– međunarodne organizacije ili drugi subjekti iz članka 4. podstavaka 4. i 5. ovoga Zakona

– zaklade, zavodi i ustanove koji su osnovani ili čiji je suosnivač Republika Hrvatska za javnu dobrobit ili u dobrotvorne svrhe, pravne osobe s javnim ovlastima te pravne osobe kojima Republika Hrvatska na temelju međunarodnih ugovora priznaje pravnu osobnost u hrvatskom pravnom poretku, sukladno njihovim djelatnostima ili nadležnostima koje su obuhvaćene predmetom ovoga Zakona

– organizacije civilnog društva

– pravne osobe upisane u sudski registar.

Nadležnosti i obveze nositelja provedbe

Članak 11.

(1) Proračunski korisnici, kao nositelji provedbe, vlastitim razvojnim i humanitarnim projektima, programima i drugim aktivnostima pružaju razvojnu suradnju partnerskim zemljama, samostalno ili u suradnji sa subjektima iz članka 10. ovoga Zakona, sukladno svojim nadležnostima, planovima i osiguranim proračunskim sredstvima.

(2) Proračunski korisnici dužni su dostavljati Ministarstvu na njegov zahtjev podatke o korištenju sredstava za pružanje razvojne suradnje u skladu s pravilima Odbora za razvojnu pomoć OECD-a, u svrhu pripreme Izvješća kojeg je Ministarstvo nositelj.

Dodjela sredstava za bilateralnu razvojnu suradnju

Članak 12.

Sredstva za ostvarivanje bilateralne razvojne suradnje dodjeljuju se:

– financijskim doprinosom tijelu državne uprave, jedinici lokalne i područne (regionalne) samouprave, nadležnoj stručnoj službi Vlade Republike Hrvatske, zakladi, zavodu, pravnim osobama iz članka 10. ovoga Zakona, ili drugom nositelju ili sunositelju provedbe u Republici Hrvatskoj, trećoj zemlji ili partnerskoj zemlji, međunarodnoj organizaciji, fondu ili drugoj međunarodnoj instituciji s nadležnostima u provedbi razvojne suradnje, pri čemu se definira ciljna partnerska zemlja ili regija

– ugovaranjem s organizacijama civilnog društva putem javnog poziva u skladu s kriterijima, mjerilima i postupcima financiranja i ugovaranja projekata i programa za korisnike državnog proračuna

– izravnim financijskim doprinosom partnerskim zemljama u obliku proračunskih potpora i drugim financijskim instrumentima iz članka 9. podstavaka 6. i 7. ovoga Zakona, u skladu s uvjetima za odobravanje takvih potpora i instrumenata

– financijskim instrumentima namijenjenima aktivnostima privatnog sektora u projektima i programima razvojne suradnje iz članka 9. podstavka 5. ovoga Zakona, pri čemu se definira svrha i ciljna partnerska zemlja ili regija.

Dodjela sredstava za multilateralnu razvojnu suradnju

Članak 13.

Sredstva za ostvarivanje multilateralne razvojne suradnje dodjeljuju se uplatom doprinosa, članarina ili drugih financijskih uplata putem ili u korist međunarodnih organizacija, institucija, programa i fondova te pravnim osobama iz članka 10. ovoga Zakona, pri čemu nije definirana ciljna partnerska zemlja ili regija.

Uvjeti za dodjelu sredstava

Članak 14.

Sredstva za provedbu bilateralne i multilateralne razvojne suradnje dodjeljuju se u skladu s uvjetima i kriterijima za financiranje ili sufinanciranje projekata i programa razvojne suradnje te aktom strateškog planiranja iz članka 5. ovoga Zakona.

PRIJELAZNE I ZAVRŠNE ODREDBE

Postupci u tijeku i podzakonski akti

Članak 15.

(1) Postupci ugovaranja i provedbe projekata i programa razvojne suradnje koji su započeti prije stupanja na snagu ovoga Zakona dovršit će se po odredbama Zakona o razvojnoj suradnji i humanitarnoj pomoći inozemstvu (»Narodne novine«, br. 146/08.).

(2) Odluku o osnivanju Povjerenstva iz članka 7. ovoga Zakona Vlada Republike Hrvatske donijet će u roku od šest mjeseci od dana stupanja na snagu ovoga Zakona.

Prestanak važenja Zakona

Članak 16.

Danom stupanja na snagu ovoga Zakona prestaje važiti Zakon o razvojnoj suradnji i humanitarnoj pomoći inozemstvu (»Narodne novine«, br. 146/08.).

Stupanje na snagu

Članak 17.

Ovaj Zakon stupa na snagu osmoga dana od dana objave u »Narodnim novinama«.

Klasa: 022-02/23-01/20
Zagreb, 26. siječnja 2024.

HRVATSKI SABOR

Predsjednik
Hrvatskoga sabora
Gordan Jandroković, v. r.

254

Na temelju članka 89. Ustava Republike Hrvatske, donosim

ODLUKU
O PROGLAŠENJU ZAKONA O KIBERNETIČKOJ SIGURNOSTI

Proglašavam Zakon o kibernetičkoj sigurnosti, koji je Hrvatski sabor donio na sjednici 26. siječnja 2024.

Klasa: 011-02/24-02/03
Urbroj: 71-10-01/1-24-2
Zagreb, 1. veljače 2024.

Predsjednik
Republike Hrvatske
Zoran Milanović, v. r.

ZAKON
O KIBERNETIČKOJ SIGURNOSTI

DIO PRVI
OSNOVNE ODREDBE

Cilj i predmet Zakona

Članak 1.

(1) Ovim se Zakonom uređuju postupci i mjere za postizanje visoke zajedničke razine kibernetičke sigurnosti, kriteriji za kate-

gorizaciju ključnih i važnih subjekata, zahtjevi kibernetičke sigurnosti za ključne i važne subjekte, posebni zahtjevi za upravljanje podacima o registraciji naziva domena i kontrola njihove provedbe, dobrovoljni mehanizmi kibernetičke zaštite, nadležna tijela u području kibernetičke sigurnosti i njihove zadaće i ovlasti, stručni nadzor nad provedbom zahtjeva kibernetičke sigurnosti, prekršajne odredbe, praćenje provedbe ovoga Zakona i druga pitanja od značaja za područje kibernetičke sigurnosti.

(2) Ovim se Zakonom uspostavlja okvir strateškog planiranja i odlučivanja u području kibernetičke sigurnosti te utvrđuju nacionalni okviri upravljanja kibernetičkim incidentima velikih razmjera i kibernetičkim krizama.

(3) Postizanje i održavanje visoke zajedničke razine kibernetičke sigurnosti, posebno kroz razvoj i kontinuirano unaprjeđenje politika kibernetičke zaštite i njihove provedbe, razvoj nacionalnih sposobnosti u području kibernetičke sigurnosti, jačanje suradnje i koordinacije svih relevantnih tijela, jačanje suradnje javnog i privatnog sektora, promicanje razvoja, integracije i upotrebe relevantnih naprednih i inovativnih tehnologija, promicanje i razvoj obrazovanja i osposobljavanja u području kibernetičke sigurnosti te razvojne aktivnosti usmjerene na jačanje svijesti o kibernetičkoj sigurnosti od nacionalnog su značaja za Republiku Hrvatsku.

(4) Cilj je ovoga Zakona uspostavljanje sustava upravljanja kibernetičkom sigurnošću koji će osigurati djelotvornu provedbu postupaka i mjera za postizanje visoke razine kibernetičke sigurnosti u sektorima od posebne važnosti za nesmetano obavljanje ključnih društvenih i gospodarskih aktivnosti i pravilno funkcioniranje unutarnjeg tržišta.

Popis priloga koji su sastavni dio Zakona

Članak 2.

Sastavni su dio ovoga Zakona:

– Prilog I. Sektori visoke kritičnosti (u daljnjem tekstu: Prilog I. ovoga Zakona)

– Prilog II. Drugi kritični sektori (u daljnjem tekstu: Prilog II. ovoga Zakona)

– Prilog III. Popis nadležnosti u području kibernetičke sigurnosti (u daljnjem tekstu: Prilog III. ovoga Zakona) i

– Prilog IV. Obvezni sadržaj nacionalnog akta strateškog planiranja iz područja kibernetičke sigurnosti (u daljnjem tekstu: Prilog IV. ovoga Zakona).

Usklađivanje propisa s pravnim aktima Europske unije

Članak 3.

Ovim se Zakonom u hrvatsko zakonodavstvo preuzima Direktiva (EU) 2022/2555 Europskog parlamenta i Vijeća od 14. prosinca 2022. o mjerama za visoku zajedničku razinu kibernetičke sigurnosti širom Unije, izmjeni Uredbe (EU) br. 910/2014 i Direktive (EU) 2018/1972 i stavljanju izvan snage Direktive (EU) 2016/1148 (Direktiva NIS2) (SL L 333/80, 27. 12. 2022.).

Pojmovi

Članak 4.

(1) U smislu ovoga Zakona pojedini pojmovi imaju sljedeće značenje:

1. *aktivna kibernetička zaštita* je zaštita koja uvodi napredni pristup koji umjesto reaktivnog odgovora na incidente, podrazumijeva njihovu prevenciju odnosno aktivno sprječavanje, otkrivanje, praćenje, analizu i ublažavanje povreda sigurnosti mrežnih i informacijskih sustava, u kombinaciji s upotrebom kapaciteta koji se primjenjuju unutar i izvan mrežnog i informacijskog sustava koji je cilj kibernetičkog napada

2. *CSIRT* je kratica za Computer Security Incident Response Team, odnosno nadležno tijelo za prevenciju i zaštitu od kibernetičkih incidenata, za koju se koristi i kratica CERT (Computer Emergency Response Team)

3. *CSIRT mreža* je mreža nacionalnih CSIRT-ova osnovana u svrhu razvoja povjerenja i pouzdanja te promicanja brze i učinkovite operativne suradnje među državama članicama Europske unije (u daljnjem tekstu: države članice), koju uz predstavnike nacionalnih CSIRT-ova čine i predstavnici nadležnog tijela za prevenciju i zaštitu od kibernetičkih incidenata Europske unije (CERT-EU)

4. *digitalna usluga* je svaka usluga informacijskog društva odnosno svaka usluga koja se uobičajeno pruža uz naknadu, na daljinu, elektroničkim sredstvima te na osobni zahtjev primatelja usluge, gdje u smislu ovoga pojma:

a) »na daljinu« znači da se usluga pruža, a da strane nisu istodobno prisutne

b) »elektroničkim sredstvima« znači da se usluga od početka šalje i na odredištu prima putem elektroničke opreme za obradu, uključujući digitalno sažimanje i pohranjivanje podataka, te da se u cjelini šalje, prenosi i prima žičanim, radijskim, svjetlosnim ili drugim elektromagnetskim sustavom

c) »na osobni zahtjev primatelja usluge« znači da se usluga pruža prijenosom podataka na osobni zahtjev

5. *elektronička komunikacijska usluga* je usluga koja se uobičajeno pruža uz naknadu putem elektroničkih komunikacijskih mreža, a obuhvaća, uz iznimku usluga pružanja sadržaja ili obavljanja uredničkog nadzora nad sadržajem koji se prenosi uporabom elektroničkih komunikacijskih mreža i usluga, sljedeće vrste usluga:

a) »uslugu pristupa internetu« odnosno javno dostupnu elektroničku komunikacijsku uslugu kojom se omogućuje pristup internetu te time povezivanje s gotovo svim krajnjim točkama interneta, bez obzira na mrežnu tehnologiju i terminalnu opremu koja se upotrebljava

b) »interpersonalnu komunikacijsku uslugu« odnosno uslugu koja se, u pravilu, pruža uz naknadu, a omogućuje izravnu interpersonalnu i interaktivnu razmjenu obavijesti putem elektroničkih komunikacijskih mreža između ograničenog broja osoba, pri čemu osobe koje pokreću komunikaciju ili sudjeluju u njoj određuju njezina primatelja ili više njih. Ova usluga ne obuhvaća usluge koje omogućuju interpersonalnu i interaktivnu komunikaciju samo kao manje bitnu pomoćnu značajku koja je suštinski povezana s drugom uslugom i

c) usluge koje se sastoje, u cijelosti ili većim dijelom, od prijenosa signala, kao što su usluge prijenosa koje se upotrebljavaju za pružanje usluga komunikacije između strojeva i za radiodifuziju

6. *EU-CyCLONe mreža* je Europska mreža organizacija za vezu za kibernetičke krize osnovana s ciljem djelovanja na operativnoj razini kao posrednik između tehničke razine (CSIRT mreže) i političke razine, a u svrhu stvaranja učinkovitog procesa operativnog procjenjivanja i upravljanja tijekom kibernetičkih incidenata velikih razmjera i kibernetičkih kriza, kao i podupiranja procesa donošenja odluka o složenim kibernetičkim pitanjima na političkoj razini

7. *IKT* je informacijsko-komunikacijska tehnologija

8. *IKT proces* je IKT proces kako je definiran u članku 2. točki 14. Uredbe (EU) 2019/881 Europskog parlamenta i Vijeća od 17. travnja 2019. o ENISA-i (Agencija Europske unije za kibernetičku sigurnost) te o kibernetičkoj sigurnosnoj certifikaciji u području informacijske i komunikacijske tehnologije i stavljanju izvan snage Uredbe (EU) br. 526/2013 (Akt o kibernetičkoj sigurnosti) (Tekst značajan za EGP) (SL L 151/15, 7. 6. 2019.) (u daljnjem tekstu: Uredba (EU) 2019/881)

9. *IKT proizvod* je IKT proizvod kako je definiran u članku 2. točki 12. Uredbe (EU) 2019/881

10. *IKT usluga* je IKT usluga kako je definirana u članku 2. točki 13. Uredbe (EU) 2019/881

11. *incident* je događaj koji ugrožava dostupnost, autentičnost, cjelovitost ili povjerljivost pohranjenih, prenesenih ili obrađenih podataka ili usluga koje mrežni i informacijski sustavi nude ili kojima omogućuju pristup

12. *internetska tražilica* je internetska tražilica kako je definirana u članku 2. točki 5. Uredbe (EU) 2019/1150 Europskog parlamenta i Vijeća od 20. lipnja 2019. o promicanju pravednosti i transparentnosti za poslovne korisnike usluga internetskog posredovanja (SL L 186, 11. 7. 2019.)

13. *internetsko tržište* je digitalna usluga kojom se upotrebom softvera, uključujući mrežne stranice, dio mrežnih stranica ili aplikacija kojima upravlja trgovac ili kojima se upravlja u njegovo ime potrošačima omogućuje sklapanje ugovora na daljinu s drugim trgovcima ili potrošačima

14. *istraživačka organizacija* je subjekt čiji je primarni cilj provođenje primijenjenog istraživanja ili eksperimentalnog razvoja radi iskorištavanja rezultata tog istraživanja u komercijalne svrhe, ali koji ne uključuje obrazovne ustanove

15. *izbjegnuti incident* je svaki događaj koji je mogao ugroziti dostupnost, autentičnost, cjelovitost ili povjerljivost pohranjenih, prenesenih ili obrađenih podataka ili usluga koje mrežni i informacijski sustavi nude ili kojima omogućuju pristup, ali je uspješno spriječen ili se nije ostvario

16. *javna elektronička komunikacijska mreža* je elektronička komunikacijska mreža koja se u cijelosti ili većim dijelom upotrebljava za pružanje javno dostupnih elektroničkih komunikacijskih usluga koje podržavaju prijenos podataka među završnim točkama mreže

17. *javni subjekti* su pravne osobe čiji je osnivač Republika Hrvatska ili jedinica lokalne ili područne (regionalne) samouprave, pravne osobe koje obavljaju javnu službu, pravne osobe koje se na temelju posebnog propisa financiraju pretežito ili u cijelosti iz državnog proračuna ili iz proračuna jedinica lokalne i područne (regionalne) samouprave odnosno iz javnih sredstava i trgovačka društva u kojima Republika Hrvatska i jedinice lokalne i područne (regionalne) samouprave imaju zasebno ili zajedno većinsko vlasništvo, ne uključujući Hrvatsku narodnu banku

18. *jedinstvena kontaktna točka* je nacionalna kontaktna točka odgovorna za nacionalnu koordinaciju i suradnju s drugim državama članicama u pitanjima sigurnosti mrežnih i informacijskih sustava

19. *kibernetička prijetnja* je kibernetička prijetnja kako je definirana u članku 2. točki 8. Uredbe (EU) 2019/881

20. *kibernetički sigurnosni incident velikih razmjera* je incident na razini Europske unije koji uzrokuje poremećaje koji premašuju sposobnost jedne države članice za odgovor na incident ili koji ima znatan učinak na najmanje dvije države članice, kao i incident na nacionalnoj razini koji uzrokuje poremećaje koji premašuju sposobnost sektorskog CSIRT tijela za odgovor na incident ili koji ima znatan učinak na najmanje dva sektora te se u takvim slučajevima pokreću procedure upravljanja kibernetičkim krizama, usklađene s postojećim nacionalnim općim okvirom upravljanja krizama i okvirom za upravljanje kibernetičkim krizama Europske unije

21. *kibernetička sigurnost* je kibernetička sigurnost kako je definirana u članku 2. točki 1. Uredbe (EU) 2019/881

22. *kvalificirani pružatelj usluga povjerenja* je kvalificirani pružatelj usluga povjerenja kako je definiran u članku 3. točki 20. Uredbe (EU) br. 910/2014 o elektroničkoj identifikaciji i uslugama povjerenja za elektroničke transakcije na unutarnjem tržištu i stavljanju izvan snage Direktive 1999/93/EZ (SL L 257/73 28. 8. 2014. – u daljnjem tekstu: Uredba (EU) br. 910/2014)

23. *kvalificirana usluga povjerenja* je kvalificirana usluga povjerenja kako je definirana u članku 3. točki 17. Uredbe (EU) br. 910/2014

24. *mreža za isporuku sadržaja* je mreža zemljopisno raspoređenih poslužitelja u svrhu osiguravanja visoke dostupnosti, pristupačnosti ili brze isporuke digitalnog sadržaja i usluga korisnicima interneta u ime pružatelja sadržaja i usluga

25. *mrežni i informacijski sustav* čine:

a) »elektronička komunikacijska mreža« odnosno prijenosni sustavi koji se temelje na stalnoj infrastrukturi ili centraliziranom upravljačkom kapacitetu i, ako je primjenjivo, oprema za prospajanje (komutaciju) ili usmjeravanje i druga sredstva, uključujući dijelove mreže koji nisu aktivni, a koji omogućuju prijenos signala žičanim, radijskim, svjetlosnim ili drugim elektromagnetskim sustavom, što obuhvaća satelitske mreže, nepokretne zemaljske mreže (s prospajanjem kanala i prospajanjem paketa, uključujući internet), zemaljske mreže pokretnih komunikacija, elektroenergetske kabelske sustave u mjeri u kojoj se upotrebljavaju za prijenos signala, radiodifuzijske mreže i mreže kabelske televizije, bez obzira na vrstu podataka koji se prenose

b) svaki uređaj ili skupina povezanih ili srodnih uređaja od kojih jedan ili više njih programski izvršava automatsku obradu digitalnih podataka ili

c) digitalni podaci koji se pohranjuju, obrađuju, dobivaju ili prenose elementima opisanima u podtočkama a) i b) ove točke, u svrhu njihova rada, uporabe, zaštite i održavanja

26. *nacionalni akt strateškog planiranja iz područja kibernetičke sigurnosti* je sveobuhvatan okvir kojim se definiraju posebni ciljevi i prioriteti u području kibernetičke sigurnosti i upravljanje za njihovo postizanje

27. *nadležna tijela za provedbu posebnih zakona* su Hrvatska narodna banka, Hrvatska agencija za nadzor financijskih usluga i Hrvatska agencija za civilno zrakoplovstvo

28. *nadležna tijela za provedbu zahtjeva kibernetičke sigurnosti* su središnje državno tijelo za kibernetičku sigurnost, središnje državno tijelo za informacijsku sigurnost, regulatorno tijelo za mrežne djelatnosti, tijelo državne uprave nadležno za razvoj digitalnog društva i tijelo državne uprave nadležno za znanost i obrazovanje

29. *nadležni CSIRT* je CSIRT pri središnjem državnom tijelu za kibernetičku sigurnost ili CSIRT pri Hrvatskoj akademskoj i istraživačkoj mreži – CARNET (u daljnjem tekstu: CARNET), ovisno o podjeli nadležnosti utvrđenoj ovim Zakonom

30. *norma* je norma kako je definirana u članku 2. točki 1. Uredbe (EU) br. 1025/2012 Europskog parlamenta i Vijeća o europskoj normizaciji, o izmjeni direktiva Vijeća 89/686/EEZ i 93/15/EEZ i direktiva 94/9/EZ, 94/25/EZ, 95/16/EZ, 97/23/EZ, 98/34/EZ, 2004/22/EZ, 2007/23/EZ, 2009/23/EZ i 2009/105/EZ Europskog parlamenta i Vijeća te o stavljanju izvan snage Odluke Vijeća 87/95/EEZ i Odluke br. 1673/ 2006/EZ Europskog parlamenta i Vijeća (SL L 316, 14. 11. 2012. – u daljnjem tekstu: Uredba (EU) br. 1025/2012)

31. *osobni podaci* su svi podaci kako su definirani člankom 4. stavkom 1. točkom 1. Uredbe (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (Opća uredba o zaštiti podataka) (SL L 119/1, 4. svibnja 2016.) (u daljnjem tekstu: Uredba (EU) 2016/679), a osobito informacije potrebne za identifikaciju korisnika domena i kontaktnih točaka koje upravljaju nazivima domena, kao i IP adrese (adresa internet protokola koja se koristi na svakom uređaju spojenom na internet), jedinstveni lokatori resursa (URL-ovi), nazivi domena, adrese e-pošte, vremenski žigovi i druge informacije koje u određenim slučajevima, u okviru aktivnosti koje se provode na temelju ovoga Zakona, mogu otkrivati osobne podatke

32. *ozbiljna kibernetička prijetnja* je kibernetička prijetnja za koju se na temelju njezinih tehničkih obilježja može pretpostaviti da može imati ozbiljan učinak na mrežne i informacijske sustave nekog subjekta ili korisnike usluga subjekta, uzrokovanjem znatne materijalne ili nematerijalne štete odnosno prekida usluga korisnicima

33. *platforma za usluge društvenih mreža* je platforma koja krajnjim korisnicima omogućuje međusobno povezivanje, dijeljenje i otkrivanje sadržaja te komuniciranje na više uređaja, posebno preko razgovora, objava, videozapisa i preporuka

34. *postupanje s incidentom* su sve radnje i postupci čiji je cilj sprečavanje, otkrivanje, analiza, zaustavljanje incidenta ili odgovor na njega te oporavak od incidenta

35. *predstavnik* je fizička ili pravna osoba koja ima poslovni nastan u Europskoj uniji koju su pružatelj usluga sustava naziva domena (u daljnjem tekstu: pružatelj usluga DNS-a), registar naziva vršne nacionalne internetske domene, registrar, pružatelj usluga računalstva u oblaku, pružatelj usluga podatkovnog centra, pružatelj mreža za isporuku sadržaja, pružatelj upravljanih usluga, pružatelj upravljanih sigurnosnih usluga, ili pružatelj internetskog tržišta, pružatelj internetske tražilice ili pružatelj platforme za usluge društvenih mreža koji nema poslovni nastan u Europskoj uniji izričito imenovali da djeluje u njihovo ime i kojoj se nadležno tijelo ili CSIRT mogu obratiti umjesto samom subjektu u pogledu obveza tog subjekta na temelju ovoga Zakona

36. *privatni subjekti* su fizičke ili pravne osobe osnovane i priznate kao takve na temelju nacionalnog prava mjesta svojeg poslovnog nastana koje mogu, djelujući u vlastito ime, ostvarivati prava i preuzimati obveze

37. *pružatelj upravljanih sigurnosnih usluga* je pružatelj upravljanih usluga koji provodi ili pruža pomoć za aktivnosti povezane s upravljanjem kibernetičkim sigurnosnim rizicima

38. *pružatelj upravljanih usluga* je subjekt koji pruža usluge povezane s instalacijom, upravljanjem, radom ili održavanjem IKT proizvoda, mreža, infrastrukture, aplikacija ili bilo kojih drugih mrežnih i informacijskih sustava, u obliku pomoći ili aktivnog upravljanja koje se provodi u prostorima klijenata ili na daljinu

39. *pružatelj usluga DNS-a* je subjekt koji pruža:

a) javno dostupne rekurzivne usluge razlučivanja naziva domena krajnjim korisnicima interneta i/ili

b) mjerodavne usluge razlučivanja naziva domena za upotrebu trećih strana, uz iznimku korijenskih poslužitelja naziva

40. *pružatelj usluga povjerenja* je pružatelj usluga povjerenja kako je definiran u članku 3. točki 19. Uredbe (EU) br. 910/2014

41. *ranjivost* je slabost, osjetljivost ili nedostatak IKT proizvoda ili IKT usluga koje kibernetička prijetnja može iskoristiti

42. *registar naziva vršne nacionalne internetske domene* je subjekt kojem je delegirana određena vršna internetska domena i koji je odgovoran za upravljanje njome, uključujući registraciju naziva domena u okviru vršne domene i tehničko upravljanje vršnom domenom, uključujući upravljanje njezinim poslužiteljima naziva, održavanje njezinih baza podataka i distribuciju datoteka iz zone vršne domene u poslužitelje naziva, neovisno o tome obavlja li sam subjekt bilo koju od tih operacija ili za njihovo obavljanje koriste vanjskog davatelja usluge, ali su isključene situacije u kojima registar koristi nazive vršnih domena samo za vlastitu upotrebu. U Republici Hrvatskoj to je CARNET

43. *registrar* je subjekt koji pruža usluge registracije naziva domena odnosno pravna ili fizička osoba koja obavlja samostalnu djelatnost ovlaštena za registraciju i administraciju.hr domena u ime registra naziva vršne nacionalne internetske domene

44. *regulatorno tijelo za mrežne djelatnosti* je Hrvatska regulatorna agencija za mrežne djelatnosti

45. *rizik* je mogućnost gubitka ili poremećaja uzrokovana incidentom koji se izražava kao kombinacija opsega takvog gubitka ili poremećaja i vjerojatnosti pojave tog incidenta

46. *sigurnost mrežnih i informacijskih sustava* je sposobnost mrežnih i informacijskih sustava da na određenoj razini pouzdanosti odolijevaju svim događajima koji mogu ugroziti dostupnost, autentičnost, cjelovitost ili povjerljivost pohranjenih, prenesenih ili obrađenih podataka ili usluga koje ti mrežni i informacijski sustavi nude ili kojima omogućuju pristup

47. *sistemski rizik* je rizik od poremećaja u funkcioniranju usluge odnosno u obavljanju djelatnosti koji bi mogao imati ozbiljne negativne posljedice za jedan ili više sektora ili bi mogao imati prekogranični učinak

48. *Skupina za suradnju* je skupina osnovana u svrhu podupiranja i olakšavanja strateške suradnje i razmjene informacija među državama članicama te razvijanja povjerenja i sigurnosti na razini Europske unije u području kibernetičke sigurnosti

49. *središnje državno tijelo za informacijsku sigurnost* je Ured Vijeća za nacionalnu sigurnost

50. *središnje državno tijelo za kibernetičku sigurnost* je Sigurnosno-obavještajna agencija

51. *središnje državno tijelo za obavljanje poslova u tehničkim područjima informacijske sigurnosti* je Zavod za sigurnost informacijskih sustava

52. *središte za razmjenu internetskog prometa* je mrežni instrument koji omogućuje međupovezivanje više od dviju neovisnih mreža (autonomnih sustava), prije svega u svrhu olakšavanja razmjene internetskog prometa, koji omogućuje međupovezivanje samo za autonomne sustave i za koji nije potrebno da internetski promet između bilo kojih dvaju autonomnih sustava sudionika prođe kroz bilo koji treći autonomni sustav te koji takav promet ne mijenja i ne utječe na njega ni na koji drugi način

53. *subjekt* je svaki javni subjekt, privatni subjekt i subjekt javnog sektora

54. *subjekti javnog sektora* su tijela državne uprave, druga državna tijela, pravne osobe s javnim ovlastima, jedinice lokalne i područne (regionalne) samouprave, kao i privatni i javni subjekti za koje se provodi kategorizacija na temelju ovoga Zakona zbog njihove uloge u upravljanju, razvijanju ili održavanju državne informacijske infrastrukture

55. *sustav naziva domena* ili *DNS* je hijerarhijsko raspoređeni sustav imenovanja koji omogućuje utvrđivanje internetskih usluga i resursa, čime se krajnjim korisnicima uređaja omogućuje korištenje internetskim uslugama usmjeravanja i povezivosti za pristupanje tim uslugama i resursima

56. *sustav obrazovanja* obuhvaća rani i predškolski odgoj i obrazovanje, osnovno obrazovanje, srednje obrazovanje i visoko obrazovanje, praćenje, vrednovanje i razvoj sustava te provedbu programa

57. *tehnička specifikacija* je tehnička specifikacija kako je definirana u članku 2. točki 4. Uredbe (EU) br. 1025/2012

58. *tijelo državne uprave nadležno za razvoj digitalnog društva* je Središnji državni ured za razvoj digitalnog društva

59. *tijelo državne uprave nadležno za znanost i obrazovanje* je Ministarstvo znanosti i obrazovanja

60. *tijelo nadležno za zaštitu osobnih podataka* je Agencija za zaštitu osobnih podataka ili drugo nadzorno tijelo iz članaka 55. i 56. Uredbe (EU) 2016/679

61. *treća strana pružatelj IKT usluga* je pružatelj IKT usluga kako je definiran u članku 3. točki 19. Uredbe (EU) 2022/2554 Europskog parlamenta i Vijeća od 14. prosinca 2022. o digitalnoj operativnoj otpornosti za financijski sektor i o izmjeni uredbi (EZ) br.

