P.Z.E. br. 561

HRVATSKI SABOR

KLASA: 022-02/23-01/94
URBROJ: 65-23-2

Zagreb, 27. rujna 2023.

ZASTUPNICAMA I ZASTUPNICIMA
HRVATSKOGA SABORA

PREDSJEDNICAMA I PREDSJEDNICIMA
RADNIH TIJELA

Na temelju članka 178. Poslovnika Hrvatskoga sabora u prilogu upućujem ***Prijedlog zakona o kibernetičkoj sigurnosti,*** koji je predsjedniku Hrvatskoga sabora podnijela Vlada Republike Hrvatske, aktom od 27. rujna 2023. godine.

Ovim zakonskim prijedlogom usklađuje se zakonodavstvo Republike Hrvatske sa zakonodavstvom Europske unije, te se u prilogu dostavlja i Izjava o njegovoj usklađenosti s pravnom stečevinom Europske unije.

Za svoje predstavnike, koji će u njezino ime sudjelovati u radu Hrvatskoga sabora i njegovih radnih tijela, Vlada je odredila potpredsjednika Vlade Republike Hrvatske i ministra hrvatskih branitelja Tomu Medveda i državne tajnike Darka Nekića i dr. sc. Špiru Janovića, dr. med.

PREDSJEDNIK

Gordan Jandroković

VLADA REPUBLIKE HRVATSKE

KLASA: 022-03/23-01/43
URBROJ: 50301-29/23-23-5

Zagreb, 27. rujna 2023.

PREDSJEDNIKU HRVATSKOGA SABORA

PREDMET: Prijedlog zakona o kibernetičkoj sigurnosti

Na temelju članka 85. Ustava Republike Hrvatske („Narodne novine“, br. 85/10. - pročišćeni tekst i 5/14.- Odluka Ustavnog suda Republike Hrvatske) i članka 172. Poslovnika Hrvatskoga sabora („Narodne novine“, br. 81/13., 113/16., 69/17., 29/18., 53/20., 119/20. - Odluka Ustavnog suda Republike Hrvatske, 123/20. i 86/23 - Odluka Ustavnog suda Republike Hrvatske), Vlada Republike Hrvatske podnosi Prijedlog zakona o kibernetičkoj sigurnosti.

Ovim zakonskim prijedlogom usklađuje se zakonodavstvo Republike Hrvatske sa zakonodavstvom Europske unije, te se u prilogu dostavlja i Izjava o njegovoj usklađenosti s pravnom stečevinom Europske unije.

Za svoje predstavnike, koji će u njezino ime sudjelovati u radu Hrvatskoga sabora i njegovih radnih tijela, Vlada je odredila potpredsjednika Vlade Republike Hrvatske i ministra hrvatskih branitelja Tomu Medveda i državne tajnike Darka Nekića i dr. sc. Špiru Janovića, dr. med.

PREDSJEDNIK

mr. sc. Andrej Plenković

VLADA REPUBLIKE HRVATSKE

PRIJEDLOG ZAKONA O KIBERNETIČKOJ SIGURNOSTI

Zagreb, rujan 2023.

PRIJEDLOG ZAKONA O KIBERNETIČKOJ SIGURNOSTI

I. 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).

II. OCJENA STANJA, OSNOVNA PITANJA KOJA SE UREĐUJU PREDLOŽENIM ZAKONOM TE POSLJEDICE KOJE ĆE DONOŠENJEM ZAKONA PROISTEĆI

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. ovoga 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] uredba (financijski sektor) ili CER[2] direktiva (kritična infrastruktura). Dodatno je NIS2 povezan i s CSA[3] aktom (kibernetička sigurnosna certifikacija) iz 2019. godine, a u tijeku je usuglašavanje CRA[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] 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] (poboljšane mogućnosti odgovora na incidente kroz infrastrukturu i osposobljene institucije) i *Cyber Skills Academy*[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.

---

[1] DORA – Digital Operating Resiliency 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)

[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

[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)

[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.

[5] https://ec.europa.eu/commission/presscorner/detail/en/ip_23_2243

[6] Akt o kibernetičkoj sloidarnosti

[7] Akademija kibernetičkih vještina

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] 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 novoga 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]. 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] razmjenu informacija o kibernetičkim incidentima i koordiniranje odgovora na kibernetičke napade u stvarnom ili gotovo stvarnom vremenu.

---

[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*).

[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.

[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

- Na temelju odluke Nacionalnog vijeća za kibernetičku sigurnost i Koordinacije za sustav domovinske sigurnosti, SOA od 2020. godine provodi operativnu razinu koordinacije[11] u upravljanju kibernetičkim napadima velikih razmjera i kibernetičkim krizama u Republici Hrvatskoj.
- SOA sudjeluje kao hrvatski predstavnik u EU-CyCLONe[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

SOA-e, niz otvorenih izvora, kao i komercijalni industrijski sigurnosni izvori te EU i NATO platforme za razmjenu podataka.

[11] Uska suradnja između SOA-e, MUP-a, MORH-a, VSOA-e, ZSIS-a, Nacionalnog CERT-a, HAKOM-a i HNB-a.

[12] EU-CyCLONe mreža – European Cyber Crises Liaisone Organisation Network (Europska mreža organizacija za vezu za kibernetičke krize)

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. ovoga 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 ovoga Zakona primjenjuju u cijelosti, od zahtjeva za primjenom mjera, preko izvještavanja o incidentima, provedbe nezavisne ocjene sukladnosti, do nadzora (*ex-ante* pristup). Prilog II. ovoga 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 ovoga 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 ovoga 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 ovoga Zakona povezana su sa sektorima, podsektorima i vrstama subjekata za koje su nadležni u Prilogu III. ovoga 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] i sektor pružatelja usluga povjerenja[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. ovoga 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] tijela, Zakonom se utvrđuju za svaki pojedini sektor, podsektor i vrstu subjekta prema Prilogu III. ovoga 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. ovoga 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 ovoga 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 novoga 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

[13] EECC – European Electronic Communications Code - DIREKTIVA (EU) 2018/1972 EUROPSKOG PARLAMENTA I VIJEĆA od 11. prosinca 2018. o Europskom zakoniku elektroničkih komunikacija

[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

[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

područja iz ovoga 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.

III. OCJENA POTREBNIH SREDSTAVA ZA PROVOĐENJE ZAKONA

Za provedbu ovoga Zakona u Državnom proračunu za 2023. godinu 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 ovoga Zakona te mogućnostima korištenja sredstava iz EU fondova koji će biti raspoloživi u svrhu provedbe NIS2 direktive u državama članicama.

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 ovoga Zakona i druga pitanja od značaja za područje kibernetičke sigurnosti.

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

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

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

Popis priloga koji su sastavni dio Zakona

Članak 2.

Sastavni dio ovoga Zakona su:

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

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

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

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

Usklađivanje propisa s pravnim aktima Europske unije

Članak 3.

Ovim 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 ovoga Zakona pojedini pojmovi imaju sljedeće značenje:

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

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

3. *„CSIRT mreža“* je mreža nacionalnih CSIRT-ova osnovana 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 ovoga 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 ovoga Zakona, mogu otkrivati osobne podatke

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

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

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

35. *„predstavnik”* je fizička ili pravna osoba koja ima poslovni nastan u Europskoj uniji koju su pružatelj usluga 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 ovoga Zakona

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

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

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

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

a) javno dostupne rekurzivne usluge razlučivanja naziva domena krajnjim korisnicima interneta i/ili
b) mjerodavne usluge razlučivanja naziva domena za upotrebu trećih strana, uz iznimku korijenskih poslužitelja naziva

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

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

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

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

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

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

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

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

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

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

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

52. *„središte za razmjenu internetskog prometa”* je mrežni instrument koji omogućuje međupovezivanje više od dviju neovisnih mreža (autonomnih sustava), 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. ovoga 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 ovoga Zakona zbog njihove uloge u upravljanju, razvijanju ili održavanju državne informacijske infrastrukture

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

56. *„sustav obrazovanja”* obuhvaća rani i predškolski odgoj i obrazovanje, osnovno obrazovanje, srednje obrazovanje i visoko obrazovanje, praćenje, vrednovanje i razvoj sustava, te 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“* je Ministarstvo znanosti i obrazovanja

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

61. *„treća strana pružatelj IKT usluga“* je pružatelj IKT usluga kako je definiran u članku 3. 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 ovoga Zakona nastaju ili se koriste klasificirani podaci ili drugi podaci za koje su posebnim propisima utvrđena pravila postupanja radi zaštite njihove tajnosti ili povjerljivosti, na takve podatke primjenjuju se posebni propisi o njihovoj zaštiti.

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

Primjena pravila o zaštiti osobnih podataka

Članak 6.

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

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

Odnos sa zakonom koji uređuje područje elektroničkih komunikacija

Članak 7.

