(5) Finansijski subjekt, koji nije klasifikovan kao mikro finansijski subjekt, dužan je da obezbijedi nezavisnu internu reviziju planova iz stava 4 ovog člana.

(6) Finansijski subjekt dužan je da uspostavi, održava i periodično testira odgovarajuće IKT planove kontinuiteta poslovanja, naročito za kritične ili važne funkcije koje, na osnovu zaključenih ugovora, obavljaju ili isporučuju treće strane koje pružaju IKT usluge.

(7) Finansijski subjekt je dužan da, u okviru opšte politike kontinuiteta poslovanja, sprovodi analizu uticaja na poslovanje odnosno analizu svoje izloženosti ozbiljnim poremećajima u poslovanju.

(8) Finansijski subjekt je dužan da, u okviru analize uticaja na poslovanje iz stava 7 ovog člana, na osnovu kvalitativnih i kvantitativnih kriterijuma, korišćenjem raspoloživih internih i eksternih podataka i analize scenarija, procijeni potencijalni uticaj ozbiljnih poremećaja u poslovanju.

(9) Finansijski subjekt je dužan da prilikom vršenja analize uticaja na poslovanje iz stava 7 ovog člana uzme u obzir kritičnost identifikovanih poslovnih funkcija, pomoćnih procesa, informacione imovine, zavisnosti od trećih strana, kao i njihovu povezanost i međuzavisnost.

(10) Finansijski subjekt je dužan da osmisli i koristi IKT imovinu i IKT usluge na način koji je u potpunosti usklađen sa rezultatima analize uticaja na poslovanje iz stava 7 ovog člana, naročito u pogledu obezbjeđivanja adekvatne redundanse svih kritičnih komponenti.

(11) Redundansa, u smislu stava 10 ovog člana, označava postojanje jedne ili više dodatnih komponenti koje preuzimaju funkciju primarne komponente u slučaju njenog prekida rada.

(12) U okviru sveobuhvatnog upravljanja IKT rizicima, finansijski subjekt dužan je da:

1) za IKT sisteme koji podržavaju funkcije finansijskog subjekta, testira planove za odgovor i oporavak u IKT oblasti iz stava 4 ovog člana i IKT planove kontinuiteta poslovanja iz stava 6 ovog člana:

- najmanje jednom godišnje; i

- u slučaju značajnih promjena IKT sistema koji podržavaju kritične ili važne funkcije finansijskog subjekta.

2) testira planove komunikacije u kriznim situacijama iz člana 20 ovog zakona.

(13) Finansijski subjekt, koji nije klasifikovan kao mikro finansijski subjekt, dužan je da testiranjem iz stava 12 tačka 1 ovog člana obuhvati scenarije sajber napada i scenarije prelazaka između primarne IKT infrastrukture i rezervnih kapaciteta, rezervnih kopija podataka, rezervnih sistema i rezervnih lokacija, neophodnih za ispunjavanje zahtjeva iz člana 18 ovog zakona.

(14) Finansijski subjekt je dužan da redovno preispituje IKT politiku kontinuiteta poslovanja iz stava 1 ovog člana i planove za odgovor i oporavak u IKT oblasti iz stava 4 ovog člana, uzimajući u obzir rezultate testiranja iz stava 12 ovog člana, preporuke revizije i zahtjeve nadležnog organa.

(15) Finansijski subjekt, koji nije klasifikovan kao mikro finansijski subjekt, dužan je da odredi odgovorno lice ili organizacionu jedinicu za upravljanje kriznim situacijama koja je, u slučaju pokretanja planova za odgovor i oporavak u IKT oblasti iz stava 4 ovog člana ili IKT planova kontinuiteta poslovanja iz stava 6 ovog člana, naročito dužna da utvrdi jasne procedure za upravljanje internom i eksternom komunikacijom u skladu sa članom 20 ovog zakona.

(16) U slučaju pokretanja IKT planova za odgovor i oporavak u IKT oblasti iz stava 4 ovog člana ili IKT planova kontinuiteta poslovanja iz stava 6 ovog člana, finansijski subjekt je dužan da vodi evidenciju aktivnosti prije i nakon poremećaja u radu, koja mora biti lako dostupna.

(17) Finansijski subjekt, koji nije klasifikovan kao mikro finansijski subjekt, dužan je da nadležnom organu, na njegov zahtjev, dostavi procjenu ukupnih godišnjih troškova i gubitaka koje su prouzrokovali značajni IKT incidenti.

(18) Centralno klirinško depozitarno društvo dužno je da dostavlja Komisiji kopije rezultata testova kontinuiteta poslovanja u području IKT-a ili sličnih vježbi.

Politike i procedure za izradu rezervnih kopija podataka i procedure i metode za ponovno uspostavljanje i oporavak

Član 18

(1) Kako bi se omogućilo ponovno uspostavljanje IKT sistema i povratak podataka uz minimalno trajanje prekida i ograničili poremećaji u radu i gubici, finansijski subjekt dužan je da, u okviru sistema upravljanja IKT rizicima, razvije i usvoji:

1) politike i procedure kojima se, na osnovu kritičnosti informacija i povjerljivosti podataka, utvrđuju obim i minimalna učestalost izrade rezervnih kopija podataka;

2) procedure i metode za povratak, ponovno uspostavljanje i oporavak.

(2) Finansijski subjekt je dužan da obezbijedi sisteme za izradu rezervnih kopija podataka koji se mogu koristiti u skladu sa politikama i procedurama za izradu rezervnih kopija podataka iz stava 1 tačka 1 ovog člana, kao i u skladu sa procedurama i metodama za povratak, ponovno uspostavljanje i oporavak iz stava 1 tačka 2 ovog člana.

(3) Korišćenjem sistema za izradu rezervnih kopija podataka iz stava 2 ovog člana ne smije se ugroziti bezbjednost mrežnih i informacionih sistema ni dostupnost, autentičnost, integritet ili povjerljivost podataka.

(4) Finansijski subjekt je dužan da periodično testira procedure za izradu rezervnih kopija podataka iz stava 1 tačka 1 ovog člana, kao i procedure i metode za povratak, ponovno uspostavljanje i oporavak iz stava 1 tačka 2 ovog člana.

(5) Kada finansijski subjekt koristi sopstvene sisteme za povraćaj podataka iz rezervnih kopija, dužan je da obezbijedi da se za te potrebe koriste IKT sistemi koji su fizički i logički odvojeni od izvornih IKT sistema iz kojih podaci potiču.

(6) IKT sistemi iz stava 5 ovog člana koji su namijenjeni za oporavak, moraju biti bezbjedno zaštićeni od neovlašćenog pristupa i IKT kompromitacija i omogućiti blagovremeno ponovno uspostavljanje usluga, pri čemu se, po potrebi, koriste rezervne kopije podataka i sistema.

(7) Finansijski subjekt, koji nije klasifikovan kao mikro finansijski subjekt, dužan je da održava rezervne IKT kapacitete koji imaju resurse, sposobnosti i funkcije dovoljne za adekvatno obezbjeđivanje potreba poslovnih procesa.

(8) Finansijski subjekt koji je klasifikovan kao mikro finansijski subjekt dužan je da, u skladu sa svojim rizičnim profilom, procijeni potrebu održavanja rezervnih IKT kapaciteta iz stava 7 ovog člana.

(9) Finansijski subjekat je dužan da, prilikom određivanja ciljnog vremena oporavka i ciljne tačke oporavka za svaku funkciju, uzme u obzir značaj te funkcije, a naročito da li se radi o kritičnoj ili važnoj funkciji, kao i potencijalni ukupni uticaj ciljeva oporavka na efikasnost tržišta.

(10) Ciljno vrijeme oporavka i ciljna tačka oporavka iz stava 9 ovog člana moraju biti takvi da, u ekstremnim scenarijima, obezbjeđuju ispunjavanje dogovorenih nivoa usluga.

(11) Prilikom oporavka od IKT incidenta, finansijski subjekt je dužan da sprovede sve neophodne kontrole, uključujući višestruke provjere i usklađivanja, kako bi obezbijedio održavanje najvišeg nivoa integriteta podataka.

(12) Kontrole iz stava 11 ovog člana moraju se sprovoditi i prilikom rekonstrukcije podataka iz eksternih izvora, radi obezbjeđivanja usklađenosti svih podataka između sistema.

(13) Centralna druga ugovorena strana dužna je da uspostavi planove koji moraju omogućiti oporavak svih transakcija koje su bile u toku u trenutku nastanka poremećaja, kako bi se obezbijedio nesmetan i siguran nastavak poslovanja centralne druge ugovorne strane i omogućilo izvršenje obaveze na predviđeni datum.

(14) Pružalac usluga dostave podataka dužan je da obezbijedi odgovarajuće resurse i infrastrukturu za izradu rezervnih kopija i obnovu sistema, radi kontinuiranog pružanja i održavanja svojih usluga.

(15) Centralno klirinško depozitarno društvo dužno je održavati najmanje jedno sekundarno mjesto obrade, opremljeno odgovarajućim resursima, sposobnostima, funkcijama i osobljem, kako bi se zadovoljile poslovne potrebe.

(16) Sekundarno mjesto obrade iz stava 15 ovog člana:

1) mora biti geografski udaljeno od primarnog mjesta obrade kako bi se osigurao različit profil rizika i spriječilo da bude pogođeno istim događajem koji je zahvatio primarno mjesto;

2) mora omogućavati kontinuitet kritičnih ili važnih funkcija na način identičan primarnom mjestu ili pružati nivo usluga potreban za izvršenje ključnih operacija finansijskog subjekta u skladu sa ciljevima oporavka;

3) mora biti odmah dostupno osoblju finansijskog subjekta kako bi se osigurao kontinuitet kritičnih ili važnih funkcija u slučaju nedostupnosti primarnog mjesta obrade.

Usavršavanje u cilju jačanja digitalne operativne otpornosti

Član 19

(1) Finansijski subjekt je dužan da obezbijedi kapacitete i odredi lica zadužena za prikupljanje informacija o ranjivostima, sajber prijetnjama, IKT incidentima, a naročito o sajber napadima, kao i za analizu njihovog mogućeg uticaja na digitalnu operativnu otpornost finansijskog subjekta.

(2) Finansijski subjekt je dužan da uspostavi proces naknadne analize IKT incidenata, koji se sprovodi nakon što značajan IKT incident poremeti obavljanje njegovih osnovnih aktivnosti, u cilju analize uzroka poremećaja i utvrđivanja potrebnih poboljšanja u IKT operacijama ili u IKT politici kontinuiteta poslovanja iz člana 17 stav 1 ovog zakona.

(3) Finansijski subjekt, koji nije klasifikovan kao mikro finansijski subjekt, dužan je da nadležnom organu, na njegov zahtjev, dostavi informacije o izmjenama koje su sprovedene nakon analize IKT incidenta iz stava 2 ovog člana.

(4) Naknadnom analizom IKT incidenta iz stava 2 ovog člana mora se utvrditi da li su uspostavljene procedure bile ispoštovane i da li su preduzete mjere bile djelotvorne, uključujući:

1) brzinu reagovanja na bezbjednosna upozorenja i utvrđivanja uticaja IKT incidenta i njegove ozbiljnosti;

2) kvalitet i brzinu sprovođenja forenzičke analize, u slučajevima kada je to svrsishodno;

3) efikasnost interne eskalacije incidenta;

4) efikasnost interne i eksterne komunikacije.

(5) Finansijski subjekt je dužan da obezbijedi da se iskustva stečena kroz testiranje digitalne operativne otpornosti iz čl. 27 do 32 ovog zakona, kao i iz nastalih IKT incidenata, a naročito sajber napada, saznanja o izazovima koji su se pojavili prilikom pokretanja planova za odgovor i oporavak u IKT oblasti iz člana 17 stav 4 ovog zakona i IKT planova kontinuiteta poslovanja iz člana 17 stav 6 ovog zakona, relevantne informacije dobijene od drugih subjekata, kao i informacije u vezi sa zahtjevima nadležnog organa, blagovremeno, adekvatno i kontinuirano koriste u okviru procesa procjene IKT rizika.

(6) Finansijski subjekt je dužan da iskustva, saznanja i informacije iz stava 5 ovog člana, na odgovarajući način, uzme u obzir prilikom preispitivanja relevantnih komponenti sistema upravljanja IKT rizicima.

(7) Finansijski subjekt je dužan da prati efikasnost sprovođenja strategije digitalne operativne otpornosti iz člana 12 stav 1 ovog zakona.

(8) Finansijski subjekt je dužan da evidentira i prati promjenu ukupnog profila IKT rizika tokom vremena, analizira učestalost, vrste, razmjere i trendove IKT incidenata, a naročito sajber napada i njihovih obrazaca, kako bi razumio nivo svoje izloženosti IKT riziku, posebno u odnosu na kritične ili važne funkcije i unaprijedio stepen svoje zrelosti i spremnosti u oblasti sajber bezbjednosti.

(9) Finansijski subjekt je dužan da obezbijedi da viši IKT kadar, najmanje jednom godišnje, podnosi izvještaj organu upravljanja o zaključcima izvedenim iz iskustava, saznanja i informacija iz stava 5 ovog člana, sa predlozima za dalje postupanje.

(10) Finansijski subjekt je dužan da osmisli i sprovodi programe za podizanje svijesti o IKT bezbjednosti i obuke o digitalnoj operativnoj otpornosti, kao obavezne djelove svojih programa obuke zaposlenih.

(11) Programi i obuke iz stava 10 ovog člana primjenjuju se na sve zaposlene i članove višeg rukovodstva, a nivo njihove složenosti mora biti prilagođen nadležnostima i poslovima koje ta lica obavljaju.

(12) Finansijski subjekt je dužan da, kada je to primjenljivo, uključi treće strane koje pružaju IKT usluge u odgovarajuće programe obuke, u skladu sa članom 38 stav 3 tačka 11 ovog zakona.

(13) Finansijski subjekt, koji nije klasifikovan kao mikro finansijski subjekt, dužan je da kontinuirano prati trendove u razvoju tehnologija, kako bi bolje razumio mogući uticaj primjene novih tehnologija na zahtjeve u oblasti IKT bezbjednosti i digitalnu operativnu otpornost.

(14) Finansijski subjekt, koji nije klasifikovan kao mikro finansijski subjekt, dužan je da bude upoznat sa najnovijim metodama za upravljanje IKT rizicima, kako bi mogao efikasno da odgovori na postojeće i nove oblike sajber napada.

Komunikacija u kriznim situacijama

Član 20

(1) Finansijski subjekt je dužan da, u okviru sistema upravljanja IKT rizicima, utvrdi planove komunikacije u kriznim situacijama, koji omogućavaju da na odgovoran način saopštava informacije, najmanje o značajnim IKT incidentima i značajnim ranjivostima, klijentima, poslovnim partnerima i široj javnosti, u zavisnosti od slučaja.

(2) Finansijski subjekt je dužan da, u okviru sistema upravljanja IKT rizicima, utvrdi i primjenjuje politike komunikacije za zaposlene i sa eksternim zainteresovanim stranama.

(3) Politike komunikacije iz stava 2 ovog člana, u dijelu koji se odnosi na zaposlene, moraju uzeti u obzir da se mora praviti razlika između zaposlenih koje je potrebno samo informisati i zaposlenih koji učestvuju u upravljanju IKT rizicima, odnosno koji su zaduženi za odgovor i oporavak.

(4) Najmanje jedno lice u finansijskom subjektu mora biti zaduženo za sprovođenje strategije komunikacije u slučaju IKT incidenata i da, u tu svrhu, obavlja poslove informisanja medija i javnosti.

Pojednostavljeni sistem upravljanja IKT rizicima

Član 21

(1) Odredbe čl. 8 do 19 ovog zakona ne primjenjuju se na malo i nepovezano investiciono društvo i malu instituciju za profesionalnu penzionu štednju.

(2) Finansijski subjekti iz stava 1 ovoga člana dužni su da:

1) uspostave i održavaju pouzdan i dokumentovan sistem upravljanja IKT rizikom, koji detaljno opisuje mehanizme i mjere usmjerene na brzo, efikasno i sveobuhvatno upravljanje IKT rizikom, uključujući i zaštitu relevantnih fizičkih komponenti i infrastrukture;

2) kontinuirano prate bezbjednost i funkcionisanje svih IKT sistema;

3) minimiziraju uticaj IKT rizika korišćenjem pouzdanih, otpornih i ažurnih IKT sistema, protokola i alata koji su primjereni za podršku obavljanju njihovih aktivnosti i pružanju usluga, kao i za adekvatnu zaštitu dostupnosti, autentičnosti, integriteta i povjerljivosti podataka u mrežnim i informacionim sistemima;

4) omoguće pravovremeno identifikovanje izvora IKT rizika i anomalija u mrežnim i informacionim sistemima, kao i brzo postupanje u slučaju IKT incidenata;

5) identifikuju ključne zavisnosti od trećih strana koje pružaju IKT usluge;

6) obezbijede kontinuitet kritičnih ili važnih funkcija pomoću planova kontinuiteta poslovanja i mjera odgovora i oporavka, koje uključuju najmanje mjere izrade rezervnih kopija podataka i povraćaja podataka iz rezervnih kopija;

7) redovno testiraju efikasnost kontrola koje se sprovode u skladu sa tač. 1 i 3, kao i planove i mjere iz tačke 6 ovog stava;

8) u skladu sa potrebama i profilom IKT rizika, koriste relevantne operativne zaključke koji proizlaze iz testiranja iz tačke 7 ovog stava i analiza nakon incidenata u procesu procjene IKT rizika, kao i da razvijaju programe za podizanje svijesti o IKT bezbjednosti i obuke iz oblasti digitalne operativne otpornosti za zaposlene i rukovodstvo.