1060/2009, (EU) br. 648/2012, (EU) br. 600/2014, (EU) br. 909/2014 i (EU) 2016/1011 (SL L 333/1 27. 12. 2022. – u daljnjem tekstu: Uredba (EU) 2022/2554)

62. *upravljačko tijelo ključnog i važnog subjekta* je tijelo ili tijela imenovana u skladu sa zakonom kojim se uređuje osnivanje i poslovanje subjekta, a koja raspolažu ovlastima za upravljanje i vođenje poslova subjekta

63. *usluga podatkovnog centra* je usluga koja uključuje strukture ili skupine struktura namijenjenih centraliziranom smještaju, međupovezivanju i radu opreme informacijske tehnologije i mreža za usluge pohrane, obrade i prijenosa podataka, uključujući sve objekte i infrastrukturu za distribuciju električne energije i kontrolu okoliša

64. *usluga povjerenja* je usluga povjerenja kako je definirana u članku 3. točki 16. Uredbe (EU) br. 910/2014

65. *usluga računalstva u oblaku* je digitalna usluga koja omogućuje administraciju na zahtjev i širok daljinski pristup nadogradivom i elastičnom skupu djeljivih računalnih resursa, među ostalim kad su takvi resursi raspoređeni na nekoliko lokacija

66. *zaposlenik subjekta* je fizička osoba koja u radnom odnosu obavlja određene poslove za subjekt, uključujući fizičku osobu koja je, prema propisu o trgovačkim društvima, kao član uprave ili izvršni direktor ili fizička osoba koja je u drugom svojstvu prema posebnom zakonu, pojedinačno i samostalno ili zajedno i skupno, ovlaštena voditi poslove subjekta, ili fizičku osobu koja kao radnik u radnom odnosu obavlja određene poslove za subjekt.

(2) Izrazi koji se koriste u ovome Zakonu, a imaju rodno značenje odnose se jednako na muški i ženski rod.

Primjena posebnih propisa o zaštiti tajnosti i povjerljivosti podataka

Članak 5.

(1) Ako u provedbi ovoga Zakona nastaju ili se koriste klasificirani podaci ili drugi podaci za koje su posebnim propisima utvrđena pravila postupanja radi zaštite njihove tajnosti ili povjerljivosti, na takve podatke primjenjuju se posebni propisi o njihovoj zaštiti.

(2) Ovaj se Zakon ne primjenjuje na informacijske sustave sigurnosno akreditirane za postupanje s klasificiranim podacima.

Primjena pravila o zaštiti osobnih podataka

Članak 6.

(1) Primjena odredaba ovoga Zakona ne utječe na obveze pružatelja javnih elektroničkih komunikacijskih mreža ili pružatelje javno dostupnih elektroničkih komunikacijskih usluga da obrađuju osobne podatke sukladno posebnim propisima o zaštiti osobnih podataka i zaštiti privatnosti.

(2) Primjena odredaba ovoga Zakona ne utječe na obveze ključnih i važnih subjekata da u slučaju povrede osobnih podataka postupaju sukladno odredbama članaka 33. i 34. Uredbe (EU) 2016/679.

Odnos sa zakonom kojim se uređuje područje elektroničkih komunikacija

Članak 7.

(1) Primjena odredaba ovoga Zakona ne utječe na obvezu provedbe temeljnih zahtjeva za elektroničku komunikacijsku infrastrukturu i drugu povezanu opremu propisanih zakonom kojim je uređeno područje elektroničkih komunikacija.

(2) Primjena odredaba ovoga Zakona ne utječe na pravila upravljanja vršnom nacionalnom internetskom domenom te prava i obveze korisnika domena propisanih zakonom kojim je uređeno područje elektroničkih komunikacija.

Primjena posebnih zakona u pitanjima kibernetičke sigurnosti

Članak 8.

(1) Ako su za ključne i važne subjekte iz pojedinih sektora iz Priloga I. i Priloga II. ovoga Zakona posebnim zakonima propisani zahtjevi koji po svom sadržaju i svrsi odgovaraju zahtjevima kibernetičke sigurnosti iz ovoga Zakona, ili predstavljaju strože zahtjeve, na te se subjekte primjenjuju odgovarajuće odredbe tog posebnog zakona u onim pitanjima koja su vezano uz te zahtjeve i njihovu provedbu tim propisima uređena, uključujući odredbe o nadzoru nad provedbom zahtjeva.

(2) Zahtjevi iz stavka 1. ovoga članka po svom sadržaju i svrsi odgovaraju zahtjevima kibernetičke sigurnosti iz ovoga Zakona ako:

– su po svom učinku barem jednakovrijedni mjerama upravljanja kibernetičkim sigurnosnim rizicima utvrđenim ovim Zakonom

– je posebnim zakonom utvrđen neposredan, po potrebi i automatski i izravan pristup obavijestima o incidentima nadležnom CSIRT-u te ako su obveze obavještavanja o značajnim incidentima iz posebnog zakona po učinku barem jednakovrijedne obvezama obavještavanja o značajnim incidentima utvrđenim ovim Zakonom.

(3) Tijela koja su prema posebnim zakonima iz stavka 1. ovoga članka nadležna za sektor odnosno podsektor i/ili subjekt iz Priloga I. i Priloga II. ovoga Zakona i nadležna tijela za provedbu zahtjeva kibernetičke sigurnosti dužna su prilikom primjene stavaka 1. i 2. ovoga članka međusobno surađivati i razmjenjivati relevantne informacije te voditi računa o smjernicama Europske komisije kojima se objašnjava primjena povezanog mjerodavnog prava Europske unije.

DIO DRUGI
KATEGORIZACIJA SUBJEKATA

POGLAVLJE I.
KRITERIJI ZA PROVEDBU KATEGORIZACIJE SUBJEKATA

Opći kriteriji za provedbu kategorizacije ključnih subjekata

Članak 9.

U kategoriju ključnih subjekata razvrstavaju se:

– privatni i javni subjekti iz Priloga I. ovoga Zakona koji prelaze gornje granice za srednje subjekte maloga gospodarstva utvrđene zakonom kojim se uređuju osnove za primjenu poticajnih mjera gospodarske politike usmjerenih razvoju, restrukturiranju i tržišnom prilagođavanju maloga gospodarstva

– kvalificirani pružatelji usluga povjerenja, registar naziva vršne nacionalne internetske domene te pružatelji usluga DNS-a, neovisno o njihovoj veličini

– pružatelji javnih elektroničkih komunikacijskih mreža ili javno dostupnih elektroničkih komunikacijskih usluga koji predstavljaju srednji subjekt maloga gospodarstva na temelju zakona kojim se uređuju osnove za primjenu poticajnih mjera gospodarske politike usmjerenih razvoju, restrukturiranju i tržišnom prilagođavanju maloga gospodarstva ili koji prelaze gornje granice za srednje subjekte maloga gospodarstva

– informacijski posrednici u razmjeni elektroničkog računa među poduzetnicima, neovisno o njihovoj veličini i

– subjekti koji su utvrđeni kao kritični subjekti na temelju zakona kojim se uređuje područje kritične infrastrukture, neovisno o njihovoj veličini.

Opći kriteriji za provedbu kategorizacije važnih subjekata

Članak 10.

U kategoriju važnih subjekata razvrstavaju se:

– privatni i javni subjekti iz Priloga II. ovoga Zakona koji predstavljaju srednji subjekt maloga gospodarstva na temelju zakona kojim se uređuju osnove za primjenu poticajnih mjera gospodarske politike usmjerenih razvoju, restrukturiranju i tržišnom prilagođavanju maloga gospodarstva ili koji prelaze gornje granice za srednje subjekte maloga gospodarstva

– privatni i javni subjekti iz Priloga I. ovoga Zakona koji nisu utvrđeni kao ključni subjekti na temelju članka 9. podstavka 1. ovoga Zakona, a predstavljaju srednji subjekt maloga gospodarstva na temelju zakona kojim se uređuju osnove za primjenu poticajnih mjera gospodarske politike usmjerenih razvoju, restrukturiranju i tržišnom prilagođavanju maloga gospodarstva

– pružatelji usluga povjerenja koji nisu kategorizirani kao ključni subjekti na temelju članka 9. podstavka 2. ovoga Zakona, neovisno o njihovoj veličini, i

– pružatelji javnih elektroničkih komunikacijskih mreža ili javno dostupnih elektroničkih komunikacijskih usluga koji nisu kategorizirani kao ključni subjekti na temelju članka 9. podstavka 3. ovoga Zakona, neovisno o njihovoj veličini.

Posebni kriteriji za provedbu kategorizacije ključnih i važnih subjekata

Članak 11.

Iznimno od članka 9. podstavka 1. i članka 10. podstavaka 1. i 2. ovoga Zakona, privatni i javni subjekti iz Priloga I. i Priloga II. ovoga Zakona mogu se razvrstati u kategoriju ključnih ili važnih subjekata, neovisno o njihovoj veličini, ako:

– je subjekt jedini pružatelj usluge koja je ključna za održavanje ključnih društvenih ili gospodarskih djelatnosti

– bi poremećaj u funkcioniranju usluge koju pruža subjekt odnosno poremećaj u obavljanju djelatnosti subjekta mogao imati znatan učinak na javnu sigurnost, javnu zaštitu ili javno zdravlje

– bi poremećaj u funkcioniranju usluge koju pruža subjekt odnosno poremećaj u obavljanju djelatnosti subjekta mogao uzrokovati znatne sistemske rizike u sektorima iz Priloga I. i Priloga II. ovoga Zakona, posebno u sektorima u kojima bi takav poremećaj mogao imati prekogranični učinak ili

– je subjekt značajan zbog svoje posebne važnosti na nacionalnoj, regionalnoj ili lokalnoj razini za određeni sektor ili vrstu usluge ili za druge međuovisne sektore u Republici Hrvatskoj.

Kategorizacija subjekata javnog sektora

Članak 12.

(1) U kategoriju ključnih subjekata razvrstavaju se, neovisno o njihovoj veličini:

– tijela državne uprave i

– druga državna tijela i pravne osobe s javnim ovlastima, ovisno o rezultatima provedene procjene njihove važnosti za nesmetano obavljanje ključnih društvenih ili gospodarskih djelatnosti.

(2) Iznimno od članka 9. podstavka 1. i članka 10. podstavka 2. ovoga Zakona, privatni i javni subjekti koji upravljaju, razvijaju ili održavaju državnu informacijsku infrastrukturu sukladno zakonu kojim se uređuje državna informacijska infrastruktura razvrstavaju se u kategoriju ključnih subjekata, neovisno o njihovoj veličini.

(3) Jedinice lokalne i područne (regionalne) samouprave razvrstavaju se, neovisno o njihovoj veličini, u kategoriju važnih subjekata, ovisno o rezultatima provedene procjene njihove važnosti za nesmetano obavljanje ključnih društvenih ili gospodarskih djelatnosti.

Kategorizacija subjekata iz sustava obrazovanja

Članak 13.

Iznimno od članka 10. podstavka 1. ovoga Zakona, privatni i javni subjekti iz sustava obrazovanja razvrstavaju se, neovisno o njihovoj veličini, u kategoriju važnih subjekata, ovisno o rezultatima provedene procjene njihove posebne važnosti na nacionalnoj ili regionalnoj razini za obavljanje odgojnog odnosno obrazovnog rada.

Određivanje nadležnosti na temelju teritorijalnosti

Članak 14.

(1) Subjekti iz Priloga I. i Priloga II. ovoga Zakona podliježu nadležnostima i ovlastima propisanim ovim Zakonom ako pružaju usluge odnosno obavljaju djelatnosti na području Europske unije, a imaju poslovni nastan na teritoriju Republike Hrvatske.

(2) Iznimno od stavka 1. ovoga članka, pružatelji javnih elektroničkih komunikacijskih mreža ili javno dostupnih elektroničkih komunikacijskih usluga podliježu nadležnostima i ovlastima propisanim ovim Zakonom ako svoje usluge pružaju na teritoriju Republike Hrvatske, neovisno o državi poslovnog nastana.

(3) Iznimno od stavka 1. ovoga članka, pružatelji usluga DNS-a, registar naziva vršne nacionalne internetske domene i registri, pružatelji usluga računalstva u oblaku, pružatelji usluga podatkovnog centra, pružatelji mreža za isporuku sadržaja, pružatelji upravljanih usluga, pružatelji upravljanih sigurnosnih usluga, pružatelji internetskih tržišta, pružatelji internetskih tražilica ili pružatelji platformi za usluge društvenih mreža podliježu nadležnostima i ovlastima propisanim ovim Zakonom ako na teritoriju Republike Hrvatske imaju glavni poslovni nastan ili njihov predstavnik ima poslovni nastan na teritoriju Republike Hrvatske.

(4) Subjekt ima glavni poslovni nastan u smislu stavka 3. ovoga članka ako na teritoriju Republike Hrvatske:

– pretežno donosi odluke povezane s mjerama upravljanja kibernetičkim sigurnosnim rizicima ili

– provodi mjere upravljanja kibernetičkim sigurnosnim rizicima kada se država članica u kojoj donosi odluke iz podstavka 1. ovoga stavka ne može utvrditi ili takve odluke subjekt ne donosi u Europskoj uniji ili

– ima poslovnu jedinicu s najvećim brojem zaposlenika u Europskoj uniji kada se država članica u kojoj provodi aktivnosti iz podstavka 2. ovoga stavka ne može utvrditi.

Primjena kriterija veličine subjekta

Članak 15.

(1) Prilikom utvrđivanja predstavlja li subjekt srednji subjekt maloga gospodarstva odnosno subjekt koji prelazi gornje granice za srednje subjekte maloga gospodarstva na temelju zakona kojim se uređuju osnove za primjenu poticajnih mjera gospodarske politike usmjerenih razvoju, restrukturiranju i tržišnom prilagođavanju maloga gospodarstva, uzima se u obzir:

– godišnji prosjek ukupnog broja zaposlenika subjekta i

– ukupan godišnji poslovni prihod subjekta prema financijskim izvještajima za prethodnu godinu ili ukupna aktiva subjekta ako je obveznik poreza na dobit odnosno ukupna dugotrajna imovina su-

bjekta ako je obveznik poreza na dohodak, neovisno o tome pruža li subjekt i druge usluge odnosno obavlja li i druge djelatnosti koje nisu obuhvaćene Prilogom I. i Prilogom II. ovoga Zakona.

(2) Prilikom kategorizacije subjekata vodi se računa o smjernicama Europske komisije o provedbi kriterija veličine koji se primjenjuju na mikropoduzeća i mala poduzeća.

Primjena Zakona u slučaju dvostruke kategorizacije subjekta

Članak 16.

Ako je subjekt razvrstan u kategoriju i ključnih i važnih subjekata, na takvog se subjekta primjenjuju odredbe ovoga Zakona koje se odnose na ključne subjekte.

POGLAVLJE II.
POPISI KLJUČNIH I VAŽNIH SUBJEKATA

Vođenje popisa

Članak 17.

(1) Nadležna tijela za provedbu zahtjeva kibernetičke sigurnosti i nadležna tijela za provedbu posebnih zakona provode kategorizaciju subjekata sukladno ovom Zakonu te utvrđuju i vode popise ključnih i važnih subjekata.

(2) Nadležna tijela za provedbu zahtjeva kibernetičke sigurnosti i nadležna tijela za provedbu posebnih zakona dužna su redovito, a najmanje jednom u dvije godine provjeravati popise ključnih i važnih subjekata te ih, po potrebi, ažurirati.

Dostava podataka Europskoj komisiji i Skupini za suradnju

Članak 18.

(1) Jedinstvena kontaktna točka svake dvije godine dostavlja:

– Europskoj komisiji i Skupini za suradnju podatke o broju ključnih i važnih subjekata razvrstanih na temelju članka 9. podstavaka 1., 2., 3. i 5., članka 10. i članka 12. stavka 1. podstavka 1. i stavka 3. ovoga Zakona, za svaki sektor i podsektor iz Priloga I. i Priloga II. ovoga Zakona

– Europskoj komisiji podatke o broju ključnih i važnih subjekata razvrstanih na temelju članka 11. ovoga Zakona, sektoru i podsektoru kojima pripadaju, vrsti usluge koju pružaju i odredbama članka 11. ovoga Zakona na temelju kojih je provedena kategorizacija, a dodatno, na njezin zahtjev, može Europskoj komisiji dostaviti i podatke o nazivima tih subjekata.

(2) Nadležna tijela za provedbu zahtjeva kibernetičke sigurnosti i nadležna tijela za provedbu posebnih zakona dužna su jedinstvenoj kontaktnoj točki dostavljati podatke potrebne za dostavu podataka sukladno stavku 1. ovoga članka.

Obavijesti o provedenoj kategorizaciji subjekata

Članak 19.

(1) Nadležna tijela za provedbu zahtjeva kibernetičke sigurnosti dužna su sve subjekte s popisa iz članka 17. stavka 1. ovoga Zakona koji su u njihovoj nadležnosti obavijestiti o provedenoj kategorizaciji subjekta i obvezama kojima podliježu na temelju ovoga Zakona i provedbenog propisa o zahtjevima kibernetičke sigurnosti iz ovoga Zakona.

(2) Nadležna tijela za provedbu zahtjeva kibernetičke sigurnosti dužna su subjekte u odnosu na koje je nakon ažuriranja popisa ključnih i važnih subjekata došlo do promjene u kategorizaciji subjekta obavijestiti o promjeni kategorije te činjenici da se od datuma primitka te obavijesti mijenjaju i obveze kojima podliježu na temelju ovoga Zakona i provedbenog propisa o zahtjevima kibernetičke sigurnosti iz ovoga Zakona, s naznakom bitnih promjena o kojima moraju voditi računa ovisno o promjeni kategorije o kojoj se obavještava.

(3) Nadležna tijela za provedbu zahtjeva kibernetičke sigurnosti dužna su subjekte koji se nakon ažuriranja popisa ključnih i važnih subjekata više ne smatraju ni ključnim subjektima ni važnim subjektima obavijestiti o toj činjenici te činjenici da od datuma primitka te obavijesti više ne podliježu obvezama provedbe zahtjeva kibernetičke sigurnosti iz ovoga Zakona.

(4) Nadležna tijela za provedbu zahtjeva kibernetičke sigurnosti dužna su o provedenoj kategorizaciji subjekta, kao i promjenama iz stavaka 2. i 3. ovoga članka obavijestiti subjekte u roku od 30 dana od dana provedene kategorizacije subjekta ili ažuriranja popisa ključnih i važnih subjekata.

Obveze subjekata iz Priloga I. i Priloga II. Zakona u prikupljanju podataka

Članak 20.

(1) Za potrebe kategorizacije subjekata sukladno ovom Zakonu te vođenja popisa ključnih i važnih subjekata, subjekti iz Priloga I. i Priloga II. ovoga Zakona dužni su nadležnim tijelima za provedbu zahtjeva kibernetičke sigurnosti i nadležnim tijelima za provedbu posebnih zakona, na njihov zahtjev, dostaviti sljedeće podatke:

– naziv subjekta

– adresu i ažurirane podatke za kontakt, uključujući adrese e-pošte, IP adresne raspone i telefonske brojeve

– relevantni sektor, podsektor i vrstu subjekta iz Priloga I. i Priloga II. ovoga Zakona

– popis država članica u kojima pružaju usluge obuhvaćene područjem primjene ovoga Zakona

– druge podatke o pružanju svojih usluga ili obavljanju svojih djelatnosti bitne za provedbu kategorizacije subjekta ili utvrđivanje nadležnosti nad subjektom.

(2) Rokovi za dostavu podataka na temelju stavka 1. ovoga članka određuju se ovisno o opsegu i složenosti podataka na koje se zahtjev odnosi, s tim da ostavljeni rok ne može biti kraći od 15 dana niti duži od 45 dana od dana primitka zahtjeva za dostavu podataka.

(3) Subjekti iz stavka 1. ovoga članka dužni su bez odgode, u roku od dva tjedna od datuma promjene, obavijestiti nadležno tijelo za provedbu zahtjeva kibernetičke sigurnosti odnosno nadležno tijelo za provedbu posebnih zakona o svim promjenama podataka koje su tom tijelu dostavili u skladu sa stavkom 1. ovoga članka.

Prikupljanje podataka iz drugih izvora radi provedbe kategorizacije subjekata

Članak 21.

(1) Tijela državne uprave, druga državna tijela, jedinice lokalne i područne (regionalne) samouprave, pravne osobe s javnim ovlastima i javni subjekti koji u okviru svog djelokruga prikupljaju podatke odnosno vode registre, evidencije i zbirke podataka o subjektima iz Priloga I. i Priloga II. ovoga Zakona dužni su, bez naknade, nadležnim tijelima za provedbu zahtjeva kibernetičke sigurnosti:

– redovito dostavljati popise subjekata iz Priloga I. i Priloga II. ovoga Zakona odnosno omogućiti pristup odgovarajućim podacima u registrima, evidencijama i zbirkama podataka elektroničkim putem

– na zahtjev nadležnog tijela za provedbu zahtjeva kibernetičke sigurnosti, za subjekte s popisa iz podstavka 1. ovoga stavka dostavljati:

a) podatke o njihovoj veličini i/ili

b) druge podatke o subjektima, uključujući podatke o pružanju njihovih usluga ili obavljanju njihovih djelatnosti, ako su takvi podaci potrebni za provođenje kategorizacije subjekata sukladno ovom Zakonu ili

c) ih uputiti na tijelo državne uprave, drugo državno tijelo, jedinicu lokalne i područne (regionalne) samouprave, pravnu osobu s javnim ovlastima ili javnog subjekta koji takve podatke posjeduje.

(2) Ako se podaci na temelju ovoga članka dostavljaju na zahtjev nadležnih tijela za provedbu zahtjeva kibernetičke sigurnosti, rokovi za dostavu podataka određuju se ovisno o opsegu i složenosti podataka na koje se zahtjev odnosi, s tim da ostavljeni rok ne može biti kraći od 15 dana niti duži od 45 dana od dana primitka zahtjeva za dostavu podataka.

POGLAVLJE III.
POSEBAN REGISTAR SUBJEKATA

Vođenje posebnog registra subjekata

Članak 22.

(1) Središnje državno tijelo za kibernetičku sigurnost uspostavlja i vodi poseban registar sljedećih subjekata:

– pružatelja usluga DNS-a

– registra naziva vršne nacionalne internetske domene

– registrara

– pružatelja usluga računalstva u oblaku

– pružatelja usluga podatkovnog centra

– pružatelja mreža za isporuku sadržaja

– pružatelja upravljanih usluga

– pružatelja upravljanih sigurnosnih usluga

– pružatelja internetskih tržišta

– pružatelja internetskih tražilica i

– pružatelja platformi za usluge društvenih mreža.

(2) Registar iz stavka 1. ovoga članka vodi se neovisno o obvezi vođenja popisa ključnih i važnih subjekata.

Prikupljanje podataka

Članak 23.

(1) Subjekti iz članka 22. ovoga Zakona dužni su središnjem državnom tijelu za kibernetičku sigurnost dostaviti sljedeće podatke:

– naziv subjekta

– popis usluga iz članka 22. ovoga Zakona koje pružaju

– adresu glavnog poslovnog nastana subjekta i njegovih drugih poslovnih jedinica ili adresu njegova predstavnika

– ažurirane podatke za kontakt, uključujući adrese e-pošte i telefonske brojeve subjekta i njegova predstavnika

– popis država članica u kojima pružaju usluge iz članka 22. ovoga Zakona

– IP adresne raspone subjekta.

(2) Rok za dostavu podataka na temelju stavka 1. ovoga članka je 15 dana od dana primitka zahtjeva za dostavu podataka.

(3) Subjekti iz članka 22. ovoga Zakona dužni su bez odgode, u roku od tri mjeseca od datuma promjene obavijestiti središnje državno tijelo za kibernetičku sigurnost o svim promjenama podataka koje su dostavili u skladu sa stavkom 1. ovoga članka.

(4) Po zaprimanju podaci iz stavaka 1. i 3. ovoga članka, osim podataka iz stavka 1. podstavka 6. ovoga članka, dostavljaju se bez odgode, putem jedinstvene kontaktne točke, Europskoj agenciji za kibernetičku sigurnost (u daljnjem tekstu: ENISA).

Provedbeni propis o kategorizaciji subjekata, vođenju popisa ključnih i važnih subjekata i posebnog registra subjekata

Članak 24.

Mjerila za razvrstavanje subjekata u kategoriju ključnih odnosno važnih subjekata na temelju posebnih kriterija iz članka 11. ovoga Zakona, kriteriji za provođenje procjena iz članka 12. stavka 1. podstavka 2. i stavka 3. i članka 13. ovoga Zakona, vođenje popisa ključnih i važnih subjekata, prikupljanje podataka u svrhu provođenja kategorizacije subjekata sukladno ovom Zakonu i vođenje posebnog registra subjekata iz članka 22. ovoga Zakona propisuje Vlada Republike Hrvatske (u daljnjem tekstu: Vlada) uredbom, na prijedlog središnjeg državnog tijela za kibernetičku sigurnost.

DIO TREĆI
ZAHTJEVI KIBERNETIČKE SIGURNOSTI

Opseg zahtjeva kibernetičke sigurnosti

Članak 25.

(1) Zahtjevi kibernetičke sigurnosti obuhvaćaju postupke i mjere koje su ključni i važni subjekti dužni primjenjivati radi postizanja visoke razine kibernetičke sigurnosti u pružanju svojih usluga odnosno obavljanju svojih djelatnosti, a sastoje se od:

– mjera upravljanja kibernetičkim sigurnosnim rizicima i

– obveza obavještavanja o značajnim incidentima i ozbiljnim kibernetičkim prijetnjama.

(2) Zahtjevi kibernetičke sigurnosti odnose se na sve mrežne i informacijske sustave kojima se ključni i važni subjekti služe u svom poslovanju ili u pružanju svojih usluga i sve usluge koje ključni i važni subjekti pružaju odnosno djelatnosti koje obavljaju, neovisno o tome pruža li subjekt i druge usluge odnosno obavlja li i druge djelatnosti koje nisu obuhvaćene Prilogom I. i Prilogom II. ovoga Zakona.

POGLAVLJE I.
MJERE UPRAVLJANJA KIBERNETIČKIM SIGURNOSNIM RIZICIMA I PROVJERE USKLAĐENOSTI KLJUČNIH I VAŽNIH SUBJEKATA

Primjena mjera

Članak 26.

(1) Ključni i važni subjekti dužni su provoditi odgovarajuće i razmjerne mjere upravljanja kibernetičkim sigurnosnim rizicima.

(2) Cilj je primjene mjera upravljanja kibernetičkim sigurnosnim rizicima zaštita mrežnih i informacijskih sustava i fizičkog okruženja tih sustava od incidenata, uzimajući pritom u obzir sve opasnosti kojima su ti sustavi izloženi.

(3) Mjere upravljanja kibernetičkim rizicima obuhvaćaju:

– tehničke, operativne i organizacijske mjere za upravljanje rizicima kojima su izloženi mrežni i informacijski sustavi kojima se ključni i važni subjekti služe u svom poslovanju ili u pružanju svojih usluga te

– mjere za sprečavanje ili smanjivanje na najmanju moguću mjeru učinka incidenata na mrežne i informacijske sustave ključnih i važnih subjekata, primatelje njihovih usluga ili na druge sektore, subjekte i usluge.

(4) Ključni i važni subjekti dužni su provoditi mjere upravljanja kibernetičkim sigurnosnim rizicima bez obzira na to upravljaju li i/ili održavaju svoje mrežne i informacijske sustave sami ili za to koriste vanjskog davatelja usluge.