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

(2) Primjena odredaba ovoga Zakona ne utječe na pravila upravljanja vršnom nacionalnom internetskom domenom 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. ovoga Zakona i Priloga II. ovoga Zakona posebnim zakonima propisani zahtjevi koji po svom sadržaju i svrsi odgovaraju zahtjevima kibernetičke sigurnosti iz ovoga Zakona, ili predstavljaju strože zahtjeve, na te 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. ovoga članka po svom sadržaju i svrsi odgovaraju zahtjevima kibernetičke sigurnosti iz ovoga Zakona ako:

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

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

(3) Tijela koja su prema posebnim zakonima iz stavka 1. ovoga članka nadležna za sektor odnosno podsektor i/ili subjekt iz Priloga I. i Priloga II. ovoga Zakona i nadležna tijela za provedbu zahtjeva kibernetičke sigurnosti dužna su prilikom primjene stavaka 1. i 2. ovoga članka međusobno surađivati i razmjenjivati relevantne informacije te voditi računa o smjernicama Europske komisije kojima se 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. ovoga 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 vršne nacionalne internetske domene te pružatelji usluga DNS-a, neovisno o njihovoj veličini

- pružatelji javnih elektroničkih komunikacijskih mreža ili javno dostupnih elektroničkih komunikacijskih usluga koji 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. ovoga 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. ovoga Zakona koji nisu utvrđeni kao ključni subjekti temeljem članka 9. ovoga 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. ovoga Zakona, subjekti iz Priloga I. i Priloga II. ovoga Zakona mogu se razvrstati u kategoriju ključnih ili važnih subjekata neovisno o njihovoj veličini, ako:

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

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

- bi poremećaj u funkcioniranju usluge koju pruža subjekt, odnosno poremećaj u obavljanju djelatnosti subjekta, mogao uzrokovati znatne sistemske rizike u sektorima iz Priloga I. i Priloga

II. ovoga Zakona, posebno u sektorima u kojima bi takav poremećaj mogao imati prekogranični učinak ili

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

Kategorizacija subjekata javnog sektora

Članak 12.

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

- tijela državne uprave

- 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. ovoga Zakona podliježu nadležnostima i ovlastima propisanim ovim Zakonom ako pružaju usluge odnosno obavljaju djelatnosti na području Europske unije, a imaju poslovni nastan na teritoriju Republike Hrvatske.

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

(3) Iznimno od stavka 1. ovoga članka, pružatelji usluga DNS-a, registar naziva vršne nacionalne internetske domene i 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. ovoga članka, ako na teritoriju Republike Hrvatske:

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

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

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

Primjena kriterija veličine subjekta

Članak 15.

(1) Prilikom utvrđivanja predstavlja li subjekt srednji subjekt 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. ovoga Zakona.

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

Primjena Zakona u slučaju dvostruke kategorizacije subjekta

Članak 16.

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

POGLAVLJE II.
POPISI KLJUČNIH I VAŽNIH SUBJEKATA

Vođenje popisa

Članak 17.

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

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

Dostava podataka Europskoj komisiji i Skupini za suradnju

Članak 18.

(1) Jedinstvena kontaktna točka svake dvije godine dostavlja:

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

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

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

Obavijesti o provedenoj kategorizaciji subjekata

Članak 19.

(1) Nadležna tijela za provedbu zahtjeva kibernetičke sigurnosti dužna su sve subjekte s popisa iz članka 17. stavka 1. ovoga Zakona iz njihove nadležnosti obavijestiti o provedenoj kategorizaciji subjekta i obvezama kojima podliježu temeljem ovoga 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 ovoga 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 ovoga Zakona.

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

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

Članak 20.

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

- naziv subjekta

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

- relevantni sektor i podsektor iz Priloga I. i Priloga II. ovoga Zakona

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

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

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

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

Prikupljanje podataka iz drugih izvora radi provedbe kategorizacije subjekata

Članak 21.

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

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

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

a) podatke o njihovoj veličini i/ili

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

c) ih uputiti na tijelo državne uprave, drugo državno tijelo, pravnu osobu s javnim ovlastima ili javnog subjekta koji takve podatke posjeduje.

(2) Ako se podaci temeljem ovoga 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. ovoga članka vodi se neovisno o obvezi vođenja popisa ključnih i važnih subjekata.

Prikupljanje podataka

Članak 23.

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

- naziv subjekta

- popis usluga iz članka 22. ovoga Zakona koje pružaju

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

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

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

- IP adresne raspone subjekta.

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

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

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

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

Članak 24.

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

DIO TREĆI
ZAHTJEVI KIBERNETIČKE SIGURNOSTI

Opseg zahtjeva kibernetičke sigurnosti

Članak 25.

(1) Zahtjevi kibernetičke sigurnosti obuhvaćaju postupke i mjere koje su ključni i važni subjekti dužni primjenjivati 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. ovoga 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. ovoga Zakona.

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

(7) Rok iz stavka 6. ovoga 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. ovoga 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. ovoga Zakona.

Odgovornost za provedbu mjera

Članak 29.

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

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

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

- pohađati odgovarajuća osposobljavanja

- zaposlenicima subjekta omogućiti pohađanje odgovarajućih osposobljavanja.

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

Mjere upravljanja kibernetičkim sigurnosnim rizicima

Članak 30.

(1) Mjere upravljanja kibernetičkim sigurnosnim rizicima uključuju 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. ovoga članka, ključni i važni subjekti dužni su uzeti u obzir ranjivosti specifične za svakog izravnog dobavljača i pružatelja usluge te opću kvalitetu proizvoda i kibernetičku sigurnosnu praksu svojih dobavljača i pružatelja usluga, kao i rezultate koordiniranih procjena sigurnosnih rizika ključnih lanaca opskrbe IKT uslugama, IKT sustavima ili IKT proizvodima, koje provodi Skupina za suradnju zajedno s Europskom komisijom i ENISA-om.

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. ovoga 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. ovoga članka u roku od 30 dana od dana dostave obavijesti iz članka 19. stavka 1. ovoga 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. ovoga članka u roku od 30 dana od dana dostave obavijesti iz članka 19. stavka 1. ovoga 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. ovoga Zakona, te pogođenim subjektom, obavijestiti javnost o značajnom incidentu ili zatražiti od ključnog i važnog subjekta da to učini.

Obavještavanje jedinstvene kontaktne točke i ENISA-e

Članak 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. ovoga Zakona, sukladno njezinim smjernicama.

(2) Jedinstvena kontaktna točka podnosi ENISA-i svaka tri mjeseca sažeto izvješće koje uključuje anonimizirane i agregirane podatke o značajnim incidentima, ostalim incidentima, ozbiljnim kibernetičkim prijetnjama i izbjegnutim incidentima o kojima su ključni i važni subjekti obavijestili nadležni CSIRT temeljem članaka 31. i 33. ovoga Zakona.

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

Članak 37.

(1) Obavještavanje temeljem članaka 31. i 33. ovoga Zakona i razmjena podataka o kibernetičkim prijetnjama i incidentima između nadležnih tijela iz Priloga III. ovoga Zakona obavlja se putem nacionalne platforme za prikupljanje, analizu i razmjenu podataka o kibernetičkim prijetnjama i incidentima, kao jedinstvene ulazne točke za obavještavanje o kibernetičkim prijetnjama i incidentima.

(2) Razvoj i upravljanje nacionalnom platformom iz stavka 1. ovoga članka u nadležnosti je 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. ovoga 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. ovoga Zakona, postupanja s tim obavijestima, uključujući postupanja nadležnog CSIRT-a u povodu zaprimljenih obavijesti, propisuju se uredbom iz članka 24. ovoga 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. ovoga 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. ovoga Zakona.

(3) Iznimno od stavka 2. ovoga 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. ovoga 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. ovoga 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. ovoga 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. ovoga Zakona.

(3) Ocjena sukladnosti iz stavka 1. ovoga 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. ovoga Zakona.

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

(6) Izvješće iz stavka 5. ovoga 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. ovoga 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. ovoga Zakona, subjekt za koji je ocjena provedena dužan je izvješće iz stavka 5. ovoga 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. ovoga 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. ovoga 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. ovoga Zakona, registar naziva vršne nacionalne internetske domene i registrari dužni su odbiti takav zahtjev, a podnositelja zahtjeva obavijestiti o uskraćivanju registracije domene odnosno privremenoj deaktivaciji domene i nemogućnosti 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. ovoga 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. ovoga Zakona, koje obvezno sadržavaju i postupke provjere podataka iz zahtjeva za registraciju domene.

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

Čuvanje podataka i pristup podacima o korisniku domene

Članak 48.

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

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

- identifikacijske dokumente i drugu dokumentaciju na temelju koje je utvrđen identitet korisnika domene
- zahtjev za registraciju domene i drugu dokumentacija vezanu uz registraciju domene.

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

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

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

(6) Tehničke i organizacijske mjere za zaštitu osobnih podataka o korisnicima domena uređuju se posebnim propisima 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. ovoga 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. ovoga 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. ovoga stavka.

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

Nacionalni sustav za otkrivanje kibernetičkih prijetnji i zaštitu kibernetičkog prostora

Članak 51.

(1) 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. ovoga 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. ovoga Zakona, već predstavlja dodatnu mjeru kibernetičke zaštite.

Kriteriji za provedbu procjene kritičnosti subjekta

Članak 52.

