

VLADA REPUBLIKE HRVATSKE

Zagreb, 27. rujna 2023.

|  |  |
| --- | --- |
| **Predlagatelj:** | Ministarstvo hrvatskih branitelja |

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

|  |  |
| --- | --- |
| **Predmet:** | Nacrt prijedloga zakona o kibernetičkoj sigurnosti |

**VLADA REPUBLIKE HRVATSKE**

**NACRT**

**PRIJEDLOG ZAKONA O KIBERENETIČKOJ SIGURNOSTI**

**Zagreb, rujan 2023.**

**PRIJEDLOG ZAKONA O KIBERNETIČKOJ SIGURNOSTI**

1. **USTAVNA OSNOVA ZA DONOŠENJE ZAKONA**

Ustavna osnova za donošenje Zakona o kibernetičkoj sigurnosti sadržana je u odredbi članka 2. stavka 4. podstavka 1. Ustava Republike Hrvatske („Narodne novine“, broj 85/10. - pročišćeni tekst i 5/14. - Odluka Ustavnog suda Republike Hrvatske).

1. **OCJENA STANJA I OSNOVNA PITANJA KOJA TREBA UREDITI ZAKONOM TE POSLJEDICE DONOŠENJA ZAKONA**

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 (u daljem tekstu: NIS2 direktiva), donesena je s ciljem otklanjanja problema uočenih u višegodišnjoj primjeni NIS1 direktive (Direktiva 2016/1148).

NIS2 direktiva stupila je na snagu 16. siječnja 2023. godine i stavlja van snage NIS1 direktivu iz 2016. godine s učinkom od 18. listopada 2024. te zahtijeva usklađivanje svih država članica, koje transpoziciju NIS2 direktive moraju provesti do 17. listopada 2024. godine, odnosno u roku od 21 mjesec od stupanja na snagu NIS2 direktive.

NIS2 direktiva postavlja bitno proširene zahtjeve u odnosu na NIS1 direktivu, zbog čega se postojeći Zakon o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga („Narodne novine“, broj 64/18), kojim je transponirana NIS1 direktiva u Republici Hrvatskoj, mora staviti van snage te se mora pripremiti novi okvir za upravljanje puno složenijim zahtjevima NIS2 direktive. Cilj novih, bitno proširenih NIS2 zahtjeva kibernetičke sigurnosti na razini EU je osiguravanje uvjeta za učinkovito funkcioniranje društva i gospodarstva u aktualnom digitalnom desetljeću koje donosi čitav niz disruptivnih tehnologija poput umjetne inteligencije ili kvantnog računarstva, ali isto tako i podizanje spremnosti EU-a na krize kao što je COVID-19 kriza ili ruska agresija na Ukrajinu te njihove refleksije na kibernetički prostor.

Dvije najvažnije promjene NIS2 direktive u odnosu na NIS1 direktivu su:

1. višestruko povećan broj sektora, podsektora i vrsta subjekata obveznika kibernetičke sigurnosti (više nego trostruko), koji sada obuhvaća sve ključne segmente društva (Prilog I. i Prilog II. ovog Nacrta) te
2. promjena uskog pristupa zahtjevima kibernetičke sigurnosti iz NIS1 direktive, koji su se primjenjivali samo na ključne usluge operatora i uvođenje sveobuhvatnog pristupa NIS2 direktive koji postavlja kibernetičke sigurnosne zahtjeve prema cjelokupnom poslovanju svakog od subjekata koji su NIS2 obveznici.

Usklađena primjena NIS2 zahtjeva na razini svih država članica i EU institucija osigurat će ključne ciljeve sigurnosti kritičnih kibernetičkih elemenata EU i država članica, učinkovite instrumente upravljanja organizacijom i kibernetičkim sigurnosnim procesima, suradnju svih nadležnih tijela i subjekata obveznika NIS2 direktive, kao i uspostavu reguliranog pristupa kibernetičkoj sigurnosti na razini cijele EU, odnosno uvođenje mjera za visoku zajedničku razinu kibernetičke sigurnosti širom Unije.

NIS2 direktivom želi se postići učinkovito upravljanje organizacijom i sigurnosnim procesima u kibernetičkom prostoru EU-a te u nacionalnim kibernetičkim prostorima država članica. Vrijeme uvođenja NIS2 direktive je kritično jer EU već kasni u regulaciji kibernetičke sigurnosti u odnosu na brzi razvoj tehnologije. NIS2 direktiva je središnji akt kibernetičke sigurnosti EU, ali istovremeno i samo jedan akt u paketu EU kibernetičko i sigurnosno povezanih akata donesenih 2022. godine, kao što su DORA[[1]](#footnote-1) uredba (financijski sektor) ili CER[[2]](#footnote-2) direktiva (kritična infrastruktura). Dodatno je NIS2 povezan i s CSA[[3]](#footnote-3) aktom (kibernetička sigurnosna certifikacija) iz 2019. godine, a u tijeku je usuglašavanje CRA[[4]](#footnote-4) akta (zahtjevi kibernetičke sigurnosti za proizvode s digitalnim elementima). Na sve ovo nadovezuje se potpuno novi paket akata kibernetičke sigurnosti, koji je Europska komisija (EK) objavila[[5]](#footnote-5) 18. travnja 2023. i koji sadrži dopune spomenutog CSA akta iz 2019. godine, koje su sada usklađene s NIS2 direktivom, kao i novi prijedlog *Cyber Solidarity Acta[[6]](#footnote-6)* (poboljšane mogućnosti odgovora na incidente kroz infrastrukturu i osposobljene institucije) i *Cyber Skills Academy[[7]](#footnote-7)* (virtualna platforma za razvoj znanja i vještina iz područja kibernetičke sigurnosti). Razvidno je da kibernetička sigurnost danas nužno traži uspostavu reguliranog pristupa kakav je u tradicionalnim resorima državne uprave prisutan već desetljećima (npr. promet, financije, poljoprivreda ili gospodarstvo).

Organizacijski se NIS2 transpozicija provodi na isti način kao i NIS1 transpozicija 2018. godine, kroz međuresornu radnu skupinu Nacionalnog vijeća za kibernetičku sigurnost (NVKS). NVKS je međuresorno tijelo za koordinaciju horizontalnih nacionalnih inicijativa u području kibernetičke sigurnosti, ustrojeno na temelju Nacionalne strategije kibernetičke sigurnosti Republike Hrvatske iz 2015. godine („Narodne novine“, broj: 108/15), a čine ga predstavnici 16 tijela. Dogovorom NVKS-a, NIS1 transpoziciju 2018. godine koordinirao je Ured Vijeća za nacionalnu sigurnost (UVNS), a NIS2 transpoziciju koordinira Sigurnosno-obavještajna agencija (SOA).

Jedan od ključnih ciljeva EU-a kroz NIS2 direktivu jest uvođenje reguliranog pristupa području kibernetičke sigurnosti. Razlog tome je visoka ovisnost suvremenog društva o tehnologiji koja se razvija velikom brzinom. Pri tome se ne misli samo na državni sektor ili na kritičnu infrastrukturu, već na sve segmente suvremenog društva, koji u velikom broju slučajeva mogu uzrokovati kaskadno širenje kibernetičkih incidenata i onemogućavanje ključnih društvenih i gospodarskih procesa.

Stvaranje kibernetičke otpornosti planira se postići i na EU razini i na razini država članica kroz zakonsko propisivanje, normizaciju te uvođenje procesa akreditacije i certifikacije. Na taj način uvodi se potrebna kontrola subjekata - obveznika mjera iz NIS2 direktive, kao i sustavna kontrola korištenih softverskih i hardverskih proizvoda i usluga u mrežnim i informacijskim sustavima subjekata obveznika. Ovakav pristup provodi se prvi put na razini EU na cjelovit način i u svrhu sustavne regulacije kibernetičke sigurnosti. Takav pristup uvodi odgovarajuće obveze kibernetičke sigurnosti za sve subjekte obveznike, ali istovremeno otvara gospodarski potencijal na razini EU-a za sve hrvatske tvrtke koje imaju sposobnosti u području kibernetičke sigurnosti.

Regulirani pristup kibernetičkoj sigurnosti nužno traži određenu razinu organizacijske centralizacije, kako na EU razini (npr. EK je kroz *Cyber Security Act* 2019. godine reorganizirala ENISA-u u Agenciju za kibernetičku sigurnost EU, a EU-CERT postavila za središnje tehničko tijelo za odgovor na kibernetičke incidente), tako i na razini država članica. Na razini država članica nema jednoobraznog rješenja. Različit pristup država članica u centralizaciji kibernetičke sigurnosti ponajviše je rezultat različitosti nacionalnog razvoja kibernetičkih resursa koji su se u prethodnim godinama razvili u pojedinim državama članicama. Sigurnosno-obavještajni sustavi velikog broja EU država članica korišteni su za proces centralizacije, budući da je područje kibernetičke sigurnosti integralni i vrlo važan dio nacionalne sigurnosti. To je vidljivo i iz aspekta kibernetičkih ugroza, gdje su najvažniji nacionalni resursi oni koji služe suzbijanju najvećih opasnosti za kibernetičku sigurnost, a to su prije svega državno-sponzorirani kibernetički APT[[8]](#footnote-8) napadi, ali i napadi zlonamjernim ucjenjivačkim programskim kôdovima (*Ransomware*), koje sustavno provode organizirane kriminalne skupine i koji čine značajnu štetu državama i poslovnom sektoru na globalnoj razini.

Sukladno navedenome, ovim Zakonom se predlaže organizacijski pristup kojim bi se nastavila transformacija postojećeg Centra za kibernetičku sigurnost SOA-e, kao najkompletnijeg nacionalnog resursa kibernetičke sigurnosti, a s ciljem uvođenja centralizacije upravljanja kibernetičkom sigurnošću i stvaranja novog Nacionalnog centra za kibernetičku sigurnost. Pri tome se koriste razvijene tehničke, organizacijske i stručne sposobnosti te kapaciteti koje je SOA izgradila u području kibernetičke sigurnosti. Neke od do sada izgrađenih kibernetičkih sposobnosti i resursa su:

* Centar za kibernetičku sigurnost SOA-e uspostavljen 2019. godine.
* Temeljem Odluke Vlade Republike Hrvatske iz 2021. godine, sustav SK@UT je utvrđen kao nacionalni sustav za otkrivanje naprednih kibernetičkih prijetnji i zaštitu kibernetičkog prostora[[9]](#footnote-9). U SK@UT su uključena sva ministarstva i ključna državna tijela, operatori ključne infrastrukture, primarno iz sektora energetike i transporta, kao i niz drugih tvrtki značajnih za Republiku Hrvatsku u cjelini. Sustav SK@UT omogućuje nacionalnu i globalnu[[10]](#footnote-10) razmjenu informacija o kibernetičkim incidentima i koordiniranje odgovora na kibernetičke napade u stvarnom ili gotovo stvarnom vremenu.
* Na temelju odluke Nacionalnog vijeća za kibernetičku sigurnost i Koordinacije za sustav domovinske sigurnosti, SOA od 2020. godine provodi operativnu razinu koordinacije[[11]](#footnote-11) u upravljanju kibernetičkim napadima velikih razmjera i kibernetičkim krizama u Republici Hrvatskoj.
* SOA sudjeluje kao hrvatski predstavnik u EU-CyCLONe[[12]](#footnote-12) mreži za upravljanje EU kibernetičkim krizama od 2020. godine, a pristup upravljanju kibernetičkim krizama EU-a razvijen u EU-CyCLONe mreži propisuje se kroz NIS2 zahtjeve i u Republici Hrvatskoj je u potpunosti usklađen u proteklim godinama.
* Krajem 2022. godine SOA je započela nacionalnu koordinaciju provedbe Pilot projekta EK i ENISA-e za podizanje kibernetičke otpornosti na razini EU te je ukupno osigurala povlačenje od najmanje 1,7 milijuna eura EU financijskih sredstava, za razdoblje od 2023. do 2025. godine, u kojem će 100% europskim sredstvima financirane usluge kibernetičke sigurnosti provoditi hrvatske tvrtke u privatnim i državnim entitetima iz sustava SK@UT.
* Zaključkom o zaduženjima tijela državne uprave i drugih tijela za sudjelovanje u radu radnih skupina i odbora Vijeća Europske unije, Vlada Republike Hrvatske odredila je u rujnu 2022. godine SOA-u za nacionalnog koordinatora i praćenje EU kibernetičkih pitanja kroz Horizontalnu radnu skupinu za kibernetička pitanja (HWPCI) Vijeća EU, kroz koju se usklađuju svi uvodno spomenuti kibernetički akti EU-a (NIS2, CER, CRA, CSA, …).

Polovina država članica EU je centralizaciju kibernetičke sigurnosti započela upravo kroz nacionalne sigurnosno-obavještajne sustave, kao što su Danska, Grčka, Španjolska, Francuska, Njemačka i Italija. Neke od njih (Italija, Njemačka) su kasnije svoje nacionalne centre izdvojile u zasebne agencije, ali su oni godinama uredno i uspješno funkcionirali unutar sigurnosno-obavještajnih sustava. Također i države poput Velike Britanije i Kanade, s visokim stupnjem razvoja u području kibernetičke sigurnosti, imaju ustrojene nacionalne centre u sigurnosno-obavještajnim sustavima.

Svaka je članica EU osnivanje nacionalnog centra određivala temeljem vlastitih specifičnosti, potreba i već razvijenih kapaciteta. S obzirom da je Centar za kibernetičku sigurnost SOA-e trenutno najrazvijeniji i najkompletniji nacionalni resurs kibernetičke sigurnosti u Republici Hrvatskoj od 2019. najučinkovitije rješenje je transformacija postojećeg Centra u Nacionalni centar za kibernetičku sigurnost.

Problem brzog razvoja tehnologije neumitno generira nedostatak stručnjaka i to je problem cijelog svijeta pa i Republika Hrvatske u području kibernetičke sigurnosti. Najbolji način kojim se EU i niz razvijenih zemalja pokušava nositi s ovim problemom upravo je učinkovita organizacija i odgovarajuća organizacijska centralizacija, podizanje razine regulacije područja kibernetičke sigurnosti te paralelni razvoj i poticanje obrazovnih programa. Svi ti elementi u određenoj mjeri su započeti u Republici Hrvatskoj kroz Nacionalnu strategiju kibernetičke sigurnosti iz 2015. godine, nastavljeni su NIS1 transpozicijom iz 2018. godine te se dalje planiraju nastaviti izgrađivati NIS2 transpozicijom i njenom provedbom u narednim godinama.

Povećanje broja sektora i podsektora te vrsta usluga koje zahvaća NIS2 direktiva, odnosno povećanje broja obveznika NIS direktive, predstavlja nužnost suvremenog društva. Danas sve vrste tvrtki, od najvećih tvrtki do mikro poduzetnika, koriste informacijsku i komunikacijsku tehnologiju (IKT) te se može reći da svaka tvrtka i državno tijelo dio svojih poslovnih procesa zasniva na IKT-u. Na taj način sve te tvrtke ulažu u IKT, uključujući i ulaganja u sustave kibernetičke zaštite, u sklopu svojih redovitih troškova i neovisno o NIS2 direktivi. Subjekti obveznici NIS2 direktive i one pravne osobe koje će dobrovoljno primjenjivati pojedine NIS2 mjere kibernetičke sigurnosti, dobivaju mogućnost da svoja postojeća IKT ulaganja sustavno i postupno usmjeravaju s ciljem povećanja učinkovitosti i međusobne sukladnosti subjekata obveznika i drugih pravnih osoba u svim državama članicama EU. Dakle, cilj NIS2 direktive nije trenutno uvesti dodatan trošak za IKT unutar javnog sektora i poslovne zajednice, već postupno provesti tranziciju u smjeru bolje regulacije, organizacije i standardizacije kibernetičke sigurnosti, kako bi se u konačnici smanjili rizici i troškovi prekida poslovanja i gubitaka podataka uzrokovanih kibernetičkim incidentima.

Kroz Zakon se stoga predviđa proces kategorizacije subjekata, u okviru kojeg se primjenjuju utvrđeni kriteriji za razvrstavanje subjekata u kategorije ključnih i važnih subjekata, što će se provesti u roku od godine dana od stupanja na snagu Zakona te će se nakon toga periodično, svake dvije godine, utvrđeni popis ključnih i važnih subjekata ažurirati. Tek po obavijesti o kategorizaciji započinje rok od jedne godine za usklađivanje subjekata sa zahtjevima kibernetičke sigurnosti, a sukladnost se mora verificirati u postupku nezavisne ocjene sukladnosti ili samoocjene, ovisno o tome u koju kategoriju je subjekt razvrstan, kroz razdoblje od najduže dodatne dvije godine. Na taj način postupni proces tranzicije traje punih četiri godine nakon stupanja na snagu Zakona.

Upravo ta sukladnost sa zahtjevima NIS2 direktive, koja će svima osigurati manje troškove i gubitke u slučaju kibernetičkih incidenata, ima i dodatni cilj - omogućiti gospodarskim subjektima koji se bave kibernetičkom sigurnošću povećanu konkurentnost, ne samo na hrvatskom već i na širem EU tržištu. Regulacija područja kibernetičke sigurnosti i zahtjevi sukladnosti nužni su za današnji stupanj razvoja IKT-a te ih treba promatrati kao i u slučaju tradicionalnih sektora poput prometa, koji su danas visoko regulirani i usklađeni te primjerice pojava „nesukladnih entiteta“ u prometu nikome nije prihvatljiva.

NIS2 zahtjevi kroz ovaj Zakon primjenjuju se na sektore, podsektore i vrste subjekata, popisanih u Prilozima I. i II. Zakona odnosno na isti način kako je područje primjene NIS2 zahtjeva regulirano NIS2 direktivom. Prilog I. ovog Zakona obuhvaća visoko kritične sektore, podsektore i vrste subjekata te se sastoji od 11 sektora primarno namijenjenih razvrstavanju ključnih subjekata, prema općim kriterijima za provedbu kategorizacije subjekata. Ključni subjekti su oni subjekti na koje se mjere kibernetičke sigurnosti ovog Zakona primjenjuju u cijelosti, od zahtjeva za primjenom mjera, preko izvještavanja o incidentima, provedbe nezavisne ocjene sukladnosti, do nadzora (*ex-ante* pristup). Prilog II. ovog Zakona obuhvaća sektore, podsektore i vrste subjekata koji predstavljaju druge kritične sektore, a sastoji se od osam sektora, pri čemu je prvih sedam sektora preuzeto iz Priloga II. NIS2 direktive, dok je osmi sektor, sustav obrazovanja, nacionalno dodan temeljem NIS2 preporuke državama članicama i dogovora nadležnih tijela na nacionalnoj razini. Prilog II. je primarno namijenjen razvrstavanju važnih subjekata prema općim kriterijima za provedbu kategorizacije subjekata, odnosno subjekata koji primjenjuju mjere kibernetičke sigurnosti iz ovog Zakona, ali to provode samostalno i potvrđuju kroz postupak samoocjene (*ex-post* pristup) te se za takve subjekte ne provodi redovita nezavisna ocjena sukladnosti niti redoviti nadzor. Važni subjekti dužni su izvještavati o incidentima nadležno CSIRT tijelo, ali nadzor važnog subjekta provodi se samo u slučaju kada nadležno nadzorno tijelo raspolaže informacijama koje ukazuju da važni subjekt ne provodi mjere upravljanja kibernetičkim sigurnosnim rizicima u skladu s propisanim obvezama, ili ne ispunjava obveze vezane uz obavještavanje o kibernetičkim prijetnjama i incidentima na propisani način i u propisanim ili ostavljenim rokovima, ili ne postupa po drugim zahtjevima nadležnih tijela iz ovog Zakona. Pored kategorizacije subjekata temeljem općih kriterija koji se većinom oslanjaju na veličinu subjekta, provodi se i kategorizacija subjekata temeljem posebnih kriterija, u okvirima koje nalaže NIS2 direktiva.