III. UPRAVLJANJE, KLASIFIKACIJA I IZVJEŠTAVANJE O IKT INCIDENTIMA

Proces upravljanja IKT incidentima

Član 22

(1) Finansijski subjekt je dužan da definiše, uspostavi i primijeni proces upravljanja IKT incidentima radi otkrivanja, upravljanja i obavještavanja o IKT incidentima.

(2) Finansijski subjekt je dužan da evidentira sve IKT incidente i ozbiljne sajber prijetnje.

(3) Finansijski subjekt je dužan da uspostavi adekvatne procedure i postupke kojima se obezbjeđuje da se, na dosljedan i objedinjen način postupa sa IKT incidentima, vrši njihovo praćenje i preduzimaju dalje mjere, kako bi se obezbijedilo da se osnovni uzroci IKT incidenata identifikuju, dokumentuju i tretiraju, radi sprečavanja ponavljanja takvih incidenata.

(4) Finansijski subjekt je dužan da, u okviru procesa upravljanja IKT incidentima iz stava 1 ovog člana:

1) uspostavi indikatore ranog upozorenja;

2) uspostavi procedure za identifikaciju, praćenje, evidentiranje, kategorizaciju i klasifikaciju IKT incidenata prema njihovom prioritetu i nivou ozbiljnosti, u skladu sa kriterijumima iz člana 23 stav 1 ovog zakona, uzimajući u obzir kritičnost usluga zahvaćenih incidentom;

3) dodijeli zaduženja i odgovornosti za postupanje u slučaju različitih IKT incidenata, prema njihovim vrstama i scenarijima;

4) utvrdi planove za komunikaciju sa zaposlenima, eksternim zainteresovanim stranama i medijima u skladu sa članom 20 ovog zakona, planove za obavještavanje klijenata, za postupke interne eskalacije incidenata, uključujući prigovore klijenata povezane sa IKT-om, kao i za informisanje drugih finansijskih subjekata sa kojima ima poslovnu saradnju, kada je to primjenljivo;

5) obezbijedi da se više rukovodstvo i organ upravljanja izvještavaju najmanje o značajnim IKT incidentima, uz obrazloženje njihovog uticaja, odgovora na njih i dodatnih kontrola koje je potrebno uspostaviti zbog nastanka takvih IKT incidenata;

6) uspostavi procedure za odgovor na IKT incidente, kako bi ublažio njihov uticaj i obezbijedio da usluge zahvaćene incidentom ponovo, blagovremeno postanu dostupne, funkcionalne i bezbjedne.

Klasifikacija IKT incidenata i sajber prijetnji

Član 23

(1) Finansijski subjekt je dužan da klasifikuje IKT incidente i da utvrdi njihov uticaj na osnovu sljedećih kriterijuma:

1) broja i/ili značaja klijenata zahvaćenih IKT incidentom, ili broja i/ili značaja finansijskih subjekata i institucija koje su druga ugovorna strana zahvaćena incidentom i, kada je to primjenljivo, vrijednosti ili broja transakcija zahvaćenih incidentom, kao i činjenice da li je incident narušio ugled finansijskog subjekta;

2) trajanja IKT incidenta, uključujući period prekida pružanja usluge;

3) geografske rasprostranjenosti u smislu područja koje je IKT incident zahvatio, naročito ako je zahvatio više od dvije države članice;

4) gubitka svojstva podataka usljed IKT incidenta, odnosno gubitka dostupnosti, autentičnosti, integriteta ili povjerljivosti podataka;

5) kritičnosti usluga zahvaćenih incidentom, uključujući u pogledu transakcija i operacija finansijskog subjekta;

6) ekonomskog uticaja IKT incidenta, odnosno direktnih i indirektnih troškova i gubitaka, u apsolutnom i relativnom smislu.

(2) Finansijski subjekt je dužan da klasifikuje sajber prijetnje kao ozbiljne na osnovu kritičnosti usluga koje su izložene riziku, uključujući u pogledu transakcija i operacija finansijskog subjekta, broja i/ili značaja klijenata izloženih tom riziku ili broja i/ili značaja finansijskih subjekata i institucija koje su druga ugovorna strana izložena tom riziku i geografske rasprostranjenosti u smislu područja izloženih riziku.

Izvještavanje o značajnim IKT incidentima i obavještavanje o ozbiljnim sajber prijetnjama

Član 24

(1) Finansijski subjekt je dužan da o značajnom IKT incidentu izvještava nadležni organ.

(2) Radi izvještavanja iz stava 1 ovog člana, finansijski subjekt je dužan da prikupi i analizira sve relevantne informacije o značajnom IKT incidentu, pripremi dokumentaciju iz stava 3 ovog člana i dostavi je nadležnom organu na način i u roku utvrđenom posebnim propisom nadležnog organa.

(3) Finansijski subjekt je dužan da nadležnom organu dostavi:

1) početno obavještenje;

2) prelazni izvještaj nakon početnog obavještenja iz tačke 1 ovog stava, čim dođe do značajne promjene u statusu prijavljenog značajnog IKT incidenta ili promjene u postupanju sa tim incidentom u skladu sa novim dostupnim informacijama, a nakon toga, po potrebi, ažurirane prelazne izvještaje u slučaju bitne promjene statusa incidenta, kao i na izričit zahtjev nadležnog organa;

3) završni izvještaj, nakon što izvrši analizu osnovnog uzroka incidenta, bez obzira na to da li su mjere za ublažavanje njegovog uticaja već sprovedene, i kada su dostupni konačni podaci o uticaju incidenta, a kojima se mogu zamijeniti prethodne procjene.

(4) Dokumentacija iz stava 3 ovog člana mora sadržati sve informacije koje su nadležnom organu potrebne da utvrdi ozbiljnost značajnog IKT incidenta i procijeni mogućnost prekograničnog uticaja tog incidenta.

(5) Izuzetno od stava 2 ovog člana, u slučaju da finansijski subjekt zbog tehničkih poteškoća nije u mogućnosti da dostavi početno obavještenje iz stava 3 ovog člana na način utvrđen posebnim propisom nadležnog organa, dostavljanje se može izvršiti na drugi pogodan način.

(6) Finansijski subjekt može da obavijesti nadležni organ o ozbiljnoj sajber prijetnji kada procijeni da je prijetnja relevantna za finansijski sistem, korisnike usluga ili klijente.

(7) Nadležni organ može da dostavi informacije o ozbiljnoj sajber prijetnji iz stava 6 ovog člana organima iz stava 11 ovog člana.

(8) Kada nastane značajan IKT incident koji utiče na finansijske interese klijenata, finansijski subjekt dužan je da, bez odlaganja, odmah po saznanju za takav incident, obavijesti klijente o tom incidentu i o mjerama preduzetim za ublažavanje negativnih uticaja tog incidenta.

(9) U slučaju ozbiljne sajber prijetnje, finansijski subjekt je dužan da, kada je to primjenljivo, obavijesti klijente na koje bi ta prijetnja mogla da utiiče o mjerama zaštite koje mogu da preduzmu.

(10) Finansijski subjekt može, u skladu sa zakonom, da povjeri trećoj strani obavljanje poslova obavještavanja u skladu sa ovim članom, pri čemu je taj finansijski subjekt odgovoran za usklađenost sa odredbama ovog člana.

(11) Po prijemu početnog obavještenja i svakog izvještaja iz stava 3 ovog člana, nadležni organ blagovremeno dostavlja podatke o značajnom IKT incidentu, kada je to primjenljivo, a u skladu sa njihovim nadležnostima:

1) EBA-i, ESMA-i ili EIOPA-i;

2) ECB-u, u slučaju finansijskih subjekata iz člana 2 stav 1 tač. 1, 2 i 4 ovog zakona;

3) organu koji je, u skladu sa zakonom kojim se uređuje informaciona bezbjednost, nadležan za zaštitu finansijskog subjekta od sajber prijetnji i incidenata;

4) organu koji je, u skladu sa zakonom kojim se uređuje sanacija kreditnih institucija, nadležan za sanaciju tog finansijskog subjekta, ako se ti podaci odnose na incident koji predstavlja rizik za obavljanje kritičnih funkcija u smislu tog zakona;

5) organu koji je, u skladu sa zakonom kojim se uređuje sanacija investicionih društava, nadležan za sanaciju tog finansijskog subjekta, ako se ti podaci odnose na incident koji predstavlja rizik za obavljanje ključnih funkcija u smislu tog zakona;

6) drugom javnom organu, u skladu sa zakonom.

(12) Nadležni organ je dužan da sarađuje sa EBA-om, ESMA-om, EIOPA-om i/ili ECB-om u postupku iz člana 19 stav 7 Regulative (EU) br. 2022/2554, koji ti organi sprovode radi procjene relevantnosti značajnog IKT incidenta za nadležne organe u drugim državama članicama, u skladu sa kriterijumima iz člana 11 Regulative (EU) br. 2024/1772.

(13) U slučaju da, u skladu sa članom 19 stav 7 Regulative (EU) br. 2022/2554, putem ESCB-a primi obavještenje od ECB-a o pitanjima koja su od značaja za platni sistem, Centralna banka za finansijski subjekt iz člana 2 stav 1 tač. 1, 2 i 4 ovog zakona, kada je to primjenljivo, preduzima sve neophodne mjere za zaštitu stabilnosti finansijskog sistema.

(14) Komisija obavještava relevantni nadležni organ države članice domaćina o značajnom IKT incidentu u slučaju kada Centralno klirinško depozitarno društvo ima značajnu prekograničnu aktivnost u toj državi članici domaćina, kada je vjerovatno da će značajni IKT incident imati ozbiljne posljedice po finansijska tržišta države članice domaćina, kao i u situacijama u kojima postoje aranžmani o saradnji među nadležnim organima u vezi sa nadzorom finansijskih subjekata.

Povratne informacije nadležnog organa

Član 25

(1) Nadležni organ je dužan da po prijemu dokumentacije iz člana 24 stav 3 ovog zakona, finansijskom subjektu potvrdi prijem.

(2) Po prijemu početnog obavještenja i svakog izvještaja iz člana 24 stav 3 ovog zakona, nadležni organ može, kada je to moguće, finansijskom subjektu blagovremeno pružiti relevantne i srazmjerne informacije ili opšte smjernice za dalje postupanje, naročito davanjem na uvid svih relevantnih anonimizovanih informacija i saznanja o sličnim prijetnjama, kao i da sa tim finansijskim subjektom razmotri primijenjene korektivne mjere, načine za ublažavanje i umanjenje negativnih uticaja značajnog IKT incidenta na finansijski sektor u cjelini.

(3) Aktivnostima nadležnog organa iz stava 2 ovog člana ne dovode se u pitanje tehnički doprinosi, smjernice, korektivne mjere i dalja postupanja koja, u skladu sa zakonom kojim se uređuje informaciona bezbjednost, pružaju i sprovode organi određeni tim zakonom.

(4) U slučaju iz stava 2 ovog člana, finansijski subjekt je u potpunosti odgovoran za postupanje sa značajnim IKT incidentom i za njegove posljedice.

Operativni i sigurnosni incidenti povezani sa plaćanjem

Član 26

Finansijski subjekti iz člana 2 stav 1 tač. 1 do 4 ovog zakona, dužni su da u slučaju operativnih i sigurnosnih incidenata povezanih sa plaćanjem, uključujući i značajne operativne i sigurnosne incidente povezane sa plaćanjem, shodno primjenjuju odredbe čl. 22 do 25 ovog zakona.

IV. TESTIRANJE DIGITALNE OPERATIVNE OTPORNOSTI

Opšti zahtjevi za sprovođenje testiranja digitalne operativne otpornosti

Član 27

(1) Finansijski subjekt, koji nije klasifikovan kao mikro finansijski subjekt, dužan je, u skladu sa principom proporcionalnosti iz člana 5 ovog zakona, a u cilju procjene spremnosti za upravljanje IKT incidentima, identifikovanja slabosti, nedostataka i odstupanja u digitalnoj operativnoj otpornosti i blagovremenog sprovođenja korektivnih mjera, da uspostavi, održava i redovno preispituje program za testiranje digitalne operativne otpornosti.

(2) Program za testiranje digitalne operativne otpornosti iz stava 1 ovog člana, kao dio okvira za upravljanje IKT rizicima, mora biti efikasan i sveobuhvatan i sadržati niz procjena, testova, metodologija, praksi i alata koji se sprovode i primjenjuju u skladu sa čl. 28 do 31 ovog zakona.

(3) Finansijski subjekt iz stava 1 ovog člana, dužan je da sprovodi program za testiranje digitalne operativne otpornosti primjenom pristupa zasnovanog na procjeni rizika, pri čemu mora voditi računa o promjenljivom karakteru IKT rizika, konkretnim rizicima kojima je izložen ili bi mogao biti izložen, kritičnosti informacione imovine i usluga, kao i o svim drugim relevantnim faktorima.

(4) Finansijski subjekt je dužan da obezbijedi da testiranje digitalne operativne otpornosti iz stava 1 ovog člana sprovode nezavisna interna ili eksterna lica.

(5) U slučaju kada testiranje digitalne operativne otpornosti iz stava 1 ovog člana sprovode interna lica, finansijski subjekt je dužan da za te potrebe obezbijedi dovoljne resurse i preduzme mjere za izbjegavanje sukoba interesa u fazi osmišljavanja i sprovođenja tog testiranja.

(6) Finansijski subjekt iz stava 1 ovog člana, dužan je da uspostavi politike i procedure za određivanje prioriteta, klasifikacije i otklanjanje svih problema otkrivenih tokom testiranja digitalne operativne otpornosti, kao i metodologije za internu provjeru radi dobijanja potvrde da su sve identifikovane slabosti, nedostaci i odstupanja u potpunosti otklonjeni.

(7) Finansijski subjekt iz stava 1 ovog člana, dužan je da najmanje jednom godišnje, sprovodi adekvatne testove svih IKT sistema i aplikacija koje podržavaju kritične ili važne funkcije tog finansijskog subjekta.

Testiranje IKT alata i sistema

Član 28

(1) Programom za testiranje digitalne operativne otpornosti iz člana 27 stav 1 ovog zakona mora se, u skladu sa principom proporcionalnosti iz člana 5 ovog zakona, obezbijediti sprovođenje odgovarajućih testova, kao što su:

1) procjene i skeniranja ranjivosti;
2) analize javno dostupnih izvora;
3) procjene bezbjednosti mreže;
4) analize odstupanja;
5) preispitivanja fizičke bezbjednosti;
6) upitnici i softverska rješenja za skeniranje;
7) pregledi izvornog koda, kada je to izvodljivo;
8) testiranja zasnovana na scenarijima;
9) testiranja kompatibilnosti;
10) testiranja performansi;
11) testiranja od kraja do kraja (eng. end-to-end), odnosno kroz sve faze rada;

12) penetraciona testiranja.

(2) Finansijski subjekt koji je klasifikovan kao mikro finansijski subjekt, dužan je da testiranja iz stava 1 ovog člana sprovodi primjenom pristupa zasnovanog na procjeni rizika u skladu sa strateškim planiranjem testiranja u IKT oblasti, uzimajući u obzir potrebu za održavanje uravnoteženog pristupa između obima resursa i vremena potrebnog za sprovođenje testiranja u IKT oblasti, sa jedne strane, i hitnosti, vrste rizika, kritičnosti informacione imovine i usluga, kao i drugih relevantnih faktora, uključujući sposobnost tog finansijskog subjekta da preuzme proračunate rizike, sa druge strane.

(3) Centralno klirinško depozitarno društvo i Centralna druga ugovorna strana, dužni su da sprovode procjene ranjivosti prije svake primjene ili ponovne primjene novih ili postojećih aplikacija, infrastrukturnih komponenti i IKT usluga koje podržavaju kritične ili važne funkcije finansijskog subjekta.

Napredno testiranje IKT alata, sistema i procesa zasnovano na TLPT-u

Član 29

(1) Finansijski subjekt iz stava 4 ovog člana, dužan je da sprovodi napredno testiranje u formi penetracionog testiranja vođenog prijetnjama (u daljem tekstu: TLPT), najmanje jednom u tri godine.

(2) Izuzetno od stava 1 ovog člana, nadležni organ može, uzimajući u obzir rizični profil finansijskog subjekta i operativne okolnosti, da finansijskom subjektu utvrdi obavezu promijene učestalosti naprednog testiranja.

(3) TLPT iz stava 1 ovog člana mora obuhvatiti više kritičnih ili važnih funkcija finansijskog subjekta ili sve takve funkcije, i sprovodi se na produkcionim sistemima koji podržavaju te funkcije.