(1) Procjena kritičnosti subjekta iz članka 51. stavka 2. ovoga Zakona provodi se 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. ovoga 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. ovoga članka podnose se središnjem državnom tijelu za kibernetičku sigurnost.

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

Dobrovoljna razmjena informacija o kibernetičkoj sigurnosti

Članak 53.

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

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

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

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

(5) Sporazumom iz stavka 4. ovoga članka utvrđuju se uvjeti za pristupanje mehanizmu koji se sporazumom uspostavlja, sadržaj informacija koje se razmjenjuju, mogućnost upotrebe namjenskih platformi i drugih alata za automatiziranu razmjenu 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. ovoga 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. ovoga članka nužno pohranjivati podatke o prijavitelju ranjivosti, CSIRT koordinator za otkrivanje ranjivosti dužan je voditi evidenciju pohranjenih podataka.

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

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

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

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

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

DIO PETI
STRATEŠKO PLANIRANJE I UPRAVLJANJE KIBERNETIČKOM SIGURNOSTI

Nacionalni akt strateškog planiranja iz područja kibernetičke sigurnosti

Članak 55.

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

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

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

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

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

(4) Izvještavanje, praćenje i vrednovanje akta strateškog planiranja iz stavka 1. ovoga članka provodi se u skladu s propisom 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. ovoga članka u roku od tri mjeseca od dana njegovoga donošenja, odnosno u roku od tri mjeseca od dana donošenja njegovih izmjena i/ili dopuna.

Upravljanje kibernetičkim incidentima velikih razmjera i kibernetičkim krizama

Članak 56.

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

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

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

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

- koherentnost s nacionalnim općim okvirom za upravljanje krizama

- mjere i aktivnosti za jačanje nacionalne pripravnosti

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

- zadaće i odgovornosti tijela uključenih u upravljanje kibernetičkim krizama

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

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

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

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

- sva pitanja bitna za razmjenu podataka.

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

Ocjenjivanje stanja kibernetičke sigurnosti

Članak 57.

(1) U 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. ovoga 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. ovoga članka i nacionalnih samoocjena donosi Vlada, na prijedlog središnjeg državnog tijela za kibernetičku sigurnost.

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

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

Vježbe kibernetičke sigurnosti

Članak 58.

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

(2) Vježbe kibernetičke sigurnosti organiziraju se i provode na temelju Plana provedbe vježbi kibernetičke sigurnosti 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 ovoga Zakona, uključujući nadležne CSIRT-ove.

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

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

DIO ŠESTI
NADLEŽNA TIJELA U PODRUČJU KIBERNETIČKE SIGURNOSTI

POGLAVLJE I.
NADLEŽNA TIJELA ZA PROVEDBU ZAHTJEVA KIBERNETIČKE SIGURNOSTI

Zadaće nadležnih tijela za provedbu zahtjeva kibernetičke sigurnosti

Članak 59.

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

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

- provode stručni nadzor ključnih i važnih subjekta u provedbi zahtjeva kibernetičke sigurnosti sukladno ovom Zakonu i uredbi iz članka 24. ovoga Zakona

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

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

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

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

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

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

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

Članak 60.

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

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

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

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

Zadaće središnjeg državnog tijela za kibernetičku sigurnost

Članak 61.

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

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

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

- unaprjeđuje mjere upravljanja kibernetičkim sigurnosnim rizicima kroz planiranje razvoja regulativnog okvira kibernetičke sigurnosti

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

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

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

- sudjeluje u radu EU-CyCLONe mreže i 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. ovoga 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 ovoga Zakona

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

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

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

Zadaće jedinstvene kontaktne točke

Članak 62.

Jedinstvena kontaktna točka obavlja sljedeće poslove:

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

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

- sudjeluje u radu Skupine za suradnju

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

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

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

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

Nacionalni centar za kibernetičku sigurnost

Članak 63.

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

POGLAVLJE II.
SURADNJA NADLEŽNIH TIJELA NA NACIONALNOJ RAZINI

Suradnja s nadležnim tijelima za provedbu posebnih zakona

Članak 64.

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

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

(3) Pomoć iz stavka 2. ovoga 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. ovoga Zakona.

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

Suradnja s nadležnim tijelima iz zakona 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. ovoga članka uređuju se sva bitna pitanja koja se odnose na razmjenu informacija i koordinaciju nadležnih tijela, uključujući način razmjene informacija iz stavka 1. ovoga članka, kao i informacija o provedenim nadzorima nad kritičnim subjektima.

POGLAVLJE III.
CSIRT NADLEŽNOSTI

Zadaće CSIRT-a

Članak 66.

(1) CSIRT obavlja sljedeće poslove:

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

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

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

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

- na zahtjev ključnih i važnih subjekata provodi proaktivno skeniranje mrežnih i informacijskih sustava ključnih i važnih 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. ovoga Zakona, te provedbe dobrovoljnog obavještavanja iz članka 33. ovoga Zakona

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

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

- sudjeluje u radu CSIRT mreže

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

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

- surađuje s relevantnim dionicima iz privatnog sektora te u svrhu uspostave takve suradnje promiče donošenje i primjenu zajedničkih ili normiranih praksi, planova za kategorizaciju i

taksonomiju u odnosu na postupanje s incidentima, upravljanje kibernetičkim krizama i koordinirano otkrivanje ranjivosti na temelju članka 54. ovoga Zakona

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

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

Provođenje proaktivnog neintruzivnog skeniranja javno dostupnih mrežnih i informacijskih sustava

Članak 67.

(1) 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. ovoga 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. ovoga članka.

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

Članak 68.

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

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

Osiguravanje uvjeta za obavljanje zadaća nadležnog CSIRT-a

Članak 69.

Nadležni CSIRT dužan je:

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

- osigurati povjerljivost i pouzdanost aktivnosti koje provode

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

- osigurati opremljenost odgovarajućim sustavom za upravljanje zahtjevima za rješavanje incidenata

- osigurati dovoljan broj osposobljenih zaposlenika, kao i opremljenost redundantnim sustavima i odgovarajućim radnim prostorima, 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 ovoga Zakona te

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

Određivanje nadležnosti CSIRT-a

Članak 70.

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

(2) U smislu članka 50. stavka 1. podstavka 2. ovoga Zakona, središnje državno tijelo za kibernetičku sigurnost obavlja zadaće CSIRT-a za državna tijela 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. ovoga članka predstavljaju informacije u odnosu na koje je moguće ograničiti pravo pristupa korisniku prava na pristup informacija i ponovnu uporabu informacija, ovisno o rezultatima testa razmjernosti i javnog interesa koji se provodi prema odredbama zakona kojim se uređuje pravo na pristup informacijama.

Obveza izvještavanja o povredama koje uključuju povredu osobnih podataka

Članak 74.

(1) Ako nadležno tijelo za provedbu zahtjeva kibernetičke sigurnosti, tijekom stručnog nadzora nad provedbom zahtjeva kibernetičke sigurnosti ili izvršavanja drugih aktivnosti iz ovoga Zakona, sazna za povredu obveza iz članka 25. ovoga Zakona koju je počinio 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. ovoga članka izvještava tijelo nadležno za zaštitu osobnih podataka osnovano u drugoj državi članici, nadležno tijelo za provedbu zahtjeva kibernetičke sigurnosti dužno je o istoj povredi izvijestiti i Agenciju za zaštitu osobnih podataka.

DIO OSMI
STRUČNI NADZOR NAD PROVEDBOM ZAHTJEVA KIBERNETIČKE SIGURNOSTI

POGLAVLJE I.
PROVEDBA STRUČNOG NADZORA

Provedba stručnog nadzora 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. ovoga 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 ovoga Zakona.

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

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

Provedba stručnog nadzora 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 ovoga Zakona.

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

Način provedbe stručnog nadzora i obavijest o provedbi nadzora

Članak 77.

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

- na način da se u nadziranom subjektu obavlja neposredan uvid u podatke, dokumentaciju, uvjete i načine provedbe mjera upravljanja kibernetičkim sigurnosnim rizicima, izvršavanja

propisanih obveza obavještavanja o kibernetičkim prijetnjama i incidentima te postupanja po zahtjevima nadležnih tijela iz ovoga Zakona ili

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

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

- u slučaju postojanja razloga koji 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. ovoga članka voditi računa o utjecaju provedbe nadzora na rad i poslovanje nadziranog subjekta te osigurati da provedba nadzora ne dovodi do prekida u radu i poslovanju nadziranog subjekta, osim u slučaju da stručni nadzor na drugi način nije moguće provesti.

Obveze ključnih i važnih subjekata u okviru stručnog nadzora

Članak 78.

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

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

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

- omogućavanja razgovora s nadležnim i odgovornim osobama nadziranog subjekta.

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

Opće nadzorne mjere za ključne i važne subjekte

Članak 79.

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

- provesti 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 ovoga 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. ovoga 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. ovoga članka, nadležno tijelo za provedbu zahtjeva kibernetičke sigurnosti izrađuje dodatnu analizu kibernetičke sigurnosti na temelju objektivnih, nediskriminirajućih, pravednih i transparentnih kriterija za procjenu rizika, ako je to potrebno u suradnji s nadziranim subjektom, a 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. ovoga članka, nadležno tijelo za provedbu zahtjeva kibernetičke sigurnosti dužno je navesti njezinu svrhu i pobliže odrediti podatke, dokumentaciju i druge informacije koje traži od subjekta.