NIS2 mjere kibernetičke sigurnosti dio su procesa upravljanja kibernetičkim sigurnosnim rizicima koji je obvezujući za sve subjekte NIS2 direktive. Pri tome se primjenjuju EU ili međunarodne norme za upravljanje rizicima i provedbu sigurnosnih mjera. Razina sigurnosti i primijenjene sigurnosne mjere trebaju biti proporcionalne procijenjenom riziku kibernetičke sigurnosti svakog subjekta. Pri tome su kriteriji rizika primjerice: izloženost subjekta rizicima, veličina subjekta, vjerojatnost pojave kibernetičkih napada i njihova ozbiljnost, uključujući društveni i gospodarski učinak kibernetičkih napada, izloženost mrežnih i informacijskih sustava koje subjekt koristi, kao i korištena IKT. Provodi se tzv. *„All Hazards Approach” – Failure, Accident, Attack* – otkaz, nesreća, napad, odnosno uzimaju se u obzir sve vrste uzroka koji mogu dovesti do incidenata na mrežnim i informacijskim sustavima i posljedično utjecati na funkcioniranje usluga koje subjekt pruža, odnosno djelatnosti koju obavlja, te utjecati i na druge fizičke ili pravne osobe.

Mjere upravljanja kibernetičkim sigurnosnim 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 sprječavanje 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.

Obvezujuća područja za procjenu kibernetičkih sigurnosnih rizika obuhvaćaju niz područja kao što su primjerice: postupanje s incidentima, kontinuitet poslovanja, sigurnost lanaca opskrbe, uključujući sigurnosne aspekte u pogledu odnosa između svakog subjekta i njegovih izravnih dobavljača ili pružatelja usluga, kao i mnoga druga područja.

Uloga NIS2 nadležnih tijela pri tome je kategorizirati, odnosno razvrstati subjekte obveznike NIS2 sukladno sektorskoj pripadnosti i utvrđenim kriterijima, davati smjernice subjektima, pomagati u prevenciji i odgovoru na kibernetičke incidente, pratiti periodički proces ocjene NIS2 sukladnosti ključnih subjekata te provoditi njihov periodički nadzor, kao i pratiti periodički proces samoocjene NIS2 sukladnosti važnih subjekata te prema potrebi provoditi njihov izvanredni nadzor. Sva nadležna tijela u području kibernetičke sigurnosti iz ovog Zakona povezana su sa sektorima, podsektorima i vrstama subjekata za koje su nadležni u Prilogu III. ovog Zakona.

U ovom Zakonu razlikujemo tri grupe nadležnih tijela. Nadležna tijela za provedbu posebnih zakona uključuju tzv. autonomne sektore, odnosno sektore u kojima je kibernetička sigurnost propisana sektorskim propisima na EU, odnosno nacionalnoj razini. Tu se trenutno radi o tri sektora: bankarstvo i Hrvatska narodna banka (HNB) kao nadležno tijelo, infrastrukture financijskog tržišta i Hrvatska agencija za nadzor financijskih usluga (HANFA) kao nadležno tijelo, te zračni promet i Hrvatska agencija za civilno zrakoplovstvo kao nadležno tijelo. Nadležna tijela za provedbu posebnih zakona stoga provode svoje sektorske propise koji sadrže veću ili jednaku razinu zahtjeva kibernetičke sigurnosti kao NIS2 direktiva, pri čemu se ovim Zakonom utvrđuje obveza nadležnih tijela za provedbu posebnih zakona za uključenje svojih sektorskih subjekata u razmjenu informacija i izvještavanje o incidentima na nacionalnoj razini.

Nadležna tijela za provedbu zahtjeva kibernetičke sigurnosti obuhvaćaju dvije grupe sektora, podsektora i vrsta subjekata. Prva grupa uključuje tri tzv. polu-autonomna sektora: javni sektor i Ured Vijeća za nacionalnu sigurnost (UVNS) kao nadležno tijelo, sektor elektroničkih komunikacija i Hrvatska regulatorna agencija za mrežne djelatnosti (HAKOM) kao nadležno tijelo, te pružatelji usluga povjerenja i Središnji državni ured za razvoj digitalnog društva (SDURDD) kao nadležno tijelo. Specifičnost polu-autonomnih sektora jest da je kibernetička sigurnost u određenoj mjeri propisana sektorskim propisima na EU razini i/ili nacionalnoj razini, ali je to nedovoljno u odnosu na zahtjeve NIS2 direktive. Stoga je već NIS2 direktiva stavila izvan snage pojedine članke vezane za kibernetičku sigurnost u mjerodavnim EU aktima za sektor elektroničkih komunikacija[[13]](#footnote-13) i sektor pružatelja usluga povjerenja[[14]](#footnote-14). Na sličan način je za potrebe javnog sektora potrebno primijeniti NIS2 zahtjeve kibernetičke sigurnosti, koji su značajno prošireni u odnosu na postojeće zahtjeve koji proizlaze iz propisa koji uređuju područje informacijske sigurnosti. Druga grupa nadležnih tijela za provedbu zahtjeva kibernetičke sigurnosti obuhvaća najveći broj sektora, podsektora i vrsta subjekata iz Priloga I. i II. ovog Zakona, ukupno 30 sektora, podsektora i vrsta subjekata. Ministarstvo znanosti i obrazovanja je nadležno tijelo za provedbu zahtjeva kibernetičke sigurnosti za tri sektora: sektor istraživanja, sektor sustava obrazovanja te za registar naziva vršne nacionalne internetske domene i registrare. Sigurnosno-obavještajna agencija (SOA) predstavlja središnje državno tijelo za područje kibernetičke sigurnosti koje ustrojava Nacionalni centar za kibernetičku sigurnost te pokriva preostalih 27 sektora. Nadležna CSIRT[[15]](#footnote-15) tijela, Zakonom se utvrđuju za svaki pojedini sektor, podsektor i vrstu subjekta prema Prilogu III. ovog Zakona. Nadležna CSIRT tijela za Republiku Hrvatsku su: Nacionalni centar za kibernetičku sigurnost, koji ustrojava SOA, te Nacionalni CERT, ustrojen u CARNET-u.

Zakon utvrđuje i način usklađivanja sadržaja nacionalnog akta strateškog planiranja iz područja kibernetičke sigurnosti, čiji se sadržaji detaljno razrađuju u Prilogu IV. ovog Zakona te su usklađeni s NIS2 zahtjevima za sve države članice.

Također, ovim Zakonom uvode se okviri za provedbu dobrovoljnih mehanizama kibernetičke zaštite, a koji omogućavaju subjektima koji nisu utvrđeni kao ključni ili važni subjekti da poduzimaju aktivnosti u cilju podizanja razine kibernetičke sigurnosti svojih mrežnih i informacijskih sustava, uz pružanje stručne pomoći nadležnih tijela iz ovog Zakona, a napose od strane nadležnih CSIRT-ova.

Provedba NIS2 transpozicije otvara mogućnosti usklađenog i optimalnog usmjeravanja proračunskih sredstava, ali i korištenja EU fondova za javni i za privatni sektor, kao i izbjegavanja neracionalnog multipliciranja nacionalnih kapaciteta ili neracionalnosti u pristupu opremanju radi razvoja novih sposobnosti koje već postoje u drugim tijelima. U tom smislu Zakon obvezuje nadležna tijela za provedbu zahtjeva kibernetičke sigurnosti na suradnju i međusobnu razmjenu relevantnih informacija s nacionalnim koordinacijskim centrom imenovanim temeljem 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.). Na taj način će se bolje koordinirati EU sredstva za potporu kibernetičke sigurnosti. Spomenuti Pilot projekt EK i ENISA-e, koji u razdoblju od 2023. do 2025. godine SOA koordinira na razini Republike Hrvatske, također je primjer povlačenja EU sredstava u razdoblju do uspostave i pune funkcionalnosti nacionalnog koordinacijskog centra, a poslužio je kao primjer i za pripremu novog EU prijedloga *Cyber Solidarity Acta*.

Zakonom je, radi potpunog prijenosa NIS2 direktive u nacionalno zakonodavstvo, predviđeno donošenje podzakonskih akata, uredbe Vlade Republike Hrvatske, kojom se detaljnije uređuju područja iz ovog Zakona, te nacionalnog programa za upravljanje kibernetičkim krizama, kao i nacionalnog srednjoročnog akta strateškog planiranja iz područja kibernetičke sigurnosti, s akcijskim planom za njegovu provedbu. Dodatno je, u svrhu pune funkcionalnosti transpozicije, potrebno osigurati funkcionalnost svih nadležnih tijela, osobito Nacionalnog centra za kibernetičku sigurnost koji se prvi puta ustrojava u Republici Hrvatskoj. Rok za potpuni prijenos NIS2 direktive u opisanom smislu je 17. listopada 2024. godine.

1. **OCJENA POTREBNIH SREDSTAVA ZA PROVOĐENJE ZAKONA**

Za provedbu ovog Zakona u Državnom proračunu za 2023. i projekcijama za 2024. i 2025. godinu osiguran je dio sredstava, a ostatak će se osigurati u okviru dodijeljenih limita nadležnih tijela u narednim razdobljima ovisno o stanju postojećih kapaciteta nadležnih tijela, broju subjekata obveznika provedbe zahtjeva iz ovog Zakona te mogućnostima korištenja sredstava iz EU fondova koji će biti raspoloživi u svrhu provedbe NIS2 direktive u državama članicama.

1. **TEKST PRIJEDLOGA ZAKONA**

Tekst prijedloga zakona dan je u obliku Nacrta prijedloga zakona o kibernetičkoj sigurnosti.

**PRIJEDLOG ZAKONA 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 kategorizaciju ključnih i važnih subjekata, zahtjevi kibernetičke sigurnosti za ključne i važne subjekte, posebni zahtjevi za upravljanje podacima o registraciji naziva domena, 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 ovog 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 ovog 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 dio ovoga Zakona su:

− Prilog I. Sektori visoke kritičnosti (u daljnjem tekstu: Prilog I. ovog Zakona)

− Prilog II. Drugi kritični sektori (u daljnjem tekstu: Prilog II. ovog Zakona)

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

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

**Usklađivanje propisa s pravnim aktima Europske unije**

**Članak 3.**

Ovim Zakonom se 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 ovog 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 s ciljem 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 za potrebe ovog pojma:

a) „na daljinu“ znači da se usluga pruža bez da su strane 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 izuzetak 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 temeljem 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 žičnim, 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 podstavcima 1. i 2. ove točke, u svrhu njihova rada, uporabe, zaštite i održavanja

26. *„nacionalni akt strateškog planiranja iz područja kibernetičke sigurnosti”* je sveobuhvatan okvir kojim se predviđaju strateški 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, 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 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 temeljem ovog 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 DNS-a, registar naziva vršnih domena, subjekt koji pruža usluge registracije naziva domena, 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 ovog 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 (u Republici Hrvatskoj to je Hrvatska akademska i istraživačka mreža – CARNET) 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

43. „*registrar“* jesubjekt 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), prvenstveno 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 kako su oni definirani u točkama 17., 36. i 54. ovog stavka

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 temeljem ovog 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 provedba 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“* jeMinistarstvo 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. stavku. 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 široki 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 ovog 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 ovog 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 ovog 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 koji uređuje područje elektroničkih komunikacija**

**Članak 7.**

(1) Primjena odredaba ovog 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 ovog Zakona ne utječe na pravila upravljanja vršnom nacionalnom internetskom domenom i 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. ovog Zakona i Priloga II. ovog Zakona posebnim zakonima propisani zahtjevi koji po svom sadržaju i svrsi odgovaraju zahtjevima kibernetičke sigurnosti iz ovog Zakona, ili predstavljaju strože zahtjeve, na te subjekte primjenjuju se odgovarajuće odredbe tog posebnog zakona u onim pitanjima koja su vezano uz te zahtjeve i njihovu provedbu tim propisima uređena, uključujući odredbe o nadzoru provedbe zahtjeva.

(2) Zahtjevi iz stavka 1. ovog članka po svom sadržaju i svrsi odgovaraju zahtjevima kibernetičke sigurnosti iz ovog 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. ovog članka nadležna za sektor odnosno podsektor i/ili subjekt iz Priloga I. i Priloga II. ovog Zakona i nadležna tijela za provedbu zahtjeva kibernetičke sigurnosti dužna su prilikom primjene stavaka 1. i 2. ovog članka međusobno surađivati i razmjenjivati relevantne informacije te voditi računa o smjernicama Europske komisije kojima se pojašnjava 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. ovog Zakona koji prelaze gornje granice za srednje subjekte malog 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 vršnenacionalneinternetskedomene te pružatelji usluga DNS-a, neovisno o njihovoj veličini

- pružatelji javnih elektroničkih komunikacijskih mreža ili javno dostupnih elektroničkih komunikacijskih usluga koji predstavlja srednji subjekt malog 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 malog 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 kritičnih infrastruktura, 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. ovog Zakona koji predstavljaju srednji subjekt malog 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 malog gospodarstva

- privatni i javni subjekti iz Priloga I. ovog Zakona koji nisu utvrđeni kao ključni subjekti temeljem članka 9. ovog Zakona, a predstavljaju srednji subjekt malog 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 malog gospodarstva

- pružatelji usluga povjerenja koji nisu kategorizirani kao ključni subjekti, neovisno o njihovoj veličini i

- pružatelji javnih elektroničkih komunikacijskih mreža ili javno dostupnih elektroničkih komunikacijskih usluga koji nisu kategorizirani kao ključni subjekti, 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. ovog Zakona, subjekti iz Priloga I. i Priloga II. ovog 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. ovog 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

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

- privatni i javni subjekti koji upravljaju, razvijaju ili održavaju državnu informacijsku infrastrukturu sukladno zakonu koji uređuje državnu informacijsku infrastrukturu.

(2) U kategoriju važnih subjekata razvrstavaju se, neovisno o njihovoj veličini:

- jedinice lokalne i područne (regionalne) samouprave, ovisno o rezultatima provedene procjene njihove važnosti za nesmetano obavljanje ključnih društvenih ili gospodarskih djelatnosti.

**Kategorizacija subjekata sustava obrazovanja**

**Članak 13.**

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 temeljem teritorijalnosti**

**Članak 14.**

(1) Subjekti iz Priloga I. i Priloga II. ovog 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. ovog 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. ovog članka, pružatelji usluga DNS-a, registar naziva vršne nacionalne internetske domene i registrari, 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. ovog 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. ovog 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. ovog stavka ne može utvrditi.

**Primjena kriterija veličine subjekta**

**Članak 15.**

(1) Prilikom utvrđivanja predstavlja li subjekt srednji subjekt malog gospodarstva odnosno subjekt koji prelaze gornje granice za srednje subjekte malog 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 subjekta 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. ovog 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 subjekta primjenjuju se odredbe ovog 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 temeljem članka 9. stavka 1. podstavaka 1., 2. 3. i 5., članka 10. i članka 12. stavka 1. podstavka 1. i stavka 2. ovog Zakona, za svaki sektor i podsektor iz Priloga I. I Priloga II. ovog Zakona

- Europskoj komisiji podatke o broju ključnih i važnih subjekata razvrstanih temeljem članka 11. ovog Zakona, sektoru i podsektoru kojima pripadaju, vrsti usluge koju pružaju i odredbama članka 11. ovog 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. ovog 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. ovog Zakona iz njihove nadležnosti obavijestiti o provedenoj kategorizaciji subjekta i obvezama kojima podliježu temeljem ovog Zakona i provedbenog propisa o zahtjevima kibernetičke sigurnosti.

(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 temeljem ovog Zakona i provedbenog propisa o zahtjevima kibernetičke sigurnosti, 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 niti važnim subjektima, obavijestiti o toj činjenici te činjenici da od datuma primitka te obavijesti više ne podliježu obvezama provedbe zahtjeva kibernetičke sigurnosti iz ovog Zakona.

(4) Nadležna tijela za provedbu zahtjeva kibernetičke sigurnosti dužna su o provedenoj kategorizaciji subjekta, kao i promjenama iz stavaka 2. i 3. ovog članka, obavijestiti subjekte u roku od 30 dana od 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. ovog 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 i podsektor iz Priloga I. i Priloga II. ovog Zakona

- popis država članica u kojima pružaju usluge obuhvaćene područjem primjene ovog 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 temeljem stavka 1. ovog 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 primitka zahtjeva za dostavom podataka.

(3) Subjekti iz stavka 1. ovog 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. ovog 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 rada prikupljaju podatke odnosno vode registre, evidencije i zbirke podataka o subjektima iz Priloga I. i Priloga II. ovog Zakona, dužni su, bez naknade, nadležnim tijelima za provedbu zahtjeva kibernetičke sigurnosti:

- redovito dostavljati popise subjekata iz Priloga I. i Priloga II. ovog 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. ovog 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, pravnu osobu s javnim ovlastima ili javnog subjekta koji takve podatke posjeduje.

(2) Ako se podaci temeljem ovog članka dostavljaju na zahtjev nadležnih tijela za provedbu zahtjeva kibernetičke sigurnosti, rokovi za dostavu podataka se određuju 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 primitka zahtjeva za dostavom 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. ovog članka vodi se neovisno o obvezi vođenja popisa ključnih i važnih subjekata.

**Prikupljanje podataka**

**Članak 23.**

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

- naziv subjekta

- popis usluga iz članka 22. ovog Zakona koje pružaju

- adresu glavnog poslovnog nastana subjekta i njegovih drugih poslovnih jedinica ili adresu njegovog predstavnika

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

- popis država članica u kojima pružaju usluge iz članka 22. ovog Zakona

- IP adresne raspone subjekta.

(2) Rok za dostavu podataka temeljem stavka 1. ovog članka je 15 dana od primitka zahtjeva za dostavom podataka.

(3) Subjekti iz članka 22. ovog 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. ovog članka.

(4) Po zaprimanju, podaci iz stavaka 1. i 3. ovog članka, osim podataka iz stavka 1. podstavka 6. ovog 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 temeljem posebnih kriterija iz članka 11. ovog Zakona, kriteriji za provođenje procjena iz članka 12. stavka 1. podstavka 2. i stavka 2. i članka 13. ovog 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. ovog 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 u cilju 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. ovog Zakona.

**POGLAVLJE I.**

 **MJERE UPRAVLJANJA KIBERNETIČKIM SIGURNOSNIM RIZICIMA**

**Primjena mjera**

**Članak 26.**

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

(2) Cilj primjene mjera upravljanja kibernetičkim sigurnosnim rizicima je zaštita mrežnih i informacijskih sustava i fizičkog okruženja tih sustava od incidenata uzimajući pri tome 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. ovog Zakona.

(6) Kada subjekta obavještava o promjeni u kategorizaciji subjekta temeljem članka 19. stavka 2. ovog 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 temeljem ovog Zakona i provedbenog propisa o zahtjevima kibernetičke sigurnosti.

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

**Obveza osiguranja razine sigurnosti mrežnih i informacijskih sustava proporcionalnu 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 uzimaju u obzir najnovija tehnička dostignuća koja se koriste u okviru najbolje sigurnosne prakse u području kibernetičke sigurnosti te koriste se, bez nametanja obveza ili diskriminacije u korist uporabe određene vrste tehnologije, europske i međunarodne norme i tehničke specifikacije relevantne za sigurnost mrežnih i informacijskih sustava, uzimajući pri tome 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

- uredbom iz članka 24. ovog 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) Uz osobe odgovorne za upravljanje mjerama, odredbe ovog 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 najmanje 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 kibernetičkih napada, 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 osposobljavanja 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

- korištenja 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. ovog 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.

**POGLAVLJE II.**

 **OBVEZE OBAVJEŠTAVANJA**

**Obavještavanje o značajnim incidentima**

**Članak 31.**

(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 (značajan incident).

(2) Incident se smatra značajnim:

- 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. ovog članka dostaviti tijelima kaznenog progona u slučajevima u kojima postoje osnove sumnje da su značajni incidenti nastali počinjenjem kaznenog djela, temeljem odredbi zakona kojim se uređuje kazneni postupak.