(5) Ključni i važni subjekti dužni su provesti mjere upravljanja kibernetičkim sigurnosnim rizicima u roku od godine dana od dana dostave obavijesti iz članka 19. stavka 1. ovoga Zakona.

(6) Kada subjekta obavještava o promjeni u kategorizaciji subjekta na temelju članka 19. stavka 2. ovoga Zakona, nadležno tijelo za provedbu zahtjeva kibernetičke sigurnosti dužno je u obavijesti naznačiti i primjereni rok za provedbu obveza kojima subjekt zbog promjene kategorije podliježe na temelju ovoga Zakona i provedbenog propisa o zahtjevima kibernetičke sigurnosti iz ovoga Zakona.

(7) Rok iz stavka 6. ovoga članka određuje se ovisno o opsegu i složenosti obveza o kojima se subjekta obavještava, s tim da ostavljeni rok ne može biti kraći od 60 dana niti duži od šest mjeseci od dana primitka obavijesti iz članka 19. stavka 2. ovoga Zakona.

Obveza osiguranja razine sigurnosti mrežnih i informacijskih sustava proporcionalne utvrđenom riziku

Članak 27.

(1) Ključni i važni subjekti dužni su primjenom mjera upravljanja kibernetičkim sigurnosnim rizicima osigurati razinu sigurnosti mrežnih i informacijskih sustava proporcionalnu utvrđenom riziku.

(2) Pri procjeni proporcionalnosti primijenjenih mjera upravljanja kibernetičkim sigurnosnim rizicima u obzir se uzimaju:

– stupanj izloženosti subjekta rizicima

– veličina subjekta

– vjerojatnost pojave incidenata i njihova ozbiljnost, uključujući njihov mogući društveni i gospodarski učinak.

Način provedbe mjera upravljanja kibernetičkim sigurnosnim rizicima

Članak 28.

(1) Mjere upravljanja kibernetičkim sigurnosnim rizicima provode se na način da se, bez nametanja obveza ili diskriminacije u korist uporabe određene vrste tehnologije, uzimaju u obzir najnovija tehnička dostignuća koja se koriste u okviru najbolje sigurnosne prakse u području kibernetičke sigurnosti, kao i europske i međunarodne norme i tehničke specifikacije relevantne za sigurnost mrežnih i informacijskih sustava, uzimajući pritom u obzir i trošak provedbe.

(2) Ključni i važni subjekti dužni su prilikom provedbe mjera upravljanja kibernetičkim sigurnosnim rizicima koristiti se određenim IKT proizvodima, IKT uslugama i IKT procesima te upravljanim sigurnosnim uslugama koje su certificirane na temelju europskih programa kibernetičke sigurnosne certifikacije ili nacionalnih shema kibernetičke sigurnosne certifikacije, ako je takva obveza propisana:

– mjerodavnim propisima Europske unije

– posebnim propisima kojima se uređuje područje pružanja određenih usluga odnosno obavljanja određenih djelatnosti

– ovim Zakonom ili uredbom iz članka 24. ovoga Zakona.

Odgovornost za provedbu mjera

Članak 29.

(1) Za provedbu mjera upravljanja kibernetičkim sigurnosnim rizicima sukladno ovom Zakonu odgovorni su članovi upravljačkih tijela ključnih i važnih subjekata odnosno čelnici tijela državne uprave, drugih državnih tijela i izvršna tijela jedinica lokalne i područne (regionalne) samouprave (u daljnjem tekstu: osobe odgovorne za upravljanje mjerama).

(2) Osobe odgovorne za upravljanje mjerama dužne su odobravati mjere upravljanja kibernetičkim sigurnosnim rizicima koje će subjekt primjenjivati radi usklađivanja s obvezama utvrđenim ovim Zakonom i provedbenim propisom o zahtjevima kibernetičke sigurnosti te kontrolirati njihovu provedbu.

(3) U svrhu stjecanja znanja i vještina u pitanjima upravljanja kibernetičkim sigurnosnim rizicima i njihova učinka na usluge koje subjekt pruža odnosno djelatnost koju obavlja, osobe odgovorne za upravljanje mjerama dužne su:

– pohađati odgovarajuća osposobljavanja

– zaposlenicima subjekta omogućiti pohađanje odgovarajućih osposobljavanja.

(4) Odredbe ovoga članka odnose se i na druge fizičke osobe koje na temelju ovlasti za provođenje nadzora nad vođenjem poslova subjekta ili u svojstvu pravnog predstavnika subjekta na temelju punomoći ili druge ovlasti za zastupanje ili punomoći ili druge ovlasti za donošenje odluka u ime subjekta sudjeluju u donošenju odluka o mjerama upravljanja kibernetičkim sigurnosnim rizicima i/ili njihovoj provedbi.

Mjere upravljanja kibernetičkim sigurnosnim rizicima

Članak 30.

(1) Mjere upravljanja kibernetičkim sigurnosnim rizicima uključuju sljedeće:

– politike analize rizika i sigurnosti informacijskih sustava

– postupanje s incidentima, uključujući njihovo praćenje, evidentiranje i prijavljivanje

– kontinuitet poslovanja, kao što je upravljanje sigurnosnim kopijama i oporavak od nesreća, prekida rada i incidenata iz članka 37. ovoga Zakona, te upravljanje kibernetičkim krizama

– sigurnost lanca opskrbe, uključujući sigurnosne aspekte u pogledu odnosa između subjekta i njegovih izravnih dobavljača ili pružatelja usluga

– sigurnost u nabavi, razvoju i održavanju mrežnih i informacijskih sustava, uključujući otklanjanje ranjivosti i njihovo otkrivanje

– politike i postupke za procjenu djelotvornosti mjera upravljanja kibernetičkim sigurnosnim rizicima

– osnovne prakse kibernetičke higijene i osposobljavanje o kibernetičkoj sigurnosti

– politike i postupke u pogledu kriptografije i, prema potrebi, kriptiranja

– sigurnost ljudskih resursa, politike kontrole pristupa i upravljanja programskom i sklopovskom imovinom, uključujući i redovito ažuriranje popisa ove imovine

– korištenje višefaktorske provjere autentičnosti ili rješenja kontinuirane provjere autentičnosti, zaštićene glasovne, video i tekstualne komunikacije te sigurnih komunikacijskih sustava u hitnim slučajevima unutar subjekta, prema potrebi.

(2) Pri procjeni proporcionalnosti primijenjenih mjera iz stavka 1. podstavka 4. ovoga članka ključni i važni subjekti dužni su uzeti u obzir ranjivosti specifične za svakog izravnog dobavljača i pružatelja usluge te opću kvalitetu proizvoda i kibernetičku sigurnosnu praksu svojih dobavljača i pružatelja usluga, kao i rezultate koordiniranih

procjena sigurnosnih rizika ključnih lanaca opskrbe IKT uslugama, IKT sustavima ili IKT proizvodima, koje provodi Skupina za suradnju zajedno s Europskom komisijom i ENISA-om.

(3) Mjere upravljanja kibernetičkim sigurnosnim rizicima i način njihove provedbe uredit će se uredbom iz članka 24. ovoga Zakona.

Provjere usklađenosti uspostavljenih mjera upravljanja kibernetičkim sigurnosnim rizicima

Članak 31.

(1) Ključni i važni subjekti dužni su provjeravati usklađenost uspostavljenih mjera upravljanja kibernetičkim sigurnosnim rizicima s mjerama upravljanja kibernetičkim sigurnosnim rizicima propisanim ovim Zakonom i uredbom iz članka 24. ovoga Zakona.

(2) Provjera usklađenosti iz stavka 1. ovoga članka obavlja se u postupku revizije kibernetičke sigurnosti ključnih i važnih subjekata te u postupku samoprocjene kibernetičke sigurnosti važnih subjekata.

Revizori kibernetičke sigurnosti

Članak 32.

(1) Reviziju kibernetičke sigurnosti ključnih i važnih subjekata provode revizori kibernetičke sigurnosti.

(2) Revizori kibernetičke sigurnosti su pružatelji upravljanih sigurnosnih usluga kojima je izdan:

– nacionalni sigurnosni certifikat za reviziju kibernetičke sigurnosti ili

– odgovarajući kibernetički sigurnosni certifikat na temelju mjerodavne europske sheme kibernetičke sigurnosne certifikacije.

(3) Iznimno od stavka 2. ovoga članka, revizor kibernetičke sigurnosti za tijela državne uprave i druga državna tijela je središnje državno tijelo za obavljanje poslova u tehničkim područjima informacijske sigurnosti.

(4) O provedenoj reviziji kibernetičke sigurnosti revizori kibernetičke sigurnosti sastavljaju izvješće.

Nacionalni sigurnosni certifikat za reviziju kibernetičke sigurnosti

Članak 33.

(1) Nacionalni sigurnosni certifikat za reviziju kibernetičke sigurnosti izdaje središnje državno tijelo za obavljanje poslova u tehničkim područjima informacijske sigurnosti na temelju pravila sigurnosne certifikacije za reviziju kibernetičke sigurnosti.

(2) Pravila iz stavka 1. ovoga članka donosi središnje državno tijelo za obavljanje poslova u tehničkim područjima informacijske sigurnosti, a ona obuhvaćaju:

– organizacijske i stručne zahtjeve koje moraju ispunjavati pružatelji upravljanih sigurnosnih usluga za provedbu revizije kibernetičke sigurnosti

– pravila, tehničke zahtjeve, norme i postupke koji se primjenjuju u provedbi revizije kibernetičke sigurnosti, uključujući obvezni sadržaj izvješća o provedenoj reviziji kibernetičke sigurnosti i

– postupak izdavanja i opoziva nacionalnog sigurnosnog certifikata za reviziju kibernetičke sigurnosti, prava i obveze pružatelja upravljanih sigurnosnih usluga te pravnu zaštitu u tom postupku.

(3) Pravila iz stavka 1. ovoga članka primjenjuju se ako nije donesena odgovarajuća europska shema kibernetičke sigurnosne certifikacije koja obuhvaća revizije kibernetičke sigurnosti.

(4) Središnje državno tijelo za obavljanje poslova u tehničkim područjima informacijske sigurnosti vodi javno dostupan registar pružatelja upravljanih sigurnosnih usluga iz članka 32. stavka 2. podstavka 1. ovoga Zakona.

Provedba revizije kibernetičke sigurnosti

Članak 34.

(1) Reviziju kibernetičke sigurnosti ključni subjekti dužni su provoditi najmanje jednom u dvije godine.

(2) Reviziju kibernetičke sigurnosti ključni subjekti dužni su provesti i prije isteka roka iz stavka 1. ovoga članka, kada to zatraži nadležno tijelo za provedbu zahtjeva kibernetičke sigurnosti na temelju članka 79. stavka 1. podstavka 7. ili članka 81. stavka 1. podstavka 2. ovoga Zakona.

(3) Revizija kibernetičke sigurnosti iz stavka 1. ovoga članka provodi se kao zaseban postupak ili u okviru revizije poslovanja odnosno druge provjere sukladnosti subjekata koja se provodi na temelju posebnih propisa kojima se uređuje područje pružanja određenih usluga odnosno obavljanja određenih djelatnosti.

(4) Reviziju kibernetičke sigurnosti važni subjekti dužni su provesti kada to zatraži nadležno tijelo za provedbu zahtjeva kibernetičke sigurnosti na temelju članka 79. stavka 1. podstavka 7. ovoga Zakona.

(5) Izvješće iz članka 32. stavka 4. ovoga Zakona ključni i važni subjekti dužni su dostaviti nadležnom tijelu za provedbu zahtjeva kibernetičke sigurnosti bez odgode, a najkasnije u roku od osam dana od dana njegova primitka.

(6) Iznimno od stavka 5. ovoga članka, kada je revizija kibernetičke sigurnosti provedena na zahtjev nadležnog tijela za provedbu zahtjeva kibernetičke sigurnosti na temelju članka 79. stavka 1. podstavka 7. ili članka 81. stavka 1. podstavka 2. ovoga Zakona, subjekt za koji je revizija kibernetičke sigurnosti provedena dužan je izvješće iz članka 32. stavka 4. ovoga Zakona dostaviti nadležnom tijelu za provedbu zahtjeva kibernetičke sigurnosti odmah po njegovu primitku.

(7) Troškove provedbe revizije kibernetičke sigurnosti snose ključni i važni subjekti, ako nije drugačije propisano ovim Zakonom.

Provedba samoprocjene kibernetičke sigurnosti

Članak 35.

(1) Samoprocjenu kibernetičke sigurnosti važni subjekti dužni su provoditi najmanje jednom u dvije godine.

(2) Za provedbu samoprocjene kibernetičke sigurnosti važni subjekti mogu koristiti i vanjskog davatelja takve usluge.

(3) Ako rezultati provedene samoprocjene kibernetičke sigurnosti pokazuju da su uspostavljene mjere upravljanja kibernetičkim sigurnosnim rizicima u skladu s mjerama upravljanja kibernetičkim sigurnosnim rizicima propisanim ovim Zakonom i uredbom iz članka 24. ovoga Zakona, važni subjekti sastavljaju izjavu o sukladnosti.

(4) Ako rezultati provedene samoprocjene kibernetičke sigurnosti pokazuju da uspostavljene mjere upravljanja kibernetičkim sigurnosnim rizicima nisu u skladu s mjerama upravljanja kibernetičkim sigurnosnim rizicima propisanim ovim Zakonom i uredbom iz članka 24. ovoga Zakonom, važni subjekti dužni su utvrditi plan daljnjeg postupanja, uključujući plan za pravodobnu ponovnu samoprocjenu kibernetičke sigurnosti i ispravljanje utvrđenih nedostataka.

(5) Izjavu iz stavka 3. ovoga članka i plan iz stavka 4. ovoga članka važni subjekti dužni su dostaviti nadležnom tijelu za provedbu zahtjeva kibernetičke sigurnosti bez odgode, a najkasnije u roku od osam dana od dana njihova sastavljanja.

(6) Troškove provedbe samoprocjene kibernetičke sigurnosti snose važni subjekti.

Provedbeni propis za samoprocjenu kibernetičke sigurnosti

Članak 36.

Pravila, tehnički zahtjevi, norme, obrasci i postupci koji se primjenjuju prilikom samoprocjene kibernetičke sigurnosti, uključujući sadržaj izjave o sukladnosti, uredit će se uredbom iz članka 24. ovoga Zakona.

POGLAVLJE II.
OBVEZE OBAVJEŠTAVANJA O KIBERNETIČKIM PRIJETNJAMA I INCIDENTIMA

Obavještavanje o značajnim incidentima

Članak 37.

(1) Ključni i važni subjekti dužni su nadležni CSIRT obavijestiti o svakom incidentu koji ima znatan učinak na dostupnost, cjelovitost, povjerljivost i autentičnost podataka od značaja za poslovanje subjekta i/ili kontinuitet usluga koje pružaju ili djelatnost koju obavljaju (u daljnjem tekstu: značajan incident).

(2) Incident se smatra značajnim incidentom:

– ako je uzrokovao ili može uzrokovati ozbiljne poremećaje u funkcioniranju usluga koje subjekt pruža odnosno djelatnosti koju obavlja ili financijske gubitke za subjekt

– ako je utjecao ili bi mogao utjecati na druge fizičke ili pravne osobe uzrokovanjem znatne materijalne ili nematerijalne štete.

(3) Ključni i važni subjekti dužni su obavijesti iz stavka 1. ovoga članka dostaviti tijelima kaznenog progona u slučajevima u kojima postoje osnove sumnje da su značajni incidenti nastali počinjenjem kaznenog djela, na temelju odredbi zakona kojim se uređuje kazneni postupak.

(4) Ključni i važni subjekti dužni su započeti s dostavom obavijesti iz stavka 1. ovoga članka u roku od 30 dana od dana dostave obavijesti iz članka 19. stavka 1. ovoga Zakona.

Obavještavanje primatelja usluga

Članak 38.

(1) Ključni i važni subjekti dužni su obavijestiti primatelje svojih usluga o značajnim incidentima na koje bi takav incident mogao utjecati.

(2) U slučaju pojave ozbiljne kibernetičke prijetnje ključni i važni subjekti dužni su primatelje svojih usluga na koje bi takva prijetnja mogla utjecati obavijestiti o svim mogućim mjerama zaštite ili pravnim sredstvima koje mogu uporabiti u svrhu sprečavanja ili naknade uzrokovane štete te, po potrebi, obavijestiti primatelje usluga i o samoj ozbiljnoj kibernetičkoj prijetnji.

(3) Ključni i važni subjekti dužni su započeti s dostavom obavijesti iz stavaka 1. i 2. ovoga članka u roku od 30 dana od dana dostave obavijesti iz članka 19. stavka 1. ovoga Zakona.

Obavještavanje na dobrovoljnoj osnovi

Članak 39.

Ključni i važni subjekti mogu nadležni CSIRT dobrovoljno obavijestiti o svakom incidentu, kibernetičkoj prijetnji i izbjegnutom incidentu.

Obavještavanje o značajnom incidentu s prekograničnim i međusektorskim učinkom

Članak 40.

(1) Jedinstvena kontaktna točka, na zahtjev nadležnog CSIRT-a ili prema vlastitoj procjeni, o značajnom incidentu s prekograničnim učinkom obavještava jedinstvene kontaktne točke pogođene države članice i ENISA-u, osobito ako se incident odnosi na dvije države članice ili više njih.

(2) Jedinstvena kontaktna točka, na zahtjev nadležnog CSIRT-a ili prema vlastitoj procjeni, o značajnom incidentu s međusektorskim učinkom obavještava tijela državne uprave nadležna za pogođene sektore.

Obavještavanje javnosti o značajnom incidentu

Članak 41.

Ako je za sprečavanje ili rješavanje značajnog incidenta koji je u tijeku nužno obavijestiti javnost ili ako je objava informacija o značajnom incidentu u javnom interesu iz nekog drugog razloga, nadležni CSIRT te, prema potrebi, CSIRT-ovi ili nadležna tijela drugih pogođenih država članica mogu, nakon savjetovanja s jedinstvenom kontaktnom točkom, nadležnim tijelom za provedbu zahtjeva kibernetičke sigurnosti odnosno nadležnim tijelom za provedbu posebnih zakona, ovisno o podjeli nadležnosti iz Priloga III. ovoga Zakona, te pogođenim subjektom obavijestiti javnost o značajnom incidentu ili zatražiti od ključnog i važnog subjekta da to učini.

Obavještavanje jedinstvene kontaktne točke i ENISA-e

Članak 42.

(1) Nadležni CSIRT-ovi dužni su jedinstvenu kontaktnu točku obavijestiti o značajnim incidentima, ostalim incidentima, ozbiljnim kibernetičkim prijetnjama i izbjegnutim incidentima o kojima su ih ključni i važni subjekti obavijestili na temelju članaka 37. i 39. ovoga Zakona, sukladno njezinim smjernicama.

(2) Jedinstvena kontaktna točka podnosi ENISA-i svaka tri mjeseca sažeto izvješće koje uključuje anonimizirane i agregirane podatke o značajnim incidentima, ostalim incidentima, ozbiljnim kibernetičkim prijetnjama i izbjegnutim incidentima o kojima su ključni i važni subjekti obavijestili nadležni CSIRT na temelju članaka 37. i 39. ovoga Zakona.

Nacionalna platforma za prikupljanje, analizu i razmjenu podataka o kibernetičkim prijetnjama i incidentima

Članak 43.

(1) Obavještavanje na temelju članaka 37. i 39. ovoga Zakona i razmjena podataka o kibernetičkim prijetnjama i incidentima između nadležnih tijela iz Priloga III. ovoga Zakona obavlja se putem nacionalne platforme za prikupljanje, analizu i razmjenu podataka o kibernetičkim prijetnjama i incidentima, kao jedinstvene ulazne točke za obavještavanje o kibernetičkim prijetnjama i incidentima.

(2) Razvoj i upravljanje nacionalnom platformom iz stavka 1. ovoga članka u nadležnosti je CARNET-a.

Provedbeni propis o obavještavanju o kibernetičkim prijetnjama i incidentima

Članak 44.

Kriteriji za utvrđivanje značajnih incidenata, uključujući kriterijske pragove ako su potrebni zbog specifičnosti pojedinog sektora, vrste i sadržaj obavijesti iz članaka 37. do 40. ovoga Zakona, rokovi za njihovu dostavu, postupanja s tim obavijestima, uključujući postupanja nadležnog CSIRT-a u povodu zaprimljenih obavijesti iz

članaka 37. i 39. ovoga Zakona, prava pristupa i druga pitanja bitna za korištenje nacionalne platforme za prikupljanje, analizu i razmjenu podataka o kibernetičkim prijetnjama i incidentima, uključujući mogućnosti korištenja drugih načina dostave obavijesti iz članaka 37. i 39. ovoga Zakona, propisuju se uredbom iz članka 24. ovoga Zakona.

POGLAVLJE III.
POSEBNI ZAHTJEVI ZA UPRAVLJANJE PODACIMA O REGISTRACIJI NAZIVA DOMENA

Svrha provođenja posebnih zahtjeva za upravljanje podacima o registraciji naziva domena

Članak 45.

U svrhu osiguranja pouzdanog, otpornog i sigurnog sustava naziva domena, registar naziva vršne nacionalne internetske domene i registrari dužni su provoditi posebne zahtjeve za upravljanje podacima o registraciji naziva domena.

Sadržaj informacija u bazama podataka o registraciji naziva domena i utvrđivanje identiteta korisnika domene

Članak 46.

(1) Registar naziva vršne nacionalne internetske domene i registrari dužni su osiguravati da baza podataka o registraciji naziva domena sadržava informacije potrebne za identifikaciju korisnika domene i registrara koji upravljaju nazivima domena te za kontakt s njima, i to:

– naziv domene

– datum registracije

– ime korisnika domene te adresu njegove e-pošte i telefonski broj za kontakt

– adresu e-pošte i telefonski broj za kontakt registrara koji upravlja nazivom domene.

(2) Registar naziva vršne nacionalne internetske domene i registrari dužni su utvrditi identitet korisnika domene i provjeriti njegov identitet na osnovi identifikacijskih dokumenata odnosno dokumenata, podataka ili informacija dobivenih iz vjerodostojnoga, pouzdanoga i neovisnoga izvora, uključujući, ako ga korisnik domene ima, kvalificirani certifikat za elektronički potpis ili elektronički pečat ili bilo koji drugi siguran, daljinski ili elektronički, postupak identifikacije koji su regulirala, priznala, odobrila ili prihvatila relevantna nacionalna tijela.

(3) Nepostupanje podnositelja zahtjeva za registraciju domene i korisnika domene sukladno obvezama propisanim ovim Zakonom predstavlja temelj za uskratu registracije domene odnosno brisanje domene.

Obveze registra naziva vršne nacionalne internetske domene i registrara

Članak 47.

(1) Ako zahtjev za registraciju domene ne sadržava sve podatke iz članka 46. stavka 1. podstavaka 1. do 3. ovoga Zakona, registar naziva vršne nacionalne internetske domene i registrari dužni su odbiti takav zahtjev, a podnositelja zahtjeva obavijestiti o uskraćivanju registracije domene odnosno privremenoj deaktivaciji domene i nemogućnosti njezina korištenja sve dok zahtjev ne bude uredno podnesen, i to u roku od osam dana od dana primitka takve obavijesti.

(2) Registar naziva vršne nacionalne internetske domene i registrari dužni su periodično, a najmanje jednom godišnje, za sve svoje korisnike domena provoditi provjere postojanja korisnika domene, kao i usklađenost postupanja korisnika domene s obvezama iz propisa kojim je uređeno ustrojstvo i upravljanje vršnom nacionalnom internetskom domenom.

(3) U slučaju nedostupnosti korisnika domene u okviru višekratnih provjera iz stavka 2. ovoga članka na različite registrirane podatke za kontakt korisnika domene odnosno utvrđene zlouporabe prava ili drugog nepropisnog postupanja korisnika domene, registar naziva vršne nacionalne internetske domene i registrari dužni su takvu domenu brisati.

(4) Registar naziva vršne nacionalne internetske domene i registrari dužni su uspostaviti i javno objaviti politike upravljanja bazom podataka iz članka 46. ovoga Zakona koje obvezno sadržavaju i postupke provjere podataka iz zahtjeva za registraciju domene.

(5) Registar naziva vršne nacionalne internetske domene i registrari nakon registracije naziva domene bez odgode javno objavljuju podatke o registraciji naziva domena koji nisu osobni podaci.

Čuvanje podataka i pristup podacima o korisniku domene

Članak 48.

(1) Registar naziva vršne nacionalne internetske domene i registrari dužni su podatke, informacije i dokumentaciju prikupljenu na temelju članaka 46. i 47. ovoga Zakona čuvati 25 godina od prestanka prava korisnika na korištenje domene.

(2) Dokumentacija iz stavka 1. ovoga članka mora sadržavati:

– identifikacijske dokumente i drugu dokumentaciju na temelju koje je utvrđen identitet korisnika domene

– zahtjev za registraciju domene i drugu dokumentacija vezanu uz registraciju domene.

(3) Registar naziva vršne nacionalne internetske domene i registrari dužni su tijelima kaznenog progona i nadležnom CSIRT-u, tijelu nadležnom za zaštitu osobnih podataka i drugim pravnim osobama s javnim ovlastima, kao i državnim tijelima u okviru izvršavanja javnih ovlasti, na njihov obrazloženi zahtjev, bez odgode, a najkasnije u roku od 72 sata od primitka zahtjeva, dostaviti ili na drugi odgovarajući način omogućiti pristup podacima o korisniku domene.

(4) Registar naziva vršne nacionalne internetske domene i registrari dužni su nakon isteka roka čuvanja iz stavka 1. ovoga članka osobne podatke o korisniku domene brisati, a dokumentaciju iz stavka 2. ovoga članka uništiti sukladno propisima o zaštiti osobnih podataka.

(5) Registar naziva vršne nacionalne internetske domene i registrari obvezni su u svojim politikama upravljanja iz članka 47. stavka 4. ovoga Zakona naznačiti svoju obvezu postupanja u skladu sa stavcima 1. i 3. ovoga članka.

(6) Tehničke i organizacijske mjere za zaštitu osobnih podataka o korisnicima domena uređuju se posebnim propisima kojima se uređuje ustrojstvo i upravljanje vršnom nacionalnom internetskom domenom.

Provedba kontrole usklađenosti s posebnim zahtjevima za upravljanje podacima o registraciji naziva

Članak 49.

Kontrolu usklađenosti postupanja registra naziva vršne nacionalne internetske domene i registrara s posebnim zahtjevima za upravljanje podacima o registraciji naziva domena iz članaka 45. do 48. ovoga Zakona provodi tijelo državne uprave nadležno za znanost i obrazovanje.

DIO ČETVRTI
DOBROVOLJNI MEHANIZMI KIBERNETIČKE ZAŠTITE

Provedba samoprocjena kibernetičke sigurnosti i obavještavanje o incidentima i kibernetičkim prijetnjama na dobrovoljnoj osnovi

Članak 50.

(1) Svaki subjekt koji nije kategoriziran kao ključan i važan subjekt sukladno ovom Zakonu može:

– provoditi samoprocjene kibernetičke sigurnosti za mrežne i informacijske sustave kojima se služi u svom poslovanju ili u pružanju svojih usluga

– nadležni CSIRT dobrovoljno obavijestiti o svakom značajnom incidentu, ostalim incidentima, kibernetičkim prijetnjama ili izbjegnutim incidentima, pod uvjetom da periodično provodi samoprocjene kibernetičke sigurnosti iz podstavka 1. ovoga stavka.

(2) Mogućnost provedbe samoprocjena kibernetičke sigurnosti i dobrovoljnog obavještavanja iz stavka 1. ovoga članka uredit će se uredbom iz članka 24. ovoga Zakona.

Nacionalni sustav za otkrivanje kibernetičkih prijetnji i zaštitu kibernetičkog prostora

Članak 51.

(1) Radi podizanja ukupne sposobnosti i otpornosti u području kibernetičke sigurnosti, središnje državno tijelo za kibernetičku sigurnost kontinuirano razvija nacionalni sustav za otkrivanje kibernetičkih prijetnji i zaštitu kibernetičkog prostora (u daljnjem tekstu: nacionalni sustav).

(2) Nacionalnom sustavu mogu dobrovoljno pristupiti ključni subjekti, važni subjekti i drugi subjekti koji nisu kategorizirani kao ključni ili važni subjekti sukladno ovom Zakonu, ovisno o procjeni kritičnosti subjekta koju provodi središnje državno tijelo za kibernetičku sigurnost.

(3) Pristupanje nacionalnom sustavu može se provoditi kao obvezujuća mjera kibernetičke zaštite za subjekte javnog sektora, ako je takva obveza propisana uredbom iz članka 24. ovoga Zakona.

(4) Pristupanje nacionalnom sustavu provodi se na temelju sporazuma koji sklapaju središnje državno tijelo za kibernetičku sigurnost i subjekt koji pristupa sustavu.