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. ovoga 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. ovoga 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. ovoga 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. ovoga Zakona.

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

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

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

Korektivne mjere za ključne i važne subjekte

Članak 82.

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

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

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

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

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

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

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

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

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

Posebna korektivna mjera za ključne subjekte

Članak 83.

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

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

Privremene suspenzije i zabrane obavljanja djelatnosti

Članak 84.

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

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

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

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

(3) Mjere iz stavka 1. ovoga članka ne primjenjuju se na tijela državne uprave, druga državna tijela, jedinice lokalne i područne (regionalne) samouprave i javne subjekte koji u svojstvu tijela javnog prava predstavljaju javne naručitelje u smislu propisa 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. ovoga Zakona odnosno podnošenju zahtjeva sukladno članku 84. ovoga Zakona, nadležno tijelo za provedbu zahtjeva kibernetičke sigurnosti uzima u obzir:

- ozbiljnost povrede i važnost odredaba koje nadzirani subjekt krši

- trajanje povrede

- relevantne prethodno počinjene povrede od strane istog subjekta

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

- je li nadzirani subjekt djelovao s namjerom ili nepažnjom

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

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

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

(2) Ozbiljnim povredama iz stavka 1. podstavka 1. ovoga članka 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. ovoga Zakona i

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

Izricanje novčanih kazni

Članak 86.

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

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

POGLAVLJE IV.
ZAPISNIK O PROVEDENOM STRUČNOM NADZORU

Sadržaj zapisnika

Članak 87.

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

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

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

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

Primjedbe na zapisnik

Članak 88.

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

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

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

Postupanje po primjedbama na zapisnik

Članak 89.

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

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

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

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

Sudska zaštita

Članak 90.

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

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

Članak 91.

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

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

Očevidnici o obavljenim stručnim nadzorima

Članak 92.

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

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

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

Članak 93.

Poslove stručnog nadzora nad primjenom odredaba ovoga Zakona i uredbe iz članka 24. ovoga zakona, koji se odnose na stručni nadzor 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. ovoga članka može obuhvaćati postupanje po zahtjevima za dostavu relevantnih informacija i poduzimanje nadzornih mjera ili izricanje korektivnih mjera, uključujući zahtjeve za provođenje stručnih nadzora ili ciljanih 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 ovoga članka primjenjuju se i u slučaju zaprimanja zahtjeva za uzajamnu pomoć u provedbi stručnog nadzora nad subjektima iz članka 14. stavka 3. ovoga Zakona koji pružaju usluge ili imaju mrežne i informacijske sustave na državnom području Republike Hrvatske.

Zajednička provedba nadzornih mjera

Članak 96.

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

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

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

Članak 97.

(1) Tijelo državne uprave nadležno za znanost i obrazovanje provodi kontrolu usklađenosti iz članka 49. ovoga 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. ovoga 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. ovoga članka obavijestiti subjekt nad kojim provodi kontrolu u roku od tri dana prije početka kontrole.

(3) Iznimno od stavka 2. ovoga 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. ovoga 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. ovoga 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. ovoga članka moraju sadržavati rok za provedbu naloženih mjera i rok za obavještavanje o njihovoj provedbi.

Privremene suspenzije ovlaštenja izdanih za pružanje usluga registracije domena

Članak 99.

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

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

Zapisnici o provedenim kontrolama i sudska zaštita

Članak 100.

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

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

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

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

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

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

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

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

- nadležnim tijelima tijekom stručnog nadzora ne omogući nesmetani pristup prostorima, opremi, sustavima i dokumentaciji nužnima za provođenje nadzora (članak 78. ovoga 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. ovoga 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. ovoga članka i njezinoj visini uzimaju se u obzir okolnosti iz članka 85. ovoga 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. ovoga 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. ovoga Zakona)

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

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

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

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

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

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

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

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

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

(2) Za prekršaj iz stavka 1. ovoga članka kaznit će se i 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. ovoga članka i njezinoj visini uzimaju se u obzir okolnosti iz članka 85. ovoga 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. ovoga 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. ovoga Zakona)

- prekršajno odgovorni subjekti iz članka 22. ovoga 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. ovoga Zakona)

(2) Za prekršaj iz stavka 1. ovoga članka kaznit će se i odgovorna osoba subjekta iz stavka 1. ovoga članka novčanom kaznom u iznosu od 200,00 do 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 ovoga Zakona provodili mjere za postizanje visoke razine kibernetičke sigurnosti prema odredbama Zakona o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga („Narodne novine“, broj 64/18.) i Uredbe o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga („Narodne novine“, broj 68/18.) nastavljaju s provedbom mjera na temelju tih propisa do dostave obavijesti o provedenoj kategorizaciji subjekta iz članka 19. stavaka 1. i 3. ovoga Zakona.

Članak 106.

(1) Pružatelji javnih elektroničkih komunikacijskih mreža i pružatelji javno dostupnih elektroničkih komunikacijskih usluga koji su do stupanja na snagu ovoga Zakona provodili sigurnosne zahtjeve u svrhu zaštite sigurnosti elektroničkih komunikacijskih mreža i elektroničkih komunikacijskih usluga prema odredbama članka 41. Zakona o elektroničkim komunikacijama („Narodne novine“, broj 76/22.) nastavljaju s provedbom zahtjeva na temelju članka 41. toga Zakona do dostave obavijesti o provedenoj kategorizaciji subjekta iz članka 19. stavka 1. ovoga Zakona.

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

Članak 108.

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

Članak 109.

(1) Postupci započeti prema odredbama Zakona o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga („Narodne novine“, broj 64/18.) 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 76/22.) 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. ovoga Zakona i nadležna tijela za provedbu posebnih zakona iz članka 4. stavka 1. točke 27. ovoga Zakona provest će prvu kategorizaciju subjekata i dostavu obavijesti o provedenoj kategorizaciji subjekata u roku od godinu dana od dana stupanja na snagu ovoga Zakona.

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

(3) Postupak prve kategorizacije informacijskih posrednika u razmjeni elektroničkog računa među poduzetnicima i dostava obavijesti o provedenoj kategorizaciji sukladno ovom Zakonu provest će 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. ovoga Zakona u roku od godinu dana od dana stupanja na snagu ovoga Zakona.

Članak 112.

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

Članak 113.

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

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

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

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

Članak 114.

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

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

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

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

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

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

Članak 115.

Danom stupanja na snagu ovoga Zakona prestaju važiti:

- Zakon o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga („Narodne novine“, broj 64/18.)

- članak 17. stavak 2. podstavak 4. i članak 21. Zakona o informacijskoj sigurnosti („Narodne novine“, broj 79/07.)

- članak 41. Zakona o elektroničkim komunikacijama („Narodne novine“, broj 76/22.)

- Uredba o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga („Narodne novine“, broj 68/18.)

- Odluka o osnivanju Nacionalnog vijeća za kibernetičku sigurnost i Operativno-tehničke koordinacije za kibernetičku sigurnost („Narodne novine“, br. 61/16., 28/18., 110/18., 79/19. i 136/20.) 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 osmoga 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 usluga Pojam „*elektroenergetski subjekt*“ u smislu ovoga Zakona znači pravna ili fizička osoba, koja nije krajnji kupac, a koja obavlja najmanje jednu od elektroenergetskih djelatnosti i koja je odgovorna za komercijalne i tehničke zadaće i zadaće održavanja koje su povezane s tim djelatnostima. Pojam „o*pskrba električnom energijom*“ u smislu ovoga Zakona znači kupnja i prodaja električne energije na veleprodajnom tržištu, prodaja električne energije krajnjim kupcima i skladištima energije, otkup električne energije od aktivnih kupaca, skladišta energije i proizvođača te agregiranje. Pojam „*opskrba električnom energijom koja se obavlja kao javna usluga*“ u smislu ovoga Zakona znači opskrba električnom energijom onih krajnjih kupaca koji imaju pravo na takav način opskrbe i slobodno ga izaberu ili koriste po automatizmu. Pojmovi „*elektroenergetski subjekt“, „opskrba električnom energijom“* i „*opskrba električnom energijom koja se obavlja kao javna usluga“* istovjetni su pojmovima iz članka 3. stavka 1. točaka 17., 77. i 78. Zakona o tržištu električne energije („Narodne novine“, broj 111/21.), kojim je u hrvatsko zakonodavstvo preuzeta Direktiva (EU) 2019/944 Europskog parlamenta i Vijeća od 5. lipnja 2019. o zajedničkim pravilima za unutarnje tržište električne energije i izmjeni Direktive 2012/27/EU (SL L 158, 14. 6. 2019.).
		- operatori distribucijskog sustava Pojam „*operator distribucijskog sustava*” u smislu ovoga Zakona znači fizička ili pravna osoba odgovorna za pogon i vođenje, održavanje, razvoj i izgradnju distribucijske mreže na danom području kao i zajedničkih postrojenja prema prijenosnoj mreži i, kada je to primjenjivo, međusobno povezivanje s drugim distribucijskim sustavima te za osiguravanje dugoročne sposobnosti distribucijske mreže da zadovolji razumne zahtjeve za distribuciju električne energije.