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

**Obavještavanje primatelja usluga**

**Članak 32.**

(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. ovog članka u roku od 30 dana od dana dostave obavijesti iz članka 19. stavka 1. ovog Zakona.

**Obavještavanje na dobrovoljnoj osnovi**

**Članak 33.**

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 34.**

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

**Obavještavanje javnosti o značajnom incidentu**

**Članak 35.**

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 podijeli nadležnosti iz Priloga III. ovog 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 36.**

(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 temeljem članaka 31. i 33. ovog 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 temeljem članaka 31. i 33. ovog Zakona.

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

**Članak 37.**

(1) Obavještavanje temeljem članaka 31. i 33. ovog Zakona i razmjena podataka o kibernetičkim prijetnjama i incidentima između nadležnih tijela iz Priloga III. ovog 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. ovog članka u nadležnosti je Hrvatske akademske i istraživačke mreže - CARNET (u daljnjem tekstu: CARNET).

**Provedbeni propis o zahtjevima kibernetičke sigurnosti**

**Članak 38.**

Mjere upravljanja kibernetičkim sigurnosnim rizicima, način njihove provedbe, kriteriji za utvrđivanje značajnih incidenata, uključujući kriterijske pragove ako su potrebni zbog specifičnosti pojedinog sektora, vrste i sadržaj obavijesti iz članaka 31. do 34. ovog Zakona, rokovi za njihovu dostavu, prava pristupa i druga pitanja bitna za korištenje nacionalne platforme za prikupljanje, analizu i razmjenu podataka o kibernetičkim prijetnjama i incidentima, mogućnosti korištenja drugih načina dostave obavijesti iz članaka 31. do 34. ovog Zakona, postupanja s tim obavijestima, uključujući postupanja nadležnog CSIRT-a u povodu zaprimljenih obavijesti, propisuju se uredbom iz članka 24. ovog Zakona.

**POGLAVLJE III.**

**PROVJERE USKLAĐENOSTI KLJUČNIH I VAŽNIH SUBJEKATA SA ZAHTJEVIMA KIBERNETIČKE SIGURNOSTI**

**Provjere usklađenosti sa zahtjevima kibernetičke sigurnosti**

**Članak 39.**

(1) Ključni i važni subjekti dužni su provoditi provjeru usklađenosti sa zahtjevima kibernetičke sigurnosti propisanih ovim Zakonom.

(2) Provjera usklađenosti iz stavka 1. ovog članka obavlja se u postupku ocjene sukladnosti ključnih i važnih subjekata te postupku samoocjene sukladnosti važnih subjekta.

**Tijela za ocjenu sukladnosti**

**Članak 40.**

(1) Ocjenu sukladnosti ključnih i važnih subjekata provode tijela za ocjenu sukladnosti.

(2) Tijela za ocjenu sukladnosti su privatni subjekti koji ispunjavaju organizacijske i stručne zahtjeve za autorizaciju propisane uredbom iz članka 24. ovog Zakona.

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

(4) Autorizaciju tijela za ocjenu sukladnosti iz stavka 2. ovog članka provodi središnje državno tijelo za obavljanje poslova u tehničkim područjima informacijske sigurnosti, a izdaje se na rok od pet godina.

(5) Središnje državno tijelo za obavljanje poslova u tehničkim područjima informacijske sigurnosti, tijekom važenja autorizacije provodi periodične provjere organizacijskih i stručnih zahtjeva iz stavka 2. ovog članka.

**Provedba ocjene sukladnosti**

**Članak 41.**

(1) Ocjenu sukladnosti ključni subjekti dužni su provoditi najmanje jednom u dvije godine.

(2) Ocjenu sukladnosti ključni subjekti dužni su provesti i prije proteka roka iz stavka 1. ovog članka, kad to zatraži nadležno tijelo za provedbu zahtjeva kibernetičke sigurnosti temeljem članka 79. stavka 1. podstavka 7. ili članka 81. stavka 1. podstavka 2. ovog Zakona.

(3) Ocjena sukladnosti iz stavka 1. ovog članka provodi se kao zaseban postupak ili u okviru revizije poslovanja, odnosno druge provjere sukladnosti subjekata koja se provodi temeljem posebnih propisa kojima se uređuje područje pružanja određenih usluga, odnosno obavljanja određenih djelatnosti.

(4) Ocjenu sukladnosti važni subjekti dužni su provesti kada to zatraži nadležno tijelo za provedbu zahtjeva kibernetičke sigurnosti temeljem članka 79. stavka 1. podstavka 7. ovog Zakona.

(5) O provedenoj ocjeni sukladnosti tijelo za ocjenu sukladnosti sastavlja izvješće.

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

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

(8) Troškove provedbe ocjene sukladnosti snose ključni i važni subjekti, ako nije drugačije propisano ovim Zakonom.

**Samoocjena sukladnosti važnih subjekata**

**Članak 42.**

(1) Samoocjenu sukladnosti važni subjekti dužni su provoditi najmanje jednom u dvije godine.

(2) Ako rezultati provedene samoocjene sukladnosti pokazuju da je subjekt usklađen sa zahtjevima kibernetičke sigurnosti propisanim ovim Zakonom, važni subjekti sastavljaju izjavu o sukladnosti koja sadrži elemente obuhvaćene samoocjenom sukladnosti.

(3) Izjavu iz stavka 2. ovog članka važni subjekti dužni su dostaviti nadležnom tijelu za provedbu zahtjeva kibernetičke sigurnosti bez odgode, u roku od osam dana od njezina sastavljanja.

(4) Troškove provedbe samoocjene sukladnosti snose važni subjekti.

**Registar autoriziranih tijela za ocjenu sukladnosti**

**Članak 43.**

Središnje državno tijelo za obavljanje poslova u tehničkim područjima informacijske sigurnosti vodi javno dostupan registar autoriziranih tijela za ocjenu sukladnosti.

**Provedbeni propis za ocjene i samoocjene sukladnosti**

**Članak 44.**

Pravila, tehnički zahtjevi, norme, obrasci i postupci koji se primjenjuju prilikom provođenja ocjena i samoocjena sukladnosti te organizacijski i stručni zahtjevi za autorizaciju tijela za ocjenu sukladnosti uredit će se uredbom iz članka 24. ovog Zakona.

**POGLAVLJE IV.**

**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, a osobito:

- 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 registracijom 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 sadrži sve podatke iz članka 46. stavka 1. podstavaka 1. do 3. ovog 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 njezinog korištenja sve dok zahtjev ne bude uredno podnesen i to u roku od osam dana od primitka takve obavijesti.

(2) Registar naziva vršne nacionalne internetske domene i registrari dužni su periodički, 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. ovog članka na različite registrirane kontakt podatke 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. ovog 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 temeljem članaka 46. i 47. ovog Zakona čuvati 25 godina od prestanka prava korisnika na korištenje domene.

(2) Dokumentacija iz stavka 1. ovog 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. ovog članka, osobne podatke o korisniku domene brisati, a dokumentaciju iz stavka 2. ovog 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. ovog Zakona naznačiti svoju obvezu postupanja u skladu sa stavcima 1. i 3. ovog članka.

(6) Tehničke i organizacijske mjere za zaštitu osobnih podataka o korisnicima domena uređuju se posebnim propisima koji uređuju 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 iz članaka 45. do 48. ovog Zakona provodi tijelo državne uprave nadležno za znanost i obrazovanje.

**DIO ČETVRTI**

**DOBROVOLJNI MEHANIZMI KIBERNETIČKE ZAŠTITE**

**Samoocjene sukladnosti s mjerama upravljanja kibernetičkim sigurnosnim rizicima i dobrovoljno obavještavanje o incidentima i kibernetičkim prijetnjama**

**Članak 50.**

(1) Svaki subjekt koji nije kategoriziran kao ključni i važni subjekt sukladno ovom Zakonu može:

- provoditi samoocjene sukladnosti mrežnih i informacijskih sustava, kojima se služi u svom poslovanju ili u pružanju svojih usluga, s mjerama upravljanja kibernetičkim sigurnosnim rizicima iz članka 30. ovog Zakona

- nadležni CSIRT dobrovoljno obavijestiti o svakom značajnom incidentu, ostalim incidentima, kibernetičkim prijetnjama ili izbjegnutim incidentima, pod uvjetom da periodično provodi samoocjene sukladnosti iz podstavka 1. ovog stavka.

(2) Mogućnost provedbe samoocjena sukladnosti i dobrovoljnog obavještavanja iz stavka 1. ovog članka uredit će se uredbom iz članka 24. ovog Zakona.

**Nacionalni sustav za otkrivanje kibernetičkih prijetnji i zaštitu kibernetičkog prostora**

**Članak 51.**

(1) S ciljem 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. ovog Zakona.

(4) Pristupanje nacionalnom sustavu provodi se temeljem 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. ovog Zakona, već predstavlja dodatnu mjeru kibernetičke zaštite.

**Kriteriji za provedbu procjene kritičnosti subjekta**

**Članak 52.**

(1) Procjena kritičnosti subjekta iz članka 51. stavka 2. ovog Zakona provodi se temeljem 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. ovog Zakona provodi se temeljem:

- 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. ovog 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. ovog 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. ovog 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. ovog članka odvija se između subjekata iz stavka 1. ovog članka te, prema potrebi, njihovih dobavljača ili pružatelja usluga, putem mehanizama za razmjenu informaciju uspostavljenih posebno u te svrhe.

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

(5) Sporazumom iz stavka 4. ovog 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 informaciju, 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. ovog članka dužni su obavijestiti nadležna tijela 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. ovog 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. ovog članka čuvati najduže tri godine od prijave ranjivosti, a nakon isteka tog roka, osobne podatke o prijavitelju ranjivosti brisati, a evidencije iz stavka 7. ovog članka uništiti sukladno propisima o zaštiti osobnih podataka.

(9) CSIRT koordinator za otkrivanje ranjivosti dostavlja informacije o novootkrivenim ranjivostima nadležnim CSIRT-ovima iz ovog 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 temeljem ovog 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. ovog članka obvezno se utvrđuju:

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

- okvir za praćenje i vrednovanje provedbe ciljeva i prioriteta iz podstavka 1. ovog stavka.

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

(4) Izvještavanje, praćenje i vrednovanje akta strateškog planiranja iz stavka 1. ovog članka provodi se u skladu s propisom koji 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. ovog članka u roku od tri mjeseca od dana njegovog 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. ovog 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. ovog 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. ovog 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. ovog članka u roku od tri mjeseca od njegova donošenja odnosno njegovih izmjena i dopuna ili donošenja novog programa.

**Ocjenjivanje stanja kibernetičke sigurnosti**

**Članak 57.**

(1) U cilju 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 utvrđenoj od strane Skupine za suradnju, Europske komisije i ENISA-e.

(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 koji uređuje područje kritičnih infrastruktura, razina provedbe mehanizama za razmjenu informacija o kibernetičkoj sigurnosti iz članka 53. ovog Zakona i posebna pitanja međusektorske prirode.

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

(5) Planove i programe provedbe samoocjena koje države članice provode u okviru istorazinskih ocjenjivanja iz stavka 2. ovog 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. ovog 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. ovog 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 kojeg 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 ovog 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 ključnih i važnih subjekta u provedbi zahtjeva kibernetičke sigurnosti sukladno ovom Zakonu i uredbi iz članka 24. ovog 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 ovog Zakona

- surađuju i razmjenjuju relevantne informacije s nacionalnim koordinacijskim centrom imenovanim temeljem 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. ovog članka obavljaju prema podijeli nadležnosti iz Priloga III. ovog Zakona.

(3) U slučaju da za pojedini subjekt postoji nadležnost dva ili više tijela iz Priloga III. ovog 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. ovog članka središnje državno tijelo za kibernetičku sigurnost pokreće po službenoj dužnosti, na prijedlog jednog od nadležnih tijela prema Prilogu III. ovog 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 dužni su:

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

- najmanje jednom u dvije godine provoditi samoocjene sukladnosti mrežnih i informacijskih sustava kojima se služe u svom poslovanju s mjerama upravljanja kibernetičkim sigurnosnim rizicima iz članka 30. ovog Zakona te o provedenim samoocjenama sukladnosti izvještavati središnje državno tijelo za kibernetičku sigurnost.

(2) U smislu stavka 1. podstavka 1. ovog 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. ovog 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 kroz planiranje razvoja regulativnog okvira kibernetičke sigurnosti

- prati provedbu ovog 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. ovog 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 ispred Republike Hrvatske koordinira aktivnosti vezane za upravljanje kibernetičkim krizama na razini Europske unije

- obavlja poslove jedinstvene kontaktne točke

- obavlja poslove CSIRT tijela prema podijeli nadležnosti iz Priloga III. ovog Zakona

- provodi aktivnosti u cilju otkrivanja kibernetičkih prijetnji i zaštite nacionalnog kibernetičkog prostora

- izrađuje izvješća o stanju kibernetičke sigurnosti

- surađuje s drugim nadležnim tijelima iz ovog 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. ovog Zakona, te njihovim zadaćama i svim naknadnim promjenama dostavljenih informacija

- obavještava bez odgode Europsku komisiju o odredbama ovog 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 potrebe obavljanja zadaća iz članaka 59., 61. i 62. ovog 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 temeljem posebnih zakona iz članka 8. ovog Zakona, kada to zatraže nadležna nadzorna tijela.

(3) Pomoć iz stavka 2. ovog članka pruža se temeljem 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. ovog 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 ovog 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 koji uređuje područje kritičnih infrastruktura**

**Članak 65.**

(1) Nadležna tijela za provedbu zahtjeva kibernetičke sigurnosti i nadležna tijela iz zakona koji uređuje područje kritičnih infrastruktura međusobno surađuju i razmjenjuju relevantne informacije, a osobito informacije o:

- utvrđivanju subjekata kritičnim subjektima temeljem zakona koji uređuje područje kritičnih infrastruktura

- 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 koji uređuje područje kritičnih infrastruktura.

(2) Nadležna tijela iz zakona koji uređuje područje kritičnih infrastruktura 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 tijela državne uprave iz zakona koji uređuje područje kritičnih infrastruktura.

(4) Sporazumom iz stavka 3. ovog članka uređuju se sva bitna pitanja koja se odnose na razmjenu informacija i koordinaciju nadležnih tijela, uključujući način razmjene informacija iz stavka 1. ovog 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 ovog 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 subjekta, 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 31. i 32. ovog Zakona, te provedbe dobrovoljnog obavještavanja iz članka 33. ovog 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. ovog 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. ovog Zakona

- doprinosi uvođenju i korištenju alata za sigurnu razmjenu informacija

- sudjeluje u provedbi istorazinskih ocjenjivanja koja se provode sukladno metodologiji utvrđenoj od strane Skupine za suradnju, Europske komisije i ENISA-e

- 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. ovog članka, CSIRT daje prednost prioritetnim zadaćama prema procjeni rizika, a prilikom obrade zaprimljenih obavijesti temeljem ovog Zakona daje prednost obradi obavijesti o značajnim incidentima.

(3) Kada suradnja iz stavka 1. podstavka 9. ovog 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) S ciljem 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. ovog članka ne smije imati negativan učinak na funkcioniranje usluga koje ključni i važni 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 temeljem skeniranja iz stavka 1. ovog 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, u cilju 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 ovog 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. ovog Zakona.

(2) U smislu članka 50. stavka 1. podstavka 2. ovog Zakona, središnje državno tijelo za kibernetičku sigurnost obavlja zadaće CSIRT-a za državna tijela i pravne osobe s javnim ovlastima, 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 koji uređuje zaštitu 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. ovog 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. ovog Zakona koju je počinio ključni ili važni 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. ovog 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 ključnog subjekta**

**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 ključnog subjekta provodi se i prije proteka rokova iz stavka 1. ovog članka, ako nadležno tijelo za provedbu zahtjeva kibernetičke sigurnosti raspolaže informacijama koje ukazuju 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 ovog Zakona.

(3) Terminski plan provedbe stručnih nadzora iz stavka 1. ovog 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. ovog 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 važnog subjekta**

**Članak 76.**

(1) Stručni nadzor važnog subjekta provodi se kada nadležno tijelo za provedbu zahtjeva kibernetičke sigurnosti raspolaže informacijama koje ukazuju 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 ovog Zakona.

(2) U svrhu utvrđivanja terminskih planova provedbe stručnih nadzora iz stavka 1. ovog 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 ovog Zakona ili

- uvidom u izvješća o provedenim ocjenama sukladnosti 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. ovog članka obavijestiti nadzirani subjekt najkasnije u roku od pet dana prije početka nadzora.

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

- u slučaju postojanja razloga koji ukazuju 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. ovog 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 neposredni 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 ovog Zakona

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

- zatražiti izvješća o provedenim ocjenama sukladnosti koje je provelo nadležno tijelo za ocjenu sukladnosti te druge relevantne dokaze o provedbi kibernetičkih sigurnosnih politika iz članka 30. ovog Zakona

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

- zatražiti provedbu ciljane ocjene sukladnosti.

(2) Kada se primjenjuje nadzorna mjera iz stavka 1. podstavka 7. ovog 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 s ciljem utvrđivanja preporuka za poboljšanje stanja ili smanjenje rizika kojima je subjekt izložen ili može biti izložen.

(3) Prilikom provedbe nadzornih mjera iz stavka 1. podstavaka 4. do 6. ovog 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.

**Ciljane ocjene sukladnosti**

**Članak 80.**

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

(2) Troškove ciljane ocjene sukladnosti snosi nadzirani subjekt.

(3) Iznimno od stavka 2. ovog članka, troškove ciljane ocjene sukladnosti 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. ovog Zakona, u obavljanju stručnog nadzora ključnog subjekta nadležno tijelo za provedbu zahtjeva kibernetičke sigurnosti ovlašteno je zatražiti provedbu:

- redovite ocjene sukladnosti, kada raspolaže informacijama iz kojih proizlazi da subjekt ocjenu sukladnosti nije proveo u rokovima iz članka 41. stavka 1. ovog Zakona i

- izvanredne ocjene sukladnosti, u slučaju značajnog incidenta ili kada utvrdi da su u prethodno provedenoj ocjeni sukladnosti utvrđene nepravilnosti, nedostaci ili propusti u provedbi zahtjeva kibernetičke sigurnosti koji u međuvremenu nisu otklonjeni ili raspolaže informacijama da subjekt ne provodi zahtjeve kibernetičke sigurnosti sukladno ovom Zakonu i uredbi iz članka 24. ovog Zakona.

(2) Na troškove ocjena sukladnosti provedenih temeljem stavka 1. ovog članka primjenjuje se članak 41. stavak 8. ovog Zakona.

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

- izdati obvezujuće upute ili naloge kojima se zahtijeva da otklone utvrđene nedostatke ili povrede ovoga Zakona i uredbe iz članka 24. ovog 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. ovog 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 ovog Zakona

- naložiti da u razumnom roku provedu preporuke koje su dane u izvješću o provedenoj ocjeni sukladnosti ili u okviru izrađenih analiza sigurnosti i

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

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

(3) Ako ključni ili važni 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. ovog 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. ovog 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. ovog 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 ključni subjekt ne postupi u skladu s izrečenim korektivnim mjerama iz članka 82. ovog 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. ovog Zakona

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

(2) Mjere iz stavka 1. ovoga članka primjenjuju se samo dok ključni subjekt ne postupi sukladno izrečenim korektivnim mjerama iz članka 82. ovog 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 koji uređuju javnu nabavu.

**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. ovog Zakona odnosno podnošenju zahtjeva sukladno članku 84. ovog 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. ovog Zakona s nadležnim tijelima iz ovog Zakona.

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

- 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 ocjene sukladnosti koje je zatražilo nadležno tijelo za provedbu zahtjeva kibernetičke sigurnosti ili aktivnosti praćenja koje je naložilo temeljem članka 83. ovog Zakona i

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

**Izricanje novčanih kazni**

**Članak 86.**

(1) Uz korektivne mjere propisane ovim Zakonom i podnošenje zahtjeva sukladno članku 84. ovog 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 ovog Zakona.