(5) Pristupanje nacionalnom sustavu ne utječe na obveze ključnih i važnih subjekata iz članka 25. ovoga Zakona, već predstavlja dodatnu mjeru kibernetičke zaštite.

Kriteriji za provedbu procjene kritičnosti subjekta

Članak 52.

(1) Procjena kritičnosti subjekta iz članka 51. stavka 2. ovoga Zakona provodi se na temelju sljedećih kriterija:

– važnosti i značaja usluga koje subjekt pruža ili djelatnosti koje subjekt obavlja u odnosu na druge pružatelje istih ili istovrsnih usluga i djelatnosti u Republici Hrvatskoj

– važnosti mrežnih i informacijskih sustava kojima se subjekt koristi u pružanju usluga ili obavljanju djelatnosti te njihovoj izloženosti rizicima, opasnostima i prijetnjama u kibernetičkom prostoru i

– stanju mrežnih i informacijskih sustava kojima se subjekt koristi u pružanju usluga ili obavljanju djelatnosti, i to vezano za način projektiranja, upravljanja i održavanja mrežnih i informacijskih sustava subjekta, kao i primijenjene relevantne europske i međunarodne norme i sigurnosne prakse.

(2) Procjena kritičnosti subjekta iz članka 51. stavka 2. ovoga Zakona provodi se na temelju:

– zahtjeva subjekta za pristupanje nacionalnom sustavu ili

– prijedloga za pristupanje nacionalnom sustavu koje je podnijelo tijelo državne uprave ili regulatorno tijelo nadležno za sektor kojem subjekt pripada.

(3) Zahtjevi i prijedlozi iz stavka 2. ovoga članka podnose se središnjem državnom tijelu za kibernetičku sigurnost.

(4) Podnošenje zahtjeva i prijedloga za pristupanje nacionalnom sustavu, prikupljanje podataka potrebnih za provođenje procjene kritičnosti subjekata u svrhu pristupanja sustavu i provedba pristupanja subjekata nacionalnom sustavu uredit će se uredbom iz članka 24. ovoga Zakona.

Dobrovoljna razmjena informacija o kibernetičkoj sigurnosti

Članak 53.

(1) Ključni subjekti, važni subjekti i drugi subjekti koji nisu kategorizirani kao ključni ili važni subjekti sukladno ovom Zakonu mogu međusobno dobrovoljno razmjenjivati informacije o kibernetičkoj sigurnosti u svrhu povećanja razine kibernetičke sigurnosti ili postupanja s incidentima.

(2) Razmjena informacija iz stavka 1. ovoga članka može uključivati informacije koje se odnose na kibernetičke prijetnje, uključujući informacije o izvoru prijetnje, izbjegnute incidente, ranjivosti, tehnike i postupke, pokazatelje ugroženosti, taktike, tehnike i procedure kibernetičkih napadača, indikatore kompromitacije, kibernetička sigurnosna upozorenja i preporuke o konfiguraciji kibernetičkih sigurnosnih alata za otkrivanje kibernetičkih napada.

(3) Razmjena informacija iz stavka 2. ovoga članka odvija se između subjekata iz stavka 1. ovoga članka te, prema potrebi, njihovih dobavljača ili pružatelja usluga putem mehanizama za razmjenu informacija uspostavljenih posebno u te svrhe.

(4) Mehanizmi iz stavka 3. ovoga članka uspostavljaju se na temelju sporazuma o dobrovoljnoj razmjeni informacija o kibernetičkoj sigurnosti.

(5) Sporazumom iz stavka 4. ovoga članka utvrđuju se uvjeti za pristupanje mehanizmu koji se sporazumom uspostavlja, sadržaj informacija koje se razmjenjuju, mogućnost upotrebe namjenskih platformi i drugih alata za automatiziranu razmjenu informacija, kao i svi drugi operativni elementi bitni za učinkovitu i sigurnu razmjenu informacija.

(6) Ključni i važni subjekti o svom sudjelovanju u mehanizmima za dobrovoljnu razmjenu informacija o kibernetičkoj sigurnosti iz stavka 3. ovoga članka dužni su obavijestiti nadležno tijelo za provedbu zahtjeva kibernetičke sigurnosti, a subjekti javnog sektora koji su kategorizirani kao ključni subjekti dužni su dodatno o takvom sudjelovanju i opsegu informacija koje mogu razmjenjivati s ostalim uključenim dionicima prethodno zatražiti mišljenje središnjeg državnog tijela za kibernetičku sigurnost.

Koordinirano otkrivanje ranjivosti

Članak 54.

(1) Svaka fizička i pravna osoba može anonimno prijaviti ranjivost.

(2) Prijave ranjivosti podnose se CSIRT koordinatoru za otkrivanje ranjivosti.

(3) CSIRT koordinator za otkrivanje ranjivosti djeluje kao pouzdani posrednik koji, prema potrebi, olakšava interakciju između fizičke ili pravne osobe koja prijavljuje ranjivost i proizvođača ili pružatelja potencijalno ranjivih IKT proizvoda ili IKT usluga, na zahtjev bilo koje strane.

(4) Zadaće CSIRT koordinatora za otkrivanje ranjivosti su utvrđivanje predmetnih subjekata i kontaktiranje s njima, pružanje pomoći fizičkim ili pravnim osobama koje prijavljuju ranjivost i pregovaranje o vremenskom okviru za usklađeno otkrivanje i upravljanje ranjivostima koje utječu na više subjekata.

(5) CSIRT koordinator za otkrivanje ranjivosti osigurava provedbu daljnjih mjera u pogledu prijavljene ranjivosti i osigurava anonimnost fizičke ili pravne osobe koja prijavljuje ranjivost.

(6) CSIRT koordinator za otkrivanje ranjivosti dužan je prilikom razmjene podataka o prijavljenoj ranjivosti osigurati anonimnost prijavitelja ranjivosti pomoću tehnike uklanjanja izravnih identifikatora, tehnike poopćavanja, tehnike nasumične izmjene podataka odnosno drugih poznatih tehnika.

(7) Kada je u svrhu provedbe zadaća iz stavka 4. ovoga članka nužno pohranjivati podatke o prijavitelju ranjivosti, CSIRT koordinator za otkrivanje ranjivosti dužan je voditi evidenciju pohranjenih podataka.

(8) CSIRT koordinator za otkrivanje ranjivosti dužan je podatke i evidencije iz stavka 7. ovoga članka čuvati najduže tri godine od prijave ranjivosti, a nakon isteka tog roka osobne podatke o prijavitelju ranjivosti brisati, a evidencije iz stavka 7. ovoga članka uništiti sukladno propisima o zaštiti osobnih podataka.

(9) CSIRT koordinator za otkrivanje ranjivosti dostavlja informacije o novootkrivenim ranjivostima nadležnim CSIRT-ovima iz ovoga Zakona, zajedno s uputom o načinu daljnjeg obavještavanja o ranjivostima subjekata u njihovoj nadležnosti.

(10) Nadležni CSIRT-ovi izrađuju smjernice namijenjene korisnicima ranjivih IKT proizvoda ili IKT usluga o načinu na koji se mogu ublažiti rizici koji proizlaze iz otkrivenih ranjivosti te dostavljaju obavijesti s najboljim praksama subjektima za koje su zaduženi na temelju ovoga Zakona.

(11) Ako bi prijavljena ranjivost mogla imati znatan učinak na subjekte u više od jedne države članice, CSIRT koordinator za otkrivanje ranjivosti, prema potrebi, surađuje s CSIRT-ovima drugih država članica koji su imenovani koordinatorima za otkrivanje ranjivosti u okviru CSIRT mreže.

(12) Zadaće CSIRT koordinatora za otkrivanje ranjivosti obavlja CSIRT pri središnjem državnom tijelu za kibernetičku sigurnost.

DIO PETI
STRATEŠKO PLANIRANJE I UPRAVLJANJE KIBERNETIČKOM SIGURNOSTI

Nacionalni akt strateškog planiranja iz područja kibernetičke sigurnosti

Članak 55.

(1) Vlada, na prijedlog središnjeg državnog tijela za kibernetičku sigurnost, donosi srednjoročni akt strateškog planiranja iz područja kibernetičke sigurnosti.

(2) Aktom strateškog planiranja iz stavka 1. ovoga članka utvrđuju se:

– posebni ciljevi i prioriteti u području razvoja kibernetičke sigurnosti koji najmanje obuhvaćaju javne politike iz Priloga IV. ovoga Zakona te

– okvir za praćenje i vrednovanje provedbe ciljeva i prioriteta iz podstavka 1. ovoga stavka.

(3) U svrhu razrade mjera za provedbu posebnih ciljeva i prioriteta akta strateškog planiranja iz stavka 1. ovoga članka izrađuje se akcijski plan za njegovu provedbu.

(4) Izvještavanje, praćenje i vrednovanje akta strateškog planiranja iz stavka 1. ovoga članka provodi se u skladu s propisom kojim se uređuje područje strateškog planiranja i upravljanja razvojem Republike Hrvatske.

(5) Središnje državno tijelo za kibernetičku sigurnost obavještava Europsku komisiju o donošenju akta strateškog planiranja iz stavka 1. ovoga članka u roku od tri mjeseca od dana njegova donošenja odnosno u roku od tri mjeseca od dana donošenja njegovih izmjena i/ili dopuna.

Upravljanje kibernetičkim incidentima velikih razmjera i kibernetičkim krizama

Članak 56.

(1) Središnje državno tijelo za kibernetičku sigurnost je tijelo odgovorno za upravljanje kibernetičkim incidentima velikih razmjera i kibernetičkim krizama (u daljnjem tekstu: upravljanje kibernetičkim krizama).

(2) Vlada, na prijedlog tijela odgovornog za upravljanje kibernetičkim krizama, donosi nacionalni program upravljanja kibernetičkim krizama.

(3) Nacionalnim programom iz stavka 2. ovoga članka utvrđuju se kapaciteti, sredstva i postupci upravljanja kibernetičkim krizama te se pobliže utvrđuju:

– ciljevi upravljanja kibernetičkim krizama, uključujući ciljeve razvoja nacionalnih mjera pripravnosti, kao i usklađenost s okvirom za upravljanje kibernetičkim krizama Europske unije

– koherentnost s nacionalnim općim okvirom za upravljanje krizama

– mjere i aktivnosti za jačanje nacionalne pripravnosti

– plan provedbe nacionalnih mjera pripravnosti, uključujući plan aktivnosti osposobljavanja te provedbe vježbi koje su sastavni dio plana iz članka 58. ovoga Zakona

– zadaće i odgovornosti tijela uključenih u upravljanje kibernetičkim krizama

– uloga javnog i privatnog sektora i infrastruktura bitna za upravljanje u kibernetičkim krizama te

– nacionalni postupci i koordinacija na nacionalnoj razini potrebna za osiguranje potpore koordiniranom upravljanju kibernetičkim krizama koje se provodi na razini Europske unije i učinkovitog sudjelovanja Republike Hrvatske u takvom upravljanju.

(4) Sastavni dio nacionalnog programa iz stavka 2. ovoga članka su standardne operativne procedure kojima se detaljnije utvrđuju:

– postupci upravljanja kibernetičkim krizama, uključujući njihovu integraciju u opći okvir nacionalnog kriznog upravljanja te

– sva pitanja bitna za razmjenu podataka.

(5) Tijelo odgovorno za upravljanje kibernetičkim krizama obavještava Europsku komisiju i EU-CyCLONe mrežu o donošenju nacionalnog programa iz stavka 2. ovoga članka u roku od tri mjeseca od njegova donošenja odnosno njegovih izmjena i dopuna ili donošenja novoga programa.

Ocjenjivanje stanja kibernetičke sigurnosti

Članak 57.

(1) U svrhu razmjene stečenih znanja i iskustava, jačanja povjerenja, jačanja kapaciteta i sposobnosti u području kibernetičke sigurnosti te unaprjeđenja politika iz područja kibernetičke sigurnosti organiziraju se i provode postupci samoocjene stanja kibernetičke sigurnosti.

(2) Samoocjene stanja kibernetičke sigurnosti organiziraju se i provode i na nacionalnoj razini (u daljnjem tekstu: nacionalne samoocjene), neovisno o provedbi samoocjena koje države članice provode u okviru istorazinskih ocjenjivanja koja se provode sukladno metodologiji koju su utvrdile Skupina za suradnju, Europska komisija i ENISA.

(3) U okviru nacionalnih samoocjena ocjenjuje se razina provedbe zahtjeva kibernetičke sigurnosti propisanih ovim Zakonom, razina kibernetičkih kapaciteta, uključujući dostupne financijske, tehničke i ljudske resurse, djelotvornost izvršavanja zadaća i razina provedbe suradnje nadležnih tijela za provedbu zahtjeva kibernetičke sigurnosti, nadležnih CSIRT-ova, nadležnih tijela za provedbu posebnih zakona i nadležnih tijela iz zakona kojim se uređuje područje kritične infrastrukture, razina provedbe mehanizama za razmjenu informacija o kibernetičkoj sigurnosti iz članka 53. ovoga Zakona i posebna pitanja međusektorske prirode.

(4) Na nacionalne samoocjene na odgovarajući se način primjenjuje metodologija za provedbu samoocjena država članica koju donose Skupina za suradnju, Europska komisija i ENISA.

(5) Planove i programe provedbe samoocjena koje države članice provode u okviru istorazinskih ocjenjivanja iz stavka 2. ovoga članka i nacionalnih samoocjena donosi Vlada, na prijedlog središnjeg državnog tijela za kibernetičku sigurnost.

(6) Središnje državno tijelo za kibernetičku sigurnost prije početka istorazinskih ocjenjivanja iz stavka 2. ovoga članka razmatra postojanje rizika od sukoba interesa stručnjaka za kibernetičku sigurnost imenovanih za njihovu provedbu te o utvrđenim rizicima obavještava druge države članice, Skupinu za suradnju, Europsku komisiju i ENISA-u.

(7) Kada postoje opravdani razlozi za protivljenje imenovanju pojedinog stručnjaka za kibernetičku sigurnost za provedbu istorazinskih ocjenjivanja iz stavka 2. ovoga članka, središnje državno tijelo za kibernetičku sigurnost o tome obavještava državu članicu koja provodi imenovanja.

Vježbe kibernetičke sigurnosti

Članak 58.

(1) Kako bi se postigla maksimalna razina pripravnosti, osobito u slučaju kibernetičkih kriza, radi provjere raspoloživih kapaciteta i sposobnosti u području kibernetičke sigurnosti, testiranja uspostavljenih komunikacijskih mehanizama, kao i razmjene stečenih znanja, iskustava i najboljih praksi te jačanja povjerenja provode se vježbe kibernetičke sigurnosti.

(2) Vježbe kibernetičke sigurnosti organiziraju se i provode na temelju Plana provedbe vježbi kibernetičke sigurnosti koji donosi Vlada na prijedlog središnjeg državnog tijela za kibernetičku sigurnost, za razdoblje od dvije godine.

(3) U Planu provedbe vježbi kibernetičke sigurnosti iskazuju se:

a) međunarodne vježbe kibernetičke sigurnosti – vježbe koje se provode u Republici Hrvatskoj uz sudjelovanje stručnjaka iz drugih država članica ili drugih zemalja i međunarodnih organizacija te vježbe koje se održavaju u inozemstvu uz sudjelovanje predstavnika nadležnih tijela iz Republike Hrvatske

b) nacionalne vježbe kibernetičke sigurnosti – vježbe koje planiraju, organiziraju i provode nadležna tijela iz ovoga Zakona, uključujući nadležne CSIRT-ove.

(4) Planom provedbi vježbi kibernetičke sigurnosti utvrđuje se broj planiranih vježbi, nositelji vježbi, naziv i cilj vježbi, termin i lokacija održavanja vježbi, okvirni broj sudionika vježbi, nositelji financijskih obveza za provedbu vježbi te sadržaj, rokovi i način izvještavanja o provedbi vježbi.

(5) Prijedloge planova provedbi vježbi kibernetičke sigurnosti izrađuje središnje državno tijelo za kibernetičku sigurnost u suradnji s ostalim nadležnim tijelima za provedbu zahtjeva kibernetičke sigurnosti, nadležnim CSIRT-ovima i nadležnim tijelima za provedbu posebnih zakona.

DIO ŠESTI
NADLEŽNA TIJELA U PODRUČJU KIBERNETIČKE SIGURNOSTI

POGLAVLJE I.
NADLEŽNA TIJELA ZA PROVEDBU ZAHTJEVA KIBERNETIČKE SIGURNOSTI

Zadaće nadležnih tijela za provedbu zahtjeva kibernetičke sigurnosti

Članak 59.

(1) Nadležna tijela za provedbu zahtjeva kibernetičke sigurnosti obavljaju sljedeće poslove:

– provode kategorizaciju subjekata sukladno ovom Zakonu te utvrđuju i vode popise ključnih i važnih subjekata

– provode stručni nadzor nad ključnim i važnim subjektima u provedbi zahtjeva kibernetičke sigurnosti sukladno ovom Zakonu i uredbi iz članka 24. ovoga Zakona

– u poslovima kategorizacije subjekata, postupanja u slučaju značajnih incidenata te poslovima stručnog nadzora usko surađuju i koordiniraju svoj rad s tijelima državne uprave nadležnim za pojedini sektor u kojem posluju subjekti iz njihove nadležnosti

– blisko surađuju i razmjenjuju relevantne informacije s tijelima za zaštitu osobnih podataka u rješavanju incidenata koji su doveli do povrede osobnih podataka odnosno s tijelima kaznenog progona kada su incidenti rezultat kriminalnih aktivnosti

– međusobno surađuju i razmjenjuju relevantne informacije i iskustva u provedbi ovoga Zakona

– surađuju i razmjenjuju relevantne informacije s nacionalnim koordinacijskim centrom imenovanim na temelju Uredbe (EU) 2021/887 Europskog parlamenta i Vijeća od 20. svibnja 2021. o osnivanju Europskog stručnog centra za industriju, tehnologiju i istraživanja u području kibernetičke sigurnosti i mreže nacionalnih koordinacijskih centara (SL L 202/1, 8. 6. 2021.)

– surađuju s nadležnim CSIRT-ovima i

– obavljaju i druge poslove za koje je ovim Zakonom propisano da ih obavljaju tijela nadležna za provedbu zahtjeva kibernetičke sigurnosti.

(2) Nadležna tijela za provedbu zahtjeva kibernetičke sigurnosti poslove iz stavka 1. ovoga članka obavljaju prema podjeli nadležnosti iz Priloga III. ovoga Zakona.

(3) Ako za pojedini subjekt postoji nadležnost dvaju ili više tijela iz Priloga III. ovoga Zakona, radi izbjegavanja dupliciranja i preklapanja u obavljanju poslova, središnje državno tijelo za kibernetičku sigurnost, u suradnji sa svim tijelima nadležnim za subjekt, izrađuje protokol o postupanju nadležnih tijela, vodeći računa primarno o glavnoj djelatnosti subjekta.

(4) Postupak izrade protokola iz stavka 3. ovoga članka središnje državno tijelo za kibernetičku sigurnost pokreće po službenoj dužnosti, na prijedlog jednog od nadležnih tijela prema Prilogu III. ovoga Zakona ili na prijedlog subjekta.

Primjena zahtjeva kibernetičke sigurnosti na nadležna tijela za provedbu zahtjeva kibernetičke sigurnosti

Članak 60.

(1) Nadležna tijela za provedbu zahtjeva kibernetičke sigurnosti koja nisu kategorizirana kao ključni ili važni subjekti sukladno ovom Zakonu dužna su:

– primjenjivati zahtjeve kibernetičke sigurnosti iz članka 25. ovoga Zakona u skladu s odredbama uredbe iz članka 24. ovoga Zakona koje se odnose na ključne subjekte i

– najmanje jednom u dvije godine provoditi samoprocjene kibernetičke sigurnosti za mrežne i informacijske sustave kojima se služe u svom poslovanju te o provedenim samoprocjenama kibernetičke sigurnosti izvještavati središnje državno tijelo za kibernetičku sigurnost.

(2) U smislu stavka 1. podstavka 1. ovoga članka zadaće CSIRT-a obavlja središnje državno tijelo za kibernetičku sigurnost.

Zadaće središnjeg državnog tijela za kibernetičku sigurnost

Članak 61.

(1) Središnje državno tijelo za kibernetičku sigurnost, uz poslove iz članka 59. ovoga Zakona, obavlja i sljedeće poslove:

– koordinira izradu i donošenje akta strateškog planiranja iz područja kibernetičke sigurnosti

– usmjerava i prati provedbu akta strateškog planiranja iz područja kibernetičke sigurnosti

– unaprjeđuje mjere upravljanja kibernetičkim sigurnosnim rizicima planiranjem razvoja regulativnog okvira kibernetičke sigurnosti

– prati provedbu ovoga Zakona te daje preporuke, mišljenja, smjernice i upute vezane uz provedbu zahtjeva kibernetičke sigurnosti

– potiče uspostavljanje mehanizama za dobrovoljnu razmjenu informacija o kibernetičkoj sigurnosti iz članka 53. ovoga Zakona te daje preporuke, smjernice i upute radi njihove lakše uspostave

– kao tijelo odgovorno za upravljanje kibernetičkim krizama koordinira aktivnosti vezane za upravljanje kibernetičkim krizama na nacionalnoj razini

– sudjeluje u radu EU-CyCLONe mreže i u ime Republike Hrvatske koordinira aktivnosti vezane za upravljanje kibernetičkim krizama na razini Europske unije

– obavlja poslove jedinstvene kontaktne točke

– obavlja poslove CSIRT tijela prema podjeli nadležnosti iz Priloga III. ovoga Zakona

– provodi aktivnosti u svrhu otkrivanja kibernetičkih prijetnji i zaštite nacionalnog kibernetičkog prostora

– izrađuje izvješća o stanju kibernetičke sigurnosti

– surađuje s drugim nadležnim tijelima iz ovoga Zakona

– ostvaruje međunarodnu suradnju u pitanjima kibernetičke sigurnosti u okviru svojih nadležnosti utvrđenih ovim Zakonom te

– obavlja i druge poslove za koje je ovim Zakonom propisano da ih obavlja središnje državno tijelo za kibernetičku sigurnost.

(2) Središnje državno tijelo za kibernetičku sigurnost je Sigurnosno-obavještajna agencija.

Zadaće jedinstvene kontaktne točke

Članak 62.

Jedinstvena kontaktna točka obavlja sljedeće poslove:

– obavještava bez odgode Europsku komisiju o nazivima nadležnih tijela iz članka 54. stavka 12., članka 56. stavka 1., članka 61. stavka 1. podstavaka 6., 7. i 8. i članka 70. stavka 1. ovoga Zakona te njihovim zadaćama i svim naknadnim promjenama dostavljenih informacija

– obavještava bez odgode Europsku komisiju o odredbama ovoga Zakona kojima se uređuje izricanje novčanih kazni i svim naknadnim promjenama dostavljenih informacija

– sudjeluje u radu Skupine za suradnju

– osigurava prekograničnu suradnju nadležnih tijela za provedbu zahtjeva kibernetičke sigurnosti, nadležnih tijela za provedbu posebnih zakona i nadležnih CSIRT-ova s relevantnim tijelima u drugim državama članicama i, prema potrebi, s Europskom komisijom i ENISA-om

– osigurava međusektorsku suradnju nadležnih tijela za provedbu zahtjeva kibernetičke sigurnosti, nadležnih tijela za provedbu posebnih zakona i nadležnih CSIRT-ova s drugim relevantnim tijelima na nacionalnoj razini

– izrađuje smjernice o sadržaju obavijesti, načinu i rokovima obavještavanja jedinstvene kontaktne točke o zaprimljenim obavijestima o značajnim incidentima, ostalim incidentima, kibernetičkim prijetnjama i izbjegnutim incidentima te

– obavlja i druge poslove za koje je ovim Zakonom propisano da ih obavlja jedinstvena kontaktna točka.

Nacionalni centar za kibernetičku sigurnost

Članak 63.

Za obavljanje zadaća iz članaka 59., 61. i 62. ovoga Zakona u Sigurnosno-obavještajnoj agenciji ustrojava se Nacionalni centar za kibernetičku sigurnost.

POGLAVLJE II.
SURADNJA NADLEŽNIH TIJELA NA NACIONALNOJ RAZINI

Suradnja s nadležnim tijelima za provedbu posebnih zakona

Članak 64.

(1) Središnje državno tijelo za kibernetičku sigurnost i druga nadležna tijela za provedbu zahtjeva kibernetičke sigurnosti te nadležna tijela za provedbu posebnih zakona međusobno surađuju i razmjenjuju relevantne informacije i iskustva.

(2) Središnje državno tijelo za kibernetičku sigurnost pruža pomoć u provedbi nadzornih aktivnosti koje se izvršavaju na temelju posebnih zakona iz članka 8. ovoga Zakona, kada to zatraže nadležna nadzorna tijela.

(3) Pomoć iz stavka 2. ovoga članka pruža se na temelju sporazuma o suradnji kojim se uređuju sva bitna pitanja koja se odnose na koordinaciju i provedbu nadzornih aktivnosti, uključujući mehanizam za razmjenu relevantnih informacija o nadzorima te pristup informacijama povezanima s kibernetičkom sigurnošću subjekata na koje se primjenjuju posebni zakoni iz članka 8. ovoga Zakona.

(4) Središnje državno tijelo za kibernetičku sigurnost obavještava Nadzorni forum osnovan na temelju članka 32. stavka 1. Uredbe (EU) 2022/2554 o nadzornim aktivnostima koje se provode na temelju ovoga Zakona nad ključnim i važnim subjektima koji su na temelju članka 31. Uredbe (EU) 2022/2554 određeni kao ključna treća strana pružatelj IKT usluga.

Suradnja s nadležnim tijelima iz zakona kojim se uređuje područje kritične infrastrukture

Članak 65.

(1) Nadležna tijela za provedbu zahtjeva kibernetičke sigurnosti i nadležna tijela iz zakona kojim se uređuje područje kritične infrastrukture međusobno surađuju i razmjenjuju relevantne informacije, i to informacije o:

– utvrđivanju subjekata kritičnim subjektima na temelju zakona kojim se uređuje područje kritične infrastrukture

– rizicima, prijetnjama i incidentima kojima su izloženi kritični subjekti, kao i poduzetim mjerama kao odgovor na rizike, prijetnje i incidente, neovisno o tome potječu li ti rizici, prijetnje i incidenti iz kibernetičkog ili fizičkog prostora

– zahtjevima kibernetičke sigurnosti i fizičkim mjerama zaštite koje ti subjekti provode te

– rezultatima nadzornih aktivnosti provedenih nad postupanjem kritičnih subjekata sukladno ovom Zakonu odnosno zakonu kojim se uređuje područje kritične infrastrukture.

(2) Nadležna tijela iz zakona kojim se uređuje područje kritične infrastrukture mogu zatražiti od nadležnih tijela za provedbu zahtjeva kibernetičke sigurnosti i nadležnih tijela za provedbu posebnih zakona da izvršavaju svoje nadzorne ovlasti nad subjektima koji su utvrđeni kao kritični subjekti.

(3) Razmjena informacija o kritičnim subjektima odvija se u okvirima koji se uspostavljaju sporazumom središnjeg državnog tijela za kibernetičku sigurnost i nadležnog koordinativnog tijela državne uprave iz zakona kojim se uređuje područje kritične infrastrukture.

(4) Sporazumom iz stavka 3. ovoga članka uređuju se sva bitna pitanja koja se odnose na razmjenu informacija i koordinaciju nadležnih tijela, uključujući način razmjene informacija iz stavka 1. ovoga članka, kao i informacija o provedenim nadzorima nad kritičnim subjektima.

POGLAVLJE III.
CSIRT NADLEŽNOSTI

Zadaće CSIRT-a

Članak 66.