		Pojam „operator distribucijskog sustava“ istovjetan je pojmu iz članka 3. stavka 1. točke 71. Zakona o tržištu električne energije.
		- operatori prijenosnog sustava Pojam „*operator prijenosnog sustava*” u smislu ovoga Zakona znači fizička ili pravna osoba odgovorna za pogon i vođenje, održavanje, razvoj i izgradnju prijenosne mreže na danom području, prekograničnih prijenosnih vodova prema drugim prijenosnim mrežama kao i zajedničkih postrojenja prema distribucijskoj mreži te za osiguravanje dugoročne sposobnosti prijenosne mreže da zadovolji razumne zahtjeve za prijenos električne energije. Pojam *„operator prijenosnog sustava“* istovjetan je pojmu iz članka 3. stavka 1. točke 72. Zakona o tržištu električne energije.
		- proizvođači električne energije Pojam *„proizvođač električne energije”* u smislu ovoga Zakona znači fizička ili pravna osoba koja proizvodi električnu energiju. Pojam *„proizvođač električne energije”* istovjetan je 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 energije Pojam „*agregiranje*” u smislu ovoga Zakona znači djelatnost koju obavlja fizička ili pravna osoba koja može kombiniranjem snage i/ili iz mreže preuzete električne energije više kupaca ili operatora skladišta energije ili snage i/ili u mrežu predane električne energije više proizvođača ili aktivnih kupaca ili operatora skladišta energije radi sudjelovanja na bilo kojem tržištu električne energije. Pojam „*upravljanje potrošnjom*” u smislu ovoga Zakona znači promjena u opterećenju kod krajnjih kupaca u odnosu na njihove uobičajene ili trenutačne obrasce potrošnje električne energije kao odgovor na tržišne signale, uključujući vremenski ovisnu

		promjenu cijene električne energije ili novčane poticaje, ili kao odgovor na prihvat ponude krajnjeg kupca za prodaju smanjenja ili povećanja potražnje po cijeni na organiziranim tržištima, kako je definirano u članku 2. točki 4. Provedbene uredbe Komisije (EU) br. 1348/2014 od 17. prosinca 2014. o izvješćivanju o podacima i provedbi članka 8. stavaka 2. i 6. Uredbe (EU) br. 1227/2011 Europskog parlamenta i Vijeća o cjelovitosti i transparentnosti veleprodajnog tržišta energije (Tekst značajan za EGP) (SL L 363, 18. 12. 2014.), pojedinačno ili putem agregiranja. Pojam „*skladištenje energije*" u smislu ovoga Zakona znači u kontekstu elektroenergetskog sustava, odgađanje konačne uporabe električne energije do trenutka kasnijeg od onog u kojem je proizvedena ili pretvorba električne energije u oblik energije koji se može skladištiti, skladištenje takve energije i naknadna pretvorba takve energije u električnu energiju ili njezina uporaba kao nositelja energije . Pojmovi „*agregiranje*", „*upravljanje potrošnjom*" i „*skladištenje energije*" istovjetni su 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 ovoga Zakona znači distribucija toplinske energije u obliku pare, vruće vode ili pothlađenih tekućina iz centralnih ili decentraliziranih proizvodnih postrojenja putem centralnih i zatvorenih toplinskih sustava u više zgrada ili na više lokacija radi uporabe za zagrijavanje ili hlađenje prostora ili procesa. Pojam „*centralizirano grijanje ili centralizirano hlađenje"* istovjetan je pojmu iz članka 4. stavka 1. točke 4. Zakona o obnovljivim izvorima energije i visokoučinkovitoj kogeneraciji („Narodne novine", broj 138/21.), kojim je u hrvatsko zakonodavstvo preuzeta Direktiva 2018/2001 Europskog parlamenta i Vijeća od 11. prosinca 2018. o promicanju uporabe energije iz obnovljivih izvora (preinaka) (Tekst značajan za EGP) (SL L 328, 21. 12. 2018.).

	(c) nafta	- operatori naftovoda
		- operatori proizvodnje nafte, rafinerija i tvornica nafte te njezina skladištenja i prijenosa
		- središnja tijela za zalihe Pojam *„središnje tijelo za zalihe“* u smislu ovoga Zakona znači Agencija za ugljikovodike, kao središnje tijelo u Republici Hrvatskoj za obvezne zalihe nafte i naftnih derivata, koja je jedinstveno tijelo ovlašteno formirati, održavati i prodavati obvezne zalihe. Pojam *„središnje tijelo za zalihe“* istovjetan je pojmu iz članka 3. stavka 2. točke 5. Zakona o tržištu nafte i naftnih derivata („Narodne novine“, broj 138/21.), kojim je u hrvatsko zakonodavstvo preuzeta Direktiva 2009/119/EZ Europskog parlamenta i Vijeća od 14. rujna 2009. kojom se države članice obvezuju održavati minimalne zalihe sirove nafte i/ili naftnih derivata (SL L 265/9 od 9. 10. 2009.).
	(d) plin	- opskrbljivači plinom, uključujući opskrbljivače u obvezi javne usluge Pojam *„opskrbljivač plinom“* u smislu ovoga Zakona znači energetski subjekt koji obavlja energetsku djelatnost opskrbe plinom. Pojam *„opskrbljivač plinom u obvezi javne usluge“* u smislu ovoga Zakona znači opskrbljivač plinom koji obavlja energetsku djelatnost opskrbe u obvezi javne usluge. Pojam *„opskrba plinom“* u smislu ovoga Zakona znači prodaja ili preprodaja plina kupcu, uključujući prodaju ili preprodaju UPP-a i SPP-a. Pojam *„opskrba plinom u obvezi javne usluge“* u smislu ovoga Zakona znači opskrba plinom koja se u općem gospodarskom interesu obavlja po reguliranim uvjetima radi osiguravanja sigurnosti, redovitosti, kvalitete i cijene opskrbe kućanstava. Pojmovi *„opskrbljivač plinom“, „opskrbljivač plinom u obvezi javne usluge“*, *„opskrba plinom“* i *„opskrba plinom u obvezi javne usluge“* istovjetni su pojmovima iz članka 3. stavka 2. točaka 36., 37., 38. i 39. Zakona o tržištu plina („Narodne novine“, br. 18/18. i 23/20.), kojim je u hrvatsko zakonodavstvo preuzeta Direktiva 2009/73/EZ Europskog parlamenta i Vijeća od 13. srpnja 2009. o zajedničkim pravilima za unutarnje tržište prirodnog plina i stavljanju izvan snage Direktive 2003/55/EZ (Tekst značajan za EGP) (SL L 211, 14. 8. 2009.)

		- operatori distribucijskog sustava Pojam *„operator distribucijskog sustava“* u smislu ovoga Zakona znači energetski subjekt koji obavlja energetsku djelatnost distribucije plina i odgovoran je za rad, održavanje i razvoj distribucijskog sustava na svom distribucijskom području i, gdje je izvodivo, njegovo povezivanje s drugim sustavima te za osiguranje dugoročne sposobnosti sustava da zadovoljava razumne potrebe za distribucijom plina. Pojam *„distribucija plina“* u smislu ovoga Zakona znači razvod plina distribucijskim sustavom visoke, srednje i niske tlačne razine radi isporuke plina krajnjim kupcima, uključujući pomoćne usluge, a isključujući opskrbu plinom. Pojam *„distribucijski sustav“* u smislu ovoga Zakona znači sustav plinovoda i ostalih pripadajućih objekata i opreme koji su u vlasništvu 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 ovoga Zakona znači energetski subjekt koji obavlja energetsku djelatnost transporta plina i odgovoran je za rad, održavanje i razvoj transportnog sustava na određenom području i gdje je izvodivo, njegovo povezivanje s drugim sustavima te za osiguranje dugoročne sposobnosti sustava da zadovoljava razumne potrebe za transportom plina. Pojam *„transport plina“* u smislu ovoga Zakona znači prijenos plina kroz transportni sustav, isključujući opskrbu plinom i trgovinu plinom, a uključujući tranzit plina i pomoćne usluge. Pojam *„transportni sustav“* u smislu ovoga Zakona znači objekt koji je u vlasništvu i/ili kojim upravlja operator transportnog sustava, a koji čine sustav visokotlačnih plinovoda, kompresorske stanice, mjerne stanice, mjerno-redukcijske stanice, plinski čvorovi i ostali tehnološki objekti i oprema koji se koriste za transport plina, nadzor i upravljanje, mjerenje i prijenos podataka, isključujući mrežu proizvodnih plinovoda i visokotlačne distribucijske plinovode, uključujući plin