(2) Iznimno od stavka 1. ovog članka, u stručnim nadzorima ne može se podnijeti prijava ovlaštenom tužitelju odnosno izdati prekršajni nalog sukladno prekršajnim odredbama ovog 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. ovog 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 ovog Zakona i uredbe iz članka 24. ovog 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. ovog članka vode se sukladno smjernicama središnjeg državnog tijela za kibernetičku sigurnost.

**Stručni nadzor pružatelja javnih elektroničkih komunikacijskih mreža i pružatelja javno dostupnih elektroničkih komunikacijskih usluga**

**Članak 93.**

Poslove stručnog nadzora nad primjenom odredaba ovog Zakona i uredbe iz članka 24. ovog zakona, koji se odnose na stručni nadzor pružatelja javnih elektroničkih komunikacijskih mreža i pružatelja 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 jedne države članice 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, najmanje obuhvaća:

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

- podnošenje zahtjeva za poduzimanjem 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. ovog 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 ocjena sukladnosti.

(3) Nadležno tijelo za provedbu zahtjeva kibernetičke sigurnosti kojem je upućen zahtjev za uzajamnu pomoć u provedbi stručnog nadzora ne smije odbiti zahtjev, osim u slučaju 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 je, prije odbijanja zahtjeva iz stavka 3. ovoga članka, dužno 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 je dužno savjetovati se i s Europskom komisijom i ENISA-om.

(6) Odredbe ovog članka primjenjuju se i u slučaju zaprimanja zahtjeva za uzajamnu pomoć u provedbi stručnog nadzora nad subjektima iz članka 14. stavka 3. ovog 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 ovog 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) Tijelo državne uprave nadležno za znanost i obrazovanje provodi kontrolu usklađenosti iz članka 49. ovog Zakona:

- 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. ovog Zakona ili

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

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

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

(4) Registar naziva vršne nacionalne internetske domene i registrari dužni su omogućiti provedbu kontrole usklađenosti iz članka 49. ovog Zakona te osigurati sve uvjete za njezino 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 kontrole usklađenosti iz članka 49. ovog Zakona, registru naziva vršne nacionalne internetske domene i registrarima može:

- izdati upozorenja o povredama ovoga Zakona

- izdati obvezujuće upute ili naloge kojim 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. ovog 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. ovog 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. ovog Zakona.

**Zapisnici o provedenim kontrolama i sudska zaštita**

**Članak 100.**

Prilikom provedbe kontrola usklađenosti iz članka 49. ovog Zakona na odgovarajući način se primjenjuju članci 87. do 90. te članak 92. stavak 1. ovog Zakona.

**DIO DEVETI**

**PREKRŠAJNE ODREDBE**

**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 odgovorni ključni subjekt koji:

- ne poduzima, djelomično poduzima, ili ne poduzima u roku propisane mjere upravljanja kibernetičkim sigurnosnim rizicima (članak 26. ovog Zakona)

- 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. ovog 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. ovog Zakona)

- ne obavještava o svakom značajnom incidentu ili ne dostavlja u roku obavijesti o značajnim incidentima (članak 31. ovog Zakona)

- 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 32. ovog Zakona)

- ne provede ocjenu sukladnosti najmanje jednom u dvije godine (članak 41. ovog Zakona)

- ne dostavi u propisanom roku izvješće o ocjeni sukladnosti nadležnom tijelu za provedbu zahtjeva kibernetičke sigurnosti (članak 41. ovog Zakona)

- onemogućava, ometa ili otežava provedbu ocjene sukladnosti ili ne snosi troškove provedbe ocjene sukladnosti (članak 41. ovog Zakona)

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

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

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

- ne postupi ili djelomično postupi ili ne postupi u za to ostavljenom roku po korektivnim mjerama izrečenim u stručnom nadzoru (članak 82. i 83. ovog Zakona).

(2) Za prekršaj iz stavka 1. ovoga članka kaznit će se i odgovorna osoba prekršajno odgovornog ključnog subjekta novčanom kaznom u iznosu od 1.000,00 do 6.000,00 eura.

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

**Članak 102.**

(1) Novčanom kaznom u iznosu od 5.000,00 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. ovog Zakona)

- 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. ovog 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. ovog Zakona)

- ne obavještava o svakom značajnom incidentu ili ne dostavlja u roku obavijesti o značajnim incidentima (članak 31. ovog Zakona)

- 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 32. ovog Zakona)

- ne provede samoocjenu sukladnosti najmanje jednom u dvije godine (članak 42. ovog Zakona)

- ne dostavi u propisanom roku izjavu o sukladnosti nadležnom tijelu za provedbu zahtjeva kibernetičke sigurnosti (članak 42. ovog Zakona)

- onemogućava, ometa ili otežava provedbu ciljane ocjene sukladnosti ili ne snosi troškove provedbe ocjene sukladnosti (članak 41. ovog Zakona)

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

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

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

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

(2) Za prekršaj iz stavka 1. ovoga članka kaznit će se i odgovorna osoba prekršajno odgovornog važnog subjekta novčanom kaznom u iznosu od 500,00 do 3.000,00 eura.

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

**Članak 103.**

(1) Novčanom kaznom u iznosu od 2.000,00 eura do 20.000,00 eura kaznit će se za prekršaj:

- prekršajno odgovorni subjekti iz Priloga I. i Priloga II. ovog Zakona ako ne dostave ili ne dostave u roku podatke potrebne za provedbu kategorizacije subjekata odnosno vođenje popisa ključnih i važnih subjekata ili pravovremeno ne obavještavaju o promjenama podataka (članak 20. ovog Zakona)

- prekršajno odgovorni subjekti iz članka 22. ovog Zakona ako ne dostave ili ne dostave u roku podatke potrebne za vođenje posebnog registra subjekata ili pravovremeno ne obavještavaju o promjenama podataka (članak 23. ovog Zakona)

(2) Za prekršaj iz stavka 1. ovoga članka kaznit će se i odgovorna osoba subjekta iz stavka 1. ovog članka novčanom kaznom u iznosu od 200,00 do 1.000,00 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 je nadležni 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 je regulatorno tijelo za mrežne djelatnosti.

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

**DIO DESETI**

**PRIJELAZNE I ZAVRŠNE ODREDBE**

 **Članak 105.**

Operatori ključnih usluga i davatelji digitalnih usluga koji su do stupanja na snagu ovog Zakona provodili mjere za postizanje visoke razine kibernetičke sigurnosti prema odredbama Zakona o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga („Narodne novine“, broj: 64/2018) i Uredbe o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga („Narodne novine“, broj: 68/2018) nastavljaju s provedbom mjera na temelju tih propisa do dostave obavijesti o provedenoj kategorizaciji subjekta iz članka 19. stavaka 1. i 3. ovog Zakona.

**Članak 106.**

(1) Pružatelji javnih elektroničkih komunikacijskih mreža i pružatelji javno dostupnih elektroničkih komunikacijskih usluga koji su do stupanja na snagu ovog Zakona provodili sigurnosne zahtjeve u svrhu zaštite sigurnosti elektroničkih komunikacijskih mreža i elektroničkih komunikacijskih usluga prema odredbama članka 41. Zakona o elektroničkim komunikacijama („Narodne novine“, broj: 76/2022) nastavljaju s provedbom zahtjeva na temelju članka 41. tog Zakona do dostave obavijesti o provedenoj kategorizaciji subjekta iz članka 19. stavka 1. ovog Zakona.

(2) Pružatelji usluga povjerenja koji su do stupanja na snagu ovog 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“, broj: 62/2017) nastavljaju s provedbom zahtjeva na temelju tih propisa do dostave obavijesti o provedenoj kategorizaciji subjekta iz članka 19. stavka 1. ovog Zakona.

**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. godine ostaju na snazi do njihova isteka.

**Članak 108.**

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

**Članak 109.**

(1) Postupci započeti prema odredbama Zakona o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga („Narodne novine“, broj: 64/2018) dovršit će se prema odredbama tog Zakona i propisa donesenih na temelju toga Zakona.

(2) Postupci započeti prema odredbama članka 41. Zakona o elektroničkim komunikacijama („Narodne novine“, broj: 76/2022) dovršit će se prema odredbama tog Zakona i propisa donesenih na temelju toga Zakona.

**Članak 110.**

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

(2) Postupak kategorizacije subjekata i dostava obavijesti o provedenoj kategorizaciji subjekata provest će se u roku iz stavka 1. ovog članka za sve operatore ključnih usluga s popisa iz članka 12. Zakona o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga („Narodne novine“, broj: 64/2018).

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

**Članak 111.**

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

**Članak 112.**

Rokovi za provedbu ocjena sukladnosti iz članka 41. stavka 1. ovog Zakona i stručnog nadzora nad provedbom zahtjeva kibernetičke sigurnosti iz članka 75. stavka 1. ovog Zakona počinju teći prvog sljedećeg radnog dana nakon isteka roka iz članka 26. stavka 5. ovog Zakona.

**Članak 113.**

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

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

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

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

**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 ovog Zakona u roku od 30 dana od dana stupanja na snagu ovog Zakona.

(2) Predstojnik Ureda Vijeća za nacionalnu sigurnost uskladit će Pravilnik o unutarnjem redu Ureda Vijeća za nacionalnu sigurnost s Uredbom iz stavka 1. ovog 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 ovog Zakona u roku od 30 dana od dana stupanja na snagu ovog Zakona.

(4) Ravnatelj Sigurnosno-obavještajne agencije uskladit će Pravilnik o unutarnjem redu Sigurnosno-obavještajne agencije s Uredbom iz stavka 3. ovog 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 ovog Zakona u roku od 30 dana od dana stupanja na snagu ovog Zakona.

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

**Članak 115.**

Danom stupanja na snagu ovog Zakona prestaju važiti:

- Zakon o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga („Narodne novine“, broj: 64/2018)

- članak 17. stavak 2. podstavak 4. i članak 21. Zakona o informacijskoj sigurnosti („Narodne novine“, broj: 79/2007)

- članak 41. Zakona o elektroničkim komunikacijama („Narodne novine“, broj: 76/2022)

- Uredba o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga („Narodne novine“, broj: 68/2018)

- Odluka o osnivanju Nacionalnog vijeća za kibernetičku sigurnost i Operativno-tehničke koordinacije za kibernetičku sigurnost („Narodne novine“, broj: 61/2016, 28/2018, 110/2018, 79/2019 i 136/2020) i

- 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. godine.

**Članak 116.**

Ovaj Zakon stupa na snagu osmog dana od dana objave u „Narodnim novinama“.

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 uslugaPojam „*elektroenergetski subjekt*“ u smislu ovog 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 „o*pskrba električnom energijom*“ u smislu ovog 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 ovog 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 pojmovima iz članka 3. stavka 1. točaka 17., 77. i 78. Zakona o tržištu električne energije („Narodne novine“, broj: 111/2021), 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 sustavaPojam „*operator distribucijskog sustava*” u smislu ovog 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 pojmu iz članka 3. stavka 1. točke 71. Zakona o tržištu električne energije. |  |

 |
|

|  |  |
| --- | --- |
|  | - operatori prijenosnog sustavaPojam „*operator prijenosnog sustava*” u smislu ovog 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 pojmu iz članka 3. stavka 1. točke 72. Zakona o tržištu električne energije. |

 |
|

|  |  |
| --- | --- |
|  | - proizvođači električne energijePojam *„proizvođač električne energije”* u smislu ovog Zakona znači fizička ili pravna osoba koja proizvodi električnu energiju.Pojam *„proizvođač električne energije”* istovjetan je pojmu iz članka 3. stavka 1. točke 90. Zakona o tržištu električne energije. |

 |
|

|  |  |
| --- | --- |
|  | - 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 energijePojam „*agregiranje*” u smislu ovog 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 ovog 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 оd 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 ovog 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 pojmovima iz članka 3. stavka 1. točaka 4., 93. i 109. Zakona o tržištu električne energije. |

|  |  |
| --- | --- |
|  | - 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 ovog 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 pojmu iz članka 4. stavka 1. točke 4. Zakona o obnovljivim izvorima energije i visokoučinkovitoj kogeneraciji („Narodne novine“, broj: 138/2021), 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 ovog 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 pojmu iz članka 3. stavka 2. točke 5. Zakona o tržištu nafte i naftnih derivata („Narodne novine“, broj: 138/2021), 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 uslugePojam *„opskrbljivač plinom“* u smislu ovog Zakona znači energetski subjekt koji obavlja energetsku djelatnost opskrbe plinom.Pojam *„opskrbljivač plinom u obvezi javne usluge“* u smislu ovog Zakona znači opskrbljivač plinom koji obavlja energetsku djelatnost opskrbe u obvezi javne usluge.Pojam *„opskrba plinom“* u smislu ovog Zakonaznači prodaja ili preprodaja plina kupcu, uključujući prodaju ili preprodaju UPP-a i SPP-a.Pojam *„opskrba plinom u obvezi javne usluge“* u smislu ovog Zakonaznači 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 pojmovima iz članka 3. stavka 2. točaka 36., 37., 38. i 39. Zakona o tržištu plina („Narodne novine“, broj: 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 ovog 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 ovog 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 ovog Zakona znači sustav plinovoda i ostalih pripadajućih objekata i opreme koji su u vlasništvu 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 je pojmovima iz članka 3. stavka 2. točaka 5., 6. i 30. Zakona o tržištu plina. |

 |
|

|  |  |
| --- | --- |
|  | - operatori transportnog sustava Pojam *„operator transportnog sustava“* u smislu ovog 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 ovog 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 ovog 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 pojmovima iz članka 3. stavka 2. točaka 34., 58. i 59. Zakona o tržištu plina. |

 |
|

|  |  |
| --- | --- |
|  | - operatori sustava skladišta plina Pojam *„operator sustava skladišta plina“* u smislu ovog 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 ovog 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 pojmovima iz članka 3. stavka 2. točaka 54. i 56. Zakona o tržištu plina. |

 |
|

|  |  |
| --- | --- |
|  | - operatori terminala za UPP Pojam *„operator terminala za UPP“* u smislu ovog 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 ovog 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 pojmovima iz članka 3. stavka 2. točaka 33. i 57. Zakona o tržištu plina. |

 |
|

|  |  |
| --- | --- |
|  | - poduzeća za prirodni plin Pojam *„poduzeće za prirodni plin“* u smislu ovog Zakona, a u skladu sa zakonom koji 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. 300/2008Europskog 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. Uredbi (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 lukamaPojam *„upravno tijelo zračne luke“* u smislu ovog Zakona znači tijelo koje, pored drugih aktivnosti ili ne, ima prema nacionalnim propisima ili ugovorima za cilj rukovođenje i upravljanje infrastrukturom zračne luke, te koordinaciju i nadzor djelatnosti različitih operatora u dotičnoj zračnoj luci.Pojam *„zračna luka“* u smislu ovog 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 pojmovima iz članka 3. stavka 1. podstavaka 1. i 2. Pravilnika o naknadama zračnih luka („Narodne novine“, broj: 65/2015) 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 jedinstvenog europskog neba  |

 |
|

|  |  |
| --- | --- |
| (b) | željeznički promet |

 |

|  |  |
| --- | --- |
|  | - upravitelji infrastrukture Pojam *„upravitelj infrastrukture“* u smislu ovog 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 pojmu iz članka 5. stavka 1. točke 36. Zakona o željeznici („Narodne novine“, broj: 32/2019, 20/2021 i 114/2022), 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 objekataPojam *„željeznički prijevoznik“* u smislu ovog 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 ovog Zakona znači pravna osoba odgovorna za upravljanje jednim ili 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 (pružatelj usluga).Pojmovi *„željeznički prijevoznik“* i *„operator uslužnih objekata“* istovjetni su pojmovima iz članka 5. stavka 1. točaka 22. i 46. Zakona o željeznici. |

 |
|

|  |  |
| --- | --- |
| (c) | vodeni promet |

 |

|  |  |
| --- | --- |
|  | - kompanije za prijevoz putnika unutarnjim plovnim putovima, morem i duž obale kako su definirane za pomorski promet u Prilogu I. Uredbi (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 lukamaPojam *„luka“* u smislu ovog Zakona znači morsku luku, 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 pojmu iz članka 3. stavka 1. točke 1. Zakona o sigurnosnoj zaštiti pomorskih brodova i luka („Narodne novine“, broj: 32/2019, 108/2017 i 30/2021), 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“, broj: 181/2004, 76/2007, 146/2008, 61/2011, 56/2013, 26/2015 i 17/2019) 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 оd 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 ključni dio njihove opće djelatnostiPrema 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 ovog 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 pojmu iz članka 72. stavka 1. Zakona o cestama („Narodne novine“, broj: 84/2011, 22/2013, 54/2013, 148/2013, 92/2014, 110/2019, 144/21, 114/2022 i 04/2023), 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 ovog Zakona znači uređeno tržište, MTP ili OTP.Pojam *„multilateralna trgovinska platforma ili MTP“* u smislu ovog 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 instrumentima trećih tako da nastaje ugovor u skladu s odredbama dijela drugoga glave III. poglavlja VII. Zakona o tržištu kapitala („Narodne novine“, broj: 65/2018, 17/2020 i 83/2021).Pojam „*organizirana trgovinska platforma*ili OTP“ u smislu ovog 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.Pojmovi *„mjesta trgovanja“, „multilateralna trgovinska platforma ili MTP“* i „*organizirana trgovinska platforma*ili OTP“ istovjetni su pojmovima iz članka 3. stavka 1. točaka 61., 65. i 77. Zakona o tržištu kapitala, 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 ovog Zakona znači svaka fizička ili pravna osoba ili bilo koji subjekt koji obavlja zdravstvenu djelatnost u Republici Hrvatskoj u skladu sa zakonom koji uređuje zdravstvenu zaštitu.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 ovog 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 pojmu iz članka 3. stavka 1. točke 1. Zakona o lijekovima („Narodne novine“, broj: 76/2013, 90/2014 i 100/2018), 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“, broj: 58/07) |

|  |  |
| --- | --- |
|  | - 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 ključni dio njihove općenite djelatnosti distribucije druge robe i proizvodaPojam *„voda namijenjena za ljudsku potrošnju“* u smislu ovog Zakona znači: - sva voda, bilo u njezinu izvornom stanju ili nakon obrade, koja je namijenjena za piće, kuhanje, pripremu hrane ili druge potrebe domaćinstva 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 pojmu iz članka 3. stavka 1. točke 1. Zakona o vodi za ljudsku potrošnju („Narodne novine“, broj: 30/2023), 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 ključni dio njihove općenite djelatnostiPojam *„komunalne otpadne vode“* u smislu ovog 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 ovog 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 ovog 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 pojmovima iz članka 4. stavka 1. točaka 25., 34. i 81. Zakona o vodama („Narodne novine“, broj: 66/2019, 84/2021 i 47/2023), 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 koji uređuje državnu informacijsku infrastrukturu  |

 |
|

|  |  |
| --- | --- |
|  | - 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 uslugaPojam „*davatelj poštanskih usluga*“ u smislu ovog 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 ovog 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 ovog 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 pojmovima iz članka 2. stavka 1. točkama 4., 5., 21. i 32. Zakona o poštanskim uslugama ("Narodne novine", broj 144/2012, 153/2013, 78/2015, 110/2019), 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 djelatnostPojam „*gospodarenje otpadom*“ u smislu ovog Zakona znači djelatnosti sakupljanja, prijevoza, oporabe uključujući razvrstavanje i zbrinjavanja 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 ovog Zakona znači svaka tvar ili predmet koje posjednik odbacuje, namjerava ili mora odbaciti.Pojam „*djelatnost sakupljanja otpada“* u smislu ovog Zakona znači djelatnost koja uključuje postupak sakupljanja otpada i postupak sakupljanja otpada u reciklažno dvorište.Pojam „*djelatnost prijevoza otpada“* u smislu ovog Zakona znači prijevoz otpada za vlastite potrebe ili za potrebe drugih na teritoriju Republike Hrvatske.Pojam „*djelatnost oporabe otpada“* u smislu ovog Zakona znači djelatnost koja uključuje obavljanje postupka oporabe iz Popisa postupaka oporabe otpada.Pojam „*tehnološki procesi gospodarenja otpadom“* u smislu ovog 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 ovog Zakona znači djelatnost koja uključuje obavljanje postupka zbrinjavanja otpada iz Popisa postupaka zbrinjavanja otpada.Pojam „*trgovac otpadom“* u smislu ovog 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 ovog 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 sakupljanja otpada“,* „*djelatnost prijevoza otpada“,* „*djelatnost oporabe otpada“,* „*tehnološki procesi gospodarenja otpadom“,* „*djelatnost zbrinjavanja otpada“,* „*trgovac otpadom“ i* „*posrednik“* istovjetni su pojmovima iz članka 4. stavka 1. točaka 15., 48., 11., 10., 8., 82., 13., 84. i 60. Zakona o gospodarenju otpadom ("Narodne novine", broj 84/2021), 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. Uredbi (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 ovog Zakona.Prilog I. točka 5. peta alineja ovog 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.  |
|

|  |  |
| --- | --- |
| (c) |  proizvodnja električne opreme |

 |  - subjekti koji obavljaju bilo koju od gospodarskih djelatnosti iz područja C odjeljka 27. Nacionalne klasifikacije djelatnosti 2007. – NKD 2007.  |
|

|  |  |
| --- | --- |
| (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. |
|

|  |  |
| --- | --- |
| (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.  |
|

|  |  |
| --- | --- |
| (f) |  proizvodnja ostalih prijevoznih sredstava  |

 |  - subjekti koji obavljaju bilo koju od gospodarskih djelatnosti iz područja C odjeljka 30. Nacionalne klasifikacije djelatnosti 2007. – NKD 2007.  |
|

|  |  |
| --- | --- |
| 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 | Svi | Središnje državno tijelo za kibernetičku sigurnost | - | Nacionalni centar za kibernetičku sigurnost |
| Vodeni |
| Cestovni |
| 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 elektronič-kih komunika-cijskih mreža | Hrvatska regulatorna agencija za mrežne djelatnosti | - | Nacionalni centar za kibernetičku sigurnost |
| Pružatelji javno dostupnih elektronič-kih komunika-cijskih usluga |
| 11. | Digitalna infrastruktura | - | Pružatelji središta za razmjenu internet-skog prometa | Središnje državno tijelo za kibernetičku sigurnost | - | Nacionalni centar za kibernetičku sigurnost |
| Pružatelji usluga DNS-a, osim operatora korijenskih poslužitelja naziva |
| Pružatelji usluga računalstva u oblaku |
| Pružatelji usluga podatkov-nog centra |
| Pružatelji mreže za isporuku sadržaja |
| 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 dijagnostič-kih 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. ovog Zakona utvrđuju se:

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

- upravljački okvir za postizanje ciljeva i prioriteta iz podstavka 1. ovog stavka, za razvoj i provedbu politika iz točke II. ovog 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 pojašnjenjima uloga i odgovornosti svih tijela relevantnih za provedbu politika kibernetičke sigurnosti na nacionalnoj razini

- okviri politika za bolju koordinaciju između nadležnih tijela iz ovog 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. ovog 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. ovog 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 u cilju poticanja i osiguranja dobrovoljne razmjene informacija o kibernetičkoj sigurnosti u skladu s propisima koji 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.

**O B R A Z L O Ž E N J E**

**Uz članak 1.**

Ovim se člankom utvrđuju cilj i predmet Zakona. Predmet ovog Zakona je područje kibernetičke sigurnosti i njime se uređuju postupci i mjere za postizanje visoke zajedničke razine kibernetičke sigurnosti i to kriteriji za kategorizaciju ključnih i važnih subjekata, zahtjevi kibernetičke sigurnosti za ključne i važne subjekte, 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 ovog Zakona i druga pitanja od značaja za područje kibernetičke sigurnosti. Također, ovim se Zakonom uspostavlja okvir strateškog planiranja i odlučivanja u području kibernetičke sigurnosti te utvrđuju nacionalni okviri upravljanja kibernetičkim krizama. Dodatno, ovim se člankom propisuje da su 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 značaja za Republiku Hrvatsku. Također, ovim se člankom utvrđuje da je cilj je ovog 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.

**Uz članak 2.**

Ovim se člankom utvrđuju prilozi koji čine sastavni dio Zakona i to Prilog I. pod nazivom Sektori visoke kritičnosti i Prilog II. pod nazivom Drugi kritični sektori. Prilog I. i Prilog II. sadržavaju popis sektora, podsektora i vrste subjekata na koje se odnose zahtjevi kibernetičke sigurnosti propisani ovim Zakonom i za koje se provodi kategorizacija ključnih i važnih subjekata Također, ovim člankom se utvrđuje da je sastavni dio ovog Zakona Prilog III. pod nazivom Popis nadležnosti u području kibernetičke sigurnosti. Prilog III. sadržava popis nadležnih tijela i podjele nadležnosti između tih tijela za sektore, podsektore i subjekte iz Priloga I. i II. ovog Zakona. Popisivanje sektora, podsektora i subjekata na koje se odnose zahtjevi kibernetičke sigurnosti, a slijedno i popis i podjela nadležnosti za provođenje kategorizacije ključnih i važnih subjekata i praćenje provedbe zahtjeva kibernetičke sigurnosti, sadržano je u Prilozima Zakona zbog brojnosti subjekata odnosno sektora i podsektora na koje se Zakon odnosi, a sve u cilju postizanja bolje preglednosti i jasnoće propisa. Također, isti pristup u definiranju područja primjene propisa primijenjen je i u Direktivi (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.) (u daljnjem tekstu: Direktiva (EU) 2022/2555), koja se preuzima ovim Zakonom u nacionalno zakonodavstvo. Tako se Prilozima I. i II. ovog Zakona preuzimaju Prilozi I. i II. Direktive (EU) 2022/2555. Dodatno, ovim člankom se utvrđuje kako je sastavni dio Zakona i Prilog IV. pod nazivom Obvezni sadržaj nacionalnog akta strateškog planiranja iz područja kibernetičke sigurnosti, a kojim se utvrđuje sadržaj nacionalnog akta strateškog planiranja iz područja kibernetičke sigurnosti i koji je usklađen s NIS2 zahtjevima za sve države članice.

**Uz članak 3.**

Ovim se člankom preuzima Direktiva (EU) 2022/2555.

**Uz članak 4.**

Ovim se člankom određuju značenja pojmova uporabljenih u tekstu ovog Zakona, koji su usklađeni s pojmovljem iz mjerodavne pravne stečevine Europske unije, određuju se pojmovi koji imaju značenje utvrđeno posebnim propisima te se utvrđuje rodna ravnopravnost pojmova i izraza iz ovog Zakona.

**Uz članak 5.**

Ovim se člankom uređuje odnos ovog Zakona prema posebnim propisima o zaštiti tajnosti i povjerljivosti podataka, odnosno utvrđuje se da ako u provedbi ovog Zakona nastaju ili se koriste klasificirani podaci ili drugi podaci za koje su posebnim propisima utvrđena pravila postupanja s takvim podacima radi zaštite njihove tajnosti ili povjerljivosti, na takve podatke primjenjuju se posebni propisi o njihovoj zaštiti. Također, ovim člankom određeno je da se ovaj Zakon ne primjenjuje na informacijske sustave sigurnosno akreditirane za postupanje s klasificiranim podacima.

**Uz članak 6.**

Ovim se člankom preuzima članak 2. stavak 14. podstavak 2. Direktive (EU) 2022/2555 te se njime utvrđuje kako odredbe ovog Zakona ne utječu na obveze pružatelja javnih elektroničkih komunikacijskih mreža ili pružatelje javno dostupnih elektroničkih komunikacijskih usluga obrađivati osobne podatke sukladno propisima o zaštiti osobnih podataka i propisima o zaštiti privatnosti. U pitanju su 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.) te odredbe Zakona o elektroničkim komunikacijama („Narodne novine“, broj: 76/22) kojim je u nacionalno zakonodavstvo preuzeta Direktiva 2002/58/EZ Europskog parlamenta i Vijeća od 12. srpnja 2002. o obradi osobnih podataka i zaštiti privatnosti u području elektroničkih komunikacija (Direktiva o privatnosti i elektroničkim komunikacijama) (SL L 201, 31. 7. 2002.). Nadalje, ovim se člankom utvrđuje da primjena odredaba ovog 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. Člankom 33. Uredbe (EU) 2016/679 propisan je rok za izvješćivanje nadzornog tijela o povredi osobnih podataka i minimalan sadržaj koje izvješće mora sadržavati. Člankom 34. Uredbe (EU) 2016/679 propisano je u kojem slučaju postoji obveza obavješćivanja ispitanika o povredi osobnih podataka i kako se ona provodi te utvrđuje i slučajeve kada obavješćivanje ispitanika nije obvezno.

**Uz članak 7.**

Ovim se člankom uređuje odnos ovog Zakona prema zakonu koji uređuje područje elektroničkih komunikacija. Primjena odredaba ovog Zakona ne utječe na obvezu provedbe temeljnih zahtjevaza elektroničku komunikacijsku infrastrukturu i drugu povezanu opremu te na pravila upravljanja vršnom nacionalnom internetskom domenom i prava i obveze korisnika domena propisanih zakonom kojim je uređeno područje elektroničkih komunikacija.

**Uz članak 8.**

Ovim se člankom uređuje odnos ovog Zakona prema posebnim zakonima u pitanjima kibernetičke sigurnosti. S obzirom na brojnost subjekata iz različitih sektora obuhvaćenih ovim Zakonom, a koji subjekti se nalaze u Prilogu I. i Prilogu II. ovog Zakona, te s obzirom na različitost posebnih propisa koji se primjenjuju na te sektore, ovim se člankom uređuje odnos zahtjeva kibernetičke sigurnosti iz posebnih sektorskih propisa sa zahtjevima kibernetičke sigurnosti iz ovog Zakona. Primjenjuju se posebni propisi koji te zahtjeve uređuju jednako ili strože od zahtjeva utvrđenih ovim Zakonom. Člankom se uređuje i koje minimalne uvjete moraju ostvariti zahtjevi kibernetičke sigurnosti po posebnim sektorskim propisima da bi odgovarali zahtjevima kibernetičke sigurnosti iz ovog Zakona, posebno kod provedbe mjera upravljanja kibernetičkim sigurnosnim rizicima te obvezama obavještavanja o značajnim incidentima. Tijela koja su prema posebnim zakonima iz stavka 1. ovog članka nadležna za sektor odnosno podsektor i/ili vrste subjekata iz Priloga I. i Priloga II. ovog Zakona i nadležna tijela za provedbu zahtjeva kibernetičke sigurnosti dužna su međusobno surađivati i razmjenjivati relevantne informacije te voditi računa o smjernicama Europske komisije kojima se pojašnjava primjena povezanog mjerodavnog prava Europske unije.

**Uz članak 9.**

Ovim se člankom uređuju opći kriteriji za provedbu kategorizacije ključnih subjekata, u skladu s odredbama članka 2. i članka 3. te Priloga I. Direktive (EU) 2022/2555. Dodatno, ovim se člankom utvrđuje kako se u kategoriju ključnih subjekata razvrstavaju i informacijski posrednici u razmjeni elektroničkog računa među poduzetnicima, neovisno o njihovoj veličini, kako bi se osigurala visoka razina kibernetičke sigurnosti u pružanju usluga koje pružaju ti subjekti. Budući da su u pitanju informacijski posrednici koji će svoje usluge pružati u domeni B2B (Business to Business), ova vrsta subjekata uključena je u Prilog I. ovog Zakona, točku 9., sektor Upravljane usluge IKT-a (B2B).

 **Uz članak 10.**

Ovim se člankom uređuju opći kriteriji za provedbu kategorizacije važnih subjekata, u skladu s odredbom članka 3. i Priloga II. Direktive (EU) 2022/2555.

**Uz članak 11.**

Ovim se člankom uređuju posebni kriteriji za provedbu kategorizacije ključnih i važnih subjekata, u skladu s odredbom članka 2. Direktive (EU) 2022/2555.

**Uz članak 12.**

Ovim se člankom uređuju kriteriji za provedbu kategorizacije ključnih i važnih subjekata javnog sektora, u skladu s odredbom članka 2. Direktive (EU) 2022/2555.

**Uz članak 13.**

Ovim se člankom uređuju kriteriji za provedbu kategorizacije važnih subjekata sustava obrazovanja, u skladu s odredbom članka 2. Direktive (EU) 2022/2555.

**Uz članak 14.**

Ovim se člankom uređuje način određivanja nadležnosti temeljem teritorijalnosti, u skladu s odredbom članka 26. Direktive (EU) 2022/2555.

**Uz članak 15.**

Ovim se člankom uređuje primjena kriterija veličine subjekta kojima se utvrđuje predstavlja li subjekt srednji subjekt malog gospodarstva odnosno premašuje li gornje granice za srednji subjekt malog gospodarstva na temelju zakona kojim se uređuju osnove za primjenu poticajnih mjera gospodarske politike usmjerenih razvoju, restrukturiranju i tržišnom prilagođavanju maloga gospodarstva, a vodeći računa o smjernicama Europske komisije o provedbi kriterija veličine koji se primjenjuju na mikropoduzeća i mala poduzeća. Koji subjekti predstavljaju srednje subjekte malog gospodarstva u Republici Hrvatskoj trenutno je regulirano Zakonom o poticanju razvoja malog gospodarstva („Narodne novine“, broj: 29/02, 63/07, 53/12, 56/13 i 121/16).

**Uz članak 16.**

Ovim se člankom propisuje da se na subjekt razvrstan u kategoriju i ključnih i važnih subjekata primjenjuju odredbe ovog Zakona koje se odnose na ključne subjekte.

**Uz članak 17.**

Ovim se člankom propisuje obveza vođenja popisa ključnih i važnih subjekata, obveznici istog te redovita obveza provjeravanja i ažuriranja navedenog popisa, u skladu s člankom 3. Direktive (EU) 2022/2555.

**Uz članak 18.**

Ovim se člankom propisuje obveza jedinstvene kontaktne točke da svake dvije godine, dostavlja Europskoj komisiji i Skupini za suradnju podatke o broju ključnih i važnih subjekata razvrstanih temeljem kriterija iz ovog Zakona te da dodatno, na zahtjev Europske komisije, može dostaviti i podatke o nazivima tih subjekata. Također, ovim se člankom propisuje obveza nadležnih tijela za provedbu zahtjeva kibernetičke sigurnosti i nadležnih tijela za provedbu posebnih zakona da jedinstvenoj kontaktnoj točki dostavljaju podatke potrebne za dostavu podataka o broju ključnih i važnih subjekata Europskoj komisiji i Skupini za suradnju.

**Uz članak 19.**

Ovim se člankom propisuje obveza i rok nadležnih tijela za provedbu zahtjeva kibernetičke sigurnosti da sve subjekte s popisa ključnih i važnih subjekata obavijeste o provedenoj kategorizaciji subjekta i njihovim obvezama temeljem ovog Zakona i provedbenog propisa o zahtjevima kibernetičke sigurnosti (uredba iz članka 24. ovog Zakona). Dodatno, ovim se člankom propisuje obveza i rok nadležnih tijela za provedbu zahtjeva kibernetičke sigurnosti da subjekte u odnosu na koje je nakon ažuriranja popisa ključnih i važnih subjekata došlo do promjene u kategorizaciji subjekta odnosno koji se nakon ažuriranja navedenog popisa više ne smatraju ni ključnim ni važnim subjektima, obavijeste o toj činjenici te činjenici da se time mijenjaju i njihove obveze kojima podliježu temeljem ovog Zakona i provedbenog propisa o zahtjevima kibernetičke sigurnosti (uredba iz članka 24. ovog Zakona) odnosno da više ne podliježu obvezama provedbe zahtjeva kibernetičke sigurnosti iz ovog Zakona.

**Uz članak 20.**

Ovim se člankom propisuje obveza i rok u kojem su subjekti iz Priloga I. i Priloga II. ovog Zakona dužni nadležnim tijelima za provedbu zahtjeva kibernetičke sigurnosti i nadležnim tijelima za provedbu posebnih zakona dostaviti taksativno navedene podatke za potrebe kategorizacije subjekata te vođenja popisa ključnih i važnih subjekata kao i obveza i rok u kojem su ih dužni obavijestiti o svim promjenama tih podataka, sve u skladu s člankom 3. Direktive (EU) 2022/2555.

**Uz članak 21.**

Ovim se člankom utvrđuje obveza i rok tijelima državne uprave, drugim državnim tijelima, jedinicama lokalne i područne (regionalne) samouprave, pravnim osobama s javnim ovlastima i javnim subjektima koji u okviru svog djelokruga rada prikupljaju podatke odnosno vode registre, evidencije i zbirke podataka o subjektima iz Priloga I. i Priloga II. ovog Zakona da nadležnim tijelima za provedbu zahtjeva kibernetičke sigurnosti redovito dostavljaju popise subjekata iz Priloga I. i Priloga II. ovog Zakona odnosno omoguće pristup odgovarajućim podacima u registrima, evidencijama i zbirkama podataka elektroničkim putem te da na zahtjev nadležnog tijela za provedbu zahtjeva kibernetičke sigurnosti, za iste subjekte, dostavljaju taksativno navedene podatke.

**Uz članak 22.**

Ovim se člankom propisuje obveza središnjeg državnog tijela za kibernetičku sigurnost da uspostavlja i vodi poseban registar taksativno navedenih subjekata. Također, propisano je da se predmetni registar vodi neovisno o obvezi vođenja popisa ključnih i važnih subjekata.

**Uz članak 23.**

Ovim se člankom propisuje obveza i rok subjektima iz članka 22. ovog Zakona da središnjem državnom tijelu za kibernetičku sigurnost dostave taksativno navedene podatke te obveza i rok u kojem su navedeni subjekti dužni obavijestiti središnje državno tijelo za kibernetičku sigurnost o svim promjenama podataka koje su dostavili. Također, ovim je člankom propisano da se dostavljeni podaci, osim podatka o IP adresnom rasponu subjekta, dostavljaju Europskoj agenciji za kibernetičku sigurnost (u daljnjem tekstu: ENISA), putem jedinstvene kontaktne točke.

**Uz članak 24.**

Ovim se člankom propisuje donošenje uredbe Vlade Republike Hrvatske (u daljnjem tekstu: Vlada) kao provedbenog propisa o kategorizaciji subjekata, vođenju popisa ključnih i važnih subjekata i posebnog registra subjekata.

**Uz članak 25.**

Ovim se člankom definira opseg zahtjeva kibernetičke sigurnosti, koji obuhvaćaju postupke i mjere koje su ključni i važni subjekti dužni primjenjivati u cilju 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. 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. ovog Zakona.

**Uz članak 26.**

Ovim se člankom propisuje dužnost ključnih i važnih subjekta da provode odgovarajuće i razmjerne mjere upravljanja kibernetičkim sigurnosnim rizicima, cilj primjene tih mjera te što mjere obuhvaćaju. Također, propisano je da su ključni i važni subjekti dužni provoditi navedene mjere bez obzira na to upravljaju li i/ili održavaju svoje mrežne i informacijske sustave sami ili za to koriste vanjskog davatelja usluge. Ovim se člankom propisuju i rokovi u kojima se ključni i važni subjekti dužni provesti mjere upravljanja kibernetičkim sigurnosnim rizicima.

**Uz članak 27.**

Ovim se člankom propisuje dužnost ključnih i važnih subjekta da primjenom mjera upravljanja kibernetičkim sigurnosnim rizicima osiguraju razinu sigurnosti mrežnih i informacijskih sustava proporcionalnu utvrđenom riziku. Pri procjeni proporcionalnosti primijenjenih mjera upravljanja kibernetičkim sigurnosnim rizicima u obzir se uzimaju stupanj izloženosti subjekata rizicima, veličina subjekta i vjerojatnost pojave incidenata i njihova ozbiljnost, uključujući njihov mogući društveni i gospodarski učinak.