(4) Nadležni organ određuje finansijske subjekte, koji nisu klasifikovani kao mikro finansijski subjekti i nisu subjekti iz člana 21 stav 1 ovog zakona, koji su dužni da sprovode TLPT iz stava 1 ovog člana, uzimajući u obzir princip proporcionalnosti iz člana 5 ovog zakona, na osnovu procjene:

1) uticaja aktivnosti i usluga finansijskog subjekta na finansijski sektor;

2) mogućih rizika po finansijsku stabilnost, uzimajući u obzir sistemski značaj finansijskog subjekta na:

- nacionalnom nivou;

- nivou Evropske unije, kada je to primjenljivo.

3) profila IKT rizika finansijskog subjekta, nivoa njegove zrelosti u IKT oblasti i karakteristika tehnologije koju koristi.

(5) Nadležni organ može izvršavanje pojedinih ili svih zadataka u vezi sa sprovođenjem TLPT-a, iz ovog člana i čl. 30 do 32 ovog zakona, da povjeri drugom nadležnom organu, osim određivanja finansijskih subjekata koji su dužni da sprovode TLPT.

(6) Za potrebe planiranja i sprovođenja TLPT-a iz stava 1 ovog člana, finansijski subjekt je dužan da:

1) utvrdi sve relevantne IKT sisteme, procese i tehnologije kojima se podržavaju IKT usluge i kritične ili važne funkcije, uključujući i one kojima se podržavaju kritične ili važne funkcije koje obavljaju ili isporučuju treće strane koje pružaju IKT usluge;

2) procijeni koje kritične ili važne funkcije treba da budu obuhvaćene TLPT-om; i

3) u skladu sa procjenom iz tačke 2 ovog stava, precizno definiše planirani obim TLPT-a, kao i da rezultate procjene dostavi nadležnom organu.

(7) Nadležni organ prati sve faze pripreme i sprovođenja TLPT-a i odobrava njegove ključne elemente, uključujući i planirani obim TLPT-a iz stava 6 tačka 3 ovog člana, ukoliko procijeni da su ispunjeni uslovi za sprovođenje adekvatnog i efikasnog testiranja.

Učešće treće strane koja pruža IKT usluge u TLPT-u

Član 30

(1) U slučaju kada je treća strana koja pruža IKT usluge obuhvaćena TLPT-om, finansijski subjekt je dužan da preduzme neophodne mjere i zaštitne mehanizme u skladu sa kojima se obezbjeđuje učešće tih trećih strana u TLPT-u, pri čemu ostaje odgovoran za usklađenost sa ovim zakonom.

(2) Ako se opravdano može očekivati da će učešće treće strane koja pruža IKT usluge u TLPT-u, u skladu sa stavom 1 ovog člana, negativno uticati na kvalitet ili bezbjednost usluga koje ta treća strana pruža klijentima koji nisu finansijski subjekti iz člana 2 ovog zakona, ili na povjerljivost podataka povezanih sa tim uslugama, finansijski subjekt može sa tom trećom stranom zaključiti sporazum kojim se toj trećoj strani omogućava da direktno zaključi ugovor sa eksternim licem koje vrši testiranje, radi sprovođenja objedinjenog TLPT-a kojim je obuhvaćeno više

finansijskih subjekata kojima ta treća strana pruža IKT usluge (u daljem tekstu: objadinjeni TLPT), pod koordinacijom jednog odabranog finansijskog subjekta.

(3) Objedinjeni TLPT mora obuhvatiti relevantan opseg IKT usluga kojima se podržavaju kritične ili važne funkcije koje su finansijski subjekti ugovorili sa trećom stranom koja pruža IKT usluge.

(4) Ne dovodeći u pitanje zahtjeve iz člana 29 st. 3 i 6 ovog zakona, objedinjeni TLPT se, u smislu člana 29 stav 1 ovog zakona, smatra TLPT-om koji je sproveo finansijski subjekt obuhvaćen tim testiranjem.

(5) Broj finansijskih subjekata koji učestvuju u objedinjenom TLPT-u mora biti prilagođen složenosti i vrsti usluga obuhvaćenih tim testiranjem.

(6) Finansijski subjekt je dužan da, u saradnji sa trećim stranama koje pružaju IKT usluge, drugim uključenim stranama i licima koja sprovode testiranje, osim nadležnog organa, primijeni efikasne kontrole upravljanja rizicima radi ublažavanja rizika od mogućih negativnih uticaja na podatke, oštećenja imovine i poremećaja u obavljanju kritičnih ili važnih funkcija, usluga i operacija kod samog finansijskog subjekta, drugih finansijskih subjekata sa kojima ima poslovnu saradnju, kao i u finansijskom sektoru.

Izvještavanje o TLPT-u i međusoba saradnja nadležnih organa u TLPT-u

Član 31

(1) Po završetku TLPT-a, nakon usaglašavanja izvještaja i planova za otklanjanje utvrđenih nedostataka, finansijski subjekt i, kada je to primjenljivo, eksterna lica koja su sprovela TLPT, dužni su da nadležnom organu, odnosno nadležnom organu kojem su povjereni zadaci u skladu sa članom 29 stav 5 ovog zakona, dostave rezime relevantnih nalaza, planove za otklanjanje utvrđenih nedostataka i dokumentaciju kojom se potvrđuje da je TLPT sproveden u skladu sa zahtjevima iz ovog zakona.

(2) Nadležni organ iz stava 1 ovog člana, finansijskom subjektu izdaje potvrdu da je TLPT sproveden u skladu sa zahtjevima iz ovog zakona, kada se to može utvrditi iz dostavljene dokumentacije.

(3) Izuzetno od stava 2 ovog člana, potvrdu da je TLPT sproveden u skladu sa zahtjevima iz ovog zakona, izdaje:

1) nadležni organ koji je vodio TLPT, kada je više nadležnih organa učestvovalo u testiranju;

2) TLPT organ druge države članice, kada je TLPT vodio taj organ.

(4) Za potrebe sprovođenja TLPT-a kod finansijskog subjekta koji pruža usluge u više država članica, uključujući i preko filijala, kao i sprovođenja zajedničkog TLPT-a i objedinjenog TLPT-a u slučaju kada treća strana koja pruža IKT usluge pruža IKT usluge finansijskim subjektima u više država članica, nadležni organ sarađuje sa TLPT organima drugih država članica u skladu sa odredbama člana 16 Regulative (EU) br. 2025/1190.

(5) U slučaju kada je potvrdu o sprovedenom testiranju izdao organ koji nije zadužen za nadzor finansijskog subjekta, taj finansijski subjekt je dužan da obavijesti svoj nadležni organ o dobijanju te potvrde, i uz obavještenje dostavi rezime relevantnih nalaza i planove za otklanjanje nedostataka.

(6) Finansijski subjekt je, i nakon dobijanja potvrde o sprovedenom testiranju, odgovoran za uticaj objedinjenog TLPT-a iz člana 30 stav 2 ovog zakona.

Zahtjevi za lica koja su angažovana za sprovođenje TLPT-a

Član 32

(1) Finansijski subjekt je dužan da za potrebe sprovođenja TLPT-a iz člana 29 ovog zakona angažuje interna ili eksterna lica.

(2) Finansijski subjekt koji za potrebe sprovođenja TLPT-a angažuje interna lica, dužan je da za svako treće sprovođenje TLPT-a angažuje eksterna lica.

(3) Angažovana lica za potrebe sprovođenja TLPT-a iz stava 1 ovog člana moraju da:

1) ispunjavaju najviše standarde primjerenosti i ugleda;

2) posjeduju tehničke i organizacione sposobnosti i posebno stručno znanje u oblasti saznanja o prijetnjama, penetracionih testiranja i testiranja crvenog tima;

3) posjeduju sertifikat o akreditaciji koji je izdalo tijelo za akreditaciju u skladu sa zakonom kojim se uređuje postupak akreditacije, ili se pridržavaju formalnih kodeksa ponašanja ili etičkih okvira;

4) posjeduju sertifikat o akreditaciji koji je izdalo tijelo za akreditaciju druge države članice;

5) dostave nezavisno uvjerenje ili revizorski izvještaj kojim se potvrđuje da dobro upravljaju rizicima povezanim sa sprovođenjem TLPT-a, što uključuje adekvatnu zaštitu povjerljivih informacija finansijskog subjekta i mehanizme pravne zaštite u pogledu poslovnih rizika finansijskog subjekta;

6) koja su propisno i u cjelosti osigurana od profesionalne odgovornosti, uključujući i rizike od protivpravnog i nemarnog postupanja.

(4) U slučaju angažovanja internih lica za sprovođenje TLPT-a, finansijski subjekt dužan je da obezbijedi da su, pored zahtjeva iz stava 3 ovog člana, ispunjeni i sljedeći zahtjevi:

1) to angažovanje je odobrio nadležni organ, odnosno nadležni organ kojem su povjereni zadaci u skladu sa članom 29 stav 5 ovog zakona;

2) nadležni organ je potvrdio da je finansijski subjekt obezbijedio dovoljne resurse i preduzeo mjere za izbjegavanje sukoba interesa u fazi osmišljavanja i sprovođenja testiranja; i

3) pružalac saznanja o prijetnjama nije dio finansijskog subjekta.

(5) Finansijski subjekt je dužan da obezbijedi da se ugovorom zaključenim sa eksternim licem koje sprovodi TLPT obezbjeđuje dobro upravljanje rezultatima TLPT-a i da bilo kakva obrada podataka u vezi sa tim, uključujući generisanje, izradu, agregiranje, skladištenje, izvještavanje, saopštavanje i uništavanje podataka, ne stvara rizike za tog finansijskog subjekta.

V. UPRAVLJANJE IKT RIZIKOM POVEZANIM SA TREĆIM STRANAMA

Ključna načela dobrog upravljanja IKT rizikom povezanim sa trećim stranama

Član 33

(1) Finansijski subjekt je dužan da upravlja IKT rizikom povezanim sa trećim stranama kao sastavnim dijelom IKT rizika, u okviru sistema upravljanja IKT rizicima iz člana 10 ovog zakona, u skladu sa sljedećim principima:

1) finansijski subjekt koji je zaključio ugovor o korišćenju IKT usluga radi obavljanja svojih poslovnih aktivnosti, u svakom trenutku snosi punu odgovornost za usklađenost sa ovim zakonom i propisima kojima se uređuje poslovanje tog finansijskog subjekta;

2) finansijski subjekt upravlja IKT rizikom povezanim sa trećim stranama u skladu sa principom proporcionalnosti, uzimajući u obzir:

- prirodu, obim, složenost i značaj zavisnosti u oblasti IKT-a;

- rizike koji proizilaze iz ugovora o korišćenju IKT usluga zaključenih sa trećim stranama koje pružaju IKT usluge, uzimajući u obzir kritičnost ili značaj konkretne usluge, procesa ili funkcije i potencijalni uticaj na kontinuitet i dostupnost finansijskih usluga i aktivnosti, na pojedinačnom nivou i na nivou grupe.

(2) Finansijski subjekt, koji nije klasifikovan kao mikro finansijski subjekt i nije subjekt iz člana 21 stav 1 ovog zakona, dužan je da usvoji i redovno preispituje strategiju upravljanja IKT rizikom povezanim sa trećim stranama, uzimajući u obzir strategiju IKT nabavke od više dobavljača iz člana 12 stav 3 ovog zakona, kada je to primjenljivo.

(3) Strategija iz stava 2 ovog člana obuhvata politiku korišćenja IKT usluga koje pružaju treće strane za podršku kritičnih ili važnih funkcija finansijskog subjekta, i primjenjuje se na pojedinačnoj i, kada je to primjenjivo, na potkonsolidovanoj i konsolidovanoj osnovi.

(4) Organ upravljanja finansijskog subjekta dužan je da, na osnovu procjene ukupnog rizičnog profila finansijskog subjekta, obima i složenosti poslovnih usluga, redovno preispituje rizike identifikovane u vezi sa ugovorima o korišćenju IKT usluga kojima se podržavaju kritične ili važne funkcije.

(5) Prije zaključenja ugovora o korišćenju IKT usluga, finansijski subjekt je dužan da:

1) procijeni da li se ugovorom predviđa korišćenje IKT usluga koje podržavaju kritične ili važne funkcije;

2) provjeri da li su ispunjeni zahtjevi nadležnog organa za zaključenje ugovora;

3) identifikuje i procijeni sve relevantne rizike povezane sa ugovorom, uključujući i mogućnost da ugovor doprinese povećanju rizika IKT koncentracije iz člana 37 ovog zakona;

4) sprovede detaljnu analizu potencijalnih trećih strana koje pružaju IKT usluge i, kroz postupak odabira i procjene, obezbijedi da je odabrana treća strana adekvatna za pružanje tih usluga;

5) identifikuje i procijeni sukobe interesa koje bi taj ugovor mogao da izazove.

Registar informacija o ugovorima o korišćenju IKT uslugama i obavještavanje nadležnog organa

Član 34

(1) Finansijski subjekt je dužan da, u okviru sistema upravljanja IKT rizicima, na pojedinačnoj, kao i na potkonsolidovanoj i konsolidovanoj osnovi, vodi i ažurira registar informacija o svim ugovorima o korišćenju IKT usluga koje pružaju treće strane.

(2) Informacije o ugovorima iz stava 1 ovog člana moraju biti evidentirane tako da se ugovori koji se odnose na IKT usluge za podršku kritičnih ili važnih funkcija razlikuju od ugovora koji se ne odnose na te funkcije.

(3) Finansijski subjekt je dužan da najmanje jednom godišnje dostavi nadležnom organu izvještaj o broju novih ugovora o korišćenju IKT usluga, kategorijama trećih strana koje pružaju IKT usluge, vrsti ugovora i IKT uslugama i funkcijama koje se pružaju.

(4) Finansijski subjekt je dužan da nadležnom organu, na njegov zahtjev, stavi na raspolaganje pojedine djelove ili cjelokupan registar informacija iz stava 1 ovog člana, uključujući i druge informacije koje su nadležnom organu potrebne za sprovođenje nadzora.

(5) Finansijski subjekt je dužan da blagovremeno obavijesti nadležni organ o svakom planiranom ugovoru u skladu sa kojim namjerava da koristi IKT usluge za podršku kritičnih ili važnih funkcija, kao i o svakoj funkciji koja je podržana ugovorom o korišćenju IKT usluga, a koja postane kritična ili važna funkcija.

Standardi bezbjednosti i revizije treće strane koja pruža IKT usluge

Član 35

(1) Finansijski subjekt može da zaključi ugovor sa trećom stranom koja pruža IKT usluge, ukoliko ta treća strana primjenjuje odgovarajuće standarde informacione bezbjednosti.

(2) U slučaju kada se ugovor iz stava 1 ovog člana odnosi na usluge kojima se podržavaju kritične ili važne funkcije, finansijski subjekt je dužan da, prije zaključenja tog ugovora, utvrdi da treća strana koja pruža IKT usluge primjenjuje najnovije i najviše standarde informacione bezbjednosti.

(3) Radi ostvarivanja prava pristupa, sprovođenja provjera i revizija nad trećom stranom koja pruža IKT usluge, finansijski subjekt dužan je da, primjenom pristupa zasnovanog na procjeni rizika, unaprijed odredi učestalost provjera i revizija, kao i oblasti u kojima će se sprovesti, u skladu sa opšteprihvaćenim revizorskim standardima i, kada je to primjenljivo, zahtjevima nadležnog organa u pogledu primjene tih standarda.

(4) U slučaju da ugovor zaključen sa trećom stranom koja pruža IKT usluge iz stava 1 ovog člana obuhvata korišćenje IKT usluga koje podrazumijevaju visok stepen tehničke složenosti, finansijski subjekt je dužan da provjeri da li revizori, bilo da su interni, eksterni ili grupa revizora, posjeduju odgovarajuće vještine i znanja neophodna za efikasno sprovođenje relevantnih revizija i procjena.

Raskid ugovora i izlazne strategije

Član 36

(1) Finansijski subjekt je dužan da obezbijedi da se ugovor o korišćenju IKT usluga može raskinuti u sljedećim slučajevima:

1) treća strana koja pruža IKT uslugu značajno je prekršila zakon, propis ili ugovorne obaveze;

2) praćenjem IKT rizika povezanog sa trećom stranom utvrđene su okolnosti za koje se smatra da bi mogle dovesti do promjene u izvršavanju funkcija koje se pružaju na osnovu ugovora, uključujući bitne promjene koje utiču na ugovorni odnos ili stanje treće strane koja pruža IKT usluge;

3) treća strana koja pruža IKT usluge je pokazala slabosti u pogledu upravljanja ukupnim IKT rizikom, a naročito u načinu na koji obezbjeđuje dostupnost, autentičnost, integritet i povjerljivost podataka, bez obzira da se radi o podacima o ličnosti, osjetljivim ili drugim podacima;

4) nadležni organ više nije u mogućnosti da sprovodi efikasan nadzor finansijskog subjekta zbog uslova ili okolnosti koje se tiču ugovornog odnosa.

(2) Finansijski subjekt je dužan da utvrdi izlazne strategije za IKT usluge koje podržavaju kritične ili važne funkcije.

(3) Izlaznim strategijama iz stava 2 ovog člana moraju se uzeti u obzir rizici koji mogu nastati na nivou trećih strana koje pružaju IKT usluge, a naročito mogućnost propasti tih tećih strana, pogoršanje kvaliteta IKT usluga koje se pružaju, poremećaji u poslovanju usljed neadekvatnog ili neuspješnog pružanja IKT usluga, bilo koji značajan rizik koji se odnosi na adekvatnost i kontinuitet pružanja konkretne usluge, kao i mogućnost raskida ugovora sa trećom stranom koja pruža IKT usluge u slučaju iz stava 1 ovog člana.