		za tehnološke kapacitete kojima se isključivo koristi operator transportnog sustava i operativnu akumulaciju. Pojmovi *„operator transportnog sustava“*, *„transport plina“* i *„transportni sustav“* istovjetni su 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 ovoga Zakona znači energetski subjekt koji obavlja energetsku djelatnost skladištenja plina i odgovoran je za rad, održavanje i razvoj sustava skladišta plina. Pojam *„skladištenje plina“* u smislu ovoga Zakona znači utiskivanje plina u sustav skladišta plina, skladištenje plina u radnom volumenu sustava skladišta plina i povlačenje plina iz sustava skladišta plina, uključujući pomoćne usluge. Pojmovi *„operator sustava skladišta plina“* i *„skladištenje plina“* istovjetni su 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 ovoga Zakona znači energetski subjekt koji obavlja energetsku djelatnost upravljanja terminalom za UPP i odgovoran je za rad, održavanje i razvoj terminala za UPP. Pojam *„terminal za UPP“* u smislu ovoga Zakona znači terminal koji se koristi za ukapljivanje prirodnog plina ili prihvat, iskrcaj i ponovno uplinjavanje UPP-a, uključujući pomoćne usluge i privremeno skladištenje potrebno za postupak ponovnog uplinjavanja i daljnju otpremu u transportni sustav, ali isključujući dijelove terminala za UPP koji se koriste za skladištenje. Pojmovi *„operator terminala za UPP“* i *„terminal za UPP“* istovjetni su 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 ovoga 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. 300/2008 Europskog parlamenta i Vijeća od 11. ožujka 2008. o zajedničkim pravilima u području zaštite civilnog zračnog prometa i stavljanju izvan snage Uredbe (EZ) br. 2320/2002 (Tekst značajan za EGP), koji se upotrebljavaju u komercijalne svrhe
		- upravna tijela zračne luke, zračne luke, uključujući osnovne zračne luke navedene u odjeljku 2. Priloga II. 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 lukama Pojam *"upravno tijelo zračne luke"* u smislu ovoga 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 ovoga Zakona znači svaka površina koja je posebno prilagođena za slijetanje, uzlijetanje i manevriranje zrakoplova, uključujući i pripadajuće objekte, sredstva i uređaje namijenjene za odvijanje zračnog prometa i pružanje usluga, te objekte, sredstva i uređaje za pomoć u pružanju usluga komercijalnog zračnog prijevoza. Pojmovi *"upravno tijelo zračne luke"* i *"zračna luka"* istovjetni su 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 ovoga Zakona znači pravna osoba ili u vertikalno integriranom trgovačkom društvu organizacijska jedinica odgovorna za upravljanje, održavanje i obnovu željezničke infrastrukture, kao i za sudjelovanje u razvoju željezničke infrastrukture na način koji je određen u okviru opće politike razvoja i financiranja željezničke infrastrukture Republike Hrvatske. Pojam *„upravitelj infrastrukture“* istovjetan je pojmu iz članka 5. stavka 1. točke 36. Zakona o željeznici („Narodne novine“, br. 32/19., 20/21. i 114/22.), kojim je u hrvatsko zakonodavstvo preuzeta Direktiva 2012/34/EU Europskog parlamenta i Vijeća od 21. studenoga 2012. o uspostavi jedinstvenog Europskog željezničkog prostora (preinačena) (SL L 343, 14. 12. 2012.), kako je posljednji put izmijenjena Direktivom (EU) 2016/2370 Europskog parlamenta i Vijeća od 14. prosinca 2016. o izmjeni Direktive 2012/34/EU u pogledu otvaranja tržišta za usluge domaćeg željezničkog prijevoza putnika i upravljanja željezničkom infrastrukturom (Tekst značajan za EGP) (SL L 352, 23. 12. 2016.).
		- željeznički prijevoznici, među ostalim i operatori uslužnih objekata Pojam *„željeznički prijevoznik“* u smislu ovoga Zakona znači svaka pravna osoba koja ima dozvolu za obavljanje usluga željezničkog prijevoza i čija je glavna djelatnost pružanje usluga željezničkog prijevoza putnika i/ili tereta, uz uvjet da ta pravna osoba osigura vuču vlakova; to uključuje i pravnu osobu koja pruža samo uslugu vuče vlakova. Pojam *„operator uslužnih objekata“* u smislu ovoga Zakona znači pravna osoba odgovorna za upravljanje jednim ili 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 lukama Pojam *„luka“* u smislu ovoga 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“, br. 32/19., 108/17. i 30/21.), kojim je u hrvatsko zakonodavstvo preuzeta Direktiva 2005/65/EZ Europskog parlamenta i Vijeća od 26. listopada 2005. o jačanju sigurnosne zaštite luka (Tekst značajan za EGP) (SL L 320, 25. 11. 2005.).
		- služba za nadzor i upravljanje pomorskim prometom (VTS) kako je definirana u članku 75.a stavku 1. i članku 75.b stavku 1. Pomorskog zakonika („Narodne novine“, br. 181/04., 76/07., 146/08., 61/11., 56/13., 26/15. i 17/19.) kojim je u hrvatsko zakonodavstvo preuzeta Direktiva 2002/59/EZ Europskog parlamenta i Vijeća od 27. lipnja 2002. o uspostavi sustava nadzora plovidbe i informacijskog sustava Zajednice i stavljanju izvan snage Direktive Vijeća 93/75/EEZ
	(d)cestovni promet	- tijela nadležna za ceste kako su definirana u članku 2. točki 12. Delegirane uredbe Komisije (EU) 2015/962 od 18. prosinca 2014. o dopuni Direktive 2010/40/EU Europskog parlamenta i Vijeća u pogledu pružanja usluga prometnih informacija u cijeloj Europskoj uniji u realnom vremenu (Tekst značajan za EGP), odgovorna za kontrolu upravljanja prometom, osim javnih subjekata kojima upravljanje prometom ili rad inteligentnih prometnih sustava nisu ključni dio njihove opće djelatnosti

		Prema članku 2. točki 12. Delegirane uredbe Komisije (EU) 2015/962 pojam *„tijelo nadležno za ceste”* znači svako javno tijelo koje je nadležno za planiranje, nadzor ili upravljanje cestama u okviru svoje mjesne nadležnosti.
		- operatori inteligentnih prometnih sustava Pojam *„inteligentni prometni sustavi (ITS)“* u smislu ovoga Zakona znači informacijsko-komunikacijska nadgradnja klasičnog sustava cestovnog prometa, kojim se postiže znatno poboljšanje učinaka cjelokupnog prometnog sustava. ITS uključuje ceste, vozila i korisnike cesta, a primjenjuje se u upravljanju prometom, upravljanju mobilnosti, upravljanju prometnim incidentima te za veze s ostalim vrstama prijevoza. Pojam *„inteligentni prometni sustavi (ITS)“* istovjetan je pojmu iz članka 72. stavka 1. Zakona o cestama („Narodne novine“, br. 84/11., 22/13., 54/13., 148/13., 92/14., 110/19., 144/21., 114/22. i 04/23.), kojim je u hrvatsko zakonodavstvo preuzeta Direktiva 2010/40/EZ Europskog parlamenta i Vijeća od 7. srpnja 2010. o okviru za uvođenje inteligentnih transportnih sustava u cestovnom prometu i za veze s ostalim vrstama prijevoza (Tekst značajan za EGP) (SL L 207 od 6. kolovoza 2010.).
3. Bankarstvo		- kreditne institucije kako su definirane u članku 4. točki 1. Uredbe (EU) br. 575/2013 Europskog parlamenta i Vijeća od 26. lipnja 2013. o bonitetnim zahtjevima za kreditne institucije i investicijska društva i o izmjeni Uredbe (EU) br. 648/2012 (Tekst značajan za EGP)
4. Infrastruktura financijskog tržišta		- operatori mjesta trgovanja Pojam *„mjesta trgovanja“* u smislu ovoga Zakona znači uređeno tržište, MTP ili OTP. Pojam *„multilateralna trgovinska platforma ili MTP“* u smislu ovoga Zakona znači multilateralni sustav kojim upravlja investicijsko društvo ili tržišni operater, koji u sustavu i prema unaprijed poznatim i nediskrecijskim pravilima spaja ili omogućuje spajanje ponuda za kupnju i ponuda za prodaju financijskih instrumentima trećih tako da nastaje ugovor u skladu s odredbama dijela drugoga glave III. poglavlja VII. Zakona o tržištu kapitala („Narodne novine“, br. 65/18., 17/20. i 83/21.). Pojam „*organizirana trgovinska platforma* ili OTP“ u smislu ovoga Zakona znači multilateralni sustav, koji

		nije uređeno tržište ili MTP, koji omogućuje da se u tom sustavu susretnu ponude za kupnju i ponude za prodaju obveznica, strukturiranih financijskih proizvoda, emisijskih jedinica ili izvedenica više zainteresiranih trećih strana tako da nastaje ugovor u skladu s odredbama dijela drugoga glave III. poglavlja VII. Zakona o tržištu kapitala. 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 ovoga 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 ovoga Zakona znači: - svaka tvar ili kombinacija tvari prikazana sa svojstvima liječenja ili sprječavanja bolesti kod ljudi ili