**Uz članak 28.**

Ovim se člankom propisuje način provedbe mjera upravljanja kibernetičkim sigurnosnim rizicima te obveza korištenja 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 i uredbom iz članka 24. ovog Zakona, a sve u skladu s člankom 24. Direktive (EU) 2022/2555.

**Uz članak 29.**

Ovim se člankom utvrđuju osobe odgovorne za upravljanje mjerama i njihova odgovornost za provedbu i kontrolu provedbe mjera upravljanja kibernetičkim sigurnosnim rizicima. Uz osobe odgovorne za upravljanje mjerama, navedeni članak odnosi 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, sudjeluju u donošenju odluka o mjerama upravljanja kibernetičkim sigurnosnim rizicima i/ili njihovoj provedbi. 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 te zaposlenicima subjekta omogućiti pohađanje odgovarajućih osposobljavanja. Odredbama ovog članka prenosi se članak 20. Direktive (EU) 2022/2555.

**Uz članak 30.**

Ovim se člankom utvrđuju mjere upravljanja kibernetičkim sigurnosnim rizicima odnosno sigurnosne politike u funkciji mjera upravljanja kibernetičkim sigurnosnim rizicima. Te mjere se temelje na pristupu kojim se uzimaju u obzir sve opasnosti i čiji je cilj zaštita mrežnih i informacijskih sustava i fizičkog okruženja tih sustava od incidenata. Pri procjeni proporcionalnosti primijenjene mjere koja se odnosi na sigurnost lanca opskrbe, 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. Odredbama ovog članka prenosi se članak 21. Direktive (EU) 2022/2555 te će se iste dodatno razraditi uredbom iz članka 24. ovog Zakona.

**Uz članak 31.**

Ovim se člankom propisuje dužnost ključnih i važnih subjekata obavijestiti nadležni CSIRT o svakom značajnom incidentu te se definira značajni incident. Također, propisana je obveza ključnih i važnih subjekata da obavijesti o značajnom incidentu dostavljaju tijelima kaznenog progona ukoliko postoje osnove sumnje da su ti značajni incidenti nastali počinjenjem kaznenog djela, temeljem odredbi zakona kojim se propisuju pravila kaznenog postupka. Ovim se člankom propisuju rokovi u kojima se ključni i važni subjekti dužni započeti s provedbom obveze dostave obavijesti o značajnim incidentima. Odredbama ovog članka prenosi se članak 23. Direktive (EU) 2022/2555 te će se iste dodatno razraditi uredbom iz članka 24. ovog Zakona.

**Uz članak 32.**

Ovim se člankom propisuje dužnost ključnih i važnih subjekata da obavijestiti primatelje svojih usluga o značajnim incidentima koji bi mogli negativno utjecati na pružanje usluga te o svim mjerama zaštite ili pravnim sredstvima koje primatelji usluga mogu uporabiti u slučaju pojave ozbiljne kibernetičke prijetnje koja bi mogla na njih utjecati. Ovim se člankom propisuju rokovi u kojima se ključni i važni subjekti dužni započeti s provedbom obveze obavještavanja primatelja svojih usluga. Odredbama ovog članka prenosi se članak 23. Direktive (EU) 2022/2555 te će se iste dodatno razraditi uredbom iz članka 24. ovog Zakona.

**Uz članak 33.**

Ovim se člankom uređuje mogućnost ključnih i važnih subjekata da dobrovoljno obavještavaju

nadležni CSIRT o svakom incidentu, kibernetičkoj prijetnji i izbjegnutom incidentu. Odredba ovog članka u skladu je s člancima 23. i 30. Direktive (EU) 2022/2555 te će se ista dodatno razraditi uredbom iz članka 24. ovog Zakona.

**Uz članak 34.**

Ovim se člankom propisuje dužnost jedinstvene kontaktne točke da, na zahtjev nadležnog CSIRT-a i prema vlastitoj procjeni, obavještava o značajnom incidentu s prekograničnim učinkom jedinstvene kontaktne točke pogođene države članice i ENISA-u, osobito ako se incident odnosi na dvije države članice ili više njih. Također, ovim se člankom propisuje dužnost jedinstvene kontaktne točke da, na zahtjev nadležnog CSIRT-a i prema vlastitoj procjeni, o značajnom incidentu s međusektorskim učinkom obavještava tijela državne uprave nadležna za pogođene sektore. Odredba ovog članka će se dodatno razraditi uredbom iz članka 24. ovog Zakona.

**Uz članak 35.**

Ovim se člankom propisuje tko, kada i pod uvjetima obavještava javnost o značajnom incidentu koji je u tijeku. Odredba ovog članka u skladu je s člankom 23. Direktive (EU) 2022/2555 te će se ista dodatno razraditi uredbom iz članka 24. ovog Zakona.

**Uz članak 36.**

Ovim se člankom propisuje dužnost nadležnih CSIRT-ova obavijestiti jedinstvenu kontaktnu točku o značajnim incidentima, ostalim incidentima, ozbiljnim kibernetičkim prijetnjama i izbjegnutim incidentima o kojima su ga ključni i važni subjekti obavijestili sukladno smjernicama jedinstvene kontaktne točke. 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. Odredba ovog članka u skladu je s člankom 23. Direktive (EU) 2022/2555 te će se ista dodatno razraditi uredbom iz članka 24. ovog Zakona.

**Uz članak 37.**

Ovim se člankom utvrđuje nacionalna platforma za prikupljanje, analizu i razmjenu podataka o kibernetičkim prijetnjama i incidentima, kao jedinstvena ulazna točka za obavještavanje o kibernetičkim prijetnjama i incidentima. Razvoj i upravljanje nacionalnom platformom iz ovog članka Zakona u nadležnosti je Hrvatske akademske i istraživačke mreže - CARNET (u daljnjem tekstu: CARNET), a bazira se na CARNET-ovoj PiXi platformi za prikupljanje, analizu i razmjenu podataka o računalno-sigurnosnim prijetnjama i incidentima kao jedinstvenom mjestu za prijavu računalno-sigurnosnih incidenata.

**Uz članak 38.**

Ovim se člankom utvrđuje da će se mjere upravljanja kibernetičkim sigurnosnim rizicima, način njihove provedbe, kriteriji za utvrđivanje značajnih incidenata, uključujući kriterijske pragove ako su potrebni zbog specifičnosti pojedinog sektora, vrste i sadržaj obavijesti, rokovi za dostavu obavijesti o kibernetičkim prijetnjama i incidentima, prava pristupa i druga pitanja bitna za korištenje nacionalne platforme za prikupljanje, analizu i razmjenu podataka o kibernetičkim prijetnjama i incidentima, mogućnosti korištenja drugih načina dostave obavijesti, postupanja s tim obavijestima, uključujući postupanja nadležnog CSIRT-a u povodu zaprimljenih obavijesti, propisati i dodatno razraditi uredbom iz članka 24. Zakona.

**Uz članak 39.**

Ovim se člankom propisuje dužnost ključnih i važnih subjekata da provode provjeru usklađenosti sa zahtjevima kibernetičke sigurnosti. Navedena provjera usklađenosti obavlja se u postupku ocjene sukladnosti ključnih i važnih subjekata te postupku samoocjene sukladnosti važnih subjekta.

**Uz članak 40.**

Ovim se člankom određuju tijela za ocjenu sukladnosti. Tijela za ocjenu sukladnosti su privatni subjekti koji ispunjavaju organizacijske i stručne zahtjeve za autorizaciju propisane uredbom iz članka 24. ovog Zakona, uz iznimku za tijela državne uprave i druga državna tijela za koja je tijelo za ocjenu sukladnosti središnje državno tijelo za obavljanje poslova u tehničkim područjima informacijske sigurnosti. Dodatno, propisano je da autorizaciju navedenih privatnih subjekata, koji ispunjavaju organizacijske i stručne zahtjeve za autorizaciju propisane uredbom iz članka 24. ovog Zakona, provodi središnje državno tijelo za obavljanje poslova u tehničkim područjima informacijske sigurnosti, a izdaje se na rok od pet godina. Isto tijelo tijekom važenja autorizacije provodi periodične provjere organizacijskih i stručnih zahtjeva.

**Uz članak 41.**

Ovim se člankom uređuje način i rokovi provedbe ocjene sukladnosti ključnih i važnih subjekata te se propisuje obveza tijela za ocjenu sukladnosti da sastavi izvješće o provedenoj ocjeni sukladnosti, a koje izvješće ključni i važni subjekti dostavljaju nadležnom tijelu za provedbu zahtjeva kibernetičke sigurnosti u propisanim rokovima. Troškove provedbe ocjene sukladnosti snose ključni i važni subjekti, ako nije drugačije propisano ovim Zakonom.

**Uz članak 42.**

Ovim se člankom uređuje način i rokovi provedbe samoocjena sukladnosti važnih subjekata. Ako rezultati provedene samoocjene sukladnosti pokazuju da je subjekt usklađen sa zahtjevima kibernetičke sigurnosti propisanim ovim Zakonom, važni subjekti sastavljaju izjavu o sukladnosti koja sadrži elemente obuhvaćene samoocjenom sukladnosti, a koju izjavu dostavljaju nadležnom tijelu za provedbu zahtjeva kibernetičke sigurnosti u propisanom roku. Troškove provedbe samoocjene sukladnosti snose važni subjekti.

**Uz članak 43.**

Ovim se člankom utvrđuje obveza vođenja i javne objave registra autoriziranih tijela za ocjenu sukladnosti.

**Uz članak 44.**

Ovim se člankom utvrđuje da će se pravila, tehnički zahtjevi, norme, obrasci i postupci koji se primjenjuju prilikom obavljanja ocjena i samoocjena sukladnosti te organizacijski i stručni zahtjevi za autorizaciju tijela za ocjenu sukladnosti detaljnije urediti uredbom iz članka 24. ovog Zakona.

**Uz članak 45.**

Ovim se člankom propisuje obveza registra naziva vršne nacionalne internetske domene i registrara da provode posebne zahtjeve za upravljanje podacima o registraciji naziva domena, u svrhu osiguranja pouzdanog, otpornog i sigurnog sustava naziva domena.

**Uz članak 46.**

Ovim se člankom propisuje obveza registra naziva vršne nacionalne internetske domene i registrara da osiguravaju da baza podataka o registraciji naziva domena sadrži informacije potrebne za identifikaciju korisnika domene i registrara koji upravljaju nazivima domena te za kontakt s njima, a osobito taksativno navedene informacije. Također, ovim člankom propisana je obveza registra naziva vršne nacionalne internetske domene i registrara 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. Nepostupanje podnositelja zahtjeva za registracijom domene i korisnika domene sukladno obvezama propisanim ovim Zakonom predstavlja temelj za uskratu registracije domene odnosno brisanje domene. Odredbama ovog članka prenosi se članak 28. Direktive (EU) 2022/2555.

**Uz članak 47.**

Ovim se člankom propisuje obveza registra naziva vršne nacionalne internetske domene i registrara da odbiju svaki zahtjev za registracijom domene koji ne sadrži sve podatke iz članka 46. stavka 1. podstavaka 1. do 3. ovog Zakona, te da podnositelja zahtjeva obavijeste o uskraćivanju registracije domene odnosno privremenoj deaktivaciji domene i nemogućnosti njezinog korištenja sve dok zahtjev ne bude uredno podnesen i to u roku od osam dana od primitka takve obavijesti. Dodatno, propisana je obveza registra naziva vršne nacionalne internetske domene i registrara da periodički, a najmanje jednom godišnje, za sve svoje korisnike domena provode provjere postojanja korisnika domene, kao i usklađenost postupanja korisnika domene sukladno obvezama utvrđenim propisom kojim je uređeno ustrojstvo i upravljanje vršnom nacionalnom internetskom domenom. U slučaju nedostupnosti korisnika domene u okviru navedenih višekratnih provjera na različite registrirane kontakt podatke korisnika domene odnosno zlouporabe prava ili drugog nepropisnog postupanja korisnika domene, registar naziva vršne nacionalne internetske domene i registrari dužni su takvu domenu brisati. Također, propisana je obveza registra naziva vršne nacionalne internetske domene i registrara da uspostave i javno objave politike upravljanja navedenom bazom podataka kao i obveza da nakon registracije naziva domene bez odgode javno objavljuju podatke o registraciji naziva domena koji nisu osobni podaci.

**Uz članak 48.**

Ovim se člankom propisuje obveza registra naziva vršne nacionalne internetske domene i registrara da podatke, informacije i dokumentaciju prikupljenu temeljem članaka 46. i 47. ovog Zakona čuvati 25 godina od prestanka prava korisnika na korištenje domene, što ta dokumentacija mora sadržavati, kao i njihova obveza da 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, dostave ili na drugi odgovarajući način omoguće pristup podacima o korisniku domene te da takvu obvezu postupanja naznače u svojim politikama upravljanja. Također, ovim člankom propisana je obveza registra naziva vršne nacionalne internetske domene i registrara da nakon isteka propisanog roka čuvanja, osobne podatke o korisniku domene brišu, a dokumentaciju unište sukladno propisima o zaštiti osobnih podataka. Tehničke i organizacijske mjere za zaštitu osobnih podataka o korisnicima domena uredit će se posebnim propisima koji uređuju ustrojstvo i upravljanje vršnom nacionalnom internetskom domenom. Vezano uz rok čuvanja za podatke, informacije i dokumentaciju prikupljenu temeljem članaka 46. i 47. ovog Zakona, napominje se kako je isti određen prema najdužem zastarnom roku za pokretanje kaznenog postupka za potrebe kojeg ti podaci, informacije i dokumentacija može biti prikupljanja (kazneno djelo terorizma iz članka 97. stavka 1. podstavka 10. Kaznenog zakona Republike Hrvatske, „Narodne novine“, broj: 125/11, 144/12, 56/15, 61/15, 101/17, 118/18, 126/19, 84/21 i 114/22).

**Uz članak 49.**

Ovim se člankom propisuje da kontrolu usklađenosti postupanja registra naziva vršne nacionalne internetske domene i registrara provodi tijelo državne uprave nadležno za znanost i obrazovanje.

**Uz članak 50.**

Ovim se člankom uređuje mogućnost samoocjene sukladnosti s mjerama upravljanja kibernetičkim sigurnosnim rizicima i dobrovoljnog obavještavanja nadležnog CSIRT-a o značajnom incidentu, ostalim incidentima, kibernetičkim prijetnjama ili izbjegnutim incidentima u slučajevima kada subjekt nije kategoriziran kao ključni i važni subjekt sukladno ovom Zakonu. Mogućnost provedbe samoocjena sukladnosti i dobrovoljnog obavještavanja uredit će se uredbom iz članka 24. ovog Zakona.

**Uz članak 51.**

Ovim se člankom propisuje da središnje državno tijelo za kibernetičku sigurnost kontinuirano razvija nacionalni sustav za otkrivanje kibernetičkih prijetnji i zaštitu kibernetičkog prostora s ciljem podizanja ukupne sposobnosti i otpornosti u području kibernetičke sigurnosti te koji sve subjekti mogu pristupiti istome temeljem sklopljenog sporazuma sa središnjim državnim tijelom za kibernetičku sigurnost. Nacionalni sustav se temelji na sustavu SK@UT, kao sustavu za otkrivanje, rano upozorenje i zaštitu od državno sponzoriranih kibernetičkih napada, APT kampanja te drugih kibernetičkih ugroza, a koji se sastoji od distribuirane mreže senzora u ključnim državnim tijelima i pravnim osobama. SK@UT omogućuje otkrivanje sofisticiranih kibernetičkih napada u najranijim fazama napada i u bilo kojem segmentu kibernetičkog prostora koji pokriva mreža senzora. Ovakav pristup povezuje najsloženije tehničke sustave za zaštitu kibernetičkog prostora čime se bitno smanjuje rizik kompromitacije ključnih nacionalnih informacijskih resursa. Pristupanje nacionalnom sustavu ne utječe na obveze ključnih i važnih subjekata iz članka 25. ovog Zakona.

**Uz članak 52.**

Ovim se člankom propisuje da središnje državno tijelo za kibernetičku sigurnost provodi procjenu kritičnosti subjekata temeljem taksativno navedenih kriterija, a u povodu zahtjeva subjekta za pristupanje nacionalnom sustavu ili prijedloga za pristupanje nacionalnom sustavu koje je podnijelo tijelo državne uprave odnosno regulatorno tijelo nadležno za sektor kojem subjekt pripada. 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. ovog Zakona.

**Uz članak 53.**

Ovim se člankom propisuje mogućnost ključnih subjekata, važnih subjekata i drugih subjekata koji nisu kategorizirani kao ključni i važni subjekti sukladno ovom Zakonu, da međusobno dobrovoljno razmjenjuju informacije o kibernetičkoj sigurnosti u svrhu povećanja razine kibernetičke sigurnosti ili postupanja s incidentima te je propisano koje sve informacije ta razmjena može uključivati i između kojih subjekata se može odvijati, putem mehanizama za razmjenu informaciju uspostavljenih posebno u te svrhe. Ti mehanizmi se uspostavljaju na temelju sporazuma o dobrovoljnoj razmjeni informacija o kibernetičkoj sigurnosti, kojim se utvrđuju uvjeti za pristupanje mehanizmu koji se sporazumom uspostavlja, sadržaj informacija koji se razmjenjuju, mogućnost upotrebe namjenskih platformi i drugih alata za automatiziranu razmjenu informaciju, kao i svi drugi operativni elementi bitni za učinkovitu i sigurnu razmjenu informacija. Ključni i važni subjekti o svom sudjelovanju u mehanizmima za dobrovoljnu razmjenu informacija o kibernetičkoj sigurnosti dužni su obavijestiti nadležna tijela 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 zatražiti mišljenje središnjeg državnog tijela za kibernetičku sigurnost.

**Uz članak 54.**

Ovim se člankom propisuje mogućnost svake fizičke i pravne osobe da anonimno prijavi ranjivost IKT proizvoda ili IKT usluga, podošenjem prijave CSIRT koordinatoru za otkrivanje ranjivosti. 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. 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 otkrivanje i upravljanje ranjivostima koje utječu na više subjekata te osiguravanje provedbe daljnjih mjera u pogledu prijavljene ranjivosti i osiguravanje anonimnosti fizičke ili pravne osobe koja prijavljuje ranjivost. Ovim člankom utvrđuju se obveze CSIRT koordinator za otkrivanje ranjivosti vezano uz osiguranje anonimnosti prijavitelja ranjivosti te čuvanje i postupanje s podacima o prijavitelju ranjivosti. CSIRT koordinator za otkrivanje ranjivosti dostavlja informacije o novootkrivenim ranjivostima nadležnim CSIRT-ovima iz ovog Zakona, zajedno s uputom o načinu daljnjeg obavještavanja o ranjivostima subjekata u njihovoj nadležnosti. 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 temeljem ovog Zakona. 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. Zadaće CSIRT koordinatora za otkrivanje ranjivosti obavlja CSIRT pri središnjem državnom tijelu za kibernetičku sigurnost. Odredbama ovog članka prenosi se članak 12. Direktive (EU) 2022/2555.

**Uz članak 55.**

Ovim se člankom propisuje da Vlada, na prijedlog središnjeg državnog tijela za kibernetičku sigurnost, donosi srednjoročni akt strateškog planiranja iz područja kibernetičke sigurnosti te se taksativno navodi što se tim aktom utvrđuje. U svrhu razrade mjera za provedbu posebnih ciljeva i prioriteta navedenog akta strateškog planiranja, izrađuje se akcijski plan za njegovu provedbu. Izvještavanje, praćenje i vrednovanje navedenog akta strateškog planiranja provodi se u skladu s propisom koji uređuje područje strateškog planiranja i upravljanja razvojem Republike Hrvatske (Zakon o sustavu strateškog planiranja i upravljanja razvojem Republike Hrvatske, „Narodne novine“ 123/2017, 151/2022) te su odredbe ovog članka usklađene s istim. Prema navedenom Zakonu srednjoročni akti strateškog planiranja se izrađuju i donose za razdoblje od pet do deset godina te su, između ostalog, definirani i kao nacionalni planovi koje donosi Vlada. Središnje državno tijelo za kibernetičku sigurnost obavještava Europsku komisiju o donošenju navedenog akta strateškog planiranja u roku od tri mjeseca od dana njegovog donošenja, odnosno u roku od tri mjeseca od dana donošenja njegovih izmjena i/ili dopuna.