(4) Finansijski subjekt je dužan da obezbijedi da raskid ugovora o korišćenju IKT usluga ne dovede do:

1) poremećaja poslovnih aktivnosti tog finansijskog subjekta;

2) ograničavanja usklađenosti sa regulatornim zahtjevima;

3) narušavanja kontinuiteta i kvaliteta usluga koje se pružaju klijentima.

(5) Finansijski subjekt je dužan da obezbijedi da su planovi za raskid ugovornih odnosa iz stava 1 ovog člana sveobuhvatni, dokumentovani i da se, u skladu sa principom proporcionalnosti iz člana 5 ovog zakona, dovoljno testiraju i periodično preispituju.

(6) Finansijski subjekt je dužan da utvrdi alternativna rješenja i razvije tranzicione planove koji mu omogućavaju da, na siguran i cjelovit način, prenese ugovorene IKT usluge i povezane podatke sa treće strane koja pruža IKT usluge na alternativne pružaoce usluga ili ih reintegriše u okviru sopstvenih kapaciteta, kao i da obezbijedi njihovo uklanjanje kod treće strane koja je pružala IKT usluge.

(7) Finansijski subjekt je dužan da uspostavi odgovarajuće mjere za nepredviđene situacije radi očuvanja kontinuiteta poslovanja u slučaju nastanka okolnosti iz stava 3 ovog člana.

Procjena rizika IKT koncentracije na nivou finansijskog subjekta

Član 37

(1) Prilikom identifikacije i procjene rizika iz člana 33 stav 5 tačka 3 ovog zakona, finansijski subjekt je dužan da uzme u obzir da li bi zaključivanje ugovora o IKT uslugama koje podržavaju kritične ili važne funkcije dovelo do:

1) angažovanja treće strane koja pruža IKT uslugu koja se ne može lako zamijeniti; ili

2) postojanja više ugovora o IKT uslugama koje podržavaju kritične ili važne funkcije sa istom trećom stranom koja pruža IKT usluge ili sa usko povezanim trećim stranama koje pružaju IKT usluge.

(2) Finansijski subjekt je dužan da procijeni prednosti i troškove alternativnih rješenja, kao što je angažman različitih trećih strana koje pružaju IKT usluge, uzimajući u obzir da li i na koji način predviđena rješenja odgovaraju poslovnim potrebama i ciljevama utvrđenim u strategiji digitalne operativne otpornosti tog finansijskog subjekta.

(3) Ako je ugovorom o korišćenju IKT usluga kojima se podržavaju kritične ili važne funkcije predviđeno da treća strana koja pruža IKT uslugu, radi pružanja tih usluga, može kao podizvođače angažovati druge pružaoce IKT usluga, finansijski subjekt je dužan da procijeni prednosti i rizike koji mogu proizaći iz tog angažovanja, naročito u slučaju angažovanja IKT podizvođača sa sjedištem u trećoj zemlji.

(4) U slučaju ugovora o korišćenju IKT usluga kojima se podržavaju kritične ili važne funkcije, finansijski subjekt je dužan da razmotri propise koji bi se primjenjivali u slučaju insolventnosti treće strane koja pruža IKT usluge, uključujući stečaj i likvidaciju, kao i sva ograničenja koja bi mogla nastati u slučaju potrebe za hitnim povratkom podataka finansijskog subjekta.

(5) U slučaju da se ugovor o korišćenju IKT usluga kojima se podržavaju kritične ili važne funkcije zaključuje sa trećom stranom koja pruža IKT usluge sa sjedištem u trećoj zemlji, finansijski subjekt je dužan da, pored elemenata iz stava 4 ovog člana, razmotri i usklađenost sa odredbama propisa kojima se uređuje zaštita podataka, kao i mogućnost sprovođenja zakona u toj trećoj zemlji.

(6) Ako je ugovorom o korišćenju IKT usluga kojima se podržavaju kritične ili važne funkcije predviđena mogućnost angažovanja podizvođača, finansijski subjekt je dužan da procijeni da li, i na koji način, potencijalno dugi ili složeni lanci podugovaranja mogu uticati na njegovu sposobnost da u potpunosti prati ugovorene funkcije, kao i na mogućnost nadležnog organa da sprovodi efikasan nadzor tog finansijskog subjekta.

Ključne ugovorne odredbe

Član 38

(1) Prava i obaveze finansijskog subjekta i treće strane koja pruža IKT usluge moraju biti uređene ugovorom.

(2) Ugovor iz stava 1 ovog člana sadrži i sporazume o nivou usluga, i mora biti dostupan ugovornim stranama u papirnom ili elektronskom obliku koji se može preuzeti u pristupačnom i trajnom formatu.

(3) Ugovor o korišćenju IKT usluga mora da sadrži:

1) jasan i potpun opis svih funkcija i IKT usluga koje će pružati treća strana koja pruža IKT usluge;

2) odredbe da li treća strana koja pruža IKT usluge može angažovati podizvođače radi pružanja IKT usluge kojom se podržava kritična ili važna funkcija, ili radi pružanja njenih bitnih djelova, i pod kojim uslovima;

3) lokacije, odnosno regije ili države, sa kojih će se pružati ugovorene i, kada je to primjenljivo, podugovorene funkcije i IKT usluge, kao i lokacije na kojima će se obrađivati podaci, uključujući lokacije na kojima će se skladištiti podaci;

4) obavezu treće strane koja pruža IKT usluge da unaprijed obavijesti finansijski subjekt o namjeri promjene lokacija iz tačke 3 ovog stava;

5) odredbe o zaštiti dostupnosti, autentičnosti, integriteta i povjerljivosti podataka, uključujući podatke o ličnosti;

6) odredbe kojima se finansijskom subjektu obezbjeđuje mogućnost pristupa, obnove i povratka podataka o ličnosti i drugih podataka u slučaju insolventnosti, sanacije ili prestanka poslovanja treće strane koja pruža IKT usluge, kao i u slučaju raskida ugovora;

7) opise nivoa usluga, uključujući njihova ažuriranja, odnosno izmjene;

8) obavezu treće strane koja pruža IKT usluge da pruži pomoć finansijskom subjektu bez dodatne naknade ili po unaprijed utvrđenoj cijeni, u slučaju IKT incidenta koji je povezan sa IKT uslugom koju ta treća strana pruža finansijskom subjektu;

9) obavezu treće strane koja pruža IKT usluge da u sarađuje sa nadležnim organom i organom koji je zadužen za sanaciju finansijskog subjekta u skladu sa zakonom kojim se uređuje sanacija finansijskog subjekta, uključujući i saradnju sa licima koja ovlaste ti organi;

10) prava i uslove za raskid ugovora, sa rokovima za dostavljanje obavještenja o namjeri raskida ugovora, u skladu sa zahtjevima organa iz tačke 9 ovog stava;

11) uslove za učešće treće strane koja pruža IKT usluge u programima za podizanje svijesti o IKT bezbjednosti i obukama o digitalnoj operativnoj otpornosti u skladu sa odredbama člana 19 stav 12 ovog zakona.

(4) Ugovor o korišćenju IKT usluga kojima se podržavaju kritične ili važne funkcije mora, pored elemenata iz stava 3 ovog člana, da sadrži i:

1) detaljan opis nivoa usluga, uključujući njihova ažuriranja i izmjene, sa preciznim kvantitativnim i kvalitativnim ciljevima učinka u okviru dogovorenih nivoa usluga, kako bi se finansijskom subjektu omogućilo efikasno praćenje IKT usluga i preduzimanje, bez odlaganja, odgovarajućih korektivnih mjera u slučaju da dogovoreni nivoi usluga nisu ispunjeni;

2) obavezu treće strane koja pruža IKT usluge da finansijskom subjektu dostavlja obavještenja i izvještaje, sa rokovima za njihovo dostavljanje, uključujući i obavještenja o svim okolnostima koje bitno utiču ili bi mogle bitno uticati na sposobnost treće strane koja pruža IKT usluge da efikasno pruža IKT usluge kojima se podržavaju kritične ili važne funkcije, u skladu sa dogovorenim nivoima usluga;

3) zahtjeve koje treća strana koja pruža IKT usluge mora ispunjavati u pogledu primjene i testiranja planova za nepredviđene okolnosti, kao i primjene IKT bezbjednosnih mjera, alata i politika kojima se obezbjeđuje adekvatan nivo bezbjednosti, potreban finansijskom subjektu za pružanje usluga u skladu sa zakonom;

4) obavezu treće strane koja pruža IKT usluge da učestvuje u TLPT-u finansijskog subjekta i bude maksimalno kooperativna tokom njegovog sprovođenja, u skladu sa odredbama čl. 29 do 32 ovog zakona;

5) pravo kontinuiranog praćenja učinka treće strane koja pruža IKT usluge, što obuhvata:

- neograničena prava finansijskog subjekta, treće strane koju je ovlastio finansijski subjekt i nadležnog organa na pristup, sprovođenje provjera, reviziju, odnosno nadzor nad i kod treće strane koja pruža IKT usluge, kao i pravo na dobijanje kopija relevantne dokumentacije treće strane koja pruža IKT usluge, tako da se ostvarivanje tih prava ne može isključiti ili ograničiti drugim ugovorima ili politikama;

- pravo da se, u slučaju kada bi ostvarivanje prava iz alineje 1 ove tačke moglo ugroziti prava drugih klijenata treće strane koja pruža IKT usluge, dogovore alternativni načini provjere učinka treće strane koja pruža IKT usluge, kojima se obezbjeđuje razuman nivo uvjerenja o kvalitetu i bezbjednosti pruženih usluga;

- obavezu treće strane koja pruža IKT usluge da u potpunosti sarađuje tokom neposrednih provjera, revizija i nadzora koje sprovodi nadležni organ, finansijski subjekt ili treća strana koju je ovlastio finansijski subjekt;

- obavezu treće strane koja pruža IKT usluge da sarađuje sa glavnim nadzornim organom, koji je određen u skladu sa članom 31 stav 1 tačka b) Regulative (EU) br. 2022/2554, tokom nadzora koji sprovodi taj organ;

- obavezu dostavljanja informacija potrebnih za određivanje obima, procedura koje će se primjenjivati i učestalosti provjera, revizija i nadzora iz al. 3 i 4 ove tačke.

6) odredbe neophodne za realizaciju izlazne strategije, naročito obavezni i adekvatni tranzicioni period:

- tokom kojeg će treća strana koja pruža IKT usluge nastaviti pružanje relevantnih funkcija i IKT usluga, radi ublažavanja rizika od nastanka poremećaja kod finansijskog subjekta ili radi obezbjeđivanja njegove efikasne sanacije i restrukturiranja;

- tokom kojeg finansijski subjekt može zamijeniti treću stranu koja pruža IKT usluge ili reintegrisati IKT usluge u okviru sopstvenih kapaciteta, u skladu sa složenošću tih usluga.

(5) Izuzetno od stava 4 tačka 5 ovog člana, finansijski subjekt koji je klasifikovan kao mikro finansijski subjekt može ugovoriti sa trećom stranom koja pruža IKT usluge da se pravo tog finansijskog subjekta na pristup, sprovođenje provjeru i reviziju nad i kod treće strane koja pruža IKT usluge može povjeriti nezavisnoj trećoj strani, koju odredi treća strana koja pruža IKT usluge, u kom slučaju finansijski subjekt od nezavisne treće strane, u svakom trenutku, može zahtijevati informacije i potvrde o učinku treće strane koja pruža IKT usluge.

(6) Prilikom usaglašavanja odredbi ugovora sa trećom stranom koja pruža IKT usluge, finansijski subjekt je dužan da razmotri primjenu standardizovanih ugovornih klauzula koje su javni organi razvili za određene usluge.

VI. RAZMJENA INFORMACIJA

Razmjena informacija i saznanja o sajber prijetnjama

Član 39

(1) Finansijski subjekti mogu međusobno razmjenjivati informacije i saznanja o sajber prijetnjama, uključujući indikatore ugroženosti, taktike, tehnike i procedure, bezbjednosna upozorenja i alate za konfiguraciju, u mjeri u kojoj ta razmjena:

1) ima za cilj jačanje digitalne operativne otpornosti finansijskih subjekata, naročito podizanjem svijesti o sajber prijetnjama, ograničavanje ili sprečavanje njihovog širenja, unapređenje odbrambenih kapaciteta, tehnika za otkrivanje prijetnji, strategija za ublažavanje uticaja ili postupaka odgovora i oporavka;

2) se sprovodi u okviru pouzdane zajednice finansijskih subjekata;

3) se ostvaruje kroz sporazume za razmjenu informacija kojima se štiti potencijalno osjetljiva priroda tih informacija, koji su uređeni pravilima ponašanja kojima se obezbjeđuje potpuna zaštita povjerljivih poslovnih informacija, podataka o ličnosti u skladu sa propisom kojim se uređuje zaštita podataka o ličnosti i primjena pravila u oblasti zaštite konkurencije.

(2) Sporazumima za razmjenu informacija iz stava 1 tačka 3 ovog člana moraju se utvrditi uslovi za učešće u razmjeni informacija i, kada je to primjenjivo, učešće i uloga javnih organa koji mogu biti uključeni u tim sporazumima, trećih strana koje pružaju IKT usluge, kao i operativni elementi, uključujući i upotrebu posebnih IT platformi.

(3) Finansijski subjekt je dužan da obavijesti nadležni organ bez odlaganja ako je učesnik u sporazumu za razmjenu informacija iz stava 1 tačka 3 ovog člana, odnosno kada prestane sa učešćem u tom sporazumu.

VII. NADZOR NAD SPROVOĐENJEM ODREDBI OVOG ZAKONA I NADZORNE MJERE

Obim nadležnosti

Član 40

(1) Nadzor nad sprovođenjem ovog zakona vrši nadležni organ.

(2) U sprovođenju nadzora iz stava 1 ovog člana, nadzorni organ:

1) izriče mjere finansijskom subjektu;

2) podnosi predloge za pokretanje prekršajnih postupaka zbog kršenja odredbi ovog zakona.

(3) Nadzor iz stava 2 tačka 1 ovog člana sprovodi se u skladu sa ovim zakonom i zakonom kojim se uređuje osnivanje i poslovanje finansijskog subjekta.

(4) U vršenju nadzora iz stava 1 ovog člana, nadležni organ može naročito da:

1) pristupi svim dokumentima ili podacima u bilo kom obliku koje smatra relevantnim za izvršavanje svojih ovlašćenja i pribavi kopije tih dokumenata ili podataka;

2) sprovede neposredni nadzor ili kontrolu, koji uključuju, ali nisu ograničeni na:

- ovlašćenje da od finansijskog subjekta i lica zaposlenih u finansijskom subjektu zahtijeva pisana i usmena objašnjenja o činjenicama koje se odnose na predmet i svrhu nadzora ili kontrole;

- obavljanje razgovora sa bilo kojim fizičkim ili pravnim licem za koje ocijeni da ima relevantna saznanja, uz izričitu saglasnost tog lica, u svrhu prikupljanja informacija koje se odnose na predmet kontrole;

3) zahtijeva sprovođenje korektivnih mjera zbog kršenja odredbi ovog zakona.

(5) Pored mjera koje je nadležni organ ovlašćen da izriče u skladu sa zakonom kojim se uređuje osnivanje i poslovanje finansijskog subjekta, nadležni organ je ovlašćen da u vršenju nadzora u skladu sa ovim zakonom:

1) naloži finansijskom subjektu i odgovornom licu u finansijskom subjektu da prekine, postupanje koje predstavlja kršenje ovog zakona i propisa donesenih na osnovu ovog zakona;

2) naloži finansijskom subjektu da privremeno ili trajno prekine sa postupanjem koje nadležni organ smatra kršenjem ovog zakona i propisa donesenih na osnovu ovog zakona i da spriječi ponavljanje takvog postupanja;

3) izrekne kaznu, uključujući i novčanu kaznu, kako bi se obezbijedilo da finansijski subjekt nastavi sa ispunjavanjem zahtjeva iz ovog zakona i propisa donesenih na osnovu ovog zakona;

4) uputi zahtjev, u skladu sa zakonom, za dostavljanje evidencije telekomunikacionog operatera o prometu podataka koji su od značaja za utvrđivanje povrede ovog zakona i propisa donesenih na osnovu ovog zakona, kada postoji opravdana sumnja na takvu povredu;

5) izda javno obavještenje o kršenju zakona, u kojem može da navede identitet finansijskog subjekta koji je bio predmet nadzora, odnosno kontrole, lica u tom finansijskom subjektu odgovorna za kršenje zakona i propisa donesenih na osnovu ovog zakona kao i prirodu tog kršenja.

(6) Nadležni organ može naložiti finansijskom subjektu da razriješi člana upravnog odbora ili drugo lice sa rukovodeće funkcije u tom finansijskom subjektu kada utvrdi njegovu odgovornost za kršenje ovog zakona.

(7) Finansijski subjekt kome je naložena mjera iz st. 5 ili 6 ovog člana, dužan je da izvrši tu mjeru na način i u roku utvrđenim rješenjem o izricanju mjere.