(1) CSIRT obavlja sljedeće poslove:

– prati i analizira kibernetičke prijetnje, ranjivosti i incidente i, na njihov zahtjev, pruža pomoć ključnim i važnim subjektima u vezi s praćenjem njihovih mrežnih i informacijskih sustava u stvarnom ili gotovo stvarnom vremenu

– pruža rana upozorenja i najave te informira ključne i važne subjekte, druga nadležna tijela iz ovoga Zakona ili druge relevantne dionike o kibernetičkim prijetnjama, ranjivostima i incidentima, ako je moguće u gotovo stvarnom vremenu

– obrađuje zaprimljene obavijesti o incidentima te, ako to dopuštaju okolnosti, nakon primitka obavijesti o incidentu, dostavlja ključnim i važnim subjektima relevantne informacije u pogledu daljnjeg postupanja, a osobito informacije koje bi mogle pridonijeti djelotvornom rješavanju incidenta

– odgovara na incidente te pruža pomoć ključnim i važnim subjektima, na njihov zahtjev ili uz njihovu suglasnost

– na zahtjev ključnih i važnih subjekata provodi proaktivno skeniranje mrežnih i informacijskih sustava ključnih i važnih subjekata, radi otkrivanja ranjivosti s potencijalno značajnim učinkom

– prikuplja i analizira računalne forenzičke podatke i provodi dinamičku analizu rizika i incidenata u sektorima za koje je nadležan te izrađuje pregled situacije o stanju u sektoru u pogledu kibernetičke sigurnosti

– donosi smjernice za ujednačavanje i unapređenje stanja provedbe obveze obavještavanja iz članaka 37. i 38. ovoga Zakona te provedbe dobrovoljnog obavještavanja iz članka 39. ovoga Zakona

– u suradnji s nadležnim tijelom za provedbu zahtjeva kibernetičke sigurnosti, određuje prekogranične i međusektorske učinke značajnih incidenata

– surađuje s drugim CSIRT-ovima na nacionalnoj i međunarodnoj razini

– sudjeluje u radu CSIRT mreže

– pruža uzajamnu pomoć u skladu sa svojim kapacitetima i kompetencijama drugim članovima CSIRT mreže, na njihov zahtjev

– surađuje i, prema potrebi, razmjenjuje relevantne informacije sa sektorskim ili međusektorskim zajednicama ključnih i važnih subjekata uspostavljenih na temelju sporazuma o dobrovoljnoj razmjeni informacija o kibernetičkoj sigurnosti iz članka 53. ovoga Zakona

– surađuje s relevantnim dionicima iz privatnog sektora te u svrhu uspostave takve suradnje promiče donošenje i primjenu zajedničkih ili normiranih praksi, planova za kategorizaciju i taksonomiju u odnosu na postupanje s incidentima, upravljanje kibernetičkim krizama i koordinirano otkrivanje ranjivosti na temelju članka 54. ovoga Zakona

– pridonosi uvođenju i korištenju alata za sigurnu razmjenu informacija

– sudjeluje u provedbi istorazinskih ocjenjivanja koja se provode sukladno metodologiji koju su utvrdile Skupina za suradnju, Europska komisija i ENISA

– sudjeluje u provedbi samoocjena stanja kibernetičke sigurnosti koja se provode na nacionalnoj razini te

– obavlja druge poslove za koje je ovim Zakonom propisano da ih obavlja nadležni CSIRT.

(2) Pri obavljanju zadaća iz stavka 1. ovoga članka CSIRT daje prednost prioritetnim zadaćama prema procjeni rizika, a prilikom obrade zaprimljenih obavijesti, na temelju ovoga Zakona, daje prednost obradi obavijesti o značajnim incidentima.

(3) Kada suradnja iz stavka 1. podstavka 9. ovoga članka uključuje sudjelovanje CSIRT-a u međunarodnim mrežama za suradnju i/ili suradnju s CSIRT-ovima trećih zemalja, CSIRT je dužan koristiti se odgovarajućim protokolima za razmjenu informacija.

Provođenje proaktivnog neintruzivnog skeniranja javno dostupnih mrežnih i informacijskih sustava

Članak 67.

(1) Radi otkrivanja ranjivih ili nesigurno konfiguriranih mrežnih i informacijskih sustava CSIRT može provoditi proaktivno neintruzivno skeniranje javno dostupnih mrežnih i informacijskih sustava ključnih i važnih subjekata iz svoje nadležnosti.

(2) Skeniranje iz stavka 1. ovoga članka ne smije imati negativan učinak na funkcioniranje usluga koje ključan i važan subjekt pruža i na djelatnost koju obavlja.

(3) Nadležni CSIRT dužan je obavijestiti ključnog i važnog subjekta o otkrivenim ranjivostima ili nesigurno konfiguriranim mrežnim i informacijskim sustavima na temelju skeniranja iz stavka 1. ovoga članka.

Suradnja subjekata s nadležnim CSIRT-om i nepostojanje odgovornosti CSIRT-a za uzrokovanu štetu

Članak 68.

(1) Ključni i važni subjekti dužni su surađivati s nadležnim CSIRT-om i s njim razmjenjivati potrebne informacije u postupku rješavanja incidenata.

(2) CSIRT u obavljanju svojih zadaća ne može snositi odgovornost za štetu uzrokovanu incidentom na mrežnim i informacijskim sustavima ključnih i važnih subjekata.

Osiguravanje uvjeta za obavljanje zadaća nadležnog CSIRT-a

Članak 69.

Nadležni CSIRT dužan je:

– osigurati visoku razinu dostupnosti svojih usluga komuniciranja izbjegavanjem jedinstvenih točki prekida, uz raspoloživost sredstava za mogućnost dvosmjernog komuniciranja te jasno određenim i poznatim komunikacijskim kanalima za njihove klijente i suradnike

– osigurati povjerljivost i pouzdanost aktivnosti koje provode

– svoje prostore i informacijske sustave za potporu smjestiti na sigurne lokacije

– osigurati opremljenost odgovarajućim sustavom za upravljanje zahtjevima za rješavanje incidenata

– osigurati dovoljan broj osposobljenih zaposlenika, kao i opremljenost redundantnim sustavima i odgovarajućim radnim prostorima, radi osiguravanja kontinuiteta u obavljanju CSIRT zadaća i razvoju tehničkih sposobnosti potrebnih za obavljanje CSIRT zadaća

– raspolagati sigurnom i otpornom komunikacijskom i informacijskom infrastrukturom za razmjenu informacija s ključnim i važnim subjektima te drugim relevantnim dionicima iz ovoga Zakona te

– osigurati i druge resurse koji su potrebni za učinkovito obavljanje CSIRT zadaća.

Određivanje nadležnosti CSIRT-a

Članak 70.

(1) Središnje državno tijelo za kibernetičku sigurnost, kroz Nacionalni centar za kibernetičku sigurnost i CARNET, kroz Nacionalni CERT, obavljaju zadaće CSIRT-a na nacionalnoj razini, prema podjeli nadležnosti iz Priloga III. ovoga Zakona.

(2) U smislu članka 50. stavka 1. podstavka 2. ovoga Zakona, središnje državno tijelo za kibernetičku sigurnost obavlja zadaće CSIRT-a za državna tijela, pravne osobe s javnim ovlastima i jedinice lokalne i područne (regionalne) samouprave, a CARNET obavlja zadaće CSIRT-a za javne i privatne subjekte, uključujući građanstvo.

Zadaće od javnog interesa

Članak 71.

Zadaće koje su ovim Zakonom utvrđene za središnje državno tijelo za kibernetičku sigurnost, nadležna tijela za provedbu zahtjeva kibernetičke sigurnosti i nadležne CSIRT-ove, uključujući zadaće vezane uz suradnju, pružanje pomoći i razmjenu informacija, na nacionalnoj i međunarodnoj razini, nužne su za osiguranje djelotvorne provedbe postupaka i mjera za postizanje visoke razine kibernetičke sigurnosti u sektorima od posebne važnosti za nesmetano obavljanje ključnih društvenih i gospodarskih aktivnosti i pravilno funkcioniranje unutarnjeg tržišta te je izvršavanje tih zadaća od javnog interesa.

DIO SEDMI
ZAŠTITA I OBRADA OSOBNIH PODATAKA I PRISTUP INFORMACIJAMA

Zaštita i obrada osobnih podataka

Članak 72.

Na obradu osobnih podataka koju provode nadležna tijela za provedbu zahtjeva kibernetičke sigurnosti i nadležni CSIRT-ovi u okviru svojih zadaća propisanih ovim Zakonom primjenjuje se Uredba (EU) 2016/679.

Ograničenja u korištenju i pravu pristupa informacijama

Članak 73.

(1) Popisi ključnih i važnih subjekata, kao i svi ostali zapisi koji nastaju u okviru provedbe ovoga Zakona koriste se i razmjenjuju isključivo u svrhu izvršavanja zahtjeva iz ovoga Zakona, uz poštivanje potrebe ograničavanja pristupa tim zapisima, pod uvjetima propisanim zakonom kojim se uređuje zaštita fizičkih osoba u vezi s obradom i razmjenom osobnih podataka u svrhe sprječavanja, istraživanja, otkrivanja ili progona kaznenih djela ili izvršavanja kaznenih sankcija.

(2) Popisi i ostali zapisi iz stavka 1. ovoga članka predstavljaju informacije u odnosu na koje je moguće ograničiti pravo pristupa korisniku prava na pristup informacija i ponovnu uporabu informacija, ovisno o rezultatima testa razmjernosti i javnog interesa koji se provodi prema odredbama zakona kojim se uređuje pravo na pristup informacijama.

Obveza izvještavanja o povredama koje uključuju povredu osobnih podataka

Članak 74.

(1) Ako nadležno tijelo za provedbu zahtjeva kibernetičke sigurnosti tijekom stručnog nadzora nad provedbom zahtjeva kibernetičke sigurnosti ili izvršavanja drugih aktivnosti iz ovoga Zakona sazna za povredu obveza iz članka 25. ovoga Zakona koju je počinio ključan ili važan subjekt koja uključuje povredu osobnih podataka, dužno je o toj povredi i utvrđenom činjeničnom stanju izvijestiti tijelo nadležno za zaštitu osobnih podataka bez nepotrebne odgode.

(2) Ako o povredi iz stavka 1. ovoga članka izvještava tijelo nadležno za zaštitu osobnih podataka osnovano u drugoj državi članici, nadležno tijelo za provedbu zahtjeva kibernetičke sigurnosti dužno je o istoj povredi izvijestiti i Agenciju za zaštitu osobnih podataka.

DIO OSMI
STRUČNI NADZOR NAD PROVEDBOM ZAHTJEVA KIBERNETIČKE SIGURNOSTI

POGLAVLJE I.
PROVEDBA STRUČNOG NADZORA

Provedba stručnog nadzora nad ključnim subjektom

Članak 75.

(1) Stručni nadzor nad provedbom zahtjeva kibernetičke sigurnosti (u daljnjem tekstu: stručni nadzor) u ključnom subjektu provodi se najmanje jednom u roku od tri do pet godina.

(2) Stručni nadzor nad ključnim subjektom provodi se i prije isteka rokova iz stavka 1. ovoga članka ako nadležno tijelo za provedbu zahtjeva kibernetičke sigurnosti raspolaže informacijama koje upozoravaju da subjekt ne provodi mjere upravljanja kibernetičkim sigurnosnim rizicima u skladu s propisanim obvezama ili da ne ispunjava obveze vezane uz obavještavanje o kibernetičkim prijetnjama i incidentima na propisani način i u propisanim ili ostavljenim rokovima ili da ne postupa po zahtjevima nadležnih tijela iz ovoga Zakona.

(3) Terminski plan provedbe stručnih nadzora iz stavka 1. ovoga članka utvrđuje se godišnjim planom rada nadležnog tijela za provedbu zahtjeva kibernetičke sigurnosti.

(4) U svrhu utvrđivanja terminskih planova provedbe stručnih nadzora iz stavka 1. ovoga članka te odlučivanja o prioritetima u provedbi nadzora nadležno tijelo za provedbu zahtjeva kibernetičke sigurnosti može razvrstavati ključne subjekte prema kategoriji rizičnosti.

Provedba stručnog nadzora nad važnim subjektom

Članak 76.

(1) Stručni nadzor nad važnim subjektom provodi se kada nadležno tijelo za provedbu zahtjeva kibernetičke sigurnosti raspolaže informacijama koje upozoravaju da subjekt ne provodi mjere upravljanja kibernetičkim sigurnosnim rizicima u skladu s propisanim obvezama ili da ne ispunjava obveze vezane uz obavještavanje o kibernetičkim prijetnjama i incidentima na propisani način i u propisanim ili ostavljenim rokovima ili da ne postupa po zahtjevima nadležnih tijela iz ovoga Zakona.

(2) U svrhu utvrđivanja terminskih planova provedbe stručnih nadzora iz stavka 1. ovoga članka te odlučivanja o prioritetima u provedbi nadzora nadležno tijelo za provedbu zahtjeva kibernetičke sigurnosti može razvrstavati važne subjekte prema kategoriji rizičnosti.

Način provedbe stručnog nadzora i obavijest o provedbi nadzora

Članak 77.

(1) Nadležna tijela za provedbu zahtjeva kibernetičke sigurnosti provode stručni nadzor:

– na način da se u nadziranom subjektu obavlja neposredan uvid u podatke, dokumentaciju, uvjete i načine provedbe mjera upravljanja kibernetičkim sigurnosnim rizicima, izvršavanja propisanih obveza obavještavanja o kibernetičkim prijetnjama i incidentima te postupanja po zahtjevima nadležnih tijela iz ovoga Zakona ili

– uvidom u izvješća o provedenim revizijama kibernetičke sigurnosti te po potrebi drugim, dodatno zatraženim i dostavljenim podacima i dokumentaciji nadziranog subjekta.

(2) Nadležno tijelo za provedbu zahtjeva kibernetičke sigurnosti dužno je o provedbi stručnog nadzora iz stavka 1. podstavka 1. ovoga članka obavijestiti nadzirani subjekt najkasnije u roku od pet dana prije dana početka nadzora.

(3) Iznimno od stavka 2. ovoga članka, kada se stručni nadzori provode na temelju članka 75. stavka 2. i članka 76. stavka 1. ovoga Zakona, stručni nadzor iz stavka 1. podstavka 1. ovoga članka može biti proveden bez prethodne obavijesti:

– u slučaju postojanja razloga koji upozoravaju na potrebu za hitnim postupanjem subjekta sa značajnim incidentom ili

– radi sprečavanja ili ublažavanja rizika koji proizlaze iz ozbiljne kibernetičke prijetnje.

(4) Nadležno tijelo za provedbu zahtjeva kibernetičke sigurnosti dužno je pri provedbi stručnog nadzora iz stavka 1. podstavka 1. ovoga članka voditi računa o utjecaju provedbe nadzora na rad i poslovanje nadziranog subjekta te osigurati da provedba nadzora ne dovodi do prekida u radu i poslovanju nadziranog subjekta, osim u slučaju da stručni nadzor na drugi način nije moguće provesti.

Obveze ključnih i važnih subjekata u okviru stručnog nadzora

Članak 78.

Ključni i važni subjekti dužni su omogućiti provedbu stručnog nadzora te osigurati sve uvjete za neometano provođenje stručnog nadzora, što posebno uključuje obvezu:

– omogućavanja nesmetanog pristupa i korištenja prostorima, opremom, sustavima i drugom infrastrukturom ili tehničkim sredstvima nadziranog subjekta

– omogućavanja uvida i korištenja, uključujući izradu preslika, svih potrebnih podataka i dokumentacije

– omogućavanja razgovora s nadležnim i odgovornim osobama nadziranog subjekta.

POGLAVLJE II.
OVLASTI NADLEŽNIH TIJELA ZA PROVEDBU ZAHTJEVA KIBERNETIČKE SIGURNOSTI U PROVEDBI STRUČNOG NADZORA

Opće nadzorne mjere za ključne i važne subjekte

Članak 79.

(1) Nadležno tijelo za provedbu zahtjeva kibernetičke sigurnosti ovlašteno je u obavljanju stručnog nadzora:

– provesti neposredan uvid u podatke, dokumentaciju i mrežne i informacijske sustave

– neposredno provjeriti uvjete i načine provedbe mjera upravljanja kibernetičkim sigurnosnim rizicima, uključujući nasumične provjere

– neposredno ostvariti uvid u dokumentaciju izvršavanja propisanih obveza obavještavanja o kibernetičkim prijetnjama i incidentima te drugih postupanja po zahtjevima nadležnih tijela iz ovoga Zakona

– zatražiti podatke i dokumentaciju potrebnu za ocjenjivanje proporcionalnosti mjera upravljanja kibernetičkim sigurnosnim rizicima koje subjekt primjenjuje

– zatražiti izvješća o provedenim revizijama kibernetičke sigurnosti koje je proveo revizor kibernetičke sigurnosti iz članka 32. ovoga Zakona te druge relevantne dokaze o provedbi kibernetičkih sigurnosnih politika iz članka 30. ovoga Zakona

– zatražiti i druge podatke, dokumentaciju i informacije potrebne za provedbu nadzora

– zatražiti provedbu ciljane revizije kibernetičke sigurnosti.

(2) Prilikom provedbe nadzornih mjera iz stavka 1. podstavaka 4. do 6. ovoga članka nadležno tijelo za provedbu zahtjeva kibernetičke sigurnosti dužno je navesti njezinu svrhu i pobliže odrediti podatke, dokumentaciju i druge informacije koje traži od subjekta.

(3) Kada se primjenjuje nadzorna mjera iz stavka 1. podstavka 7. ovoga članka, nadležno tijelo za provedbu zahtjeva kibernetičke sigurnosti izrađuje dodatnu analizu kibernetičke sigurnosti na temelju objektivnih, nediskriminirajućih, pravednih i transparentnih kriterija za procjenu rizika, ako je to potrebno u suradnji s nadziranim subjektom, a radi utvrđivanja preporuka za poboljšanje stanja ili smanjenje rizika kojima je subjekt izložen ili može biti izložen.

Ciljane revizije kibernetičke sigurnosti

Članak 80.

(1) Provođenje i opseg ciljane revizije kibernetičke sigurnosti određuje se ovisno o dostupnim podacima o procjeni rizika kojima je nadzirani subjekt izložen ili može biti izložen.

(2) Troškove ciljane revizije kibernetičke sigurnosti snosi nadzirani subjekt.

(3) Iznimno od stavka 2. ovoga članka, troškove ciljane revizije kibernetičke sigurnosti može snositi nadležno tijelo za provedbu zahtjeva kibernetičke sigurnosti ako se ocjena provodi u okviru provedbe hitnih mjera koje je potrebno poduzeti kako bi se izbjegli ili spriječili značajni incidenti ili ublažile posljedice značajnih incidenata ili drugih rizika kojima je nadzirani subjekt izložen, a koji imaju ili mogu imati prekogranični ili međusektorski učinak.

Posebne nadzorne mjere za ključne subjekte

Članak 81.

(1) Osim nadzornih mjera iz članka 79. ovoga Zakona, u obavljanju stručnog nadzora nad ključnim subjektom nadležno tijelo za provedbu zahtjeva kibernetičke sigurnosti ovlašteno je zatražiti provedbu:

– redovite revizije kibernetičke sigurnosti, kada raspolaže informacijama iz kojih proizlazi da subjekt reviziju kibernetičke sigurnosti nije proveo u rokovima iz članka 34. stavka 1. ovoga Zakona i

– izvanredne revizije kibernetičke sigurnosti, u slučaju značajnog incidenta ili kada utvrdi da su u prethodno provedenoj reviziji kibernetičke sigurnosti utvrđene nepravilnosti, nedostaci ili propusti u provedbi mjera upravljanja kibernetičkim sigurnosnim rizicima koji u međuvremenu nisu otklonjeni ili raspolaže informacijama da subjekt ne provodi mjere upravljanja kibernetičkim sigurnosnim rizicima sukladno ovom Zakonu i uredbi iz članka 24. ovoga Zakona.

(2) Na troškove revizija kibernetičke sigurnosti provedenih na temelju stavka 1. ovoga članka primjenjuje se članak 34. stavak 7. ovoga Zakona.

(3) Kada se primjenjuje posebna nadzorna mjera iz stavka 1. podstavka 2. ovoga članka za slučaj značajnog incidenta, nadležno tijelo za provedbu zahtjeva kibernetičke sigurnosti izrađuje dodatnu analizu kibernetičke sigurnosti iz članka 79. stavka 3. ovoga Zakona.

POGLAVLJE III.
KOREKTIVNE MJERE, PRIVREMENE SUSPENZIJE I ZABRANE OBAVLJANJA DJELATNOSTI

Korektivne mjere za ključne i važne subjekte

Članak 82.

(1) Nadležno tijelo za provedbu zahtjeva kibernetičke sigurnosti, ovisno o rezultatima stručnog nadzora, ključnim i važnim subjektima može izreći sljedeće korektivne mjere:

– izdati upozorenja o povredama ovoga Zakona i uredbe iz članka 24. ovoga Zakona

– izdati obvezujuće upute ili naloge kojima se zahtijeva da otklone utvrđene nedostatke ili povrede ovoga Zakona i uredbe iz članka 24. ovoga Zakona, uz navođenje mjera koje subjekt treba provesti radi sprečavanja značajnih incidenata ili otklanjanja njihovih posljedica

– naložiti da prestanu s postupanjem koje je u suprotnosti s ovim Zakonom i uredbom iz članka 24. ovoga Zakona i da ne ponavljaju takvo postupanje

– naložiti da osiguraju da su njihove mjere upravljanja kibernetičkim sigurnosnim rizicima u skladu s propisanim obvezama ili da ispune obveze obavještavanja o kibernetičkim prijetnjama i incidentima na propisani način i u propisanom ili ostavljenom roku odnosno da na određeni način i/ili ostavljenom roku postupe po zahtjevima nadležnih tijela iz ovoga Zakona

– naložiti da u razumnom roku provedu preporuke koje su dane u izvješću o provedenoj reviziji kibernetičke sigurnosti ili u okviru izrađenih analiza sigurnosti i

– naložiti da objave aspekte povreda ovoga Zakona i uredbe iz članka 24. ovoga Zakona na određeni način.

(2) Upute i nalozi iz stavka 1. ovoga članka moraju sadržavati rok za provedbu korektivnih mjera i rok za obavještavanje o provedbi izrečenih korektivnih mjera.

(3) Ako ključan ili važan subjekt ne postupi sukladno izrečenim korektivnim mjerama iz stavka 1. podstavaka 1. do 5. ovoga članka, nadležno tijelo za provedbu zahtjeva kibernetičke sigurnosti odredit će subjektu dodatni primjereni rok za provedbu korektivnih mjera.

(4) Iznimno od stavka 3. ovoga članka, u iznimnim slučajevima nadziranom subjektu neće se odrediti dodatni primjeren rok za provedbu korektivnih mjera, ako bi to onemogućilo poduzimanje hitnih mjera koje su naložene radi sprečavanja značajnih incidenata ili odgovora na takve incidente.

Posebna korektivna mjera za ključne subjekte

Članak 83.

(1) Osim korektivnih mjera iz članka 82. ovoga Zakona, nadležno tijelo za provedbu zahtjeva kibernetičke sigurnosti može na određeno razdoblje imenovati službenika za praćenje usklađenosti ključnog subjekta sa zahtjevima kibernetičke sigurnosti.

(2) Odluka o imenovanju iz stavka 1. ovoga članka mora sadržavati razdoblje za koje se imenuje službenik za praćenje usklađenosti subjekta sa zahtjevima kibernetičke sigurnosti i njegove zadaće.

Privremene suspenzije i zabrane obavljanja djelatnosti

Članak 84.

(1) Ako ključan subjekt ne postupi u skladu s izrečenim korektivnim mjerama iz članka 82. ovoga Zakona, nadležno tijelo za provedbu zahtjeva kibernetičke sigurnosti može:

– zatražiti nadležno tijelo da privremeno suspendira ovlaštenje izdano subjektu za pružanje usluga ili obavljanje djelatnosti iz Priloga I. odnosno Priloga II. ovoga Zakona

– zahtijevati od nadležnog tijela privremenu zabranu obavljanja upravljačkih dužnosti u ključnom subjektu fizičkim osobama iz članka 29. ovoga Zakona.

(2) Mjere iz stavka 1. ovoga članka primjenjuju se samo dok ključni subjekt ne postupi sukladno izrečenim korektivnim mjerama iz članka 82. ovoga Zakona.

(3) Mjere iz stavka 1. ovoga članka ne primjenjuju se na tijela državne uprave, druga državna tijela, jedinice lokalne i područne (regionalne) samouprave i javne subjekte koji u svojstvu tijela javnog prava predstavljaju javne naručitelje u smislu propisa kojim se uređuje javna nabava.

Okolnosti koje se uzimaju u obzir prilikom donošenja odluka o izricanju korektivnih mjera, predlaganju privremenih suspenzija i zabrane obavljanja djelatnosti

Članak 85.

(1) Prilikom donošenja odluka o izricanju korektivnih mjera iz članaka 82. i 83. ovoga Zakona odnosno podnošenju zahtjeva sukladno članku 84. ovoga Zakona nadležno tijelo za provedbu zahtjeva kibernetičke sigurnosti uzima u obzir:

– ozbiljnost povrede i važnost odredaba koje nadzirani subjekt krši

– trajanje povrede

– relevantne prethodno počinjene povrede od strane istog subjekta

– štetu koja je uzrokovana, uključujući financijske ili gospodarske gubitke, učinke na druge usluge ili djelatnosti i broj pogođenih korisnika

– je li nadzirani subjekt djelovao s namjerom ili nepažnjom

– mjere koje je nadzirani subjekt poduzeo radi sprečavanja ili ublažavanja štete

– postupanja sukladna relevantnim kodeksima ponašanja ili pravilima i uvjetima certificiranja za pružanje usluga odnosno obavljanje djelatnosti i

– razinu suradnje osoba iz članka 29. ovoga Zakona s nadležnim tijelima iz ovoga Zakona.

(2) Ozbiljnim povredama iz stavka 1. podstavka 1. ovoga članka smatraju se:

– opetovane povrede

– neprijavljivanje ili nerješavanje značajnih incidenata

– neuklanjanje nepravilnosti i nedostataka u skladu s uputama ili nalozima nadležnog tijela za provedbu zahtjeva kibernetičke sigurnosti

– onemogućavanje ili otežavanje provedbe postupka revizije kibernetičke sigurnosti koje je zatražilo nadležno tijelo za provedbu zahtjeva kibernetičke sigurnosti ili aktivnosti praćenja koje je naložilo na temelju članka 83. ovoga Zakona i

– davanje lažnih ili izrazito netočnih informacija povezanih s provedbom zahtjeva kibernetičke sigurnosti ili drugih obveza koje za nadziranog subjekta proizlaze iz ovoga Zakona ili uredbe iz članka 24. ovoga Zakona.

Izricanje novčanih kazni

Članak 86.

(1) Uz korektivne mjere propisane ovim Zakonom i podnošenje zahtjeva sukladno članku 84. ovoga Zakona, nadležno tijelo za provedbu zahtjeva kibernetičke sigurnosti može protiv prekršajno odgovornih ključnih i važnih subjekata podnijeti prijavu ovlaštenom tužitelju odnosno izdati prekršajni nalog sukladno prekršajnim odredbama ovoga Zakona.

(2) Iznimno od stavka 1. ovoga članka, u stručnim nadzorima ne može se podnijeti prijava ovlaštenom tužitelju odnosno izdati prekršajni nalog sukladno prekršajnim odredbama ovoga Zakona ako je nadziranom subjektu tijelo nadležno za zaštitu osobnih podataka za povrede osobnih podataka koje proizlaze iz istog postupanja subjekta izreklo upravnu novčanu kaznu sukladno Uredbi (EU) 2016/679.

POGLAVLJE IV.
ZAPISNIK O PROVEDENOM STRUČNOM NADZORU

Sadržaj zapisnika

Članak 87.

(1) Nakon provedenoga stručnog nadzora nadležno tijelo za provedbu zahtjeva kibernetičke sigurnosti sastavlja zapisnik o provedenom nadzoru (u daljnjem tekstu: zapisnik).

(2) Primjerak zapisnika dostavlja se čelniku nadziranog subjekta odnosno drugoj odgovornoj osobi za nadzirani subjekt (u daljnjem tekstu: odgovorna osoba).

(3) Zapisnik obvezno sadržava naznaku predmeta stručnog nadzora, utvrđeno činjenično stanje i uputu o pravu na podnošenje primjedbi na zapisnik.

(4) Ako su u provedenom stručnom nadzoru utvrđene povrede propisanih obveza ili neusklađenost sa zahtjevima kibernetičke sigurnosti, zapisnik obvezno sadržava opis utvrđenih povreda i neusklađenosti, izrečene nadzorne mjere te obvezu obavještavanja o poduzetim korektivnim mjerama.

Primjedbe na zapisnik

Članak 88.

(1) Odgovorna osoba može izjaviti primjedbe na zapisnik, u pisanom obliku, u roku koje mu je za dostavu primjedbi odredilo nadležno tijelo za provedbu zahtjeva kibernetičke sigurnosti.

(2) Prilikom određivanja rokova za dostavu primjedbi vodi se računa o veličini subjekta, opsežnosti provedenog stručnog nadzora te s tim u svezi utvrđenog činjeničnog stanja, primijenjenih nadzornih mjera, kao i utvrđenih rezultata stručnog nadzora.

(3) Iznimno od stavka 2. ovoga članka, u iznimnim slučajevima nadziranom subjektu neće se omogućiti podnošenje primjedbi na zapisnik, ako bi to onemogućilo poduzimanje hitnih mjera koje su naložene radi sprečavanja značajnih incidenata ili odgovora na takve incidente.

Postupanje po primjedbama na zapisnik

Članak 89.