**Uz članak 56.**

Ovim se člankom utvrđuje da je središnje državno tijelo za kibernetičku sigurnost tijelo odgovorno za upravljanje kibernetičkim krizama. Propisano je i da Vlada, na prijedlog tijela odgovornog za upravljanje kibernetičkim krizama, donosi nacionalni program upravljanja kibernetičkim krizama kojim se utvrđuju taksativno navedena pitanja te čiji sastavni dio čine 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. Tijelo odgovorno za upravljanje kibernetičkim krizama obavještava Europsku komisiju i EU-CyCLONe mrežu o donošenju navedenog nacionalnog programa u roku od tri mjeseca od njegova donošenja odnosno njegovih izmjena i dopuna ili donošenja novog programa.

**Uz članak 57.**

Ovim se člankom uređuje organiziranje i provedba postupaka samoocjene stanja kibernetičke sigurnosti te se definira okvir nacionalnih samoocjena. Samoocjene stanja kibernetičke sigurnosti organiziraju se i provode u okviru istorazinskih ocjenjivanja koja se provode sukladno metodologiji utvrđenoj od strane Skupine za suradnju, Europske komisije i ENISA-e te na nacionalnoj razini, a na koju se na odgovarajući način primjenjuje metodologija za provedbu samoocjena država članica koju donosi Skupina za suradnju, Europska komisija i ENISA. Planove i programe provedbe samoocjena donosi Vlada, na prijedlog središnjeg državnog tijela za kibernetičku sigurnost. Ovim se člankom osigurava provedba obveza država članica u odnosu na postupke imenovanja stručnjaka za kibernetičku sigurnost za provedbu istorazinskih ocjenjivanja.

**Uz članak 58.**

Ovim se člankom propisuje provođenje vježbi kibernetičke sigurnosti. Navedene vježbe organiziraju se i provode na temelju Plana provedbe vježbi kibernetičke sigurnosti kojeg donosi Vlada na prijedlog središnjeg državnog tijela za kibernetičku sigurnost u suradnji s ostalim nadležnim tijelima za provedbu zahtjeva kibernetičke sigurnosti, nadležnim CSIRT-ovima i nadležnim tijelima za provedbu posebnih zakona, za razdoblje od dvije godine. Dodatno, ovim je člankom propisano da se u Planu provedbe vježbi kibernetičke sigurnosti iskazuju međunarodne vježbe kibernetičke sigurnosti i nacionalne vježbe kibernetičke sigurnosti te što iste obuhvaćaju. 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.

**Uz članak 59.**

Ovim se člankom utvrđuje nadležnost državnih tijela i pravnih osoba s javnim ovlastima u provedbi zahtjeva kibernetičke sigurnosti za koje se u Zakonu koristi zajednički pojam nadležna tijela za provedbu zahtjeva kibernetičke sigurnosti, a to su Ured Vijeća za nacionalnu sigurnost, Sigurnosno-obavještajna agencija, Hrvatska regulatorna agencija za mrežne djelatnosti, Središnji državni ured za razvoj digitalnog društva i Ministarstvo znanosti i obrazovanja te njihove ovlasti, poslovi i zadaće koje obavljaju u okviru djelokruga kibernetičke sigurnosti. Podjela nadležnosti navedenih tijela po sektorima i podsektorima odnosno vrstama subjekata sadržana je u Prilogu III. ovog Zakona.

**Uz članak 60.**

Ovim se člankom utvrđuje obveza za nadležna tijela za provedbu zahtjeva kibernetičke sigurnosti, koja nisu kategorizirana kao ključni ili važni subjekti, primjenjivati zahtjeve kibernetičke sigurnosti odnosno provoditi mjere upravljanja kibernetičkim sigurnosnim rizicima i obavještavati nadležni CSIRT o značajnim incidentima i ozbiljnim kibernetičkim prijetnjama, a sve u skladu s odredbama ovog Zakona i propisa donesenog na temelju ovog Zakona koje se odnose na ključne subjekte. Također, ovim se člankom za ta ista tijela propisuje obveza da najmanje jednom u dvije godine provode samoocjene sukladnosti mrežnih i informacijskih sustava kojima se služe u svom poslovanju s mjerama upravljanja kibernetičkim sigurnosnim rizicima iz ovog Zakona, a o provedenim samoocjenama sukladnosti izvještavaju središnje državno tijelo za kibernetičku sigurnost. Stavkom 2. ovog članka se utvrđuje nadležni CSIRT za dostavu obavijesti o značajnim incidentima i ozbiljnim kibernetičkim prijetnjama.

**Uz članak 61.**

Ovim se člankom utvrđuje nadležnost središnjeg državnog tijela za kibernetičku sigurnost, njegove ovlasti, poslovi i zadaće, i to uz ovlasti, poslove i zadaće koje za njega proizlaze iz članka 59. ovog Zakona, kao jednog od nadležnih tijela za provedbu zahtjeva kibernetičke sigurnosti, ovim člankom se taksativno propisuju i drugi poslovi u nadležnosti središnjeg državnog tijela za kibernetičku sigurnost. Ovim člankom se utvrđuje da je Sigurnosno-obavještajna agencija središnje državno tijelo za kibernetičku sigurnost.

**Uz članak 62.**

Ovim se člankom utvrđuju poslovi jedinstvene kontaktne točke, kao jednu od funkcionalnosti koje je Republika Hrvatska dužna osigurati na nacionalnoj razini i sukladno Direktivi (EU) 2022/2555. Sukladno ovom Zakonu, poslove jedinstvene kontaktne točke obavljat će središnje državno tijelo za kibernetičku sigurnost odnosno Sigurnosno-obavještajna agencija.

**Uz članak 63.**

Ovim se člankom utvrđuje da se za potrebe obavljanja zadaća iz ovog Zakona u Sigurnosno-obavještajnoj agenciji ustrojava Nacionalni centar za kibernetičku sigurnost. Centralizacija upravljanja kibernetičkom sigurnošću tijekom posljednjih nekoliko godina provedena je u gotovo svim državama članicama EU, a u Republici Hrvatskoj se provodi u okviru transpozicije Direktive (EU) 2022/2555. Potreba centralizacije i uspostave nadležnog centra i središnjeg državnog tijela za kibernetičku sigurnost posljedica je iznimno brzog uvođenja novih tehnoloških rješenja, kao i aktualnih kriznih situacija (COVID, ruska agresija na Ukrajinu), ali i još bržeg tehnološkog napretka koji se očekuje u narednim godinama (umjetna inteligencija, kvantno računarstvo, …). Stoga se kibernetička sigurnost počinje na razini EU regulirati kao horizontalni zahtjev u okviru čega se svaka država mora oslanjati na jasne nadležnosti i koordinaciju kibernetičkih sposobnosti i resursa.

**Uz članak 64.**

Ovim se člankom uređuju okviri suradnje središnjeg državnog tijela za kibernetičku sigurnosti i nadležnih tijela za provedbu zahtjeva kibernetičke sigurnosti s nadležnim tijelima za provedbu posebnih zakona (Hrvatska narodna banka, Hrvatska agencija za nadzor financijskih usluga i Hrvatska agencija za civilno zrakoplovstvo). Ovim se člankom uređuje obveza obavještavanja Nadzornog forum osnovanog na temelju članka 32. stavka 1. Uredbe (EU) 2022/2554 o nadzornim aktivnostima koje se provode na temelju ovog Zakona nad ključnim i važnim subjektima koji su na temelju članka 31. Uredbe (EU) 2022/2554 određeni kao ključna treća strana pružatelj IKT usluga.

**Uz članak 65.**

Ovim se člankom uređuju okviri suradnje središnjeg državnog tijela za kibernetičku sigurnosti i nadležnih tijela za provedbu zahtjeva kibernetičke sigurnosti s nadležnim tijelima iz zakona koji uređuje područje kritičnih infrastruktura.

**Uz članak 66.**

Ovim se člankom utvrđuju zadaće CSIRT-a, kao jedne od funkcionalnosti koje je Republika Hrvatska dužna osigurati na nacionalnoj razini i sukladno Direktivi (EU) 2022/2555. Uvažavajući široki opseg obavještavanja prema nadležnim CSIRT-ovima koji se uvodi ovim Zakonom, ovim člankom propisuje se da CSIRT daje prednost prioritetnim zadaćama prema procjeni rizika, a prilikom obrade zaprimljenih obavijesti temeljem ovog Zakona daje prednost obradi obavijesti o značajnim incidentima.

**Uz članak 67.**

Ovim se člankom propisuje da CSIRT može provoditi proaktivno neintruzivno skeniranje javno dostupnih mrežnih i informacijskih sustava ključnih i važnih subjekata, uz uvjet da takvo skeniranje ne smije imati negativan učinak na funkcioniranje usluga koje ključni i važni subjekt pruža i na djelatnost koju obavlja, te obvezu nadležnog CSIRT-a obavijestiti ključnog i važnog subjekta o otkrivenim ranjivostima ili nesigurno konfiguriranim mrežnim i informacijskim sustavima.

**Uz članak 68.**

Ovim se člankom propisuje obveza ključnih i važnih subjekata surađivati s nadležnim CSIRT-om i s njim razmjenjivati potrebne informacije u postupku rješavanja incidenata. Također, ovim se člankom utvrđuje kako CSIRT u obavljanju svojih zadaća ne može snositi odgovornost za štetu uzrokovanu incidentom na mrežnim i informacijskim sustavima ključnih i važnih subjekata.

**Uz članak 69.**

Ovim se člankom utvrđuju uvjeti koje moraju osigurati nadležni CSIRT-ovi da bi obavljaju svoje zadaće.

**Uz članak 70.**

Ovim se člankom utvrđuje kako zadaće CSIRT-a iz ovog Zakona obavljaju središnje državno tijelo za kibernetičku sigurnost, kroz Nacionalni centar za kibernetičku sigurnost, i CARNET, kroz Nacionalni CERT i to prema podjeli nadležnosti za sektore, podsektore i subjekte iz Priloga I. i Priloga II. ovog Zakona kako je ona definirana u Priloga III. ovog Zakona. Također, stavkom 2. ovog članka se utvrđuje podjela nadležnosti između CSIRT-ova za subjekte koji nisu kategorizirani kao ključni i važni subjekt sukladno ovom Zakonu, a nadležni CSIRT dobrovoljno obavještavaju o svakom značajnom incidentu, ostalim incidentima, kibernetičkim prijetnjama ili izbjegnutim incidentima temeljem članka 50. stavka 1. podstavka 2. ovog Zakona.

**Uz članak 71.**

Ovim se člankom propisuje kako su zadaće središnjeg državnog tijela za kibernetičku sigurnost, nadležnih tijela za provedbu zahtjeva kibernetičke sigurnosti i nadležnih CSIRT-ova iz ovog Zakona, uključujući zadaće vezane uz suradnju, pružanje pomoći i razmjenu informacija, na nacionalnoj razini 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 da se izvršavanje tih zadaća smatra izvršavanjem zadaća od javnog interesa. Ova odredba je posebno važna u kontekstu zakonitosti obrade osobnih podataka u okviru izvršavanja zadaća na koje se ova odredba odnosi, te se njome preuzima članak 2. stavak 14. Direktive (EU) 2022/2555 u dijelu koji se odnosu na nadležna tijela, jedinstvene kontaktne točke i CSIRT-ove.

**Uz članak 72.**

Ovim se člankom propisuje kako se na obradu osobnih podataka koju provode nadležna tijela za provedbu zahtjeva kibernetičke sigurnosti i nadležni CSIRT-ovi u okviru njihovih zadaća utvrđenih ovim Zakonom primjenjuje Uredba (EU) 2016/679.

**Uz članak 73.**

Ovim člankom utvrđuje se da se popisi ključnih i važnih subjekata, kao i svi ostali zapisi koji nastaju u okviru provedbe ovoga Zakona, koriste i razmjenjuju isključivo u svrhu izvršavanja zahtjeva iz ovoga Zakona, uz poštivanje potrebe ograničavanja pristupa tim zapisima pod uvjetima propisanim zakonom koji uređuje zaštitu fizičkih osoba u vezi s obradom i razmjenom osobnih podataka u svrhe sprječavanja, istraživanja, otkrivanja, ili progona kaznenih djela ili izvršavanja kaznenih sankcija. Stavkom 2. se utvrđuje da popisi ključnih i važnih subjekata i ostali zapisi iz stavka 1. 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 koji uređuje pravo na pristup informacijama.

**Uz članak 74.**

Ovim je člankom propisana obveza nadležnim tijelima za provedbu zahtjeva kibernetičke sigurnosti da, ako tijekom stručnog nadzora nad provedbom zahtjeva kibernetičke sigurnosti ili izvršavanja drugih aktivnosti iz ovoga Zakona, saznaju za povredu obveza iz članka 25. ovog Zakona koju je počinio ključni ili važni subjekt i koja uključuje povredu osobnih podataka, da o toj povredi i utvrđenom činjeničnom stanju izvijeste tijelo nadležno za zaštitu osobnih podataka bez nepotrebne odgode. Ako o povredi 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. Ovim se člankom preuzima članak 35. stavci 1. i 3. Direktive (EU) 2022/2555.

**Uz članak 75.**

Ovim se člankom propisuje provedba stručnog nadzora nad provedbom zahtjeva kibernetičke sigurnosti u ključnim subjektima i to da se stručni nadzor ključnog subjekta provodi najmanje jednom u roku od tri do pet godina te da se stručni nadzor ključnog subjekta provodi i prije proteka tih rokova, ako nadležno tijelo za provedbu zahtjeva kibernetičke sigurnosti raspolaže informacijama koje ukazuju 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 ovog Zakona. Također, ovim člankom se propisuje da se terminski plan provedbe stručnih nadzora ključnog subjekta utvrđuje godišnjim planom rada nadležnog tijela za provedbu zahtjeva kibernetičke sigurnosti te da u svrhu utvrđivanja terminskih planova i odlučivanja o prioritetima u provedbi nadzora ta tijela mogu ključne subjekte razvrstavati prema kategoriji rizičnosti.

**Uz članak 76.**

Ovim se člankom propisuje provedba stručnog nadzora nad provedbom zahtjeva kibernetičke sigurnosti u važnim subjektima i to da se stručni nadzor važnog subjekta provodi kada nadležno tijelo za provedbu zahtjeva kibernetičke sigurnosti raspolaže informacijama koje ukazuju 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 ovog Zakona.

**Uz članak 77.**

Ovim člankom utvrđuju se načini provedbe stručnog nadzora nad provedbom zahtjeva kibernetičke sigurnosti i to: 1. neposredna provedba odnosno 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 ovog Zakona ili 2. posredna provedba odnosno uvidom u izvješća o provedenim ocjenama sukladnosti te po potrebi drugim, dodatno zatraženim i dostavljenim podacima i dokumentaciji nadziranog subjekta. Također, ovim člankom utvrđuje se obveza nadležnih tijela za provedbu zahtjeva kibernetičke sigurnosti da o neposrednoj provedbi stručnog nadzora obavijeste nadzirani subjekt najkasnije u roku od pet dana prije početka nadzora, kao i iznimka od takve obveze odnosno mogućnost provođenja nadzora iz članka 75. stavka 2. i članka 76. stavka 1. ovog Zakona bez prethodne obavijesti u slučaju postojanja razloga koji ukazuju na potrebu za hitnim postupanjem subjekta sa značajnim incidentom ili radi sprečavanja ili ublažavanja rizika koji proizlaze iz ozbiljne kibernetičke prijetnje. Također, ovim člankom se utvrđuje obveza osiguranja provedbe stručnog nadzora na način 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.

**Uz članak 78.**

Ovim se člankom utvrđuju obveze ključnih i važnih subjekata u okviru stručnog nadzora i to obvezu omogućavanja provedbe stručnog nadzora te osiguravanja svih uvjeta 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 te omogućavanje razgovora s nadležnim i odgovornim osobama nadziranog subjekta.

**Uz članak 79.**

Ovim se člankom propisuju ovlasti nadležnih tijela u obavljanju stručnog nadzora ključnih i važnih subjekata u vidu taksativno utvrđenih općih nadzornih mjera, budući da se iste odnose i na stručne nadzore ključnih subjekata i na stručne nadzore važnih subjekata.

**Uz članak 80.**

Ovim se člankom propisuju okviri provedbe ciljanih ocjena sukladnosti i to ovisno o kojim podacima i okolnostima se određuje njezino provođenje i opseg, kao i tko snosi troškove ciljane ocjene sukladnosti.

**Uz članak 81.**

Ovim se člankom propisuju dodatne ovlasti nadležnih tijela u obavljanju stručnog nadzora ključnih subjekata u vidu taksativno utvrđenih posebnih nadzornih mjera, budući da se iste odnose samo na stručne nadzore ključnih subjekata.

**Uz članak 82.**

Ovim člankom taksativno se utvrđuju korektivne mjere koje nadležna tijela za provedbu zahtjeva kibernetičke sigurnosti mogu u stručnom nadzoru izreći ključnim i važnim subjektima. Također, ovim člankom propisuje se kako u slučaju izricanja uputa i naloga, te upute i nalozi moraju sadržavati rok za provedbu korektivnih mjera i rok za obavještavanje o provedbi izrečenih korektivnih mjera, kao i obveza nadležnih tijela za provedbu zahtjeva kibernetičke sigurnosti odrediti subjektima dodatni primjereni rok za provedbu korektivnih mjera, ako ključni ili važni subjekt ne postupi sukladno izrečenim korektivnim mjerama. Nadalje, ovim člankom utvrđuje se da 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.

**Uz članak 83.**

Ovim člankom utvrđuje se mogućnost izricanja posebne korektivne mjere za ključne subjekte u vidu imenovanja na određeno razdoblje službenika za praćenje usklađenosti subjekta sa zahtjevima kibernetičke sigurnosti. Stavkom 2. utvrđuje se što mora sadržavati odluka o imenovanju službenika za praćenje usklađenosti subjekta sa zahtjevima kibernetičke sigurnosti.

**Uz članak 84.**

Ovim člankom preuzima se članak 32. stavak 5. Direktive (EU) 2022/2555 te se tako njime propisuje ovlast nadležnim tijelima za provedbu zahtjeva kibernetičke sigurnosti da ključnim subjektima, koji ne postupe u skladu s izrečenim korektivnim mjerama iz članka 82. ovog Zakona, mogu zatražiti nadležno tijelo da privremeno suspendira ovlaštenje izdano ključnom subjektu za pružanje usluga ili obavljanje djelatnosti iz Priloga I. odnosno Priloga II. ovog Zakona te zahtijevati od nadležnog tijela privremenu zabranu obavljanja upravljačkih dužnosti u ključnom subjektu fizičkim osobama iz članka 29. ovog Zakona. Stavkom 2. utvrđuje se kako se privremene suspenzije i privremene zabrane iz stavka 1. ovog članka primjenjuju samo dok ključni subjekt ne postupi sukladno izrečenim korektivnim mjerama iz članka 82. ovog Zakona, a stavkom 3. se propisuje kako se te mjere ne primjenjuju 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 koji uređuju javnu nabavu.

**Uz članak 85.**

Ovim člankom taksativno se utvrđuju okolnosti koje nadležna tijela za provedbu zahtjeva kibernetičke sigurnosti uzimaju u obzir prilikom donošenja odluka o izricanju korektivnih mjera iz članaka 82. i 83. ovog Zakona odnosno podnošenju zahtjeva sukladno članku 84. ovog Zakona te se dodatno utvrđuje što se osobito smatra ozbiljnim povredama.