(8) Finansijski subjekt dužan je da u potpunosti sarađuje sa nadležnim organom tokom postupka nadzora ili kontrole i da na zahtjev nadležnog organa za potrebe sprovođenja nadzora ili kontrole dostavi zahtijevana pisana ili usmena objašnjenja o činjenicama koje se odnose na predmet i svrhu nadzora ili kontrole.

Način utvrđivanja mjera

Član 41

(1) Nadležni organ izvršava ovlašćenje za izricanje mjera iz člana 40 ovog zakona, u skladu sa zakonom kojim se uređuje osnivanje i poslovanje finansijskog subjekta, i to:

1) neposrednim postupanjem;

2) u saradnji sa nadležnim i drugim organima;

3) povjeravanjem pojedinih poslova drugim organima, u okviru sopstvene odgovornosti; ili

4) podnošenjem zahtjeva nadležnom pravosudnom organu.

(2) Prilikom odlučivanja o vrsti i visini mjere iz člana 40 stav 4 ovog zakona, nadležni organ uzima u obzir stepen namjere ili nehat u postupanju kojim je izvršeno kršenje odredbi ovog zakona i propisa donesenih na osnovu ovog zakona kao i sve druge relevantne okolnosti, naročito:

1) značaj, težinu i trajanje kršenja, odnosno ponavljanje ili učestalost kršenja;

2) stepen odgovornosti finansijskog subjekta, odnosno fizičkog lica odgovornog za kršenje;

3) finansijsku sposobnost finansijskog subjekta, odnosno fizičkog lica odgovornog za kršenje;

4) iznos stečene dobiti ili izbjegnutog gubitka finansijskog subjekta, odnosno fizičkog lica odgovornog za kršenje, ako se taj iznos može utvrditi;

5) gubitke trećih lica nastale kršenjem, ako se mogu utvrditi;

6) saradnju finansijskog subjekta, odnosno fizičkog lica odgovornog za kršenje, sa nadležnim organom, bez prejudiciranja obaveze povraćaja koristi ili izbjegnutog gubitka;

7) prethodna kršenja i izrečene mjere finansijskom subjektu, odnosno fizičkom licu odgovornom za kršenje.

(3) Mjere nadležnog organa izrečene u skladu sa odredbama ovog zakona, moraju biti efikasne, srazmjerne i odvraćajuće.

Saradnja u slučaju krivičnog djela

Član 42

Nadležni organ je dužan da u okviru svoje nadležnosti sarađuje sa pravosudnim organima i organima nadležnim za sprovođenje krivičnih sankcija radi razmjene informacija potrebnih za vođenje istraga i postupka u vezi sa sprovođenjem sankcija za krivično djelo u oblasti digitalne operativne otpornosti propisano zakonom.

Objavljivanje podataka o izrečenim novčanim kaznama i prekršajima finansijskih subjekata i odgovornim licima u finansijskim subjektima

Član 43

(1) Nadležni organ na svojoj internet stranici, bez odlaganja, objavljuje podatke o novčanim kaznama izrečenim pravosnažnim rješenjem iz člana 40 stav 4 tačka 3 ovog zakona i pravosnažnim kaznama finansijskom subjektu i odgovornom licu u finansijskom subjektu izrečenim u prekršajnom postupku zbog kršenja odredbi ovog zakona ili propisa donesenih na osnovu ovog zakona.

(2) Podaci iz stava 1 ovog člana sadrže informacije o vrsti i prirodi kršenja, naziv finansijskog subjekta i ime i prezime odgovornih lica u finansijskom subjektu kome je izrečena kazna.

(3) Izuzetno od st. 1 i 2 ovog člana, ako na pojedinačnoj osnovi nadležni organ procijeni da objavljivanje identiteta finansijskog subjekta ili ličnih podataka odgovornih lica u finansijskom subjektu nije srazmjerno utvrđenom kršenju, ili bi objavljivanje ugrozilo stabilnost finansijskog tržišta, istražne radnje u krivičnom postupku koje su u toku, ili bi objavljivanje prouzrokovalo nesrazmjernu štetu za finansijski subjekt ili odgovorna lica, koju je moguće utvrditi, nadležni organ može da:

1) odloži objavljivanje podataka iz st. 1 i 2 ovog člana do prestanka razloga za neobjavljivanje;

2) izvrši objavljivanje na način kojim se ne odaju podaci iz st. 1 i 2 ovog člana, s tim što se i to objavljivanje može odložiti;

3) ne objavi podatke iz st. 1 i 2 ovog člana ako ocijeni da opcije iz tač. 1 i 2 ovog stava ne mogu u dovoljnoj mjeri obezbijediti stabilnost finansijskog tržišta ili da to objavljivanje nije srazmjerno težini izrečene kazne.

(4) Podaci iz st. 1, 2 i 3 ovog člana ostaju na internet stranici nadležnog organa pet godina od dana objavljivanja.

VIII. SARADNJA NADLEŽNIH ORGANA SA DRUGIM ORGANIMA

Saradnja sa organima iz zakona kojim se uređuje informaciona bezbjednost

Član 44

(1) Nadležni organ, u sprovođenju ovog zakona, može ostvarivati komunikaciju i razmjenjivati informacije sa organom koji je u skladu sa zakonom kojim se uređuje informaciona bezbjednost određen kao jedinstvena nacionalna kontakt tačka za informacionu bezbjednost.

(2) Nadležni organ, u sprovođenju ovog zakona, može ostvarivati komunikaciju i razmjenjivati informacije sa organom koji je u skladu sa zakonom kojim se uređuje informaciona bezbjednost nadležan za zaštitu finansijskih subjekata od sajber prijetnji i incidenata i od njega može zatražiti relevantnu pomoć.

(3) Saradnja iz stava 2 ovog člana uređuje se sporazumima između nadležnih organa i tog organa.

Saradnja sa organima Evropske unije i organima trećih država

Član 45

(1) Nadležni organ može, u cilju jačanja saradnje u oblasti upravljanja IKT rizicima koji se odnose na angažovanje trećih strana, zaključivati sporazume sa nadzornim i regulatornim organima Evropske unije i trećih država.

(2) Sporazumi iz stava 1 ovog člana mogu obuhvatati razmjenu iskustava i primjera dobre prakse, saradnju u preispitivanju okvira upravljanja IKT rizicima, mjera za njihovo ublažavanje, kao i razmjenu informacija u vezi sa postupanjem u slučaju IKT incidenata.

(3) Nadležni organi dužni su da sarađuju sa EBA-om, ESMA-om i EIOPA-om u sporovođenju aktivnosti nadzora kritičnih trećih strana koje pružaju IKT usluge radi razmjene podataka, informacija o incidentima, mjerama i rizicima, na način i u obimu utvrđenom Regulativom (EU) br. 2022/2554.

(4) Nadležni organ je dužan da obavještava EBA-u, ESMA-u i EIOPA-u o objedinjenim podacima o zavisnostima finansijskih subjekata u Crnoj Gori od kritičnih trećih strana koje pružaju IKT usluge, radi usklađivanja sa praksom na nivou Evropske unije i učešća u zajedničkim mehanizmima nadzora.

(5) Podaci iz stava 4 ovog člana prikupljaju se i dostavljaju iz registara ugovora koje finansijski subjekat vodi u skladu sa ovim zakonom.

(6) Nadležni organ je dužan da sarađuje sa glavnim nadzornim organom, koji je određen u skladu sa članom 31 stav 1 tačka b) Regulative (EU) br. 2022/2554, na način i u obimu utvrđenom Regulativom, a u cilju blagovremene razmjene svih relevantnih informacija o kritičnim trećim stranama koje pružaju IKT usluge, potrebnim za sprovođenje njihovih nadležnosti u skladu sa Regulativom, posebno u vezi sa rizicima, pristupima i mjerama koje su preduzete u okviru ovlašćenja glavnog nadzornog organa u pogledu sprovođenja nadzora.

(7) Nadležni organ je dužan da sarađuje sa EBA-om, ESMA-om i EIOPA-om i drugim relevantnim organima, u vezi sa učešćem u uspostavljanju mehanizma za razmjenu dobre prakse u cilju unapređenja međusektorske svijesti o stanju i identifikaciji zajedničkih ranjivosti i rizika u oblasti sajber bezbjednosti, uključujući i učešće u razvoju i sprovođenju vježbi za upravljanje kriznim i nepredviđenim situacijama, scenarijima sajber napada i drugih

aktivnosti koje doprinose uspostavljanju efikasnog i koordinisanog odgovora na nivou Evropske unije u slučaju značajnih prekograničnih IKT incidenata ili srodnih prijetnji sa sistemskim uticajem na finansijski sektor, na način i u obimu utvrđenom Regulativom (EU) br. 2022/2554.

(8) Nadležni organ je dužan da obavještava Evropsku komisiju EBA-u, ESMA-u i EIOPA-u o:

1) propisima kojima se bliže uređuju zahtjevi iz ovog zakona, kao i o izmjenama tih propisa u rokovima propisanim Regulativom (EU) 2022/2554;

2) informacijama koje se razmjenjuju sa pravosudnim organima i organima nadležnim za sprovođenje krivičnih sankcija u skladu sa članom 42 ovog zakona.

IX. POSLOVNA TAJNA I ZAŠTITA PODATAKA O LIČNOSTI

Čuvanje poslovne tajne

Član 46

(1) Sve povjerljive informacije koje nadležni organ primi, razmijeni ili prenese u vezi sa sprovođenjem ovog zakona smatraju se tajnom u skladu sa zakonom i podliježu obavezi čuvanja tajne.

(2) Obaveza čuvanja poslovne tajne iz stava 1 ovog člana odnosi se na sva lica zaposlena ili angažovana od strane nadležnog organa, kao i sva druga pravna ili fizička lica kojima nadležni organ, u skladu sa zakonom, povjeri obavljanje pojedinih poslova ili ovlašćenja, uključujući revizore i spoljne eksperte.

(3) Informacije koje predstavljaju poslovnu tajnu ne mogu se saopštavati trećim licima, osim ako je to propisano ovim zakonom ili drugim propisom.

(4) Sve informacije koje se razmjenjuju između nadležnih organa u skladu sa ovim zakonom, a koje se odnose na poslovanje finansijskog subjekta ili operativne uslove, ekonomske ili lične, smatraju se povjerljivim, osim ako nadležni organ prilikom dostavljanja informacija izričito ne navede da se iste mogu objavljivati ili ako je njihovo objavljivanje nužno za vođenje sudskog postupka.

(5) Obavještavanje i razmjena podataka između nadležnih organa, odnosno između nadležnih organa i drugih organa u skladu sa ovim zakonom, ne predstavlja kršenje obaveze čuvanja povjerljivih informacija utvrđene posebnim zakonom.

Obrada i zaštita podataka o ličnosti

Član 47

(1) Nadležni organ obrađuje podatke o ličnosti samo u mjeri u kojoj je to neophodno za izvršavanje ovlašćenja u skladu sa ovim zakonom, naročito prilikom vršenja nadzora i kontrole, zahtijeva za dostavljanje informacija, komunikacije, objavljivanja informacija, evaluacije, provjere, procjene i izrade planova nadzora.

(2) Obrada podataka o ličnosti iz stava 1 ovog člana vrši se u skladu sa zakonom kojim se uređuje zaštita podataka o ličnosti.

(3) Podaci o ličnosti iz stava 1 ovog člana mogu se čuvati samo onoliko koliko je potrebno za vršenje ovlašćenja u vezi sa nadzorom finansijskog subjekta, a najduže 15 godina.

(4) Izuzetno od stava 3 ovog člana, podaci o ličnosti se mogu čuvati duže u slučaju vođenja sudskih postupaka, odnosno do okončanja postupka.

X. PROPISI O DIGITALNOJ OPERATIVNOJ OTPORNOSTI

Propisi Centralne banke o digitalnoj operativnoj otpornosti

Član 48

(1) Centralna banka, za finansijske subjekte iz člana 2 stav 1 tač. 1 do 4 ovog zakona, propisuje način sprovođenja procjene i dostavljanja podataka iz člana 17 stav 17 ovog zakona.

(2) Centralna banka, za finansijske subjekte iz člana 2 stav 1 tač. 1 do 4 ovog zakona, bliže propisuje:

1) sadržaj i način dostavljanja izvještaja o preispitivanju sistema upravljanja IKT rizicima iz člana 11 stav 3 ovog zakona;

2) zahtjeve za politike, procedure, protokole i alate za IKT bezbjednost iz člana 15 stav 2 ovog zakona;

3) zahtjeve za upravljanje pravima pristupa i kontrolu pristupa iz člana 15 stav 4 tačka 3 ovog zakona;

4) zahtjeve za mehanizme za brzo otkrivanje neuobičajenih aktivnosti iz člana 16 stav 1 ovog zakona i kriterijume za otkrivanje incidenata i aktiviranje procesa odgovora iz člana 16 stav 3 ovog zakona;

5) sadržaj i sprovođenje IKT politike kontinuiteta poslovanja iz člana 17 stav 1 ovog zakona;

6) sadržaj i sprovođenje planova za odgovor i oporavak u IKT oblasti iz člana 17 stav 4 ovog zakona;

7) zahtjeve za testiranje IKT planova kontinuiteta poslovanja iz člana 17 stav 12 ovog zakona.

(3) Centralna banka bliže propisuje:

1) za finansijske subjekte iz člana 2 stav 1 tač. 1 do 4 ovog zakona:

- kriterijume iz člana 23 stav 1 ovog zakona i pragove značajnosti za utvrđivanje značajnih IKT incidenata;

- kriterijume iz člana 23 stav 2 ovog zakona i pragove značajnosti za utvrđivanje ozbiljnih sajber prijetnji;

2) podatke iz izvještaja o značajnim IKT incidentima i značajnim operativnim ili sigurnosnim incidentima povezanim sa plaćanjem koje prosljeđuje drugim organima, u skladu sa odredbama člana 24 stav 11 ovog zakona.

(4) Centralna banka, za finansijske subjekte iz člana 2 stav 1 tač. 1 do 4 ovog zakona, propisuje:

1) sadržaj obavještenja i izvještaja o značajnom IKT incidentu iz člana 24 stav 3 ovog zakona, u skladu sa kriterijumima iz člana 23 stav 1 ovog zakona;

2) rokove za dostavljanje obavještenja i izvještaja o značajnom IKT incidentu iz člana 24 stav 3 ovog zakona;

3) sadržaj obavještenja o ozbiljnoj sajber prijetnji iz člana 24 stav 6 ovog zakona;

4) obrasce i postupke za obavještavanje o značajnom IKT incidentu iz člana 24 stav 3 ovog zakona i o ozbiljnoj sajber prijetnji iz člana 24 stav 6 ovog zakona.

(5) Centralna banka, za finansijske subjekte iz člana 2 stav 1 tač. 1 do 4 ovog zakona, bliže propisuje:

1) kriterijume iz člana 29 stav 4 ovog zakona za određivanje subjekata koji su dužni da sprovode TLPT;

2) zahtjeve i standarde koji se primjenjuju na angažovanje internih lica za potrebe sprovođenja TLPT-a;

3) zahtjeve koji se odnose na:

- obim TLPT-a iz člana 29 st. 3 i 6 ovog zakona;

- metodologiju za sprovođenje TLPT-a i postupke koji se primjenjuju u svakoj pojedinačnoj fazi testiranja;

- rezultate TLPT-a, završetak testiranja, otklanjanje utvrđenih nedostataka i potvrdu o sprovedenom testiranju.

(6) Centralna banka, za finansijske subjekte iz člana 2 stav 1 tač. 1 do 4 ovog zakona, bliže propisuje sadržaj politike iz člana 33 stav 3 ovog zakona o korišćenju IKT usluga koje pružaju treće strane, a kojima se podržavaju kritične ili važne funkcije.

(7) Centralna banka, za finansijske subjekte iz člana 2 stav 1 tač. 1 do 4 ovog zakona, propisuje način vođenja i obrasce za vođenje registra informacija o ugovorima o korišćenju IKT usluga iz člana 34 stav 1 ovog zakona.

(8) Centralna banka, za finansijske subjekte iz člana 2 stav 1 tač. 1 do 4 ovog zakona, bliže propisuje uslove za angažovanje podizvođača iz člana 38 stav 3 tačka 2 ovog zakona.

(9) Finansijski subjekt iz člana 2 stav 1 tač. 1 do 4 ovog zakona dužan je da postupi u skladu sa propisima Centralne banke iz st. 1 do 8 ovog člana.

Propisi Komisije o digitalnoj operativnoj otpornosti

Član 49

(1) Komisija, za finansijske subjekte iz člana 2 stav 1 tač. 5 do 14 ovog zakona, propisuje način sprovođenja procjene i dostavljanja podataka iz člana 17 stav 17 ovog zakona.

(2) Komisija, za finansijske subjekte iz člana 2 stav 1 tač. 5 do 14 ovog zakona, bliže propisuje:

1) sadržaj i način dostavljanja izvještaja o preispitivanju sistema upravljanja IKT rizicima iz člana 11 stav 3 ovog zakona;

2) zahtjeve za politike, procedure, protokole i alate za IKT bezbjednost iz člana 15 stav 2 ovog zakona;

3) zahtjeve za upravljanje pravima pristupa i kontrolu pristupa iz člana 15 stav 4 tačka 3 ovog zakona;

4) zahtjeve za mehanizme za brzo otkrivanje neuobičajenih aktivnosti iz člana 16 stav 1 ovog zakona i kriterijume za otkrivanje incidenata i aktiviranje procesa odgovora iz člana 16 stav 3 ovog zakona;

5) sadržaj i sprovođenje IKT politike kontinuiteta poslovanja iz člana 17 stav 1 ovog zakona;

6) sadržaj i sprovođenje planova za odgovor i oporavak u IKT oblasti iz člana 17 stav 4 ovog zakona;

7) zahtjeve za testiranje IKT planova kontinuiteta poslovanja iz člana 17 stav 12 ovog zakona.