(1) Ako nadležno tijelo za provedbu zahtjeva kibernetičke sigurnosti utvrdi da su primjedbe na zapisnik u cijelosti ili djelomično osnovane, sastavit će dopunski zapisnik kojim će odlučiti o primjedbama.

(2) Ako nadležno tijelo za provedbu zahtjeva kibernetičke sigurnosti utvrdi da su primjedbe na zapisnik u cijelosti neosnovane, obvezan je o tome dostaviti pisanu obavijest nadziranom subjektu.

(3) Dopunski zapisnik iz stavka 1. odnosno obavijest iz stavka 2. ovoga članka dostavlja se odgovornoj osobi u roku od 30 dana od dana primitka primjedbi.

(4) Protiv dopunskog zapisnika i obavijesti iz stavka 3. ovoga članka primjedbe nisu dopuštene.

Sudska zaštita

Članak 90.

Nakon dostave dopunskog zapisnika odnosno obavijesti iz članka 89. ovoga Zakona ovlaštena osoba nadziranog subjekta može tužbom pred nadležnim upravnim sudom zatražiti ocjenu zakonitosti postupanja nadležnog tijela za provedbu zahtjeva kibernetičke sigurnosti u odnosu na predmet stručnog nadzora i zapisnik sastavljen o provedenom stručnom nadzoru.

Obvezujuće upute za tijela državne uprave, druga državna tijela i jedinice lokalne i područne (regionalne) samouprave

Članak 91.

(1) Ako su u stručnom nadzoru tijela državne uprave, drugih državnih tijela i jedinica lokalne i područne (regionalne) samouprave utvrđeni nedostaci i povrede ovoga Zakona i uredbe iz članka 24. ovoga Zakona, a nadzirano tijelo ne provede izrečene korektivne mjere u ostavljenom roku, središnje državno tijelo za informacijsku sigurnost dostavlja središnjem državnom tijelu za kibernetičku sigurnost izvješće o rezultatima stručnog nadzora tog tijela.

(2) Središnje državno tijelo za kibernetičku sigurnost izdaje obvezujuće upute o provedbi mjera koje je čelnik nadziranog tijela dužan osigurati, određujući i rok provedbe tih mjera te o tome obavještava Vladu.

Očevidnici o obavljenim stručnim nadzorima

Članak 92.

(1) Nadležna tijela za provedbu zahtjeva kibernetičke sigurnosti dužna su voditi očevidnike o obavljenim stručnim nadzorima.

(2) Očevidnici iz stavka 1. ovoga članka vode se sukladno smjernicama središnjeg državnog tijela za kibernetičku sigurnost.

Stručni nadzor nad pružateljima javnih elektroničkih komunikacijskih mreža i pružateljima javno dostupnih elektroničkih komunikacijskih usluga

Članak 93.

Poslove stručnog nadzora nad primjenom odredaba ovoga Zakona i uredbe iz članka 24. ovoga Zakona koji se odnose na stručni nadzor nad pružateljima javnih elektroničkih komunikacijskih mreža i pružateljima javno dostupnih elektroničkih komunikacijskih usluga obavljaju inspektori elektroničkih komunikacija u skladu s ovim Zakonom i zakonom kojim je uređeno područje elektroničkih komunikacija.

POGLAVLJE V.
UZAJAMNA POMOĆ U PROVEDBI STRUČNIH NADZORA S NADLEŽNIM TIJELIMA DRUGIH DRŽAVA ČLANICA

Provedba nadzora s prekograničnim elementima

Članak 94.

Nadležno tijelo za provedbu zahtjeva kibernetičke sigurnosti može stručni nadzor ključnog ili važnog subjekta koji pruža usluge u više od jednoj državi članici ili pruža usluge u jednoj ili više država članica, a njegovi se mrežni i informacijski sustavi nalaze u drugoj državi članici ili u više njih, provoditi uz međusobnu uzajamnu pomoć i u suradnji s nadležnim tijelima tih država članica.

Okviri pružanja uzajamne pomoći

Članak 95.

(1) Uzajamna pomoć iz članka 94. ovoga Zakona obuhvaća:

– slanje obavijesti, putem jedinstvene kontaktne točke, o poduzetim nadzornim mjerama i izrečenim korektivnim mjerama te davanje savjeta

– podnošenje zahtjeva za poduzimanje nadzornih mjera ili izricanje korektivnih mjera i

– nakon primitka obrazloženog zahtjeva, pružanje pomoći razmjerne vlastitim resursima kako bi se nadzorne mjere ili izrečene korektivne mjere mogle provesti na djelotvoran, učinkovit i dosljedan način.

(2) Uzajamna pomoć iz stavka 1. podstavka 3. ovoga članka može obuhvaćati postupanje po zahtjevima za dostavu relevantnih informacija i poduzimanje nadzornih mjera ili izricanje korektivnih mjera, uključujući zahtjeve za provođenje stručnih nadzora ili ciljanih revizija kibernetičke sigurnosti.

(3) Nadležno tijelo za provedbu zahtjeva kibernetičke sigurnosti kojem je upućen zahtjev za uzajamnu pomoć u provedbi stručnog nadzora ne smije odbiti zahtjev, osim kada utvrdi da:

– nije nadležan za pružanje zatražene pomoći

– da zatražena pomoć nije razmjerna ovlastima nadležnog tijela ili

– da se zahtjev odnosi na informacije ili uključuje aktivnosti koje bi, u slučaju da se otkriju ili provedu, bile protivne interesima nacionalne sigurnosti, javne sigurnosti ili obrane.

(4) Nadležno tijelo za provedbu zahtjeva kibernetičke sigurnosti dužno je prije odbijanja zahtjeva iz stavka 3. ovoga članka savjetovati se s nadležnim tijelima države članice koja je podnijela zahtjev.

(5) U slučaju iz stavka 4. ovoga članka, na zahtjev uključene države članice, nadležno tijelo za provedbu zahtjeva kibernetičke sigurnosti dužno je savjetovati se i s Europskom komisijom i ENISA-om.

(6) Odredbe ovoga članka primjenjuju se i u slučaju zaprimanja zahtjeva za uzajamnu pomoć u provedbi stručnog nadzora nad subjektima iz članka 14. stavka 3. ovoga Zakona koji pružaju usluge ili imaju mrežne i informacijske sustave na državnom području Republike Hrvatske.

Zajednička provedba nadzornih mjera

Članak 96.

Nadležno tijelo za provedbu zahtjeva kibernetičke sigurnosti može s nadležnim tijelima drugih država članica zajednički provoditi nadzorne mjere iz ovoga Zakona.

POGLAVLJE VI.
KONTROLA USKLAĐENOSTI S POSEBNIM ZAHTJEVIMA ZA UPRAVLJANJE PODACIMA O REGISTRACIJI NAZIVA DOMENA

Način provedbe kontrola, obavijesti o provedbi kontrola i obveze subjekata nad kojima se provodi kontrola

Članak 97.

(1) Kontrola usklađenosti iz članka 49. ovoga Zakona (u daljnjem tekstu: kontrola usklađenosti) provodi se u svakom subjektu kontrole najmanje jednom godišnje.

(2) Tijelo državne uprave nadležno za znanost i obrazovanje provodi kontrole usklađenosti:

– na način da se u registru naziva vršne nacionalne internetske domene i registrarima obavlja neposredan uvid u podatke, dokumentaciju, uvjete i načine provedbe posebnih zahtjeva za upravljanje podacima o registraciji naziva domena iz članaka 45. do 48. ovoga Zakona ili

– uvidom u zatražene i dostavljene podatke i dokumentaciju kontroliranog subjekta.

(3) Tijelo državne uprave nadležno za znanost i obrazovanje dužno je o provedbi kontrola iz stavka 2. podstavka 1. ovoga članka obavijestiti subjekt nad kojim provodi kontrolu najkasnije u roku od pet dana prije dana početka kontrole.

(4) Iznimno od stavka 2. ovoga članka, kontrola usklađenosti može biti provedena bez prethodne obavijesti u slučaju postojanja opravdanih razloga za hitno postupanje.

(5) Registar naziva vršne nacionalne internetske domene i registrari dužni su omogućiti provedbu kontrola usklađenosti te osigurati sve uvjete za njihovo neometano provođenje, što posebno uključuje obvezu:

– omogućavanja nesmetanog pristupa i korištenja prostorima, opremom, sustavima i drugom infrastrukturom ili tehničkim sredstvima registra naziva vršne nacionalne internetske domene i registrara

– omogućavanja uvida i korištenja, uključujući izradu preslika, svih potrebnih podataka i dokumentacije

– omogućavanje razgovora s nadležnim i odgovornim osobama registra naziva vršne nacionalne internetske domene i registrara.

Izricanje korektivnih mjera

Članak 98.

(1) Tijelo državne uprave nadležno za znanost i obrazovanje, ovisno o rezultatima provedene kontrole usklađenosti, registru naziva vršne nacionalne internetske domene i registrarima može:

– izdati upozorenja o povredama ovoga Zakona

– izdati obvezujuće upute ili naloge kojima se zahtijeva da otklone utvrđene nedostatke ili povrede ovoga Zakona, uz navođenje mjera koje subjekt treba provesti radi otklanjanja tih nedostataka ili povreda.

(2) Upute i nalozi iz stavka 1. ovoga članka moraju sadržavati rok za provedbu naloženih mjera i rok za obavještavanje o njihovoj provedbi.

Privremene suspenzije ovlaštenja izdanih za pružanje usluga registracije domena

Članak 99.

(1) Ako registrari ne postupe u skladu s upozorenjima, uputama ili nalozima iz članka 98. ovoga Zakona, tijelo državne uprave nadležno za znanost i obrazovanje zatražit će CARNET da privremeno suspendira ovlaštenje izdano subjektu za pružanje usluga registracija domena.

(2) Mjera iz stavka 1. ovoga članka primjenjuje se samo dok subjekt ne postupi sukladno upozorenjima, uputama ili nalozima iz članka 98. ovoga Zakona.

Zapisnici o provedenim kontrolama i sudska zaštita

Članak 100.

Prilikom provedbe kontrola usklađenosti na odgovarajući se način primjenjuju članci 87. do 90. te članak 92. stavak 1. ovoga Zakona.

DIO DEVETI
PREKRŠAJNE ODREDBE

Novčane kazne za ključne subjekte

Članak 101.

(1) Novčanom kaznom u iznosu od 10.000,00 eura do 10.000.000,00 eura ili u iznosu od 0,5 % do najviše 2 % ukupnog godišnjeg prometa dotičnog subjekta na svjetskoj razini ostvarenog u prethodnoj financijskoj godini, ovisno o tome koji je iznos veći, kaznit će se za prekršaj prekršajno odgovoran ključan subjekt:

– koji ne poduzima, djelomično poduzima ili ne poduzima u roku propisane mjere upravljanja kibernetičkim sigurnosnim rizicima (članak 26. ovoga Zakona)

– koji se prilikom provedbe mjera upravljanja kibernetičkim sigurnosnim rizicima ne koristi certificiranim IKT proizvodima, IKT uslugama i IKT procesima, ako je takva obveza propisana za subjekta (članak 28. ovoga Zakona)

– čije osobe odgovorne za upravljanje mjerama ne odobravaju mjere upravljanja kibernetičkim sigurnosnim rizicima i/ili ne kontroliraju njihovu provedbu odnosno ne osiguravaju provedbu odgovarajućih osposobljavanja u svrhu stjecanja znanja i vještina u pitanjima upravljanja kibernetičkim sigurnosnim rizicima i njihova učinka na usluge koje subjekt pruža odnosno djelatnost koju obavlja (članak 29. ovoga Zakona)

– koji ne obavještava o svakom značajnom incidentu ili ne dostavlja u roku obavijesti o značajnim incidentima (članak 37. ovoga Zakona)

– koji ne obavještava ili ne obavještava u roku primatelje usluga o značajnim incidentima i ozbiljnim kibernetičkim prijetnjama te o svim mjerama ili pravnim sredstvima koje ti primatelji mogu poduzeti kao odgovor na prijetnju (članak 38. ovoga Zakona)

– koji ne provede reviziju kibernetičke sigurnosti najmanje jednom u dvije godine (članak 34. ovoga Zakona)

– koji ne dostavi u propisanom roku izvješće o provedenoj reviziji kibernetičke sigurnosti nadležnom tijelu za provedbu zahtjeva kibernetičke sigurnosti (članak 34. ovoga Zakona)

– koji onemogućava, ometa ili otežava provedbu revizije kibernetičke sigurnosti ili ne snosi troškove provedbe revizije kibernetičke sigurnosti (članak 34. ovoga Zakona)

– koji ne surađuje s nadležnim CSIRT-om i s njim ne razmjenjuje potrebne informacije u postupku rješavanja incidenata (članak 68. ovoga Zakona)

– koji ne surađuje s nadležnim tijelom pri obavljanju nadzora ili mu ne dostavlja tražene podatke ili dokumentaciju (članci 77. i 79. ovoga Zakona)

– koji nadležnim tijelima tijekom stručnog nadzora ne omogući nesmetani pristup prostorima, opremi, sustavima i dokumentaciji nužnima za provođenje nadzora (članak 78. ovoga Zakona)

– koji ne postupi ili djelomično postupi ili ne postupi u za to ostavljenom roku po korektivnim mjerama izrečenim u stručnom nadzoru (članci 82. i 83. ovoga Zakona).

(2) Za prekršaj iz stavka 1. ovoga članka kaznit će se i fizičke osobe koje su sukladno članku 29. ovoga Zakona odgovorne za upravljanje mjerama prekršajno odgovornog ključnog subjekta, novčanom kaznom u iznosu od 1000,00 do 6000,00 eura.

(3) Pri odlučivanju o izricanju kazne sukladno stavcima 1. i 2. ovoga članka i njezinoj visini uzimaju se u obzir okolnosti iz članka 85. ovoga Zakona.

Novčane kazne za važne subjekte

Članak 102.

(1) Novčanom kaznom u iznosu od 5000,00 eura do 7.000.000,00 eura ili u iznosu od 0,2 % do najviše 1,4 % ukupnog godišnjeg prometa dotičnog subjekta na svjetskoj razini ostvarenog u prethodnoj financijskoj godini, ovisno o tome koji je iznos veći, kaznit će se za prekršaj prekršajno odgovorni važni subjekt:

– koji ne poduzima, djelomično poduzima ili ne poduzima u roku propisane mjere upravljanja kibernetičkim sigurnosnim rizicima (članak 26. ovoga Zakona)

– koji se prilikom provedbe mjera upravljanja kibernetičkim sigurnosnim rizicima ne koristi certificiranim IKT proizvodima, IKT uslugama i IKT procesima, ako je takva obveza propisana za subjekta (članak 28. ovoga Zakona)

– čije osobe odgovorne za upravljanje mjerama ne odobravaju mjere upravljanja kibernetičkim sigurnosnim rizicima i/ili ne kontroliraju njihovu provedbu odnosno ne osiguravaju provedbu odgovarajućih osposobljavanja u svrhu stjecanja znanja i vještina u pitanjima upravljanja kibernetičkim sigurnosnim rizicima i njihova učinka na usluge koje subjekt pruža odnosno djelatnost koju obavlja (članak 29. ovoga Zakona)

– koji ne obavještava o svakom značajnom incidentu ili ne dostavlja u roku obavijesti o značajnim incidentima (članak 37. ovoga Zakona)

– koji ne obavještava ili ne obavještava u roku primatelje usluga o značajnim incidentima i ozbiljnim kibernetičkim prijetnjama te o svim mjerama ili pravnim sredstvima koje ti primatelji mogu poduzeti kao odgovor na prijetnju (članak 38. ovoga Zakona)

– koji ne provede samoprocjenu kibernetičke sigurnosti najmanje jednom u dvije godine (članak 35. ovoga Zakona)

– koji ne dostavi u propisanom roku izjavu o sukladnosti ili plan daljnjeg postupanja nadležnom tijelu za provedbu zahtjeva kibernetičke sigurnosti (članak 35. ovoga Zakona)

– koji onemogućava, ometa ili otežava provedbu ciljane revizije kibernetičke sigurnosti ili ne snosi troškove provedbe revizije kibernetičke sigurnosti (članak 34. ovoga Zakona)

– koji ne surađuje s nadležnim CSIRT-om i s njim ne razmjenjuje potrebne informacije u postupku rješavanja incidenta (članak 68. ovoga Zakona)

– koji ne surađuje s nadležnim tijelom pri obavljanju nadzora ili mu ne dostavlja tražene podatke ili dokumentaciju (članci 77. i 79. ovoga Zakona)

– koji nadležnim tijelima tijekom stručnog nadzora ne omogući nesmetani pristup prostorima, opremi, sustavima i dokumentaciji nužnima za provođenje nadzora (članak 78. ovoga Zakona)

– koji ne postupi ili djelomično postupi ili ne postupi u za to ostavljenom roku po korektivnim mjerama izrečenim u stručnom nadzoru (članak 82. ovoga Zakona).

(2) Za prekršaj iz stavka 1. ovoga članka kaznit će se i fizičke osobe koje su sukladno članku 29. ovoga Zakona odgovorne za upravljanje mjerama prekršajno odgovornog važnog subjekta, novčanom kaznom u iznosu od 500,00 do 3000,00 eura.

(3) Pri odlučivanju o izricanju kazne sukladno stavcima 1. i 2. ovoga članka i njezinoj visini uzimaju se u obzir okolnosti iz članka 85. ovoga Zakona.

Novčane kazne za nepoštivanje obveze dostave podataka

Članak 103.

(1) Novčanom kaznom u iznosu od 2000,00 eura do 20.000,00 eura kaznit će se za prekršaj prekršajno odgovorni subjekti:

– iz Priloga I. i Priloga II. ovoga Zakona ako ne dostave ili ne dostave u roku podatke potrebne za provedbu kategorizacije subjekata odnosno vođenje popisa ključnih i važnih subjekata ili pravodobno ne obavještavaju o promjenama podataka (članak 20. ovoga Zakona)

– iz članka 22. ovoga Zakona ako ne dostave ili ne dostave u roku podatke potrebne za vođenje posebnog registra subjekata ili pravodobno ne obavještavaju o promjenama podataka (članak 23. ovoga Zakona).

(2) Za prekršaj iz stavka 1. ovoga članka kaznit će se i odgovorna osoba subjekta iz stavka 1. ovoga članka novčanom kaznom u iznosu od 200,00 do 1000,00 eura.

Ovlašteni tužitelj

Članak 104.

(1) U slučaju postojanja sumnje da je počinjen prekršaj, nadležno tijelo za provedbu zahtjeva kibernetičke sigurnosti podnosi prijavu ovlaštenom tužitelju.

(2) Ovlašteni tužitelj u smislu ovoga Zakona nadležni je državni odvjetnik koji podnosi optužni prijedlog.

(3) Iznimno od stavka 2. ovoga članka, ovlašteni tužitelj za prekršaje koje počine pružatelji javnih elektroničkih komunikacijskih mreža i pružatelji javno dostupnih elektroničkih komunikacijskih usluga regulatorno je tijelo za mrežne djelatnosti.

(4) Iznimno od stavka 2. ovoga članka, ovlašteni tužitelj za prekršaje koje počine pružatelji usluga povjerenja tijelo je državne uprave nadležno za razvoj digitalnog društva.

DIO DESETI
PRIJELAZNE I ZAVRŠNE ODREDBE

Obveze operatora ključnih usluga i davatelja digitalnih usluga u prijelaznom razdoblju

Članak 105.

Operatori ključnih usluga i davatelji digitalnih usluga koji su do stupanja na snagu ovoga Zakona provodili mjere za postizanje visoke razine kibernetičke sigurnosti prema odredbama Zakona o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga (»Narodne novine«, br. 64/18.) i Uredbe o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga (»Narodne novine«, br. 68/18.) nastavljaju s provedbom mjera na temelju tih propisa do dostave obavijesti o provedenoj kategorizaciji subjekta iz članka 19. stavaka 1. i 3. ovoga Zakona.

Obveze pružatelja javnih elektroničkih komunikacijskih mreža, pružatelja javno dostupnih elektroničkih komunikacijskih usluga i pružatelja usluga povjerenja u prijelaznom razdoblju

Članak 106.

(1) Pružatelji javnih elektroničkih komunikacijskih mreža i pružatelji javno dostupnih elektroničkih komunikacijskih usluga koji su do stupanja na snagu ovoga Zakona provodili sigurnosne za-

htjeve u svrhu zaštite sigurnosti elektroničkih komunikacijskih mreža i elektroničkih komunikacijskih usluga prema odredbama članka 41. Zakona o elektroničkim komunikacijama (»Narodne novine«, br. 76/22.) nastavljaju s provedbom zahtjeva na temelju članka 41. toga Zakona do dostave obavijesti o provedenoj kategorizaciji subjekta iz članka 19. stavka 1. ovoga Zakona.

(2) Pružatelji usluga povjerenja koji su do stupanja na snagu ovoga Zakona provodili sigurnosne zahtjeve u svrhu zaštite sigurnosti usluga povjerenja prema odredbama Uredbe (EU) br. 910/2014 o elektroničkoj identifikaciji i uslugama povjerenja za elektroničke transakcije na unutarnjem tržištu i stavljanju izvan snage Direktive 1999/93/EZ i Zakona o provedbi Uredbe (EU) br. 910/2014 Europskog parlamenta i Vijeća od 23. srpnja 2014. o elektroničkoj identifikaciji i uslugama povjerenja za elektroničke transakcije na unutarnjem tržištu i stavljanju izvan snage Direktive 1999/93/EZ (»Narodne novine«, br. 62/17.) nastavljaju s provedbom zahtjeva na temelju tih propisa do dostave obavijesti o provedenoj kategorizaciji subjekta iz članka 19. stavka 1. ovoga Zakona.

Prijelazna odredba o sklopljenim sporazumima o pristupanju nacionalnom sustavu

Članak 107.

Sporazumi o pristupanju nacionalnom sustavu koji su sklopljeni na temelju Odluke o mjerama i aktivnostima za podizanje nacionalnih sposobnosti pravovremenog otkrivanja i zaštite od državno sponzoriranih kibernetičkih napada, Advanced Persistent Threat (ATP) kampanja te drugih kibernetičkih ugroza, klasa: 022-03/21-04/91, urbroj: 50301-29/09-21-2, od 1. travnja 2021., ostaju na snazi do njihova isteka.

Rok za usklađivanje sa zahtjevima koji se odnose na upravljanje podacima o registraciji naziva domena i provođenje provjera za postojeće korisnike domena

Članak 108.

Registar naziva vršne nacionalne internetske domene i registrari dužni su uskladiti se sa zahtjevima iz ovoga Zakona koji se odnose na upravljanje podacima o registraciji naziva domena i provesti provjere iz članka 47. stavka 2. ovoga Zakona za postojeće korisnike domena u roku od godine dana od dana stupanja na snagu ovoga Zakona.

Započeti postupci

Članak 109.

(1) Postupci započeti prema odredbama Zakona o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga (»Narodne novine«, br. 64/18.) dovršit će se prema odredbama toga Zakona i propisa donesenih na temelju toga Zakona.

(2) Postupci započeti prema odredbama članka 41. Zakona o elektroničkim komunikacijama (»Narodne novine«, br. 76/22.) dovršit će se prema odredbama toga Zakona i propisa donesenih na temelju toga Zakona.

Rok za provedbu prve kategorizacije subjekata

Članak 110.

(1) Nadležna tijela za provedbu zahtjeva kibernetičke sigurnosti iz članka 4. stavka 1. točke 28. ovoga Zakona i nadležna tijela za provedbu posebnih zakona iz članka 4. stavka 1. točke 27. ovoga Zakona provest će prvu kategorizaciju subjekata i dostavu obavijesti o provedenoj kategorizaciji subjekata u roku od godinu dana od dana stupanja na snagu ovoga Zakona.

(2) Postupak kategorizacije subjekata i dostava obavijesti o provedenoj kategorizaciji subjekata provest će se u roku iz stavka 1. ovoga članka za sve operatore ključnih usluga s popisa iz članka 12. Zakona o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga (»Narodne novine«, br. 64/18.).

(3) Postupak prve kategorizacije informacijskih posrednika u razmjeni elektroničkog računa među poduzetnicima i dostava obavijesti o provedenoj kategorizaciji sukladno ovom Zakonu provest će se u roku od tri mjeseca od stupanja na snagu zakona kojim se uređuje razmjena elektroničkog računa između poduzetnika.

Rok za uspostavu posebnog registra subjekata

Članak 111.

Središnje državno tijelo za kibernetičku sigurnost uspostavit će poseban registar subjekata iz članka 22. ovoga Zakona u roku od godinu dana od dana stupanja na snagu ovoga Zakona.

Početak roka za provedbu revizija sigurnosti i stručnih nadzora

Članak 112.

Rokovi za provedbu revizija kibernetičke sigurnosti iz članka 34. stavka 1. ovoga Zakona i stručnog nadzora nad provedbom zahtjeva kibernetičke sigurnosti iz članka 75. stavka 1. ovoga Zakona počinju teći prvog sljedećeg radnog dana nakon isteka roka iz članka 26. stavka 5. ovoga Zakona.

Donošenje provedbenih propisa

Članak 113.

(1) Vlada će uredbu iz članka 24. ovoga Zakona donijeti u roku od devet mjeseci od dana stupanja na snagu ovoga Zakona.

(2) Vlada će srednjoročni akt strateškog planiranja iz članka 55. ovoga Zakona donijeti u roku od 24 mjeseca od dana stupanja na snagu ovoga Zakona.

(3) Vlada će nacionalni program upravljanja kibernetičkim krizama iz članka 56. ovoga Zakona donijeti u roku od tri mjeseca od dana stupanja na snagu ovoga Zakona.

(4) Vlada će Plan provedbe vježbi kibernetičke sigurnosti iz članka 58. ovoga Zakona donijeti u roku od 12 mjeseci od dana stupanja na snagu ovoga Zakona.

(5) Zavod za sigurnost informacijskih sustava će pravila iz članka 33. stavka 1. ovoga Zakona donijeti u roku od devet mjeseci od dana stupanja na snagu uredbe iz stavka 1. ovoga članka.

Donošenje propisa o unutarnjem ustrojstvu i unutarnjem redu

Članak 114.

(1) Vlada će, na prijedlog predstojnika Ureda Vijeća za nacionalnu sigurnost, uz prethodnu suglasnost predsjednika Republike Hrvatske, uskladiti Uredbu o unutarnjem ustrojstvu Ureda Vijeća za nacionalnu sigurnost s odredbama ovoga Zakona u roku od 30 dana od dana stupanja na snagu ovoga Zakona.

(2) Predstojnik Ureda Vijeća za nacionalnu sigurnost uskladit će Pravilnik o unutarnjem redu Ureda Vijeća za nacionalnu sigurnost s Uredbom iz stavka 1. ovoga članka, uz prethodnu suglasnost Vijeća za nacionalnu sigurnost, u roku od 30 dana od dana stupanja na snagu Uredbe.

(3) Vlada će, na prijedlog ravnatelja Sigurnosno-obavještajne agencije, uz prethodnu suglasnost predsjednika Republike Hrvatske, uskladiti Uredbu o unutarnjem ustrojstvu Sigurnosno-obavještajne agencije s odredbama ovoga Zakona u roku od 30 dana od dana stupanja na snagu ovoga Zakona.

(4) Ravnatelj Sigurnosno-obavještajne agencije uskladit će Pravilnik o unutarnjem redu Sigurnosno-obavještajne agencije s Uredbom iz stavka 3. ovoga članka, uz prethodnu suglasnost predstojnika Ureda Vijeća za nacionalnu sigurnost, u roku od 30 dana od dana stupanja na snagu Uredbe.

(5) Vlada će, na prijedlog ravnatelja Zavoda za sigurnost informacijskih sustava, uz prethodnu suglasnost Savjeta za koordinaciju sigurnosno-obavještajnih agencija, uskladiti Uredbu o unutarnjem ustrojstvu Zavoda za sigurnost informacijskih sustava s odredbama ovoga Zakona u roku od 30 dana od dana stupanja na snagu ovoga Zakona.

(6) Ravnatelj Zavoda za sigurnost informacijskih sustava uskladit će Pravilnik o unutarnjem redu Zavoda za sigurnost informacijskih sustava s Uredbom iz stavka 5. ovoga članka, uz prethodnu suglasnost Vlade, u roku od 30 dana od dana stupanja na snagu Uredbe.

Prestanak važenja propisa

Članak 115.

(1) Danom stupanja na snagu ovoga Zakona prestaju važiti:

– Zakon o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga (»Narodne novine«, br. 64/18.)

– članak 17. stavak 2. podstavak 4. i članak 21. Zakona o informacijskoj sigurnosti (»Narodne novine«, br. 79/07.)

– članak 41. Zakona o elektroničkim komunikacijama (»Narodne novine«, br. 76/22.)