		- svaka tvar ili kombinacija tvari koja se može upotrijebiti ili primijeniti na ljudima u svrhu obnavljanja, ispravljanja ili prilagodbe fizioloških funkcija farmakološkim, imunološkim ili metaboličkim djelovanjem ili za postavljanje medicinske dijagnoze. Pojam *„lijek“* istovjetan je 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 proizvoda Pojam *„voda namijenjena za ljudsku potrošnju“* u smislu ovoga Zakona znači: - sva voda, bilo u njezinu izvornom stanju ili nakon obrade, koja je namijenjena za piće, kuhanje, pripremu hrane ili druge potrebe 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 30/23.), kojim je u hrvatsko zakonodavstvo

		preuzeta Direktiva (EU) 2020/2184 Europskog parlamenta i Vijeća od 16. prosinca 2020. o kvaliteti vode namijenjene za ljudsku potrošnju (preinaka) (Tekst značajan za EGP) (SL L 435, 23. 12. 2020.).
7.Otpadne vode		- poduzeća koja prikupljaju, odlažu ili pročišćavaju komunalne otpadne vode, sanitarne otpadne vode ili industrijske otpadne vode, isključujući poduzeća kojima prikupljanje, odlaganje ili pročišćavanje komunalnih otpadnih voda, otpadnih voda iz kućanstva ili industrijskih otpadnih voda nije ključni dio njihove općenite djelatnosti Pojam *„komunalne otpadne vode“* u smislu ovoga Zakona znači otpadne vode sustava javne odvodnje koje čine sanitarne otpadne vode ili otpadne vode koje su mješavina sanitarnih otpadnih voda s industrijskim otpadnim vodama i/ili oborinskim vodama određene aglomeracije. Pojam *„sanitarne otpadne vode“* u smislu ovoga Zakona znači otpadne vode koje se nakon korištenja ispuštaju iz stambenih objekata i uslužnih objekata te koje uglavnom potječu iz ljudskog metabolizma i aktivnosti kućanstava. Pojam „*industrijske otpadne vode*“ u smislu ovoga Zakona znači sve otpadne vode, osim sanitarnih otpadnih voda i oborinskih voda, koje se ispuštaju iz prostora korištenih za obavljanje trgovine ili industrijske djelatnosti. Pojmovi *„komunalne otpadne vode“*, *„sanitarne otpadne vode“* i *„industrijske otpadne vode“* istovjetni su pojmovima iz članka 4. stavka 1. točaka 25., 34. i 81. Zakona o vodama („Narodne novine“, br. 66/19., 84/21. i 47/23.), kojim je u hrvatsko zakonodavstvo preuzeta Direktiva Vijeća 91/271/EEZ od 21. svibnja 1991. o pročišćavanju komunalnih otpadnih voda (SL L 135, 30. 5. 1991.), dopunjena Direktivom Komisije 98/15/EZ od 27. veljače 1998. s obzirom na određene zahtjeve utvrđene u Dodatku I. (Tekst značajan za EGP) (SL L 67, 7. 3. 1998.).
8.Digitalna infrastruktura		- pružatelji središta za razmjenu internetskog prometa
		- pružatelji usluga DNS-a, osim operatora korijenskih poslužitelja naziva
		- registar naziva vršne nacionalne internetske domene
		- pružatelji usluga računalstva u oblaku
		- pružatelji usluga podatkovnog centra

		- pružatelji mreže za isporuku sadržaja
		- pružatelji usluga povjerenja
		- pružatelji javnih elektroničkih komunikacijskih mreža
		- pružatelji javno dostupnih elektroničkih komunikacijskih usluga
9.Upravljanje uslugama IKT-a (B2B)		- pružatelji upravljanih usluga
		- pružatelji upravljanih sigurnosnih usluga
		- informacijski posrednici kako su definirani propisom kojim se uređuje razmjena elektroničkog računa između poduzetnika
10. Javni sektor		- tijela državne uprave
		- druga državna tijela i pravne osobe s javnim ovlastima
		- privatni i javni subjekti koji upravljaju, razvijaju ili održavaju državnu informacijsku infrastrukturu sukladno zakonu 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 usluga Pojam „*davatelj poštanskih usluga*“ u smislu ovoga Zakona znači pravna ili fizička osoba koja obavlja poštanske usluge, uključujući „*davatelja univerzalne usluge*“ kao davatelja poštanskih usluga koji obavlja univerzalnu uslugu u Republici Hrvatskoj. Pojam „*poštanska usluga*“ u smislu ovoga Zakona znači usluga koja uključuje svako postupanje s poštanskim pošiljkama od strane davatelja poštanskih usluga, a osobito prijam, usmjeravanje, prijenos i uručenje poštanskih pošiljaka u unutarnjem ili međunarodnom poštanskom prometu. „*Poštanska*

		usluga" ne uključuje prijenos pošiljke primatelju koji pošiljatelj obavlja sam (samodostava), prijevoz kao samostalnu uslugu te prijam, prijenos i uručenje poštanskih pošiljaka izravno od pošiljatelja do primatelja po individualnom zahtjevu, bez usmjeravanja, na način da isti radnik davatelja usluga obavlja sve navedene radnje (kurirska usluga). Pojam „*univerzalna usluga*" u smislu ovoga Zakona znači skup poštanskih usluga određene kakvoće, koje su dostupne po pristupačnoj cijeni svim korisnicima poštanskih usluga na cijelom području Republike Hrvatske, neovisno o njihovoj zemljopisnoj lokaciji. Pojmovi „*davatelj poštanskih usluga*", „*davatelj univerzalne usluge*", „*poštanska usluga*" i „*univerzalna usluga*" istovjetni su pojmovima iz članka 2. stavka 1. točkama 4., 5., 21. i 32. Zakona o poštanskim uslugama („Narodne novine", br. 144/12., 153/13., 78/15. i 110/19.), kojim je u hrvatsko zakonodavstvo preuzeta Direktiva (EU) 97/67/EZ Europskog parlamenta i Vijeća od 15. prosinca 1997. o zajedničkim pravilima za razvoj unutarnjeg tržišta poštanskih usluga u Zajednici i poboljšanje kvalitete usluga (SL L 15, 21. 1. 1998.).
		- pružatelji kurirskih usluga
2. Gospodarenje otpadom		- subjekti koji se bave gospodarenjem otpadom, isključujući subjekte kojima gospodarenje otpadom nije glavna gospodarska djelatnost Pojam „*gospodarenje otpadom*" u smislu ovoga Zakona znači djelatnosti 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 ovoga Zakona znači svaka tvar ili predmet koje posjednik odbacuje, namjerava ili mora odbaciti. Pojam „*djelatnost sakupljanja otpada"* u smislu ovoga Zakona znači djelatnost koja uključuje postupak sakupljanja otpada i postupak sakupljanja otpada u reciklažno dvorište. Pojam „*djelatnost prijevoza otpada"* u smislu ovoga Zakona znači prijevoz otpada za vlastite potrebe ili za potrebe drugih na teritoriju Republike Hrvatske.

		Pojam „*djelatnost oporabe otpada“* u smislu ovoga Zakona znači djelatnost koja uključuje obavljanje postupka oporabe iz Popisa postupaka oporabe otpada. Pojam „*tehnološki procesi gospodarenja otpadom“* u smislu ovoga Zakona znači određene funkcionalno-tehnološke cjeline gospodarenja otpadom kojima se opisuje materijalni tok otpada, a uključuju prikupljanje, prihvat, skladištenje, prethodno razvrstavanje i razvrstavanje, miješanje otpada, pakiranje, popravak, čišćenje, provjera budućeg proizvoda i drugi procesi u sklopu postupka oporabe i zbrinjavanja otpada. Pojam „*djelatnost zbrinjavanja otpada“* u smislu ovoga Zakona znači djelatnost koja uključuje obavljanje postupka zbrinjavanja otpada iz Popisa postupaka zbrinjavanja otpada. Pojam „*trgovac otpadom“* u smislu ovoga Zakona znači pravna ili fizička osoba - obrtnik koja u svoje ime i za svoj račun kupuje i prodaje otpad, uključujući trgovca otpadom koji ne preuzima otpad u neposredni posjed. Pojam „*posrednik“* u smislu ovoga Zakona znači pravna ili fizička osoba - obrtnik koja obavlja djelatnost posredovanja u gospodarenju otpadom, uključujući i posrednika koji ne preuzima otpad u neposredni posjed. Pojmovi „*gospodarenje otpadom*“, „*otpad“, „djelatnost 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 84/21.), 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 ovoga Zakona. Prilog I. točka 5. peta alineja ovoga Zakona upućuje na *„subjekte koji proizvode medicinske proizvode koji se smatraju ključnima tijekom izvanrednog stanja u području javnog zdravlja“* odnosno na „*popis ključnih medicinskih proizvoda u slučaju izvanrednog stanja u području javnog zdravlja”* u smislu članka 22. Uredbe (EU) 2022/123.
	(b) proizvodnja računala te elektroničkih i optičkih proizvoda	- subjekti koji obavljaju bilo koju od gospodarskih djelatnosti iz područja C odjeljka 26. Nacionalne klasifikacije djelatnosti 2007. – NKD 2007.