(3) Komisija bliže propisuje:

1) za finansijske subjekte iz člana 2 stav 1 tač. 5 do 14 ovog zakona:

- kriterijume iz člana 23 stav 1 ovog zakona i pragove značajnosti za utvrđivanje značajnih IKT incidenata;

- kriterijume iz člana 23 stav 2 ovog zakona i pragove značajnosti za utvrđivanje ozbiljnih sajber prijetnji;

2) podatke iz izvještaja o značajnim IKT incidentima i značajnim operativnim ili sigurnosnim incidentima povezanim sa plaćanjem koje prosljeđuje drugim organima, u skladu sa odredbama člana 24 stav 11 ovog zakona.

(4) Komisija, za finansijske subjekte iz člana 2 stav 1 tač. 5 do 14 ovog zakona, propisuje:

1) sadržaj obavještenja i izvještaja o značajnom IKT incidentu iz člana 24 stav 3 ovog zakona, u skladu sa kriterijumima iz člana 23 stav 1 ovog zakona;

2) rokove za dostavljanje obavještenja i izvještaja o značajnom IKT incidentu iz člana 24 stav 3 ovog zakona;

3) sadržaj obavještenja o ozbiljnoj sajber prijetnji iz člana 24 stav 6 ovog zakona;

4) obrasce i postupke za obavještavanje o značajnom IKT incidentu iz člana 24 stav 3 ovog zakona i o ozbiljnoj sajber prijetnji iz člana 24 stav 6 ovog zakona.

(5) Komisija, za finansijske subjekte iz člana 2 stav 1 tač. 5 do 14 ovog zakona, bliže propisuje:

1) kriterijume iz člana 29 stav 4 ovog zakona za određivanje subjekata koji su dužni da sprovode TLPT;

2) zahtjeve i standarde koji se primjenjuju na angažovanje internih lica za potrebe sprovođenja TLPT-a;

3) zahtjeve koji se odnose na:

- obim TLPT-a iz člana 29 st. 3 i 6 ovog zakona;

- metodologiju za sprovođenje TLPT-a i postupke koji se primjenjuju u svakoj pojedinačnoj fazi testiranja;

- rezultate TLPT-a, završetak testiranja, otklanjanje utvrđenih nedostataka i potvrdu o sprovedenom testiranju.

(6) Komisija, za finansijske subjekte iz člana 2 stav 1 tač. 5 do 14 ovog zakona, bliže propisuje sadržaj politike iz člana 33 stav 3 ovog zakona o korišćenju IKT usluga koje pružaju treće strane, a kojima se podržavaju kritične ili važne funkcije.

(7) Komisija, za finansijske subjekte iz člana 2 stav 1 tač. 5 do 14 ovog zakona, propisuje način vođenja i obrasce za vođenje registra informacija o ugovorima o korišćenju IKT usluga iz člana 34 stav 1 ovog zakona.

(8) Komisija, za finansijske subjekte iz člana 2 stav 1 tač. 5 do 14 ovog zakona, bliže propisuje uslove za angažovanje podizvođača iz člana 38 stav 3 tačka 2 ovog zakona.

(9) Komisija bliže propisuje kriterijume za pojednostavljeni sistem upravljanja IKT rizicima iz člana 21 ovog zakona.

(10) Finansijski subjekt iz člana 2 stav 1 tač. 5 do 14 ovog zakona dužan je da postupi u skladu sa propisima Komisije iz st. 1 do 9 ovog člana.

Propisi Agencije o digitalnoj operativnoj otpornosti

Član 50

(1) Agencija, za finansijske subjekte iz člana 2 stav 1 tač. 15 do 25 ovog zakona, propisuje način sprovođenja procjene i dostavljanja podataka iz člana 17 stav 17 ovog zakona.

(2) Agencija, za finansijske subjekte iz člana 2 stav 1 tač. 15 do 25 ovog zakona, bliže propisuje:

1) sadržaj i način dostavljanja izvještaja o preispitivanju sistema upravljanja IKT rizicima iz člana 11 stav 3 ovog zakona;

2) zahtjeve za politike, procedure, protokole i alate za IKT bezbjednost iz člana 15 stav 2 ovog zakona;

3) zahtjeve za upravljanje pravima pristupa i kontrolu pristupa iz člana 15 stav 4 tačka 3 ovog zakona;

4) zahtjeve za mehanizme za brzo otkrivanje neuobičajenih aktivnosti iz člana 16 stav 1 ovog zakona i kriterijume za otkrivanje incidenata i aktiviranje procesa odgovora iz člana 16 stav 3 ovog zakona;

5) sadržaj i sprovođenje IKT politike kontinuiteta poslovanja iz člana 17 stav 1 ovog zakona;

6) sadržaj i sprovođenje planova za odgovor i oporavak u IKT oblasti iz člana 17 stav 4 ovog zakona;

7) zahtjeve za testiranje IKT planova kontinuiteta poslovanja iz člana 17 stav 12 ovog zakona.

(3) Agencija bliže propisuje:

1) za finansijske subjekte iz člana 2 stav 1 tač. 15 do 25 ovog zakona:

- kriterijume iz člana 23 stav 1 ovog zakona i pragove značajnosti za utvrđivanje značajnih IKT incidenata;

- kriterijume iz člana 23 stav 2 ovog zakona i pragove značajnosti za utvrđivanje ozbiljnih sajber prijetnji;

2) podatke iz izvještaja o značajnim IKT incidentima i značajnim operativnim ili sigurnosnim incidentima povezanim sa plaćanjem koje prosljeđuje drugim organima, u skladu sa odredbama člana 24 stav 11 ovog zakona.

(4) Agencija, za finansijske subjekte iz člana 2 stav 1 tač. 15 do 25 ovog zakona, propisuje:

1) sadržaj obavještenja i izvještaja o značajnom IKT incidentu iz člana 24 stav 3 ovog zakona, u skladu sa kriterijumima iz člana 23 stav 1 ovog zakona;

2) rokove za dostavljanje obavještenja i izvještaja o značajnom IKT incidentu iz člana 24 stav 3 ovog zakona;

3) sadržaj obavještenja o ozbiljnoj sajber prijetnji iz člana 24 stav 6 ovog zakona;

4) obrasce i postupke za obavještavanje o značajnom IKT incidentu iz člana 24 stav 3 ovog zakona i o ozbiljnoj sajber prijetnji iz člana 24 stav 6 ovog zakona.

(5) Agencija, za finansijske subjekte iz člana 2 stav 1 tač. 15 do 25 ovog zakona, bliže propisuje:

1) kriterijume iz člana 29 stav 4 ovog zakona za određivanje subjekata koji su dužni da sprovode TLPT;

2) zahtjeve i standarde koji se primjenjuju na angažovanje internih lica za potrebe sprovođenja TLPT-a;

3) zahtjeve koji se odnose na:

- obim TLPT-a iz člana 29 st. 3 i 6 ovog zakona;

- metodologiju za sprovođenje TLPT-a i postupke koji se primjenjuju u svakoj pojedinačnoj fazi testiranja;

- rezultate TLPT-a, završetak testiranja, otklanjanje utvrđenih nedostataka i potvrdu o sprovedenom testiranju.

(6) Agencija, za finansijske subjekte iz člana 2 stav 1 tač. 15 do 25 ovog zakona, bliže propisuje sadržaj politike iz člana 33 stav 3 ovog zakona o korišćenju IKT usluga koje pružaju treće strane, a kojima se podržavaju kritične ili važne funkcije.

(7) Agencija, za finansijske subjekte iz člana 2 stav 1 tač. 15 do 25 ovog zakona, propisuje način vođenja i obrasce za vođenje registra informacija o ugovorima o korišćenju IKT usluga iz člana 34 stav 1 ovog zakona.

(8) Agencija, za finansijske subjekte iz člana 2 stav 1 tač. 15 do 25 ovog zakona, bliže propisuje uslove za angažovanje podizvođača iz člana 38 stav 3 tačka 2 ovog zakona.

(9) Finansijski subjekt iz člana 2 stav 1 tač. 15 do 25 ovog zakona dužan je da postupi u skladu sa propisima Agencije iz st. 1 do 8 ovog člana.

Propisi drugih nadležnih organa

Član 51

(1) Propise iz člana 48 ovog zakona za finansijske subjekte iz člana 2 stav 1 tač. 26 i 27 ovog zakona donosi nadležni organ iz člana 3 stav 1 tačka 4 ovog zakona.

(2) Finansijski subjekt iz člana 2 stav 1 tač. 26 i 27 ovog zakona dužan je da postupi u skladu sa propisima iz stava 1 ovog člana.

XI. KAZNENE ODREDBE

Član 52

(1) Novčanom kaznom od 5.000 eura do 40.000 eura kazniće se za prekršaj pravno lice, ako:

1) nema uspostavljen sistem upravljanja i sistem interne kontrole kojima se obezbjeđuje efikasno i pouzdano upravljanje IKT rizicima u skladu sa članom 10 st. 5 i 6 ovog zakona, radi postizanja visokog nivoa digitalne operativne otpornosti (član 9 stav 2);

2) ne odredi organizacioni dio koji je odgovoran za praćenje realizacije ugovora zaključenih sa trećim stranama koje pružaju IKT usluge ili ne imenuje člana višeg rukovodstva koji će biti odgovoran za nadzor povezane izloženosti riziku i pripadajuće dokumentacije (član 9 stav 4);

3) nema uspostavljen pouzdan, sveobuhvatan i dobro dokumentovan sistem upravljanja IKT rizicima kao dio opšteg sistema upravljanja rizicima, kojim se omogućava brzo, efikasno i sveobuhvatno tretiranje IKT rizika i obezbjeđuje visok nivo digitalne operativne otpornosti (član 10 st. 1 i 2);

4) u skladu sa sistemom upravljanja IKT rizicima ne svede na najmanju moguću mjeru uticaj IKT rizika primjenom odgovarajućih strategija, politika, procedura, IKT protokola i alata iz člana 10 stav 2 ovog zakona (član 10 stav 3);

5) ne dostavi nadležnom organu, na njegov zahtjev, potpune i ažurne informacije o IKT rizicima i sistemu upravljanja IKT rizicima iz člana 10 stav 1 ovog zakona (član 10 stav 4);

6) ne dodijeli odgovornost za upravljanje i nadzor nad IKT rizikom kontrolnoj funkciji ili ne obezbijedi odgovarajući nivo njene nezavisnosti, na način da se izbjegava sukob interesa i razdvajanje poslova u kojima IKT rizik nastaje, poslova kontrolnih funkcija i poslova interne revizije, u skladu sa modelom tri linije odbrane ili internim modelom za upravljanje i kontrolu rizika (član 10 st. 5 i 6);

7) kontinuirano ne unaprjeđuje sistem upravljanja IKT rizicima iz člana 10 stav 1 ovog zakona na osnovu iskustava stečenih kroz njegovu praktičnu primjenu i praćenje, i ako taj ne preispituje i ne ažurira na način propisan članom 11 stav 1 ovog zakona (član 11 st. 1 i 2);

8) ne dostavi nadležnom organu, na njegov zahtjev, izvještaj o preispitivanju i ažuriranju sistema upravljanja IKT rizicima (član 11 stav 3);

9) ne obezbijedi redovne interne revizije sistema upravljanja IKT rizicima iz člana 10 stav 1 ovog zakona, u skladu sa planom revizije, od strane nezavisnih revizora koji posjeduju znanje, vještine i iskustvo u oblasti IKT rizika (član 11 st. 4 i 5);

10) ne uspostavi formalan proces koji omogućava blagovremeno otklanjanje ključnih nepravilnosti i nedostataka utvrđenih revizijom iz člana 11 stav 4 ovog zakona, kao i adekvatnu primjenu i praćenje tog postupka (član 11 stav 6);

11) u strategiji digitalne operativne otpornosti, koja predstavlja sastavni dio sistema upravljanja IKT rizicima iz člana 10 stav 1 ovog zakona, ne utvrdi način primjene tog sistema (član 12 st. 1 i 2);

12) ne koristi ili ne održava ažurnim IKT sisteme, protokole i alate na način propisan članom 13 ovog zakona (član 13);

13) ne identifikuje, ne klasifikuje ili ne dokumentuje adekvatno sve poslovne funkcije podržane IKT-om, zaduženja i odgovornosti, informacionu imovinu i IKT imovinu koja podržava te funkcije ili njihove uloge i međuzavisnosti u pogledu IKT rizika (član 14 stav 1);

14) po potrebi, a najmanje jednom godišnje ne preispituje adekvatnost klasifikacije iz člana 14 stav 1 ovog zakona i cjelokupne pripadajuće dokumentacije (član 14 stav 2);

15) kontinuirano ne identifikuje sve izvore IKT rizika a naročito izloženosti riziku prema drugim finansijskim subjektima i od drugih finansijskih subjekata, ili ne procjenjuje sajber prijetnje i IKT ranjivosti koje se odnose na njegove poslovne funkcije podržane IKT-om, informacionu imovinu i IKT imovinu (član 14 stav 3);

16) redovno, a najmanje jednom godišnje, ne razmatra scenarije rizika koji mogu uticati na njegove poslovne funkcije podržane IKT-om, informacionu imovinu i IKT imovinu (član 14 stav 4);

17) nije sprovelo procjenu rizika u slučaju svake značajne promjene u infrastrukturi mrežnih i informacionih sistema i procesima ili procedurama koje utiču na njegove poslovne funkcije podržane IKT-om, informacionu imovinu ili IKT imovinu (član 14 stav 5);

18) ne identifikuje svu informacionu imovinu i IKT imovinu, uključujući mrežne resurse, hardversku opremu i imovinu na udaljenim lokacijama, ili ne evidentira posebno informacionu imovinu i IKT imovinu koja se smatra kritičnom (član 14 stav 6);

19) ne dokumentuje konfiguraciju informacione imovine i IKT imovine i informacije o povezanosti i međuzavisnosti između različite infromacione i IKT imovine (član 14 stav 7);

20) ne identifikuje i ne dokumentuje sve procese koji zavise od trećih strana koje pružaju IKT usluge i ako ne identifikuje međusobne povezanosti sa trećim stranama koje pružaju IKT usluge kojima se podržavaju kritične ili važne funkcije (član 14 stav 8);

21) radi postupanja u skladu sa članom 14 st. 1, 6, 7 i 8 ovog zakona ne vodi odgovarajuće registre, koje mora da ažurira redovno i u slučaju svake značajne promjene iz člana 14 stav 5 ovog zakona (član 14 stav 9);

22) redovno, a najmanje jednom godišnje ne sprovodi procjenu IKT rizika za sve zastarjele IKT sisteme kao i vanredno prije i nakon povezivanja tehnologija, aplikacija ili sistema (član 14 stav 10);

23) ne prati kontinuirano ili ne kontroliše bezbjednost i funkcionisanje IKT sistema i alata, i na najmanju moguću mjeru ne svede uticaj IKT rizika na IKT sisteme, primjenom odgovarajućih IKT bezbjednosnih alata, politika i procedura (član 15 stav 1);

24) ne osmisli, kreira i/ili nabavi i primijeni politike, procedure, protokole i alate za IKT bezbjednost u cilju obezbjeđivanja otpornosti, kontinuiteta i dostupnosti IKT sistema, a naročito onih koji podržavaju kritične ili važne funkcije, i u cilju održavanja visokog nivoa dostupnosti, autentičnosti, integriteta i povjerljivosti podataka, bez obzira da li su u stanju mirovanja, upotrebi ili prenosu (član 15 stav 2);

25) radi ostvarivanja ciljeva iz člana 15 stav 2 ovog zakona ne koristi IKT rješenja i procese koji su primjereni, u smislu člana 5 ovog zakona, na način propisan članom 15 stav 3 ovog zakona:

26) u okviru sistema upravljanja IKT rizicima ne postupa na način propisan članom 15 stav 4 ovog zakona;

27) strukturu za upravljanje mrežom i infrastrukturom iz člana 15 stav 4 tačka 2 ovog zakona ne kreira i ne implementira na način kojim se omogućava brzo ukidanje ili segmentiranje mrežnog pristupa, kako bi se u najvećoj mogućoj mjeri ograničilo i spriječilo širenje zaraze, a naročito u slučaju međusobno povezanih finansijskih procesa (član 15 stav 5);

28) postupak upravljanja IKT promjenama iz člana 15 stav 4 tačka 5 ovog zakona nije odobren od strane odgovarajućih linija i nivoa odlučivanja finansijskog subjekta, i ne sprovodi se u skladu sa posebno utvrđenim protokolima finansijskog subjekta (član 15 stav 7);