– Uredba o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga (»Narodne novine«, br. 68/18.) i

– Odluka o osnivanju Nacionalnog vijeća za kibernetičku sigurnost i Operativno-tehničke koordinacije za kibernetičku sigurnost (»Narodne novine«, br. 61/16., 28/18., 110/18., 79/19. i 136/20.).

(2) Odluka o mjerama i aktivnostima za podizanje nacionalnih sposobnosti pravovremenog otkrivanja i zaštite od državno sponzoriranih kibernetičkih napada, *Advanced Persistent Threat* (ATP) kampanja te drugih kibernetičkih ugroza, klasa: 022-03/21-04/91, urbroj: 50301-29/09-21-2, od 1. travnja 2021., ostaje na snazi do stupanja na snagu uredbe iz članka 113. stavka 1. ovoga Zakona.

Stupanje na snagu Zakona

Članak 116.

Ovaj Zakon stupa na snagu osmoga dana od dana objave u »Narodnim novinama«.

Klasa: 022-02/23-01/94
Zagreb, 26. siječnja 2024.

HRVATSKI SABOR

Predsjednik
Hrvatskoga sabora
Gordan Jandroković, v. r.

PRILOG I.

SEKTORI VISOKE KRITIČNOSTI

Sektor	Podsektor	Vrsta subjekta
1. Energetika	(a) električna energija	– elektroenergetski subjekti koju obavljaju funkciju opskrbe električnom energijom, uključujući opskrbu električnom energijom koja se obavlja kao javna usluga Pojam *elektroenergetski subjekt* u smislu ovoga Zakona znači pravna ili fizička osoba koja nije krajnji kupac, a koja obavlja najmanje jednu od elektroenergetskih djelatnosti i koja je odgovorna za komercijalne i tehničke zadaće i zadaće održavanja koje su povezane s tim djelatnostima. Pojam *opskrba električnom energijom* u smislu ovoga Zakona znači kupnja i prodaja električne energije na veleprodajnom tržištu, prodaja električne energije krajnjim kupcima i skladištima energije, otkup električne energije od aktivnih kupaca, skladišta energije i proizvođača te agregiranje. Pojam *opskrba električnom energijom koja se obavlja kao javna usluga* u smislu ovoga Zakona znači opskrba električnom energijom onih krajnjih kupaca koji imaju pravo na takav način opskrbe i slobodno ga izaberu ili koriste po automatizmu. Pojmovi *elektroenergetski subjekt, opskrba električnom energijom* i *opskrba električnom energijom koja se obavlja kao javna usluga* istovjetni su s pojmovima iz članka 3. stavka 1. točaka 17., 77. i 78. Zakona o tržištu električne energije („Narodne novine“, br. 111/21. i 83/23.) kojim je u hrvatsko zakonodavstvo preuzeta Direktiva (EU) 2019/944 Europskog parlamenta i Vijeća od 5. lipnja 2019. o zajedničkim pravilima za unutarnje tržište električne energije i izmjeni Direktive 2012/27/EU (SL L 158, 14. 6. 2019.).
		– operatori distribucijskog sustava Pojam *operator distribucijskog sustava* u smislu ovoga Zakona znači fizička ili pravna osoba odgovorna za pogon i vođenje, održavanje, razvoj i izgradnju distribucijske mreže na danom području, kao i zajedničkih postrojenja prema prijenosnoj mreži i, kada je to primjenjivo, međusobno povezivanje s drugim distribucijskim sustavima te za osiguravanje dugoročne sposobnosti distribucijske mreže da zadovolji razumne zahtjeve za distribuciju električne energije. Pojam *operator distribucijskog sustava* istovjetan je s pojmom iz članka 3. stavka 1. točke 71. Zakona o tržištu električne energije („Narodne novine“, br. 111/21. i 83/23.).
		– operatori prijenosnog sustava Pojam *operator prijenosnog sustava* u smislu ovoga Zakona znači fizička ili pravna osoba odgovorna za pogon i vođenje, održavanje, razvoj i izgradnju prijenosne mreže na danom području, prekograničnih prijenosnih vodova prema drugim prijenosnim mrežama, kao i zajedničkih postrojenja prema distribucijskoj mreži te za osiguravanje dugoročne sposobnosti prijenosne mreže da zadovolji razumne zahtjeve za prijenos električne energije. Pojam *operator prijenosnog sustava* istovjetan je s pojmom iz članka 3. stavka 1. točke 72. Zakona o tržištu električne energije („Narodne novine“, br. 111/21. i 83/23.).
		– proizvođači električne energije Pojam *proizvođač električne energije* u smislu ovoga Zakona znači fizička ili pravna osoba koja proizvodi električnu energiju. Pojam *proizvođač električne energije* istovjetan je s pojmom iz članka 3. stavka 1. točke 90. Zakona o tržištu električne energije („Narodne novine“, br. 111/21. i 83/23.).
		– nominirani operatori tržišta električne energije kako su definirani u članku 2. točki 8. Uredbe (EU) 2019/943 Europskog parlamenta i Vijeća od 5. lipnja 2019. o unutarnjem tržištu električne energije (SL L 158, 14. 6. 2019.)
		– sudionici na tržištu kako su definirani u članku 2. točki 25. Uredbe (EU) 2019/943 koji pružaju usluge agregiranja, upravljanja potrošnjom ili skladištenja energije Pojam *agregiranje* u smislu ovoga Zakona znači djelatnost koju obavlja fizička ili pravna osoba koja može kombiniranjem snage i/ili iz mreže preuzete električne energije više kupaca ili operatora skladišta energije ili snage i/ili u mrežu predane električne energije više proizvođača ili aktivnih kupaca ili operatora skladišta energije radi sudjelovanja na bilo kojem tržištu električne energije. Pojam *upravljanje potrošnjom* u smislu ovoga Zakona znači promjena u opterećenju kod krajnjih kupaca u

		odnosu na njihove uobičajene ili trenutačne obrasce potrošnje električne energije kao odgovor na tržišne signale, uključujući vremenski ovisnu promjenu cijene električne energije ili novčane poticaje, ili kao odgovor na prihvat ponude krajnjeg kupca za prodaju smanjenja ili povećanja potražnje po cijeni na organiziranim tržištima, kako je definirano u članku 2. točki 4. Provedbene uredbe Komisije (EU) br. 1348/2014 od 17. prosinca 2014. o izvješćivanju o podacima i provedbi članka 8. stavaka 2. i 6. Uredbe (EU) br. 1227/2011 Europskog parlamenta i Vijeća o cjelovitosti i transparentnosti veleprodajnog tržišta energije (Tekst značajan za EGP) (SL L 363, 18. 12. 2014.), pojedinačno ili putem agregiranja. Pojam *skladištenje energije* u smislu ovoga Zakona znači, u kontekstu elektroenergetskog sustava, odgađanje konačne uporabe električne energije do trenutka kasnijeg od onog u kojem je proizvedena ili pretvorba električne energije u oblik energije koji se može skladištiti, skladištenje takve energije i naknadna pretvorba takve energije u električnu energiju ili njezina uporaba kao nositelja energije. Pojmovi *agregiranje*, *upravljanje potrošnjom* i *skladištenje energije* istovjetni su s pojmovima iz članka 3. stavka 1. točaka 4., 93. i 109. Zakona o tržištu električne energije („Narodne novine“, br. 111/21. i 83/23.).
		– operatori mjesta za punjenje koji su odgovorni za upravljanje i rad mjesta za punjenje kojim se krajnjim korisnicima pruža usluga opskrbe, među ostalim u ime i za račun pružatelja usluga mobilnosti
	(b) centralizirano grijanje i hlađenje	– operator sustava centraliziranog grijanja ili centraliziranog hlađenja Pojam *centralizirano grijanje ili centralizirano hlađenje* u smislu ovoga Zakona znači distribucija toplinske energije u obliku pare, vruće vode ili pothlađenih tekućina iz centralnih ili decentraliziranih proizvodnih postrojenja putem centralnih i zatvorenih toplinskih sustava u više zgrada ili na više lokacija radi uporabe za zagrijavanje ili hlađenje prostora ili procesa. Pojam *centralizirano grijanje ili centralizirano hlađenje* istovjetan je s pojmom iz članka 4. stavka 1. točke 4. Zakona o obnovljivim izvorima energije i visokoučinkovitoj kogeneraciji („Narodne novine“, br. 138/21. i 83/23.) kojim je u hrvatsko zakonodavstvo preuzeta Direktiva 2018/2001 Europskog parlamenta i Vijeća od 11. prosinca 2018. o promicanju uporabe energije iz obnovljivih izvora (preinaka) (Tekst značajan za EGP) (SL L 328, 21. 12. 2018.).
	(c) nafta	– operatori naftovoda
		– operatori proizvodnje nafte, rafinerija i tvornica nafte te njezina skladištenja i prijenosa
		– središnja tijela za zalihe Pojam *središnje tijelo za zalihe* u smislu ovoga Zakona znači Agencija za ugljikovodike, kao središnje tijelo u Republici Hrvatskoj za obvezne zalihe nafte i naftnih derivata, koja je jedinstveno tijelo ovlašteno formirati, održavati i prodavati obvezne zalihe. Pojam *središnje tijelo za zalihe* istovjetan je s pojmom iz članka 3. stavka 2. točke 5. Zakona o tržištu nafte i naftnih derivata („Narodne novine“, br. 19/14., 73/17. i 96/19.) kojim je u hrvatsko zakonodavstvo preuzeta Direktiva 2009/119/EZ Europskog parlamenta i Vijeća od 14. rujna 2009. kojom se države članice obvezuju održavati minimalne zalihe sirove nafte i/ili naftnih derivata (SL L 265/9 od 9. 10. 2009.).
	(d) plin	– opskrbljivači plinom, uključujući opskrbljivače u obvezi javne usluge Pojam *opskrbljivač plinom* u smislu ovoga Zakona znači energetski subjekt koji obavlja energetsku djelatnost opskrbe plinom. Pojam *opskrbljivač plinom u obvezi javne usluge* u smislu ovoga Zakona znači opskrbljivač plinom koji obavlja energetsku djelatnost opskrbe u obvezi javne usluge. Pojam *opskrba plinom* u smislu ovoga Zakona znači prodaja ili preprodaja plina kupcu, uključujući prodaju ili preprodaju UPP-a i SPP-a. Pojam *opskrba plinom u obvezi javne usluge* u smislu ovoga Zakona znači opskrba plinom koja se u općem gospodarskom interesu obavlja po reguliranim uvjetima radi osiguravanja sigurnosti, redovitosti, kvalitete i cijene opskrbe kućanstava. Pojmovi *opskrbljivač plinom, opskrbljivač plinom u obvezi javne usluge*, *opskrba plinom* i *opskrba plinom u obvezi javne usluge* istovjetni su s pojmovima iz članka 3. stavka 2. točaka 36., 37., 38. i 39. Zakona o tržištu plina („Narodne novine“, br. 18/18. i 23/20.) kojim je u hrvatsko zakonodavstvo preuzeta Direktiva 2009/73/EZ Europskog parlamenta i Vijeća od 13. srpnja 2009. o zajedničkim pravilima za unutarnje tržište prirodnog plina i stavljanju izvan snage Direktive 2003/55/EZ (Tekst značajan za EGP) (SL L 211, 14. 8. 2009.)
		– operatori distribucijskog sustava Pojam *operator distribucijskog sustava* u smislu ovoga Zakona znači energetski subjekt koji obavlja energetsku djelatnost distribucije plina i odgovoran je za rad, održavanje i razvoj distribucijskog sustava na svom distribucijskom području i, gdje je izvodivo, njegovo povezivanje s drugim sustavima te za osiguranje dugoročne sposobnosti sustava da zadovoljava razumne potrebe za distribucijom plina. Pojam *distribucija plina* u smislu ovoga Zakona znači razvod plina distribucijskim sustavom visoke, srednje i niske tlačne razine radi isporuke plina krajnjim kupcima, uključujući pomoćne usluge, a isključujući opskrbu plinom. Pojam *distribucijski sustav* u smislu ovoga Zakona znači sustav plinovoda i ostalih pripadajućih objekata i opreme koji su u vlasništvu operatora distribucijskog sustava i/ili kojima upravlja operator distribucijskog sustava, a koji se koristi za distribuciju plina, nadzor i upravljanje, mjerenje i prijenos podataka. Pojmovi *operator distribucijskog sustava, distribucija plina* i *distribucijski sustav* istovjetni su s pojmovima iz članka 3. stavka 2. točaka 5., 6. i 30. Zakona o tržištu plina („Narodne novine“, br. 18/18. i 23/20.).
		– operatori transportnog sustava Pojam *operator transportnog sustava* u smislu ovoga Zakona znači energetski subjekt koji obavlja energetsku djelatnost transporta plina i odgovoran je za rad, održavanje i razvoj transportnog sustava na određenom području i, gdje je izvodivo, njegovo povezivanje s drugim sustavima te za osiguranje dugoročne sposobnosti sustava da zadovoljava razumne potrebe za transportom plina. Pojam *transport plina* u smislu ovoga Zakona znači prijenos plina kroz transportni sustav, isključujući opskrbu plinom i trgovinu plinom, a uključujući tranzit plina i pomoćne usluge. Pojam *transportni sustav* u smislu ovoga Zakona znači objekt koji je u vlasništvu i/ili kojim upravlja operator transportnog sustava, a koji čine sustav visokotlačnih plinovoda, kompresorske stanice, mjerne stanice, mjerno-redukcijske stanice, plinski čvorovi i ostali tehnološki objekti i oprema koji se koriste za transport plina, nadzor i upravljanje, mjerenje i prijenos podataka, isključujući mrežu proizvodnih plinovoda i visokotlačne distribucijske plinovode, uključujući plin za tehnološke kapacitete kojima se isključivo koristi operator transportnog sustava i operativnu akumulaciju. Pojmovi *operator transportnog sustava*, *transport plina* i *transportni sustav* istovjetni su s pojmovima iz članka 3. stavka 2. točaka 34., 58. i 59. Zakona o tržištu plina („Narodne novine“, br. 18/18. i 23/20.).
		– operatori sustava skladišta plina Pojam *operator sustava skladišta plina* u smislu ovoga Zakona znači energetski subjekt koji obavlja energetsku djelatnost skladištenja plina i odgovoran je za rad, održavanje i razvoj sustava skladišta plina. Pojam *skladištenje plina* u smislu ovoga Zakona znači utiskivanje plina u sustav skladišta plina, skladištenje plina u radnom volumenu sustava skladišta plina i povlačenje plina iz sustava skladišta plina, uključujući pomoćne usluge. Pojmovi *operator sustava skladišta plina* i *skladištenje plina* istovjetni su s pojmovima iz članka 3. stavka 2. točaka 54. i 56. Zakona o tržištu plina („Narodne novine“, br. 18/18. i 23/20.).
		– operatori terminala za UPP Pojam *operator terminala za UPP* u smislu ovoga Zakona znači energetski subjekt koji obavlja energetsku djelatnost upravljanja terminalom za UPP i odgovoran je za rad, održavanje i razvoj terminala za UPP. Pojam *terminal za UPP* u smislu ovoga Zakona znači terminal koji se koristi za ukapljivanje prirodnog plina ili prihvat, iskrcaj i ponovno uplinjavanje UPP-a, uključujući pomoćne usluge i privremeno skladištenje potrebno za postupak ponovnog uplinjavanja i daljnju otpremu u transportni sustav, ali isključujući dijelove terminala za UPP koji se koriste za skladištenje. Pojmovi *operator terminala za UPP* i *terminal za UPP* istovjetni su s pojmovima iz članka 3. stavka 2. točaka 33. i 57. Zakona o tržištu plina („Narodne novine“, br. 18/18. i 23/20.).
		– poduzeća za prirodni plin

		Pojam *poduzeće za prirodni plin* u smislu ovoga Zakona, a u skladu sa zakonom kojim se uređuje tržište plina, znači fizička ili pravna osoba koja obavlja najmanje jednu od sljedećih funkcija: proizvodnju, transport, distribuciju, opskrbu, nabavu ili skladištenje prirodnog plina, uključujući UPP, a odgovorna je za komercijalne i tehničke zadatke i/ili zadatke održavanja koji su povezani s tim funkcijama, isključujući krajnje kupce.
		– operatori postrojenja za rafiniranje i obradu prirodnog plina
	(e) vodik	– operatori proizvodnje, skladištenja i prijenosa vodika
2. Promet	(a) zračni promet	– zračni prijevoznici kako su definirani u članku 3. točki 4. Uredbe (EZ) br. 300/2008 Europskog parlamenta i Vijeća od 11. ožujka 2008. o zajedničkim pravilima u području zaštite civilnog zračnog prometa i stavljanju izvan snage Uredbe (EZ) br. 2320/2002 (Tekst značajan za EGP) koji se upotrebljavaju u komercijalne svrhe
		– upravna tijela zračne luke, zračne luke, uključujući osnovne zračne luke navedene u odjeljku 2. Priloga II. Uredbe (EU) br. 1315/2013 Europskog parlamenta i Vijeća od 11. prosinca 2013. o smjernicama Unije za razvoj transeuropske prometne mreže i stavljanju izvan snage Odluke br. 661/2010/EU (Tekst značajan za EGP) te tijela koja upravljaju pomoćnim objektima u zračnim lukama Pojam *upravno tijelo zračne luke* u smislu ovoga Zakona znači tijelo koje, osim drugih aktivnosti ili ne, ima prema nacionalnim propisima ili ugovorima kao cilj rukovođenje i upravljanje infrastrukturom zračne luke te koordinaciju i nadzor djelatnosti različitih operatora u dotičnoj zračnoj luci. Pojam *zračna luka* u smislu ovoga Zakona znači svaka površina koja je posebno prilagođena za slijetanje, uzlijetanje i manevriranje zrakoplova, uključujući i pripadajuće objekte, sredstva i uređaje namijenjene za odvijanje zračnog prometa i pružanje usluga te objekte, sredstva i uređaje za pomoć u pružanju usluga komercijalnog zračnog prijevoza. Pojmovi *upravno tijelo zračne luke* i *zračna luka* istovjetni su s pojmovima iz članka 3. stavka 1. podstavaka 1. i 2. Pravilnika o naknadama zračnih luka („Narodne novine“, br. 65/15.) kojim je u hrvatsko zakonodavstvo preuzeta Direktiva 2009/12/EZ Europskog parlamenta i Vijeća od 11. ožujka 2009. o naknadama zračnih luka.
		– operatori kontrole upravljanja prometom koji pružaju usluge kontrole zračnog prometa (ATC) kako su definirani u članku 2. točki 1. Uredbe (EZ) br. 549/2004 Europskog parlamenta i Vijeća od 10. ožujka 2004. o definiranju pravnog okvira za stvaranje jedinstvenog europskog neba (Okvirna uredba) i Izjava država članica o vojnim pitanjima u svezi s jedinstvenim europskim nebom
	(b) željeznički promet	– upravitelji infrastrukture Pojam *upravitelj infrastrukture* u smislu ovoga Zakona znači pravna osoba ili u vertikalno integriranom trgovačkom društvu organizacijska jedinica odgovorna za upravljanje, održavanje i obnovu željezničke infrastrukture, kao i za sudjelovanje u razvoju željezničke infrastrukture na način koji je određen u okviru opće politike razvoja i financiranja željezničke infrastrukture Republike Hrvatske. Pojam *upravitelj infrastrukture* istovjetan je s pojmom iz članka 5. stavka 1. točke 36. Zakona o željeznici („Narodne novine“, br. 32/19., 20/21. i 114/22.) kojim je u hrvatsko zakonodavstvo preuzeta Direktiva 2012/34/EU Europskog parlamenta i Vijeća od 21. studenoga 2012. o uspostavi jedinstvenog Europskog željezničkog prostora (preinačena) (SL L 343, 14. 12. 2012.), kako je posljednji put izmijenjena Direktivom (EU) 2016/2370 Europskog parlamenta i Vijeća od 14. prosinca 2016. o izmjeni Direktive 2012/34/EU u pogledu otvaranja tržišta za usluge domaćeg željezničkog prijevoza putnika i upravljanja željezničkom infrastrukturom (Tekst značajan za EGP) (SL L 352, 23. 12. 2016.).
		– željeznički prijevoznici, među ostalim i operatori uslužnih objekata Pojam *željeznički prijevoznik* u smislu ovoga Zakona znači svaka pravna osoba koja ima dozvolu za obavljanje usluga željezničkog prijevoza i čija je glavna djelatnost pružanje usluga željezničkog prijevoza putnika i/ili tereta, uz uvjet da ta pravna osoba osigura vuču vlakova; to uključuje i pravnu osobu koja pruža samo uslugu vuče vlakova. Pojam *operator uslužnih objekata* u smislu ovoga Zakona znači pravna osoba odgovorna za upravljanje jednim ili s više uslužnih objekata (upravitelj uslužnog objekta) ili za pružanje željezničkim prijevoznicima jedne ili više usluga iz Priloga 2. točaka 2. do 4. Zakona o željeznici („Narodne novine“, br. 32/19., 20/21. i 114/22.) (pružatelj usluga).
		Pojmovi *željeznički prijevoznik* i *operator uslužnih objekata* istovjetni su s pojmovima iz članka 5. stavka 1. točaka 22. i 46. Zakona o željeznici („Narodne novine“, br. 32/19., 20/21. i 114/22.).
	(c) vodeni promet	– kompanije za prijevoz putnika unutarnjim plovnim putovima, morem i duž obale kako su definirane za pomorski promet u Prilogu I. Uredbe (EZ) br. 725/2004 Europskog parlamenta i Vijeća od 31. ožujka 2004. o jačanju sigurnosne zaštite brodova i luka (Tekst značajan za EGP), ne uključujući pojedinačna plovila kojima upravljaju te kompanije
		– upravljačka tijela luka, uključujući njihove luke kako su definirane u članku 2. točki 11. Uredbe (EZ) br. 725/2004, te subjekti koji upravljaju postrojenjima i opremom u lukama Pojam *luka* u smislu ovoga Zakona znači morska luka, tj. morski i s morem neposredno povezan kopneni prostor u utvrđenim granicama lučkog područja s izgrađenim i neizgrađenim obalama; lukobranima, uređajima, postrojenjima i drugim objektima i sustavima namijenjenim za pristajanje, sidrenje i zaštitu brodova, jahti i brodica, ukrcaj i iskrcaj putnika i tereta, uskladištenje i drugo rukovanje teretom, proizvodnju, oplemenjivanje i doradu tereta te ostale gospodarske djelatnosti koje su s tim djelatnostima u međusobnoj ekonomskoj, prometnoj ili tehnološkoj vezi. Pojam *luka* istovjetan je s pojmom iz članka 3. stavka 1. točke 1. Zakona o sigurnosnoj zaštiti pomorskih brodova i luka („Narodne novine“, br. 108/17. i 30/21.) kojim je u hrvatsko zakonodavstvo preuzeta Direktiva 2005/65/EZ Europskog parlamenta i Vijeća od 26. listopada 2005. o jačanju sigurnosne zaštite luka (Tekst značajan za EGP) (SL L 320, 25. 11. 2005.).
		– služba za nadzor i upravljanje pomorskim prometom (VTS) kako je definirana u članku 75.a stavku 1. i članku 75.b stavku 1. Pomorskog zakonika („Narodne novine“, br. 181/04., 76/07., 146/08., 61/11., 56/13., 26/15. i 17/19.) kojim je u hrvatsko zakonodavstvo preuzeta Direktiva 2002/59/EZ Europskog parlamenta i Vijeća od 27. lipnja 2002. o uspostavi sustava nadzora plovidbe i informacijskog sustava Zajednice i stavljanju izvan snage Direktive Vijeća 93/75/EEZ
	(d) cestovni promet	– tijela nadležna za ceste kako su definirana u članku 2. točki 12. Delegirane uredbe Komisije (EU) 2015/962 od 18. prosinca 2014. o dopuni Direktive 2010/40/EU Europskog parlamenta i Vijeća u pogledu pružanja usluga prometnih informacija u cijeloj Europskoj uniji u realnom vremenu (Tekst značajan za EGP),
		odgovorna za kontrolu upravljanja prometom, osim javnih subjekata kojima upravljanje prometom ili rad inteligentnih prometnih sustava nisu ključan dio njihove opće djelatnosti Prema članku 2. točki 12. Delegirane uredbe Komisije (EU) 2015/962, pojam *tijelo nadležno za ceste* znači svako javno tijelo koje je nadležno za planiranje, nadzor ili upravljanje cestama u okviru svoje mjesne nadležnosti.
		– operatori inteligentnih prometnih sustava Pojam *inteligentni prometni sustavi (ITS)* u smislu ovoga Zakona znači informacijsko-komunikacijska nadgradnja klasičnog sustava cestovnog prometa kojim se postiže znatno poboljšanje učinaka cjelokupnog prometnog sustava. ITS uključuje ceste, vozila i korisnike cesta, a primjenjuje se u upravljanju prometom, upravljanju mobilnosti, upravljanju prometnim incidentima te za veze s ostalim vrstama prijevoza. Pojam *inteligentni prometni sustavi (ITS)* istovjetan je s pojmom iz članka 72. stavka 1. Zakona o cestama („Narodne novine“, br. 84/11., 22/13., 54/13., 148/13., 92/14., 110/19., 144/21, 114/22., 04/23. i 133/23.) kojim je u hrvatsko zakonodavstvo preuzeta Direktiva 2010/40/EZ Europskog parlamenta i Vijeća od 7. srpnja 2010. o okviru za uvođenje inteligentnih transportnih sustava u cestovnom prometu i za veze s ostalim vrstama prijevoza (Tekst značajan za EGP) (SL L 207 od 6. kolovoza 2010.).
3. Bankarstvo		– kreditne institucije kako su definirane u članku 4. točki 1. Uredbe (EU) br. 575/2013 Europskog parlamenta i Vijeća od 26. lipnja 2013. o bonitetnim zahtjevima za kreditne institucije i investicijska društva i o izmjeni Uredbe (EU) br. 648/2012 (Tekst značajan za EGP)
4.Infrastruktura financijskog tržišta		– operatori mjesta trgovanja Pojam *mjesta trgovanja* u smislu ovoga Zakona znači uređeno tržište, MTP ili OTP. Pojam *multilateralna trgovinska platforma ili MTP* u smislu ovoga Zakona znači multilateralni sustav kojim upravlja investicijsko društvo ili tržišni operater koji u sustavu i prema unaprijed poznatim i nediskrecijskim pravilima spaja ili omogućuje spajanje ponuda za kupnju i ponuda za prodaju financijskih instrumenata trećih tako da nastaje ugovor u skladu s odredbama dijela drugoga glave III. poglavlja VII. Zakona o tržištu