**Uz članak 86.**

Ovim člankom osigurava se, u skladu s člankom 32. stavkom 4. točkom i), člankom 33. stavkom 4. točkom h) i člankom 34. stavkom 8. Direktive (EU) 2022/2555, izvršavanje ovlasti izricanja novčanih kazni prekršajno odgovornim ključnim i važnim subjektima te se u tu svrhu njime propisuje ovlast nadležnih tijela za provedbu zahtjeva kibernetičke sigurnosti da, uz izrečene korektivne mjere i podnošenje zahtjeva sukladno članku 84. ovog Zakona, mogu protiv prekršajno odgovornih ključnih i važnih subjekata podnijeti i prijave ovlaštenom tužitelju odnosno izdati prekršajne naloge sukladno prekršajnim odredbama Zakona. Također, ovim člankom preuzima se članak 35. stavak 2. Direktive (EU) 2022/2555 te se tako njegovim stavkom 2. propisuje da se u stručnim nadzorima nad provedbom zahtjeva kibernetičke sigurnosti ne može podnijeti prijava ovlaštenom tužitelju odnosno izdati prekršajni nalog sukladno prekršajnim odredbama ovog 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. Ovim člankom posebno se ne propisuju isključenja prekršajne odgovornosti koja su člankom 62. Prekršajnog zakona (“Narodne novine”, broj: 107/07, 39/13, 157/13, 110/15, 70/17, 118/18 I 114/22) propisana za tijela državne uprave i druga državna tijela.

**Uz članak 87.**

Ovim se člankom propisuje sadržaj zapisnika o provedenom stručnom nadzoru.

**Uz članak 88.**

Ovim se člankom propisuje mogućnost ulaganja primjedbi na zapisnik te utvrđuje kada se nadziranom subjektu neće omogućiti podnošenje primjedbi na zapisnik (ako bi to onemogućilo poduzimanje hitnih mjera koje su naložene radi sprečavanja značajnih incidenata ili odgovora na takve incidente).

**Uz članak 89.**

Ovim se člankom propisuje postupanje nadležnog tijela za provedbu zahtjeva kibernetičke sigurnosti po zaprimljenim primjedbama na zapisnik o provedenom stručnom nadzoru.

**Uz članak 90.**

Ovim se člankom propisuje sudska zaštita te se njime utvrđuje da 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.

**Uz članak 91.**

Ovim se člankom propisuje postupanje nadležnih tijela za slučaj kada su u stručnom nadzoru tijela državne uprave, drugih državnih tijela i jedinica lokalne i područne (regionalne) samouprave utvrđeni nedostaci i povrede ovog Zakona i uredbe iz članka 24. ovog Zakona, a nadzirano tijelo ne provede izrečene korektivne mjere u ostavljenom roku.

**Uz članak 92.**

Ovim se člankom propisuje da su nadležna tijela za provedbu zahtjeva kibernetičke sigurnosti dužna voditi očevidnike o obavljenim stručnim nadzorima. Radi praćenja i osiguranja raspoloživosti relevantnih podataka o provedenim stručnim nadzorima i ujednačenog postupanja svih nadležnih tijela za provedbu zahtjeva kibernetičke sigurnosti, stavkom 2. ovog članka propisano je da se očevidnici vode sukladno smjernicama središnjeg državnog tijela za kibernetičku sigurnost.

**Uz članak 93.**

Ovim člankom propisano je da poslove stručnog nadzora nad primjenom odredaba ovog Zakona i uredbe iz članka 24. ovog Zakona, koji se odnose na stručni nadzor pružatelja javnih elektroničkih komunikacijskih mreža i pružatelja javno dostupnih elektroničkih komunikacijskih usluga obavljaju inspektori elektroničkih komunikacija u skladu s ovim Zakonom i zakonom kojim je uređeno područje elektroničkih komunikacija.

**Uz članke 94., 95. i 96.**

Ovim se člancima utvrđuju okviri pružanja uzajamne pomoći u provedbi stručnih nadzora s nadležnim tijelima drugih država članica te se njima u nacionalno zakonodavstvo preuzima članak 26. stavak 5. i članak 37. Direktive (EU) 2022/2555.

**Uz članak 97.**

Ovim člankom utvrđuju se načini provedbe kontrole usklađenosti postupanja registra naziva vršne nacionalne internetske domene i registrara s posebnim zahtjevima za upravljanje podacima o registraciji naziva domena i to: 1. neposredna provedba 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 ili 2. posredna provedba uvidom u zatražene i dostavljene podatke i dokumentaciju kontroliranog subjekta. Također, ovim člankom utvrđuje se obveza nadležnog tijela za provedbu kontrole odnosno tijela državne uprave nadležnog za znanost i obrazovanje da o neposrednoj provedbi kontrole obavijeste subjekt nad kojim provodi kontrolu u roku od tri dana prije početka kontrole te se njime utvrđuju i obveze registra naziva vršne nacionalne internetske domene i registrara u okviru provedbe kontrola.

**Uz članak 98.**

Ovim člankom taksativno se utvrđuju korektivne mjere koje tijelo državne uprave nadležno za znanost i obrazovanje može izreći registru naziva vršne nacionalne internetske domene i registrarima u okviru provedbe kontrola usklađenosti njihova postupanja s posebnim zahtjevima za upravljanje podacima o registraciji naziva. Također, ovim člankom propisuje se da u slučaju izricanja uputa i naloga, te upute i nalozi moraju sadržavati rok za provedbu korektivnih mjera i rok za obavještavanje o provedbi izrečenih korektivnih mjera.

**Uz članak 99.**

Ovim se člankom propisuje postupanje tijela državne uprave nadležnog za znanost i obrazovanje za slučaj kada su u kontroli usklađenosti registrara s posebnim zahtjevima za upravljanje podacima o registraciji naziva domena utvrđeni nedostaci i povrede ovog Zakona, a registrar ne postupi u skladu s izrečenim mu korektivnim mjerama.

**Uz članak 100.**

Ovim se člankom propisuje da se prilikom provedbe kontrola usklađenosti registra naziva vršne nacionalne internetske domene i registrara s posebnim zahtjevima za upravljanje podacima o registraciji naziva domena na odgovarajući način primjenjuju članci 87. do 90. i članak 92. stavka 1. ovog Zakona odnosno odredbe koje se odnose na sastavljanje zapisnika, izjavljivanje primjedbi na zapisnik, postupanje s primjedbama, sudska zaštita te obveza vođenja očevidnika o provedenim nadzorima odnosno u ovom slučaju provedenim kontrolama usklađenosti postupanja registra naziva vršne nacionalne internetske domene i registrara s posebnim zahtjevima za upravljanje podacima o registraciji naziva domena.

**Uz članak 101., 102. i 103.**

Ovim se člancima utvrđuju prekršajne odredbe. Raspon iznosa novčanih kazni koje se mogu izreći za počinjene prekršaje ključnim i važnim subjektima u skladu su s člankom 34. stavcima 4. i 5. Direktive (EU) 2022/2555.

**Uz članak 104.**

Ovim se člankom utvrđuje da nadležno tijelo za provedbu zahtjeva kibernetičke sigurnosti u slučaju postojanja sumnje da je počinjen prekršaj podnosi prijavu ovlaštenom tužitelju te se njime propisuje tko su ovlašteni tužitelji u smislu ovog Zakona i to: 1. nadležni državni odvjetnik 2. regulatorno tijelo za mrežne djelatnosti za prekršaje koje počine pružatelji javnih elektroničkih komunikacijskih mreža i pružatelji javno dostupnih elektroničkih komunikacijskih usluga i 3. tijelo državne uprave nadležno za razvoj digitalnog društva za prekršaje koje počine pružatelji usluga povjerenja.

**Uz članak 105.**

Ovim se člankom propisuje obveza operatorima ključnih usluga i davatelji digitalnih usluga, koji su do stupanja na snagu ovog Zakona provodili mjere za postizanje visoke razine kibernetičke sigurnosti prema odredbama Zakona o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga („Narodne novine“, broj: 64/2018) i Uredbe o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga („Narodne novine“, broj: 68/2018), nastaviti s provedbom mjera na temelju tih propisa do dostave obavijesti o provedenoj kategorizaciji subjekta sukladno ovom Zakona.

**Uz članak 106.**

Ovim se člankom propisuje obveza pružateljima javnih elektroničkih komunikacijskih mreža i pružateljima javno dostupnih elektroničkih komunikacijskih usluga, koji su do stupanja na snagu ovog Zakona provodili sigurnosne zahtjeve u svrhu zaštite sigurnosti elektroničkih komunikacijskih mreža i elektroničkih komunikacijskih usluga prema odredbama članka 41. Zakona o elektroničkim komunikacijama („Narodne novine“, broj: 76/2022), nastaviti s provedbom zahtjeva na temelju članka 41. tog Zakona do dostave obavijesti o provedenoj kategorizaciji subjekta sukladno ovom Zakonu. Također, njime se propisuje i obveza ružateljima usluga povjerenja, koji su do stupanja na snagu ovog 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“, broj: 62/2017), nastaviti s provedbom zahtjeva na temelju tih propisa do dostave obavijesti o provedenoj kategorizaciji subjekta sukladno ovom Zakonu.

**Uz članak 107.**

Ovim se člankom utvrđuje da 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. godine ostaju na snazi do njihova isteka.

**Uz članak 108.**

Ovim člankom utvrđuje se rok u kojem su registar naziva vršne nacionalne internetske domene i registrari dužni uskladiti se sa zahtjevima iz ovog Zakona koji se odnose na upravljanje podacima o registraciji naziva domena te provesti provjere iz članka 47. stavka 2. ovog Zakona za postojeće korisnike domena.

**Uz članak 109.**

Ovim se člankom utvrđuje da će se postupci započeti prema odredbama Zakona o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga („Narodne novine“, broj: 64/2018) dovršiti prema odredbama tog Zakona i propisa donesenih na temelju toga Zakona. Također, budući da se ovim Zakonom, slijedom članka 43. Direktive (EU) 2022/2555, stavlja van snage odredba članka 41. Zakona o elektroničkim komunikacijama („Narodne novine“, broj: 76/2022), ovim se člankom utvrđuje da će se postupci započeti prema odredbama članka 41. Zakona o elektroničkim komunikacijama dovršiti prema odredbama tog Zakona i propisa donesenih na temelju toga Zakona.

**Uz članak 110.**

Ovim se člankom utvrđuje rok u kojem su nadležna tijela za provedbu zahtjeva kibernetičke sigurnosti i nadležna tijela za provedbu posebnih zakona dužna provesti prvu kategorizaciju subjekata i dostavu obavijesti o provedenoj kategorizaciji subjekata sukladno ovom Zakonu, uključujući pri tome i sve operatore ključnih usluga s popisa iz članka 12. Zakona o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga. Postupak prve kategorizacije informacijskih posrednikau razmjeni elektroničkog računa među poduzetnicima i dostava obavijesti tim subjektima o provedenoj kategorizaciji sukladno ovom Zakonu provest će u roku od tri mjeseca od stupanja na snagu zakona koji uređuje razmjena elektroničkog računa između poduzetnika.

**Uz članak 111.**

Ovim člankom utvrđuje se obveza središnjeg državnog tijela za kibernetičku sigurnost uspostaviti poseban registar subjekata iz članka 22. ovog Zakona u roku od godinu dana od dana stupanja na snagu ovog Zakona.

**Uz članak 112.**

Ovim se člankom utvrđuje od kada počinju teći rokovi propisani ovim Zakonom za provedbu ocjena sukladnosti sa zahtjevima kibernetičke sigurnosti i stručnog nadzora nad provedbom zahtjeva kibernetičke sigurnosti.

**Uz članak 113.**

Ovim se člankom utvrđuje da će Vlada uredbu iz članka 24. ovog Zakona donijeti u roku od devet mjeseci od dana stupanja na snagu ovog Zakona, prijedlog nacionalnog akta strateškog planiranja iz članka 55. ovog Zakona u roku od 24 mjeseca od dana stupanja na snagu ovog Zakona, nacionalni program upravljanja kibernetičkim krizama iz članka 56. ovog Zakona u roku od tri mjeseca od dana stupanja na snagu ovog Zakona, a Plana provedbe vježbi kibernetičke sigurnosti iz članka 58. ovog Zakona u roku od 12 mjeseci od dana stupanja na snagu ovog Zakona.

**Uz članak 114.**

Ovim se člankom propisuju rokovi za usklađivanje propisa o unutarnjem ustrojstvu Ureda Vijeća za nacionalnu sigurnost, Sigurnosno-obavještajne agencije i Zavoda za sigurnost informacijskih sustava, a koje je potrebno provesti uvažavajući djelokrug poslova koji se za navedena tijela utvrđuje ovim Zakonom.

**Uz članak 115.**

Ovim se člankom određuje da danom stupanja na snagu ovoga Zakona prestaje važiti Zakon o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga, članak 17. stavak 2. podstavak 4. i članak 21. Zakona o informacijskoj sigurnosti („Narodne novine“, broj: 79/2007), članak 41. Zakona o elektroničkim komunikacijama, Uredba o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga („Narodne novine“, broj: 68/2018), Odluka o osnivanju Nacionalnog vijeća za kibernetičku sigurnost i Operativno-tehničke koordinacije za kibernetičku sigurnost („Narodne novine“, broj: 61/2016, 28/2018, 110/2018, 79/2019 i 136/2020) i 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. godine.

**Uz članak 116.**

Ovim se člankom određuje stupanje na snagu ovog Zakona.

**Uz Prilog I.**

Prilog I. ovog Zakona utvrđuje visoko kritične sektore, podsektore i vrste subjekata te se sastoji od 11 sektora primarno namijenjenih razvrstavanju ključnih subjekata, prema općim kriterijima za provedbu kategorizacije subjekata.

**Uz Prilog II.**

Prilog II. ovog Zakona utvrđuje sektore, podsektore i vrste subjekata koji predstavljaju druge kritične sektore, a sastoji se od osam sektora, pri čemu je prvih sedam sektora preuzeto iz Priloga II. NIS2 direktive, dok je osmi sektor, sustav obrazovanja, nacionalno dodan temeljem NIS2 preporuke državama članicama i dogovora nadležnih tijela na nacionalnoj razini. Prilog II. je primarno namijenjen razvrstavanju važnih subjekata prema općim kriterijima za provedbu kategorizacije subjekata.

**Uz Prilog III.**

Prilog III. ovog Zakona utvrđuje nadležna tijela u području kibernetičke sigurnosti iz ovog Zakona i podjelu nadležnosti po sektorima, podsektorima i vrstama subjekata iz Priloga I. i Priloga II. Zakona.

**Uz Prilog IV.**

Prilogu IV. ovog Zakona utvrđuje sadržaj nacionalnog akta strateškog planiranja iz područja kibernetičke sigurnosti, koji je usklađen s NIS2 zahtjevima za sve države članice.

1. DORA – Digital Operating Resilency Act, ključni akt EU financijskog sektora koji se direktno primjenjuje na sve države članice i donesen je na isti dan kada i NIS2 direktiva (u RH nositelji provedbe uz MF su HNB i HANFA) [↑](#footnote-ref-1)
2. CER – Critical Entities Resiliency Directive, ključni akt za EU kritičnu infrastrukturu koji sve države članice moraju transponirati u istom roku u kojem i NIS2, pri čemu je pristup usko usklađen tako da CER direktiva pokriva fizičku sigurnost, a NIS2 kibernetičku sigurnost te se CER direktiva odnosi na ključne sektore iz Priloga I. NIS2 direktive, a svi kritični subjekti po CER direktivi (fizička sigurnost) obavezno postaju ključni subjekti po NIS2 direktivi (kibernetička sigurnost) – u RH je MUP nositelj transpozicije CER direktive [↑](#footnote-ref-2)
3. CSA – Cyber Security Act, donesen 2019. godine s direktnom primjenom na države članice EU-a, redefinirao je agenciju ENISA u EU agenciju za kibernetičku sigurnost, ali je uspostavio i zajednički EU okvir za kibernetičku sigurnosnu certifikaciju, kojim je osigurao isti okvir za uvođenje obvezujuće certifikacije pojedinih kibernetičkih proizvoda i usluga te definiranje ključnih EU i nacionalnih tijela za provedbu ovih poslova na isti način u cijeloj EU (u RH uspostavljeno Zakonom o kibernetičkoj sigurnosnoj certifikaciji, „Narodne novine“, broj: 63/2022, te kroz nadležnosti Hrvatske akreditacijske agencije – HAA i Zavoda za sigurnost informacijskih sustava - ZSIS) [↑](#footnote-ref-3)
4. CRA - Cyber Resiliency Act, direktno će se primjenjivati na sve države članice s ciljem da utvrdi EU obveze sigurnosne certifikacije pojedinih komercijalnih proizvoda, od kategorije Interneta stvari (tzv. Internet of Things – IoT), preko uređaja koji imaju ugrađeni softver ili vezu na Internet pa do softverske podrške u širem smislu. [↑](#footnote-ref-4)
5. https://ec.europa.eu/commission/presscorner/detail/en/ip\_23\_2243 [↑](#footnote-ref-5)
6. Akt o kibernetičkoj sloidarnosti [↑](#footnote-ref-6)
7. Akademija kibernetičkih vještina [↑](#footnote-ref-7)
8. APT – *Advanced Persistent Threat*, napredna ustrajna prijetnja, je kratica koja se koristi za različite vrste kibernetičkih napada koje provode državno-sponzorirane APT grupe, pri čemu takve APT kibernetičke napade obilježava visoka razina stručnosti i prikrivenosti počinitelja napada, koji napad provodi redovito u dužem vremenskom razdoblju (mjesecima), s najčešćim ciljem krađe povjerljivih podataka. U novije vrijeme taktike, tehnike i procedure (TTP) državno-sponzoriranih APT napadača sve češće koriste organizirane kriminalne skupine za ucjenjivačke kibernetičke napade (*Ransomware*). [↑](#footnote-ref-8)
9. Centar za kibernetičku sigurnost i sustav SK@UT su nacionalni sigurnosno-operativni centar (SOC) s mrežom distribuiranih senzora koji prate promet prema Internetu u više od 60 državnih, javnih i privatnih entiteta, koji su kritični za nacionalnu razinu (npr. operatori u energetici i transportu), i koji su se uključili u SK@UT sustav na principima suradnje, međusobnog povjerenja i transparentnosti, a s ciljem zaštite od sofisticiranih kibernetičkih ugroza i pomoći u odgovoru na kibernetičke napade. [↑](#footnote-ref-9)
10. SOA osigurava stalno ažuriranje indikatora kompromitacije, kao i taktika, tehnika i procedura državno-sponzoriranih APT grupa, pri čemu se koristi visoko razvijena međunarodna sigurnosno-obavještajna suradnja SOA-e, niz otvorenih izvora, kao i komercijalni industrijski sigurnosni izvori te EU i NATO platforme za razmjenu podataka. [↑](#footnote-ref-10)
11. Uska suradnja između SOA-e, MUP-a, MORH-a, VSOA-e, ZSIS-a, Nacionalnog CERT-a, HAKOM-a i HNB-a. [↑](#footnote-ref-11)
12. EU-CyCLONe mreža – European Cyber Crises Liaisone Organisation Network (Europska mreža organizacija za vezu za kibernetičke krize) [↑](#footnote-ref-12)
13. EECC – European Electronic Communications Code - DIREKTIVA (EU) 2018/1972 EUROPSKOG PARLAMENTA I VIJEĆA od 11. prosinca 2018. o Europskom zakoniku elektroničkih komunikacija [↑](#footnote-ref-13)
14. eIDAS - UREDBA (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 [↑](#footnote-ref-14)
15. CSIRT – *Computer Security Incident Response Team*, je tijelo nadležno za prevenciju i zaštitu od incidenata u okviru NIS2 sektora, a pojam je uveden NIS1 transpozicijskim Zakonom o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga [↑](#footnote-ref-15)