29) ne uspostavi mehanizme za brzo otkrivanje neuobičajenih aktivnosti u skladu sa članom 22 ovog zakona, uključujući otkrivanje problema u performansama IKT mreže i IKT incidenata, kao i mehanizme za identifikovanje potencijalnih značajnih jedinstvenih tačaka prekida (član 16 st. 1 i 3);

30) ne testira redovno mehanizme za brzo otkrivanje neuobičajenih aktivnosti na način propisan članom 28 ovog zakona (član 16 stav 2);

31) ne obezbijedi dovoljne resurse i kapacitete za praćenje aktivnosti korisnika ili otkrivanje neuobičajnih IKT događaja i IKT incidenata, a naročito sajber napada (član 16 stav 4);

32) kao pružalac usluga dostave podataka nije uspostavilo sisteme kojima se može efikasno provjeriti da li su izvještaji o trgovanju potpuni i kojima se mogu utvrditi propusti i očigledne greške i zahtijevati ponovni prenos tih izvještaja (član 16 stav 5);

33) ne uspostavi, u okviru sistema upravljanja IKT rizicima, na osnovu rezultata postupanja u skladu sa članom 14 ovog zakona, sveobuhvatnu IKT politiku kontinuiteta poslovanja (član 17 st. 1 i 2);

34) ne primjenjuje IKT politiku kontinuiteta poslovanja iz člana 17 stav 1 ovog zakona pomoću odgovarajućih, namjenskih i dokumentovanih mjera, planova, procedura i mehanizama u cilju ispunjavanja uslova iz člana 17 stav 3 ovog zakona;

35) u okviru sistema upravljanja IKT rizicima ne utvrdi i ne primjenjuje odgovarajuće planove za odgovor i oporavak u IKT oblasti (član 17 stav 4);

36) ne obezbijedi nezavisnu internu reviziju planova za odgovor i oporavak u IKT oblasti (član 17 stav 5);

37) ne uspostavi, ne održava i periodično ne testira odgovarajuće IKT planove kontinuiteta poslovanja, naročito za kritične ili važne funkcije koje, na osnovu zaključenih ugovora, obavljaju ili isporučuju treće strane koje pružaju IKT usluge (član 17 stav 6);

38) u okviru opšte politike kontinuiteta poslovanja ne sprovodi analizu uticaja na poslovanje odnosno analizu svoje izloženosti ozbiljnim poremećajima u poslovanju (član 17 stav 7);

39) u okviru analize uticaja na poslovanje iz člana 17 stav 7 ovog zakona, na osnovu kvalitativnih i kvantitativnih kriterijuma, korišćenjem raspoloživih internih i eksternih podataka i analize scenarija ne procijeni potencijalni uticaj ozbiljnih poremećaja u poslovanju (član 17 stav 8);

40) prilikom vršenja analize uticaja na poslovanje iz člana 17 stav 7 ovog zakona ne uzme u obzir kritičnost identifikovanih poslovnih funkcija, pomoćnih procesa, informacione imovine, zavisnosti od trećih strana, kao i njihovu povezanost i međuzavisnost (član 17 stav 9);

41) ne osmisli ili ne koristi IKT imovinu i IKT usluge na način koji je u potpunosti usklađen sa rezultatima analize uticaja na poslovanje iz člana 17 stav 7 ovog zakona, naročito u pogledu obezbjeđivanja adekvatne redundanse svih kritičnih komponenti (član 17 st. 10 i 11);

42) ne testira planove za odgovor i oporavak u IKT oblasti iz člana 17 stav 4 ovog zakona i IKT planove kontinuiteta poslovanja iz člana 17 stav 6 ovog zakona na način propisan članom 17 stav 12 i 13 ovog zakona ili ne testira planove komunikacije u kriznim situacijama iz člana 20 ovog zakona (član 17 st. 12 i 13);

43) redovno ne preispituje IKT politiku kontinuiteta poslovanja iz člana 17 stav 1 ovog zakona ili planove za odgovor i oporavak u IKT oblasti iz člana 17 stav 4 ovog zakona, uzimajući u obzir rezultate testiranja iz člana 17 stav 12 ovog zakona, preporuke revizije i zahtjeve nadležnog organa (član 17 stav 14);

44) nije odredilo odgovorno lice ili organizacionu jedinicu za upravljanje kriznim situacijama (član 17 stav 15);

45) u slučaju pokretanja IKT planova za odgovor i oporavak u IKT oblasti iz člana 17 stav 4 ovog zakona ili IKT planova kontinuiteta poslovanja iz člana 17 stav 6 ovog zakona ne vodi evidenciju aktivnosti prije i nakon poremećaja u radu, koja mora biti lako dostupna (član 17 stav 16);

46) ne dostavi nadležnom organu, na njegov zahtjev, procjenu ukupnih godišnjih troškova i gubitaka koje su prouzrokovali značajni IKT incidenti (član 17 stav 17);

47) kao centralno klirinško depozitarno društvo Komisiji ne dostavi kopije rezultata testova kontinuiteta poslovanja u području IKT-a ili sličnih vježbi (član 17 stav 18);

48) u okviru sistema upravljanja IKT rizicima ne razvije ili ne usvoji politike i procedure kojima se na osnovu kritičnosti informacija i povjerljivosti podataka, utvrđuju obim i minimalna učestalost izrade rezervnih kopija podataka, i ne razvije ili ne usvoji procedure i metode za povratak, ponovno uspostavljanje i oporavak (član 18 stav 1);

49) ne obezbijedi sisteme za izradu rezervnih kopija podataka koji se mogu koristiti u skladu sa politikama i procedurama za izradu rezervnih kopija podataka iz člana 18 stav 1 tačka 1 ovog zakona, kao i u skladu sa procedurama i metodama za povratak, ponovno uspostavljanje i oporavak iz člana 18 stav 1 tačka 2 ovog zakona (član 18 stav 2);

50) korišćenjem sistema za izradu rezervnih kopija podataka iz člana 18 stav 2 ovog zakona ugrozi bezbjednost mrežnih i informacionih sistema ili dostupnost, autentičnost, integritet ili povjerljivost podataka (član 18 stav 3);

51) periodično ne testira procedure za izradu rezervnih kopija podataka iz člana 18 stav 1 tačka 1 ovog zakona ili ne testira procedure i metode za povratak, ponovno uspostavljanje i oporavak iz člana 18 stav 1 tačka 2 ovog zakona (član 18 stav 4);

52) koristi sopstvene sisteme za povraćaj podataka iz rezervnih kopija, a ne obezbijedi da se za te potrebe koriste IKT sistemi koji su fizički i logički odvojeni od izvornih IKT sistema iz kojih podaci potiču (član 18 stav 5);

53) IKT sistemi iz člana 18 stav 5 ovog zakona koji su namijenjeni za oporavak, nisu bezbjedno zaštićeni od neovlašćenog pristupa i IKT kompromitacija i ako ne omogućavaju blagovremeno ponovno uspostavljanje usluga, pri čemu se, po potrebi, koriste rezervne kopije podataka i sistema (član 18 stav 6);

54) ne održava rezervne IKT kapacitete koji imaju resurse, sposobnosti i funkcije dovoljne za adekvatno obezbjeđivanje potreba poslovnih procesa (član 18 stav 7);

55) kao finansijski subjekt koji je klasifikovan kao mikro finansijski subjekt nije procijenio potrebu održavanja rezervnih IKT kapaciteta iz člana 18 stav 7 ovog zakona (član 18 stav 8);

56) prilikom određivanja ciljnog vremena oporavka i ciljne tačke oporavka za svaku funkciju ne uzme u obzir značaj te funkcije, a naročito da li se radi o kritičnoj ili važnoj funkciji, kao i potencijalni ukupni uticaj ciljeva oporavka na efikasnost tržišta (član 18 st. 9 i 10);

57) prilikom oporavka od IKT incidenta ne sprovede sve neophodne kontrole, uključujući višestruke provjere i usklađivanja, kako bi obezbijedio održavanje najvišeg nivoa integriteta podataka (član 18 st. 11 i 12);

58) kao centralna druga ugovorna stana nema plan oporavka koji omogućava oporavak svih transakcija koje su bile u toku u trenutku nastanka poremećaja kako bi se obezbijedio nesmetan i siguran nastavak poslovanja centralne druge ugovorne strane i omogućilo izvršenje obaveze na predviđeni datum (član 18 stav 13);

59) kao pružalac usluga ne obezbijedi odgovarajuće resurse i infrastrukturu za izradu rezervnih kopija i obnovu sistema, radi kontinuiranog pružanja i održavanja svojih usluga (član 18 stav 14);

60) kao centralno klirinško depozitarno društvo ne održava najmanje jedno sekundarno mjesto obrade opremljeno odgovarajućim resursima, sposobnostima, funkcijama i osobljem, kako bi se zadovoljile poslovne potrebe (član 18 st. 15 i 16);

61) ne obezbijedi kapacitete ili ne odredi lica zadužena za prikupljanje informacija o ranjivostima, sajber prijetnjama ili IKT incidentima a naročito o sajber napadima, kao i za analizu njihovog mogućeg uticaja na digitalnu operativnu otpornost finansijskog subjekta (član 19 stav 1);

62) ne uspostavi ili ne sprovodi proces naknadne analize IKT incidenata koji se sprovodi nakon što značajan IKT incident poremeti obavljanje njegovih osnovnih aktivnosti, u cilju analize uzroka poremećaja i

utvrđivanja potrebnih poboljšanja u IKT operacijama ili u IKT politici kontinuiteta poslovanja iz člana 17 stav 1 ovog zakona (član 19 st. 2 i 4);

63) ne dostavi nadležnom organu, na njegov zahtjev, informacije o izmjenama koje su sprovedene nakon analize IKT incidenta iz člana 19 stav 2 ovog zakona (član 19 stav 3);

64) ne obezbijedi da se iskustva stečena kroz testiranje digitalne operativne otpornosti iz čl. 27 do 32 ovog zakona, kao i iz nastalih IKT incidenata, a naročito sajber napada, saznanja o izazovima koji su se pojavili prilikom pokretanja planova za odgovor i oporavak u IKT oblasti iz člana 17 stav 4 ovog zakona i IKT planova kontinuiteta poslovanja iz člana 17 stav 6 ovog zakona, relevantne informacije dobijene od drugih subjekata, kao i informacije u vezi sa zahtjevima nadležnog organa, blagovremeno, adekvatno i kontinuirano koriste u okviru procesa procjene IKT rizika (član 19 stav 5);

65) iskustva, saznanja ili informacije iz člana 19 stav 5 ovog zakona na odgovarajući način ne uzima u obzir prilikom preispitivanja relevantnih komponenti sistema upravljanja IKT rizicima (član 19 stav 6);

66) ne prati efikasnost sprovođenja strategije digitalne operativne otpornosti iz člana 12 stav 1 ovog zakona (član 19 stav 7);

67) ne evidentira ili ne prati promjenu ukupnog profila IKT rizika tokom vremena ili ne analizira učestalost, vrste, razmjere i trendove IKT incidenata, a naročito sajber napada i njihovih obrazaca, kako bi razumio nivo svoje izloženosti IKT riziku, posebno u odnosu na kritične ili važne funkcije i unaprijedio stepen svoje zrelosti i spremnosti u oblasti sajber bezbjednosti (član 19 stav 8);

68) ne osmisli ili ne sprovodi programe za podizanje svijesti o IKT bezbjednosti i obuke o digitalnoj operativnoj otpornosti kao obavezne djelove svojih programa obuke zaposlenih (član 19 st. 10 i 11);

69) kada je to primjenljivo, ne uključi treće strane koje pružaju IKT usluge u odgovarajuće programe obuke, u skladu sa članom 38 stav 3 tačka 11 ovog zakona (član 19 stav 12);

70) kontinuirano ne prati trendove u razvoju tehnologija kako bi bolje razumio mogući uticaj primjene novih tehnologija na zahtjeve u oblasti IKT bezbjednosti i digitalnu operativnu otpornost (član 19 stav 13);

71) nije upoznat sa najnovijim metodama za upravljanje IKT rizicima kako bi mogao efikasno da odgovori na postojeće i nove oblike sajber napada (član 19 stav 14);

72) u okviru sistema upravljanja IKT rizicima ne utvrdi planove komunikacije u kriznim situacijama, koji mu omogućavaju da na odgovoran način saopštava informacije najmanje o značajnim IKT incidentima i značajnim ranjivostima, klijentima, poslovnim partnerima i široj javnosti, u zavisnosti od slučaja (član 20 stav 1);

73) u okviru sistema upravljanja IKT rizicima ne utvrdi ili ne primjenjuje politike komunikacije za zaposlene ili sa eksternim zainteresovanim stranama (član 20 stav 2);

74) politikama komunikacije za zaposlene ili sa eksternim zainteresovanim stranama iz člana 20 stav 2 ovog zakona, u dijelu koji se odnosi na zaposlene, ne obezbijedi razlikovanje između zaposlenih koje je potrebno samo informisati i zaposlenih koji učestvuju u upravljanju IKT rizicima, odnosno koji su zaduženi za odgovor i oporavak (član 20 stav 3);

75) ne zaduži najmanje jedno lice u finansijskom subjektu za sprovođenje strategije komunikacije u slučaju IKT incidenata da u tu svrhu obavlja poslove informisanja medija i javnosti (član 20 stav 4);

76) kao finansijski subjekt koji u skladu sa članom 21 stav 1 primjenjuje pojednostavljeni sistem upravljanja IKT rizicima ne ispunjava zahtjeve propisane članom 21 stav 2 ovog zakona;

77) ne definiše ili ne uspostavi ili ne primijeni proces upravljanja IKT incidentima radi otkrivanja, upravljanja i obavještavanja o IKT incidentima (član 22 stav 1);

78) ne evidentira sve IKT incidente ili ozbiljne sajber prijetnje (član 22 stav 2);

79) ne uspostavi adekvatne procedure i postupke kojima se obezbjeđuje da se, na dosljedan i objedinjen način postupa sa IKT incidentima, vrši njihovo praćenje i preduzimaju dalje mjere, kako bi se obezbijedilo da se osnovni uzroci IKT incidenata identifikuju, dokumentuju i tretiraju, radi sprečavanja ponavljanja takvih incidenata (član 22 stav 3);

80) u okviru procesa upravljanja IKT incidentima iz člana 22 stav 1 ovog zakona ne postupa na način propisan članom 22 stav 4 ovog zakona;

81) ne klasifikuje IKT incidente ili ne utvrdi njihov uticaj na osnovu kriterijuma propisanih članom 23 stav 1 ovog zakona;

82) ne klasifikuje sajber prijetnje kao ozbiljne na osnovu kritičnosti usluga koje su izložene riziku, uključujući u pogledu transakcija i operacija finansijskog subjekta, broja i/ili značaja klijenata izloženih tom riziku ili broja

i/ili značaja finansijskih subjekata i institucija koje su druga ugovorna strana izložena tom riziku i geografske rasprostranjenosti u smislu područja izloženih riziku (član 23 stav 2);

83) ne izvijesti nadležni organ o značajnom IKT incidentu (član 24 st. 1 do 5);

84) odmah, bez odlaganja, ne obavijesti klijente o značajnom IKT incidentu koji utiče na njihove finansijske interese ili o preduzetim mjerama za ublažavanje negativnih uticaja tog incidenta (član 24 stav 8);

85) ne obavijesti klijente, kada je to primjenljivo, o mjerama zaštite od ozbiljne sajber prijetnje koje mogu da preduzmu (član 24 stav 9);

86) u skladu sa principom proporcionalnosti iz člana 5 ovog zakona, a u cilju procjene spremnosti za upravljanje IKT incidentima, identifiovanja slabosti, nedostataka i odstupanja u digitalnoj operativnoj otpornosti i blagovremenog sprovođenja korektivnih mjera, ne uspostavi, ne održava ili redovno ne preispituje program za testiranje digitalne operativne otpornosti (član 27 stav 1);

87) program za testiranje digitalne operativne otpornosti iz člana 27 stav 1 ovog zakona, kao dio okvira za upravljanje IKT rizicima nije efikasan ili sveobuhvatan ili ne sadrži niz procjena, testova, metodologija, praksi i alata koji se sprovode i primjenjuju u skladu sa čl. 28 do 31 ovog zakona (član 27 stav 2);

88) ne sprovodi program za testiranje digitalne operativne otpornosti primjenom pristupa zasnovanog na procjeni rizika, i ne vodi računa o promjenljivom karakteru IKT rizika, konkretnim rizicima kojima je izložen ili bi mogao biti izložen, kritičnosti informacione imovine i usluga, kao i o svim drugim relevantnim faktorima (član 27 stav 3);

89) ne obezbijedi da testiranje digitalne operativne otpornosti iz člana 27 stav 1 ovog zakona sprovode nezavisna interna ili eksterna lica (član 27 stav 4);

90) u slučaju kada testiranje digitalne operativne otpornosti iz člana 27 stav 1 ovog zakona sprovode interna lica ne obezbijedi dovoljne resurse za potrebe tog testiranja ili ne preduzme mjere za izbjegavanje sukoba interesa u fazi osmišljavanja i sprovođenja tog testiranja (član 27 stav 5);

91) ne uspostavi politike i procedure za određivanje prioriteta, klasifikaciju i otklanjanje svih problema otkrivenih tokom testiranja digitalne operativne otpornosti ili ne uspostavi metodologije za internu provjeru radi dobijanja potvrde da su sve identifikovane slabosti, nedostaci i odstupanja u potpunosti otklonjeni (član 27 stav 6);