		kapitala („Narodne novine“, br. 65/18., 17/20., 83/21. i 151/22.). Pojam *organizirana trgovinska platforma* ili OTP u smislu ovoga Zakona znači multilateralni sustav, koji nije uređeno tržište ili MTP, koji omogućuje da se u tom sustavu susretnu ponude za kupnju i ponude za prodaju obveznica, strukturiranih financijskih proizvoda, emisijskih jedinica ili izvedenica više zainteresiranih trećih strana tako da nastaje ugovor u skladu s odredbama dijela drugoga glave III. poglavlja VII. Zakona o tržištu kapitala („Narodne novine“, br. 65/18., 17/20., 83/21. i 151/22.). Pojmovi *mjesta trgovanja, multilateralna trgovinska platforma ili MTP* i *organizirana trgovinska platforma* ili OTP istovjetni su s pojmovima iz članka 3. stavka 1. točaka 61., 65. i 77. Zakona o tržištu kapitala („Narodne novine“, br. 65/18., 17/20., 83/21. i 151/22.) kojim je u hrvatsko zakonodavstvo preuzeta Direktiva 2014/65/EU Europskog parlamenta i Vijeća od 15. svibnja 2014. o tržištu financijskih instrumenata i izmjeni Direktive 2002/92/EZ i Direktive 2011/61/EU (preinačena) (Tekst značajan za EGP) (SL L 173, 12. 6. 2014.).
		– središnje druge ugovorne strane (CCP-i) kako su definirane u članku 2. točki 1. Uredbe (EU) br. 648/2012 Europskog parlamenta i Vijeća od 4. srpnja 2012. o OTC izvedenicama, središnjoj drugoj ugovornoj strani i trgovinskom repozitoriju (SL L 201, 27. 7. 2012.)
5. Zdravstvo		– pružatelji zdravstvene zaštite Pojam *pružatelj zdravstvene zaštite* u smislu ovoga Zakona znači svaka fizička ili pravna osoba ili bilo koji subjekt koji obavlja zdravstvenu djelatnost u Republici Hrvatskoj u skladu sa zakonom kojim se uređuje zdravstvena zaštita. Pojam *pružatelj zdravstvene zaštite* ne odnosi se na ustrojstvene jedinice Ministarstva obrane i Oružanih snaga Republike Hrvatske i ministarstva nadležnog za pravosuđe koje obavljaju zdravstvenu djelatnost prema posebnim propisima.
		– referentni laboratoriji Europske unije iz članka 15. Uredbe (EU) 2022/2371 Europskog parlamenta i Vijeća od 23. studenoga 2022. o ozbiljnim prekograničnim prijetnjama zdravlju i o stavljanju izvan snage Odluke br. 1082/2013/EU (Tekst značajan za EGP)
		– subjekti koji obavljaju djelatnosti istraživanja i razvoja lijekova
		Pojam *lijek* u smislu ovoga Zakona znači: – svaka tvar ili kombinacija tvari prikazana sa svojstvima liječenja ili sprječavanja bolesti kod ljudi ili – svaka tvar ili kombinacija tvari koja se može upotrijebiti ili primijeniti na ljudima u svrhu obnavljanja, ispravljanja ili prilagodbe fizioloških funkcija farmakološkim, imunološkim ili metaboličkim djelovanjem ili za postavljanje medicinske dijagnoze. Pojam *lijek* istovjetan je s pojmom iz članka 3. stavka 1. točke 1. Zakona o lijekovima („Narodne novine“, br. 76/13., 90/14. i 100/18.) kojim je u hrvatsko zakonodavstvo preuzeta Direktiva 2001/83/EZ Europskog parlamenta i Vijeća od 6. studenoga 2001., o Zakoniku Zajednice koji se odnosi na lijekove za primjenu kod ljudi (SL L 311, 28. 11. 2001.).
		– subjekti koji proizvode osnovne farmaceutske proizvode i farmaceutske pripravke iz područja C odjeljka 21. Nacionalne klasifikacije djelatnosti 2007. – NKD 2007. („Narodne novine“, br. 58/07. i 72/07.)
		– subjekti koji proizvode medicinske proizvode koji se smatraju ključnima tijekom izvanrednog stanja u području javnog zdravlja („popis ključnih medicinskih proizvoda u slučaju izvanrednog stanja u području javnog zdravlja“) u smislu članka 22. Uredbe (EU) 2022/123 Europskog parlamenta i Vijeća od 25. siječnja 2022. o pojačanoj ulozi Europske agencije za lijekove u pripravnosti za krizne situacije i upravljanju njima u području lijekova i medicinskih proizvoda (Tekst značajan za EGP)
6. Voda za ljudsku potrošnju		– dobavljači i distributeri vode namijenjene za ljudsku potrošnju, isključujući distributere kojima distribucija vode za ljudsku potrošnju nije ključan dio njihove općenite djelatnosti distribucije druge robe i proizvoda Pojam *voda namijenjena za ljudsku potrošnju* u smislu ovoga Zakona znači: – sva voda, bilo u njezinu izvornom stanju ili nakon obrade, koja je namijenjena za piće, kuhanje, pripremu hrane ili druge potrebe kućanstva i u javnim i u privatnim prostorima, neovisno o njezinu podrijetlu te o tome isporučuje li se iz vodoopskrbne mreže, isporučuje li se iz cisterne ili se stavlja u boce ili ambalažu, uključujući izvorsku i stolnu vodu – sva voda koja se u poslovanju s hranom upotrebljava za proizvodnju, obradu, očuvanje ili stavljanje na tržište proizvoda ili tvari namijenjenih za ljudsku potrošnju.
		Pojam *voda namijenjena za ljudsku potrošnju* istovjetan je s pojmom iz članka 3. stavka 1. točke 1. Zakona o vodi za ljudsku potrošnju („Narodne novine“, br. 30/23.) kojim je u hrvatsko zakonodavstvo preuzeta Direktiva (EU) 2020/2184 Europskog parlamenta i Vijeća od 16. prosinca 2020. o kvaliteti vode namijenjene za ljudsku potrošnju (preinaka) (Tekst značajan za EGP) (SL L 435, 23. 12. 2020.).
7. Otpadne vode		– poduzeća koja prikupljaju, odlažu ili pročišćavaju komunalne otpadne vode, sanitarne otpadne vode ili industrijske otpadne vode, isključujući poduzeća kojima prikupljanje, odlaganje ili pročišćavanje komunalnih otpadnih voda, otpadnih voda iz kućanstva ili industrijskih otpadnih voda nije ključan dio njihove općenite djelatnosti Pojam *komunalne otpadne vode* u smislu ovoga Zakona znači otpadne vode sustava javne odvodnje koje čine sanitarne otpadne vode ili otpadne vode koje su mješavina sanitarnih otpadnih voda s industrijskim otpadnim vodama i/ili oborinskim vodama određene aglomeracije. Pojam *sanitarne otpadne vode* u smislu ovoga Zakona znači otpadne vode koje se nakon korištenja ispuštaju iz stambenih objekata i uslužnih objekata te koje uglavnom potječu iz ljudskog metabolizma i aktivnosti kućanstava. Pojam *industrijske otpadne vode* u smislu ovoga Zakona znači sve otpadne vode, osim sanitarnih otpadnih voda i oborinskih voda, koje se ispuštaju iz prostora korištenih za obavljanje trgovine ili industrijske djelatnosti. Pojmovi *komunalne otpadne vode*, *sanitarne otpadne vode* i *industrijske otpadne vode* istovjetni su s pojmovima iz članka 4. stavka 1. točaka 25., 34. i 81. Zakona o vodama („Narodne novine“, br. 66/19., 84/21. i 47/23.) kojim je u hrvatsko zakonodavstvo preuzeta Direktiva Vijeća 91/271/EEZ od 21. svibnja 1991. o pročišćavanju komunalnih otpadnih voda (SL L 135, 30. 5. 1991.), dopunjena Direktivom Komisije 98/15/EZ od 27. veljače 1998. s obzirom na određene zahtjeve utvrđene u Dodatku I. (Tekst značajan za EGP) (SL L 67, 7. 3. 1998.).
8. Digitalna infrastruktura		– pružatelji središta za razmjenu internetskog prometa
		– pružatelji usluga DNS-a, osim operatora korijenskih poslužitelja naziva
		– registar naziva vršne nacionalne internetske domene
		– pružatelji usluga računalstva u oblaku
		– pružatelji usluga podatkovnog centra
		– pružatelji mreže za isporuku sadržaja
		– pružatelji usluga povjerenja
		– pružatelji javnih elektroničkih komunikacijskih mreža
		– pružatelji javno dostupnih elektroničkih komunikacijskih usluga
9. Upravljanje uslugama IKT-a (B2B)		– pružatelji upravljanih usluga
		– pružatelji upravljanih sigurnosnih usluga
		– informacijski posrednici kako su definirani propisom kojim se uređuje razmjena elektroničkog računa između poduzetnika
10. Javni sektor		– tijela državne uprave
		– druga državna tijela i pravne osobe s javnim ovlastima
		– privatni i javni subjekti koji upravljaju, razvijaju ili održavaju državnu informacijsku infrastrukturu sukladno zakonu kojim se uređuje državna informacijska infrastruktura
		– jedinice lokalne i područne (regionalne) samouprave
11. Svemir		– operatori zemaljske infrastrukture koji su u vlasništvu, kojima upravljaju i koje vode države članice ili privatne strane te koji podupiru pružanje usluga u svemiru, isključujući pružatelje javnih elektroničkih komunikacijskih mreža

PRILOG II.

DRUGI KRITIČNI SEKTORI

Sektor	Podsektor	Vrsta subjekta
1. Poštanske i kurirske usluge		– davatelji poštanskih usluga Pojam *davatelj poštanskih usluga* u smislu ovoga Zakona znači pravna ili fizička osoba koja obavlja poštanske usluge, uključujući *davatelja univerzalne usluge* kao davatelja poštanskih usluga koji obavlja univerzalnu uslugu u Republici Hrvatskoj. Pojam *poštanska usluga* u smislu ovoga Zakona znači usluga koja uključuje svako postupanje s poštanskim pošiljkama od strane davatelja poštanskih usluga, a osobito prijam, usmjeravanje, prijenos i uručenje poštanskih pošiljaka u unutarnjem ili međunarodnom poštanskom prometu. *Poštanska usluga* ne uključuje prijenos pošiljke primatelju koji pošiljatelj obavlja sam (samodostava), prijevoz kao samostalnu uslugu te prijam, prijenos i uručenje poštanskih pošiljaka izravno od pošiljatelja do primatelja po individualnom zahtjevu, bez usmjeravanja, na način da isti radnik davatelja usluga obavlja sve navedene radnje (kurirska usluga). Pojam *univerzalna usluga* u smislu ovoga Zakona znači skup poštanskih usluga određene kakvoće koje su dostupne po pristupačnoj cijeni svim korisnicima poštanskih usluga na cijelom području Republike Hrvatske, neovisno o njihovoj zemljopisnoj lokaciji. Pojmovi *davatelj poštanskih usluga*, *davatelj univerzalne usluge*, *poštanska usluga* i *univerzalna usluga* istovjetni su s pojmovima iz članka 2. stavka 1. točkama 4., 5., 21. i 32. Zakona o poštanskim uslugama („Narodne novine“, br. 144/12., 153/13., 78/15. i 110/19.) kojim je u hrvatsko zakonodavstvo preuzeta Direktiva (EU) 97/67/EZ Europskog parlamenta i Vijeća od 15. prosinca 1997. o zajedničkim pravilima za razvoj unutarnjeg tržišta poštanskih usluga u Zajednici i poboljšanje kvalitete usluga (SL L 15, 21. 1. 1998.).
		– pružatelji kurirskih usluga
2. Gospodarenje otpadom		– subjekti koji se bave gospodarenjem otpadom, isključujući subjekte kojima gospodarenje otpadom nije glavna gospodarska djelatnost Pojam *gospodarenje otpadom* u smislu ovoga Zakona znači djelatnosti prikupljanja, prijevoza, oporabe uključujući razvrstavanje i zbrinjavanje otpada, uključujući nadzor nad obavljanjem tih djelatnosti, nadzor i mjere koje se provode na lokacijama na kojima se zbrinjavao otpad te radnje koje poduzimaju trgovac otpadom i posrednik u gospodarenju otpadom. Pojam *otpad* u smislu ovoga Zakona znači svaka tvar ili predmet koji posjednik odbacuje, namjerava ili mora odbaciti. Pojam *djelatnost prikupljanja otpada* u smislu ovoga Zakona znači djelatnost koja uključuje postupak prikupljanja otpada i postupak prikupljanja otpada u reciklažno dvorište. Pojam *djelatnost prijevoza otpada* u smislu ovoga Zakona znači prijevoz otpada za vlastite potrebe ili za potrebe drugih na teritoriju Republike Hrvatske. Pojam *djelatnost oporabe otpada* u smislu ovoga Zakona znači djelatnost koja uključuje obavljanje postupka oporabe iz Popisa postupaka oporabe otpada. Pojam *tehnološki procesi gospodarenja otpadom* u smislu ovoga Zakona znači određene funkcionalno-tehnološke cjeline gospodarenja otpadom kojima se opisuje materijalni tok otpada, a uključuju prikupljanje, prihvat, skladištenje, prethodno razvrstavanje i razvrstavanje, miješanje otpada, pakiranje, popravak, čišćenje, provjera budućeg proizvoda i drugi procesi u sklopu postupka oporabe i zbrinjavanja otpada. Pojam *djelatnost zbrinjavanja otpada* u smislu ovoga Zakona znači djelatnost koja uključuje obavljanje postupka zbrinjavanja otpada iz Popisa postupaka zbrinjavanja otpada. Pojam *trgovac otpadom* u smislu ovoga Zakona znači pravna ili fizička osoba – obrtnik koja u svoje ime i za svoj račun kupuje i prodaje otpad, uključujući trgovca otpadom koji ne preuzima otpad u neposredni posjed. Pojam *posrednik* u smislu ovoga Zakona znači pravna ili fizička osoba – obrtnik koja obavlja djelatnost posredovanja u gospodarenju otpadom, uključujući i posrednika koji ne preuzima otpad u neposredni posjed. Pojmovi *gospodarenje otpadom*, *otpad, djelatnost prikupljanja otpada, djelatnost prijevoza otpada, djelatnost oporabe otpada, tehnološki procesi gospodarenja otpadom, djelatnost zbrinjavanja otpada, trgovac otpadom i posrednik* istovjetni su s pojmovima iz članka 4. stavka 1. točaka 15., 48., 11., 10., 8., 82., 13., 84. i 60. Zakona o gospodarenju otpadom („Narodne novine“, br. 84/21. i 142/23.) kojim je u hrvatsko zakonodavstvo preuzeta Direktiva 2008/98/EZ Europskog parlamenta i Vijeća od 19. studenoga 2008. o otpadu i stavljanju izvan snage određenih direktiva (SL L 312, 22. 11. 2008.), kako je posljednji put izmijenjena Direktivom (EU) 2018/851 Europskog parlamenta i Vijeća od 30. svibnja 2018. o izmjeni Direktive 2008/98/EZ o otpadu (SL L 150, 14. 6. 2018.)
3. Izrada, proizvodnja i distribucija kemikalija		– subjekti koji se bave izradom tvari te distribucijom tvari ili mješavina kako su definirani u članku 3. točkama 9. i 14. Uredbe (EZ) br. 1907/2006 Europskog parlamenta i Vijeća EZ o registraciji, evaluaciji, autorizaciji i ograničavanju kemikalije (REACH) i osnivanju Europske agencije za kemikalije te o izmjeni Direktive 1999/45/EZ i stavljanju izvan snage Uredbe Vijeća (EEZ) br. 793/93 i Uredbe Komisije (EZ) br. 1488/94, kao i Direktive Vijeća 76/769/EEZ i direktiva Komisije 91/155/EEZ, 93/67/EEZ, 93/105/EZ i 2000/21/EZ (Tekst značajan za EGP)
		– subjekti koji se bave proizvodnjom proizvoda kako su definirani u članku 3. točki 3. Uredbe (EZ) br. 1907/2006, iz tvari ili mješavina
4. Proizvodnja, prerada i distribucija hrane		– poduzeća za poslovanje s hranom kako su definirana u članku 3. točki 2. Uredbe (EZ) br. 178/2002 Europskog parlamenta i Vijeća od 28. siječnja 2002. o utvrđivanju općih načela i uvjeta zakona o hrani, osnivanju Europske agencije za sigurnost hrane te utvrđivanju postupaka u područjima sigurnosti hrane, koja se bave veleprodajom te industrijskom proizvodnjom i preradom
5. Proizvodnja	(a) proizvodnja medicinskih proizvoda i in vitro dijagnostičkih medicinskih proizvoda	– subjekti koji proizvode medicinske proizvode kako su definirani u članku 2. točki 1. Uredbe (EU) 2017/745 Europskog parlamenta i Vijeća od 5. travnja 2017. o medicinskim proizvodima, o izmjeni Direktive 2001/83/EZ, Uredbe (EZ) br. 178/2002 i Uredbe (EZ) br. 1223/2009 te o stavljanju izvan snage direktiva Vijeća 90/385/EEZ i 93/42/EEZ (Tekst značajan za EGP) i subjekti koji proizvode in vitro dijagnostičke medicinske proizvode kako su definirani u članku 2. točki 2. Uredbe (EU) 2017/746 Europskog parlamenta i Vijeća od 5. travnja 2017. o in vitro dijagnostičkim medicinskim proizvodima te o stavljanju izvan snage Direktive 98/79/EZ i Odluke Komisije 2010/227/EU (Tekst značajan za EGP), osim subjekata koji proizvode medicinske proizvode navedene u Prilogu I. točki 5. petoj alineji ovoga Zakona. Prilog I. točka 5. peta alineja ovoga Zakona upućuje na *„subjekte koji proizvode medicinske proizvode koji se smatraju ključnima tijekom izvanrednog stanja u području javnog zdravlja“* odnosno na *„popis ključnih medicinskih proizvoda u slučaju izvanrednog stanja u području javnog zdravlja“* u smislu članka 22. Uredbe (EU) 2022/123.
	(b) proizvodnja računala te elektroničkih i optičkih proizvoda	– subjekti koji obavljaju bilo koju od gospodarskih djelatnosti iz područja C odjeljka 26. Nacionalne klasifikacije djelatnosti 2007. – NKD 2007. („Narodne novine, br. 58/07. i 72/07.).
	(c) proizvodnja električne opreme	– subjekti koji obavljaju bilo koju od gospodarskih djelatnosti iz područja C odjeljka 27. Nacionalne klasifikacije djelatnosti 2007. – NKD 2007. („Narodne novine, br. 58/07. i 72/07.).
	(d) proizvodnja strojeva i uređaja, d. n.	– subjekti koji obavljaju bilo koju od gospodarskih djelatnosti iz područja C odjeljka 28. Nacionalne klasifikacije djelatnosti 2007. – NKD 2007. („Narodne novine, br. 58/07. i 72/07.).
	(e) proizvodnja motornih vozila, prikolica i poluprikolica	– subjekti koji obavljaju bilo koju od gospodarskih djelatnosti iz područja C odjeljka 29. Nacionalne klasifikacije djelatnosti 2007. – NKD 2007. („Narodne novine, br. 58/07. i 72/07.).
	(f) proizvodnja ostalih prijevoznih sredstava	– subjekti koji obavljaju bilo koju od gospodarskih djelatnosti iz područja C odjeljka 30. Nacionalne klasifikacije djelatnosti 2007. – NKD 2007. („Narodne novine, br. 58/07. i 72/07.).
6. Pružatelji digitalnih usluga		– pružatelji internetskih tržišta
		– pružatelji internetskih tražilica
		– pružatelji platformi za usluge društvenih mreža
7. Istraživanje		– istraživačke organizacije
8. Sustav obrazovanja		– privatni i javni subjekti iz sustava obrazovanja

PRILOG III.

POPIS NADLEŽNOSTI U PODRUČJU KIBERNETIČKE SIGURNOSTI

R. br.	Sektor	Podsektor	Vrsta subjekta	Nadležno tijelo za provedbu zahtjeva kibernetičke sigurnosti	Nadležno tijelo za provedbu posebnih zakona	Nadležni CSIRT
1.	Energetika	Svi	Svi	Središnje državno tijelo za kibernetičku sigurnost	–	Nacionalni centar za kibernetičku sigurnost
2.	Promet	Zračni promet	Svi	–	Hrvatska agencija za civilno zrakoplovstvo	Nacionalni centar za kibernetičku sigurnost
3.	Promet	Željeznički Vodeni Cestovni	Svi	Središnje državno tijelo za kibernetičku sigurnost	–	Nacionalni centar za kibernetičku sigurnost
4.	Bankarstvo	–	Svi	–	Hrvatska narodna banka	Nacionalni CERT
5.	Infrastruktura financijskog tržišta	–	Svi	–	Hrvatska agencija za nadzor financijskih usluga	Nacionalni CERT
6.	Zdravstvo	–	Svi	Središnje državno tijelo za kibernetičku sigurnost	–	Nacionalni centar za kibernetičku sigurnost
7.	Voda za ljudsku potrošnju	–	Svi	Središnje državno tijelo za kibernetičku sigurnost	–	Nacionalni centar za kibernetičku sigurnost
8.	Otpadne vode	–	Svi	Središnje državno tijelo za kibernetičku sigurnost	–	Nacionalni centar za kibernetičku sigurnost
9.	Digitalna infrastruktura	–	Pružatelji usluga povjerenja	Tijelo državne uprave nadležno za razvoj digitalnog društva	–	Nacionalni centar za kibernetičku sigurnost
10.	Digitalna infrastruktura	–	Pružatelji javnih elektroničkih komunikacijskih mreža Pružatelji javno dostupnih elektroničkih komunikacijskih usluga	Hrvatska regulatorna agencija za mrežne djelatnosti	–	Nacionalni centar za kibernetičku sigurnost
11.	Digitalna infrastruktura	–	Pružatelji središta za razmjenu internetskog prometa Pružatelji usluga DNS-a, osim operatora korijenskih poslužitelja naziva Pružatelji usluga računalstva u oblaku Pružatelji usluga podatkovnog centra Pružatelji mreže za isporuku sadržaja	Središnje državno tijelo za kibernetičku sigurnost	–	Nacionalni centar za kibernetičku sigurnost
12.	Digitalna infrastruktura	–	Registar naziva vršne nacionalne internetske domene	Tijelo državne uprave nadležno za znanost i obrazovanje	–	Nacionalni CERT

13.	Upravljanje uslugama IKT-a (B2B)	–	Svi	Središnje državno tijelo za kibernetičku sigurnost	–	Nacionalni centar za kibernetičku sigurnost
14.	Javni sektor	–	Svi	Središnje državno tijelo za informacijsku sigurnost	–	Nacionalni centar za kibernetičku sigurnost
15.	Svemir	–	Svi	Središnje državno tijelo za kibernetičku sigurnost	–	Nacionalni centar za kibernetičku sigurnost
16.	Poštanske i kurirske usluge	–	Svi	Središnje državno tijelo za kibernetičku sigurnost	–	Nacionalni centar za kibernetičku sigurnost
17.	Gospodarenje otpadom	–	Svi	Središnje državno tijelo za kibernetičku sigurnost	–	Nacionalni centar za kibernetičku sigurnost
18.	Izrada, proizvodnja i distribucija kemikalija	–	Svi	Središnje državno tijelo za kibernetičku sigurnost	–	Nacionalni centar za kibernetičku sigurnost
19.	Proizvodnja, prerada i distribucija hrane	–	Svi	Središnje državno tijelo za kibernetičku sigurnost	–	Nacionalni centar za kibernetičku sigurnost
20.	Proizvodnja	Proizvodnja medicinskih proizvoda i in vitro dijagnostičkih medicinskih proizvoda	Svi	Središnje državno tijelo za kibernetičku sigurnost	–	Nacionalni centar za kibernetičku sigurnost
		Proizvodnja računala te elektroničkih i optičkih proizvoda				
		Proizvodnja električne opreme				
		Proizvodnja strojeva i uređaja, d. n.				
		Proizvodnja motornih vozila, prikolica i poluprikolica				
		Proizvodnja ostale opreme za prijevoz				
21.	Pružatelji digitalnih usluga	–	Svi	Središnje državno tijelo za kibernetičku sigurnost	–	Nacionalni centar za kibernetičku sigurnost
22.	Istraživanje	–	Svi	Tijelo državne uprave nadležno za znanost i obrazovanje	–	Nacionalni CERT
23.	Sustav obrazovanja	–	Svi	Tijelo državne uprave nadležno za znanost i obrazovanje	–	Nacionalni CERT

PRILOG IV.

OBVEZNI SADRŽAJ NACIONALNOG AKTA STRATEŠKOG PLANIRANJA IZ PODRUČJA KIBERNETIČKE SIGURNOSTI

I.

Nacionalnim aktom strateškog planiranja iz članka 55. ovoga Zakona utvrđuju se:

– ciljevi i prioriteti jačanja kibernetičke sigurnosti koji posebno obuhvaćaju sektore i podsektore iz Priloga I. i Priloga II. ovoga Zakona, kao i nadležna tijela iz Priloga III. ovoga Zakona

– upravljački okvir za postizanje ciljeva i prioriteta iz podstavka 1. ovoga stavka, za razvoj i provedbu politika iz točke II. ovoga Priloga, za razvoj i jačanje suradnje i koordinacije na nacionalnoj razini između nadležnih tijela za provedbu zahtjeva kibernetičke sigurnosti, jedinstvene kontaktne točke i nadležnih CSIRT-ova, kao i suradnje i koordinacije između tih tijela i nadležnih tijela za provedbu posebnih zakona, s objašnjenjima uloga i odgovornosti svih tijela relevantnih za provedbu politika kibernetičke sigurnosti na nacionalnoj razini

– okviri politika za bolju koordinaciju između nadležnih tijela iz ovoga Zakona i nadležnih tijela iz zakona kojim se uređuje područje kritičnih infrastruktura, u svrhu razmjene informacija o rizicima, kibernetičkim prijetnjama i incidentima te o rizicima, prijetnjama i incidentima izvan kibernetičkog prostora i izvršavanja nadzornih zadaća

– mehanizam za utvrđivanje relevantne imovine i procjenu kibernetičkih rizika

– mjere za osiguravanje pripravnosti i sposobnosti reagiranja na kibernetičke incidente i oporavka od kibernetičkih incidenata, uključujući suradnju javnog i privatnog sektora

– plan povećanja opće razine osviještenosti o kibernetičkoj sigurnosti među građanima i potrebne mjere

– plan razvoja nacionalnih sposobnosti u području kibernetičke sigurnosti i potrebne mjere

– popis nadležnih tijela, drugih javnih subjekata te svih ostalih subjekata koji su uključeni u provedbu nacionalnog akta strateškog planiranja u području kibernetičke sigurnosti.

II.

Nacionalnim aktom strateškog planiranja iz članka 55. ovoga Zakona razrađuju se politike:

– za rješavanje kibernetičkih sigurnosnih pitanja u lancu opskrbe za IKT proizvode i IKT usluge kojima se za pružanje svojih usluga odnosno obavljanje svojih djelatnosti koriste subjekti na koje se primjenjuje ovaj Zakon

– za uključivanje i definiranje kibernetičkih sigurnosnih zahtjeva za IKT proizvode i IKT usluge u području javne nabave, uključujući, u odnosu na kibernetičku sigurnosnu certifikaciju, kriptiranje i upotrebu kibernetičkih sigurnosnih proizvoda otvorenog koda

– za upravljanje kibernetičkim ranjivostima, uključujući promicanje i olakšavanje koordiniranog otkrivanja kibernetičkih ranjivosti u skladu s člankom 54. ovoga Zakona

– koje se odnose na održavanje opće dostupnosti, cjelovitosti i povjerljivosti javne jezgre otvorenog interneta te, ako je to potrebno, kibernetičke sigurnosti podmorskih komunikacijskih kabela

– za promicanje razvoja, integracije i upotrebe relevantnih naprednih i inovativnih tehnologija radi provedbe najsuvremenijih mjera upravljanja kibernetičkim sigurnosnim rizicima

– za promicanje i razvoj obrazovanja i osposobljavanja u području kibernetičke sigurnosti, vještina u području kibernetičke sigurnosti, informiranja te istraživačkih i razvojnih inicijativa u području kibernetičke sigurnosti, kao i smjernica o dobroj praksi i kontrolama kibernetičke higijene namijenjenih građanima, kao i javnim i privatnim subjektima

– za potporu akademskim i istraživačkim institucijama u istraživanju, razvoju, unapređivanju i poticanju uvođenja alata za kibernetičku sigurnost i sigurne informacijske i komunikacijske infrastrukture, sustava i aplikacija

– koje uključuju relevantne postupke i odgovarajuće alate za razmjenu informacija radi poticanja i osiguranja dobrovoljne razmjene informacija o kibernetičkoj sigurnosti u skladu s propisima kojima se uređuju pravila pristupa i postupanja s određenom vrstom informacija

– za jačanje kibernetičke otpornosti i osnovne razine kibernetičke higijene malih i srednjih poduzeća, osobito onih na koje se ne primjenjuje ovaj Zakon, osiguravanjem lako dostupnih smjernica i pomoći za njihove specifične potrebe i

– za promicanje aktivne kibernetičke zaštite kao dijela šireg pristupa nacionalnoj kibernetičkoj sigurnosti.

255

Na temelju članka 89. Ustava Republike Hrvatske, donosim

ODLUKU

O PROGLAŠENJU ZAKONA O IZMJENAMA I DOPUNAMA ZAKONA O MORSKOM RIBARSTVU

Proglašavam Zakon o izmjenama i dopunama Zakona o morskom ribarstvu, koji je Hrvatski sabor donio na sjednici 26. siječnja 2024.

Klasa: 011-02/24-02/04
Urbroj: 71-10-01/1-24-2
Zagreb, 1. veljače 2024.

Predsjednik
Republike Hrvatske
Zoran Milanović, v. r.

ZAKON

O IZMJENAMA I DOPUNAMA ZAKONA O MORSKOM RIBARSTVU

Članak 1.

U Zakonu o morskom ribarstvu (»Narodne novine«, br. 62/17., 14/19. i 30/23.) članak 2. mijenja se i glasi:

»Ovim Zakonom uređuje se provedba sljedećih akata:

1. Uredbe (EU) br. 1380/2013 Europskog parlamenta i Vijeća od 11. prosinca 2013. o zajedničkoj ribarstvenoj politici, izmjeni uredaba Vijeća (EZ) br. 1954/2003 i (EZ) br. 1224/2009 i stavljanju izvan snage uredaba (EZ) br. 2371/2002 i (EZ) br. 639/2004 i Odluke Vijeća 2004/585/EZ (SL L 354, 28. 12. 2013.), kako je posljednji put izmijenjena Uredbom (EU) 2015/812 Europskog parlamenta i Vijeća od 20. svibnja 2015. o izmjeni uredaba Vijeća (EZ) br. 850/98,