92) najmanje jednom godišnje ne sprovodi adekvatne testove svih IKT sistema i aplikacija koje podržavaju kritične ili važne funkcije tog finansijskog subjekta (član 27 stav 7);

93) programom za testiranje digitalne operativne otpornosti iz člana 27 stav 1 ovog zakona u skladu sa principom proporcionalnosti iz člana 5 ovog zakona ne obezbijedi sprovođenje odgovarajućih testova propisanih članom 28 stav 1 ovog zakona;

94) kao finansijski subjekt koji je klasifikovan kao mikro finansijski subjekt ne sprovodi testiranja iz člana 28 stav 1 ovog zakona na način propisan članom 28 stav 2 ovog zakona;

95) kao centralno klirinško depozitarno društvo ili kao centralna druga ugovorna stana ne sprovodi procjene ranjivosti prije svake primjene ili ponovne primjene novih ili postojećih aplikacija, infrastrukturnih komponenti i IKT usluga koje podržavaju kritične ili važne funkcije finansijskog subjekta (član 28 stav 3);

96) kao finansijski subjekt iz člana 29 stav 4 ovog zakona ne sprovodi napredno testiranje u formi penetracionog testiranja vođenog prijetnjama najmanje jednom u tri godine (član 29 stav 1);

97) kao finansijski subjekt iz člana 29 stav 4 ovog zakona ne postupi po utvrđenoj obavezi promjene učestalosti naprednog testiranja (član 29 stav 2);

98) kao finansijski subjekt iz člana 29 stav 4 ovog zakona TLPT-om ne obuhvata više kritičnih ili važnih funkcija finansijskog subjekta ili sve takve funkcije, ili TLPT ne sprovodi na produkcionim sistemima koji podržavaju te funkcije (član 29 stav 3);

99) kao finansijski subjekt iz člana 29 stav 4 ovog zakona ne sprovede sve radnje potrebne za planiranje i sprovođenje TLPT-a propisane članom 29 stav 6 ovog zakona;

100) u slučaju kada su treće strane koje pružaju IKT usluge obuhvaćene TLPT-om, ne preduzme neophodne mjere i zaštitne mehanizme u skladu sa kojima se obezbjeđuje učešće tih trećih strana u TLPT-u (član 30 stav 1);

101) u saradnji sa trećim stranama koje pružaju IKT usluge, drugim uključenim stranama i licima koja sprovode testiranje ne primjeni efikasne kontrole upravljanja rizicima radi ublažavanja rizika od mogućih negativnih uticaja na podatke ili oštećenja imovine i poremećaja u obavljanju kritičnih ili važnih funkcija, usluga ili operacija (član 30 stav 6);

102) po završetku TLPT-a, nakon usaglašavanja izvještaja i planova za otklanjanje utvrđenih nedostataka, nadležnom organu, odnosno nadležnom organu kojem su povjereni zadaci u skladu sa članom 29 stav 5 ovog zakona, ne dostavi rezime relevantnih nalaza ili planove za otklanjanje utvrđenih nedostataka ili dokumentaciju kojom se potvrđuje da je TLPT sproveden u skladu sa zahtjevima iz ovog zakona (član 31 stav 1);

103) u slučaju da mu je potvrdu o sprovedenom TLPT-u izdao organ koji nije zadužen za njegov nadzor, ne obavijesti nadležni organ o dobijanju te potvrde, i uz obavještenje ne dostavi rezime relevantnih nalaza ili planove za otklanjanje nedostataka (član 31 stav 5).

104) za svako treće sprovođenje TLPT-a ne angažuje eksterna lica (član 32 stav 2);

105) ne obezbijedi da lica angažovana za sprovođenje TLPT-a ispunjavaju zahtjeve propisane članom 32 stav 3 ovog zakona;

106) u slučaju angažovanja internih lica za sprovođenje TLPT-a, ne obezbijedi da su pored zahtjeva iz člana 32 stav 3 ovog zakona, ispunjeni dodatni zahtjevi propisani članom 32 stav 4 ovog zakona:

107) ugovorom koji je zaključio sa eksternim licem koje sprovodi TLPT ne obezbjedi dobro upravljanje rezultatima TLPT-a i da bilo kakva obrada podataka u vezi sa tim, uključujući generisanje, izradu, agregiranje, skladištenje, izvještavanje, saopštavanje i uništavanje podataka, ne stvara rizike za tog finansijskog subjekta (član 32 stav 5);

108) ne upravlja IKT rizikom povezanim sa trećim stranama kao sastavnim dijelom IKT rizika, u okviru sistema upravljanja IKT rizicima iz člana 10 ovog zakona, u skladu sa principima propisanim članom 33 stav 1 ovog zakona;

109) ne usvoji ili redovno ne preispituje strategiju upravljanja IKT rizikom povezanim sa trećim stranama uzimajući u obzir strategiju IKT nabavke od više dobavljača iz člana 12 stav 3 ovog zakona, kada je to primjenljivo (član 33 stav 2);

110) strategijom upravljanja IKT rizikom povezanim sa trećim stranama iz člana 33 stav 2 ovog zakona ne obuhvati politiku korišćenja IKT usluga koje pružaju treće strane za podršku kritičnih ili važnih funkcija finansijskog subjekta, i ako tu politiku ne primjenjuje na pojedinačnoj i kada je to primjenjivo, na potkonsolidovanoj i konsolidovanoj osnovi (član 33 stav 3);

111) prije zaključivanja ugovora o korišćenju IKT usluga ne sprovede sve procjene, provjere i analize propisane članom 33 stav 5 ovog zakona (član 33 stav 5 i član 37 stav 1);

112) u okviru sistema upravljanja IKT rizicima, na pojedinačnoj, kao i na potkonsolidovanoj i konsolidovanoj osnovi, ne vodi ili ne ažurira registar informacija o svim ugovorima o korišćenju IKT usluga koje pružaju treće strane (član 34 stav 1);

113) informacije o ugovorima iz člana 34 stav 1 ovog zakona nisu evidentirane tako da se ugovori koji se odnose na IKT usluge za podršku kritičnih ili važnih funkcija razlikuju od ugovora koji se ne odnose na te funkcije (član 34 stav 2);

114) nadležnom organu, najmanje jednom godišnje, ne dostavi izvještaj o broju novih ugovora o korišćenju IKT usluga, kategorijama trećih strana koje pružaju IKT usluge, vrsti ugovora i IKT uslugama i funkcijama koje se pružaju (član 34 stav 3);

115) nadležnom organu, na njegov zahtjev, ne stavi na raspolaganje pojedine djelove ili cjelokupan registar informacija iz člana 34 stav 1 ovog zakona, uključujući i druge informacije koje su nadležnom organu potrebne za sprovođenje nadzora (član 34 stav 4);

116) blagovremeno ne obavijesti nadležni organ o svakom planiranom ugovoru u skladu sa kojim namjerava da koristi IKT usluge za podršku kritičnih ili važnih funkcija, kao i o svakoj funkciji koja je podržana ugovorom o korišćenju IKT usluga, a koja postane kritična ili važna funkcija (član 34 stav 5);

117) zaključi ugovor sa trećom stranom koja pruža IKT usluge, koja ne primjenjuje odgovarajuće standarde informacione bezbjednosti (član 35 st. 1 i 2);

118) radi ostvarivanja prava pristupa, sprovođenja provjera i revizija nad trećom stranom koja pruža IKT usluge, nije unaprijed odredio učestalost provjera i revizija, kao i oblasti u kojima će se iste sprovesti u skladu sa opšteprihvaćenim revizorskim standardima i, kada je to primjenljivo, zahtjevima nadležnog organa u pogledu primjene tih standarda (član 35 stav 3);

119) ne provjeri da li revizori, bilo da su interni, eksterni ili grupa revizora, posjeduju odgovarajuće vještine i znanja neophodna za efikasno sprovođenje relevantnih revizija i procjena, u slučaju da ugovor zaključen sa trećom stranom koja pruža IKT usluge iz člana 35 stav 1 ovog zakona obuhvata korišćenje IKT usluga koje podrazumijevaju visok stepen tehničke složenosti (član 35 stav 4);

120) nije obezbijedio da se ugovor o korišćenju IKT usluga može raskinuti u slučajevima propisanim članom 36 stav 1 ovog zakona;

121) nije utvrdio izlazne strategije za IKT usluge koje podržavaju kritične ili važne funkcije (član 36 st. 2 i 3);

122) nije obezbijedio da raskid ugovora sa trećom stranom koja pruža IKT usluge ne dovodi do posljedica propisanih članom 36 stav 4 ovog zakona;

123) ne obezbijedi da su planovi za raskid ugovornih odnosa iz člana 36 stav 1 ovog zakona sveobuhvatni, dokumentovani ili ne obzebijedi da se u skladu sa principom proporcionalnosti iz člana 5 ovog zakona, dovoljno testiraju i periodično preispituju (član 36 stav 5);

124) nije utvrdio alternativna rješenja ili nije razvio tranzicione planove koji mu omogućavaju da, na siguran i cjelovit način, prenese ugovorene IKT usluge i povezane podatke sa treće strane koja pruža IKT usluge na alternativne pružaoce usluga ili ih reintegriše u okviru sopstvenih kapaciteta, kao i da obezbijedi njihovo uklanjanje kod treće strane koja je pružala IKT usluge (član 36 stav 6);

125) nije uspostavio odgovarajuće mjere za nepredviđene situacije radi očuvanja kontinuiteta poslovanja u slučaju nastanka okolnosti iz člana 36 stav 3 ovog zakona (član 36 stav 7);

126) ne procijeni prednosti i troškove alternativnih rješenja kao što je angažman različitih trećih strana koje pružaju IKT usluge, uzimajući u obzir da li i na koji način predviđena rješenja odgovaraju poslovnim potrebama i ciljevama utvrđenim u strategiji digitalne operativne otpornosti tog finansijskog subjekta (član 37 stav 2);

127) u slučaju ugovora o korišćenju IKT usluga kojima se podržavaju kritične ili važne funkcije, koji radi pružanja tih usluga, predviđa mogućnost treće strane koja pruža IKT usluge da kao podizvođače angažuje druge pružaoce IKT usluga, nije procijenio prednosti ili rizike koji mogu proizaći iz tog angažovanja, naročito u slučaju angažovanja IKT podizvođača sa sjedištem u trećoj zemlji (član 37 stav 3);

128) u slučaju ugovora o korišćenju IKT usluga kojima se podržavaju kritične ili važne funkcije, ne razmotri propise koji bi se primjenjivali u slučaju insolventnosti treće strane koja pruža IKT usluge, uključujući stečaj i likvidaciju, kao i sva ograničenja koja bi mogla nastati u slučaju potrebe za hitnim povratkom podataka finansijskog subjekta (član 37 stav 4);

129) u slučaju da se ugovor o korišćenju IKT usluga kojima se podržavaju kritične ili važne funkcije zaključuje sa trećom stranom koja pruža IKT usluge sa sjedištem u trećoj zemlji, pored elemenata iz člana 37 stava 4 ovog zakona, ne razmotri i usklađenost sa odredbama propisa kojima se uređuje zaštita podataka, kao i mogućnost sprovođenja zakona u toj trećoj zemlji (član 37 stav 5);

130) u slučaju da je ugovorom o korišćenju IKT usluga kojima se podržavaju kritične ili važne funkcije predviđena mogućnost angažovanja podizvođača, ne procijeni da li, i na koji način, potencijalno dugi ili složeni lanci podugovaranja mogu uticati na njegovu sposobnost da u potpunosti prati ugovorene funkcije, kao i na mogućnost nadležnog organa da sprovodi efikasan nadzor tog finansijskog subjekta (član 37 stav 6);

131) nije utvrdio prava i obaveze strana u ugovoru (član 38 stav 1);

132) ugovor o pružanju IKT usluga nije dostupan ugovornim stranama u papirnom ili elektronskom obliku koji se može preuzeti u pristupačnom i trajnom formatu, (član 38 stav 2);

133) ugovor o korišćenju IKT usluga ne sadrži elemente propisane članom 38 stav 3 ovog zakona;

134) ugovor o korišćenju IKT usluga kojima se podržavaju kritične ili važne funkcije pored elemenata iz člana 38 stav 3 ovog zakona ne sadrži dodatne elemente propisane članom 38 stav 4 ovog zakona (član 38 st. 4 i 5);

135) bez odlaganja ne obavijesti nadležni organ o svom učešću u sporazumima za razmjenu informacija iz člana 39 stav 1 tačka 3 ovog zakona, odnosno kada prestane sa učešćem u tom sporazumu (član 39 stav 3);

136) kao finansijski subjekt iz člana 2 stav 1 tač. 1 do 4 ovog zakona ne postupi u skladu sa propisom Centralne banke iz člana 48 ovog zakona (član 48 stav 9);

137) kao finansijski subjekt iz člana 2 stav 1 tač. 5 do 14 ovog zakona ne postupi u skladu sa propisom Komisije iz člana 49 ovog zakona (član 49 stav 10);

138) kao finansijski subjekt iz člana 2 stav 1 tač. 15 do 25 ovog zakona ne postupi u skladu sa propisom Agencije iz člana 50 ovog zakona (član 50 stav 9);

139) kao finansijski subjekt iz člana 2 stav 1 tač. 26 i 27 ovog zakona ne postupi u skladu sa propisom koji je nadležni organ iz člana 3 stav 1 tačka 4 ovog zakona donio u skladu sa članom 51 ovog zakona (član 51 stav 2);

140) ne sprovede mjeru koju je nadležni organ izrekao u skladu sa članom 40 st. 5 i 6 ovog zakona na način i u roku utvrđenim rješenjem o izricanju mjere (član 40 stav 7);

141) u potpunost ne sarađuje sa nadležnim organom tokom postupka nadzora ili kontrole i na zahtjev nadležnog organa za potrebe sprovođenja nadzora ili kontrole ne dostavi zahtijevana pisana ili usmena objašnjenja o činjenicama koje se odnose na predmet i svrhu nadzora ili kontrole (član 40 stav 8);

(2) Za prekršaj iz stava 1 ovog člana kazniće se odgovorno lice u pravnom licu novčanom kaznom u iznosu od 2.000 eura do 4.000 eura.

(3) Novčanom kaznom u iznosu od 2.000 eura do 4.000 eura kazniće se za prekršaj član organa upravljanja finansijskog subjekta ako:

1) ne utvrdi, ne odobri ili ne nadzire sva pravila, postupke, procese, mehanizme, mjere i resurse povezane sa sistemom upravljanja IKT rizicima iz člana 10 stav 1 ovog zakona i ne obezbijedi njihovu primjenu, i u tom cilju naročito ne ispuni uslove propisane članom 9 stav 3 ovog zakona;

2) aktivno ne unapređuje znanje i vještine potrebne za razumijevanje i procjenu IKT rizika i njegovog uticaja na poslovanje finansijskog subjekta uključujući i kroz redovne posebne obuke, srazmjerno prirodi rizika kojim se upravlja (član 9 stav 5);

3) ne obezbijedi da viši IKT kadar, najmanje jednom godišnje, podnosi izvještaj organu upravljanja o zaključcima izvedenim iz iskustava, saznanja i informacija iz člana 19 stav 5 ovog zakona, sa predlozima za dalje postupanje (član 19 stav 9);

4) na osnovu procjene ukupnog rizičnog profila finansijskog subjekta, obima i složenosti poslovnih usluga, redovno ne preispituje rizike identifikovane u vezi sa ugovorima o korišćenju IKT usluga kojima se podržavaju kritične ili važne funkcije (član 33 stav 4).

XII. PRELAZNE I ZAVRŠNA ODREDBA

Rok za donošenje propisa

Član 53

Nadležni organi će u roku od 18 mjeseci od dana stupanja na snagu ovog zakona donijeti propise za čije donošenje su ovlašćeni čl. 48 do 51 ovog zakona.

Usklađivanje sa odredbama ovog zakona

Član 54

Finansijski subjekt je dužan da izvrši usklađivanje sa odredbama ovog zakona u roku od 24 mjeseca od dana stupanja na snagu ovog zakona.

Odložena primjena

Član 55

Odredbe člana 23 stav 1 tačka 3, člana 24 stav 11 tač. 1 i 2 i st. 12, 13 i 14, člana 29 stav 4 tačka 2 alineja 2, člana 31 stav 3 tačka 2 i stav 4, člana 32 stav 3 tačka 4, člana 38 stav 4 tačka 5 alineja 4, člana 45 st. 3 do 8 ovog zakona primjenjivaće se od dana pristupanja Crne Gore Evropskoj uniji.

Stupanje na snagu

Član 56

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

Broj: 10-1/26-1/4

EPA 848 XXVIII

Podgorica, 2. februar 2026. godine

Skupština Crne Gore 28. saziva

Predsjednik,

Andrija Mandić, s.r.

∗ U ovaj zakon prenijete su odredbe Regulative (eu) 2022/2554 Evropskog parlamenta i Savjeta od 14. decembra 2022. godine o digitalnoj operativnoj otpornosti za finansijski sektor i izmjeni regulativa (EZ) br. 1060/2009, (EU) br. 648/2012, (EU) br. 600/2014, (EU) br. 909/2014 i (EU) 2016/1011 (tekst od značaja za EEP).