	(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 Vodeni Cestovni	Svi	Središnje državno tijelo za kibernetičku sigurnost	-	Nacionalni centar za kibernetičku sigurnost
4.	Bankarstvo	-	Svi	-	Hrvatska narodna banka	Nacionalni CERT
5.	Infrastruktura financijskog tržišta	-	Svi	-	Hrvatska agencija za nadzor financijskih usluga	Nacionalni CERT
6.	Zdravstvo	-	Svi	Središnje državno tijelo za kibernetičku sigurnost	-	Nacionalni centar za kibernetičku sigurnost
7.	Voda za ljudsku potrošnju	-	Svi	Središnje državno tijelo za kibernetičku sigurnost	-	Nacionalni centar za kibernetičku sigurnost
8.	Otpadne vode	-	Svi	Središnje državno tijelo za kibernetičku sigurnost	-	Nacionalni centar za kibernetičku sigurnost
9.	Digitalna infrastruktura	-	Pružatelji usluga povjerenja	Tijelo državne uprave nadležno za razvoj digitalnog društva	-	Nacionalni centar za kibernetičku sigurnost

10.	Digitalna infrastruktura	-	Pružatelji javnih elektroničkih komunikacijskih mreža Pružatelji javno dostupnih elektroničkih komunikacijskih usluga	Hrvatska regulatorna agencija za mrežne djelatnosti	-	Nacionalni centar za kibernetičku sigurnost
11.	Digitalna infrastruktura	-	Pružatelji središta za razmjenu internetskog prometa Pružatelji usluga DNS-a, osim operatora korijenskih poslužitelja naziva Pružatelji usluga računalstva u oblaku Pružatelji usluga podatkovnog centra Pružatelji mreže za isporuku sadržaja	Središnje državno tijelo za kibernetičku sigurnost	-	Nacionalni centar za kibernetičku sigurnost
12.	Digitalna infrastruktura	-	Registar naziva vršne nacionalne internetske domene	Tijelo državne uprave nadležno za znanost i obrazovanje	-	Nacionalni CERT

13.	Upravljanje uslugama IKT-a (B2B)	-	Svi	Središnje državno tijelo za kibernetičku sigurnost	-	Nacionalni centar za kibernetičku sigurnost
14.	Javni sektor	-	Svi	Središnje državno tijelo za informacijsku sigurnost	-	Nacionalni centar za kibernetičku sigurnost
15.	Svemir	-	Svi	Središnje državno tijelo za kibernetičku sigurnost	-	Nacionalni centar za kibernetičku sigurnost
16.	Poštanske i kurirske usluge	-	Svi	Središnje državno tijelo za kibernetičku sigurnost	-	Nacionalni centar za kibernetičku sigurnost
17.	Gospodarenje otpadom	-	Svi	Središnje državno tijelo za kibernetičku sigurnost	-	Nacionalni centar za kibernetičku sigurnost
18.	Izrada, proizvodnja i distribucija kemikalija	-	Svi	Središnje državno tijelo za kibernetičku sigurnost	-	Nacionalni centar za kibernetičku sigurnost
19.	Proizvodnja, prerada i distribucija hrane	-	Svi	Središnje državno tijelo za kibernetičku sigurnost	-	Nacionalni centar za kibernetičku sigurnost
20.	Proizvodnja	Proizvodnja medicinskih proizvoda i in vitro dijagnostič-kih medicinskih proizvoda Proizvodnja računala te elektroničkih i optičkih proizvoda Proizvodnja električne opreme	Svi	Središnje državno tijelo za kibernetičku sigurnost	-	Nacionalni centar za kibernetičku sigurnost

		Proizvodnja strojeva i uređaja, d. n. Proizvodnja motornih vozila, prikolica i poluprikolica Proizvodnja ostale opreme za prijevoz				
21.	Pružatelji digitalnih usluga	-	Svi	Središnje državno tijelo za kibernetičku sigurnost	-	Nacionalni centar za kibernetičku sigurnost
22.	Istraživanje	-	Svi	Tijelo državne uprave nadležno za znanost i obrazovanje	-	Nacionalni CERT
23.	Sustav obrazovanja	-	Svi	Tijelo državne uprave nadležno za znanost i obrazovanje	-	Nacionalni CERT

PRILOG IV.

Obvezni sadržaj nacionalnog akta strateškog planiranja iz područja kibernetičke sigurnosti

I.

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

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

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

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

- mehanizam za utvrđivanje relevantne imovine i procjenu kibernetičkih rizika

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

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

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

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

II.

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

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

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

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

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

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

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

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

- koje uključuju relevantne postupke i odgovarajuće alate za razmjenu informacija 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 ovoga 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 ovoga 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 ovoga Zakona uspostavljanje sustava upravljanja kibernetičkom sigurnošću koji će osigurati djelotvornu provedbu postupaka i mjera za postizanje visoke razine kibernetičke sigurnosti u sektorima od posebne važnosti za nesmetano obavljanje ključnih društvenih i gospodarskih aktivnosti i pravilno funkcioniranje unutarnjeg tržišta.

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 ovoga 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. ovoga 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. ovoga 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 ovoga 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 ovoga Zakona.

Uz članak 5.

Ovim se člankom uređuje odnos ovoga Zakona prema posebnim propisima o zaštiti tajnosti i povjerljivosti podataka, odnosno utvrđuje se da ako u provedbi ovoga 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 ovoga 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 ovoga Zakona ne utječe na obveze ključnih i važnih subjekata da u slučaju povrede osobnih podataka postupaju sukladno odredbama članaka 33. i 34. Uredbe (EU) 2016/679. 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 ovoga Zakona prema zakonu koji uređuje područje elektroničkih komunikacija. Primjena odredaba ovoga Zakona ne utječe na obvezu provedbe temeljnih zahtjeva za 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 ovoga 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. ovoga 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 ovoga 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 ovoga Zakona, posebno kod provedbe mjera upravljanja kibernetičkim sigurnosnim rizicima te obvezama obavještavanja o značajnim incidentima. Tijela koja su prema posebnim zakonima iz stavka 1. ovoga članka nadležna za sektor odnosno podsektor i/ili vrste subjekata iz Priloga I. i Priloga II. ovoga 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. ovoga 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“, br. 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 ovoga 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 ovoga 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 ovoga Zakona i provedbenog propisa o zahtjevima kibernetičke sigurnosti (uredba iz članka 24. ovoga 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 ovoga Zakona i provedbenog propisa o zahtjevima kibernetičke sigurnosti (uredba iz članka 24. ovoga Zakona) odnosno da više ne podliježu obvezama provedbe zahtjeva kibernetičke sigurnosti iz ovoga Zakona.

Uz članak 20.

Ovim se člankom propisuje obveza i rok u kojem su subjekti iz Priloga I. i Priloga II. ovoga 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. ovoga Zakona da nadležnim tijelima za provedbu zahtjeva kibernetičke sigurnosti redovito dostavljaju popise subjekata iz Priloga I. i Priloga II. ovoga 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. ovoga 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. ovoga 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. ovoga 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 ovoga 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 ovoga članka prenosi se članak 21. Direktive (EU) 2022/2555 te će se iste dodatno razraditi uredbom iz članka 24. ovoga 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 ovoga članka prenosi se članak 23. Direktive (EU) 2022/2555 te će se iste dodatno razraditi uredbom iz članka 24. ovoga 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 ovoga članka prenosi se članak 23. Direktive (EU) 2022/2555 te će se iste dodatno razraditi uredbom iz članka 24. ovoga 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 ovoga članka u skladu je s člancima 23. i 30. Direktive (EU) 2022/2555 te će se ista dodatno razraditi uredbom iz članka 24. ovoga 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 ovoga članka će se dodatno razraditi uredbom iz članka 24. ovoga Zakona.

Uz članak 35.

Ovim se člankom propisuje tko, kada i pod uvjetima obavještava javnost o značajnom incidentu koji je u tijeku. Odredba ovoga članka u skladu je s člankom 23. Direktive (EU) 2022/2555 te će se ista dodatno razraditi uredbom iz članka 24. ovoga 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 ovoga članka u skladu je s člankom 23. Direktive (EU) 2022/2555 te će se ista dodatno razraditi uredbom iz članka 24. ovoga 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 ovoga 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. ovoga 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. ovoga 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. ovoga 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 ovoga 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. ovoga 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. ovoga 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. ovoga 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“, br. 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. ovoga 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. ovoga 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. ovoga 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 ovoga 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 ovoga 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 ovoga 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“, br. 123/17. i 151/22.) te su odredbe ovoga 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 njegovoga 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 novoga 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. ovoga 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 ovoga Zakona i propisa donesenog na temelju ovoga 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 ovoga Zakona, a o provedenim samoocjenama sukladnosti izvještavaju središnje državno tijelo za kibernetičku sigurnost. Stavkom 2. ovoga 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. ovoga 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 ovoga 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 ovoga Zakona nad ključnim i važnim subjektima koji su na temelju članka 31. Uredbe (EU) 2022/2554 određeni kao ključna treća strana pružatelj IKT usluga.

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 ovoga 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 ovoga 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. ovoga Zakona kako je ona definirana u Priloga III. ovoga Zakona. Također, stavkom 2. ovoga 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. ovoga 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 ovoga 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. ovoga 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 ovoga 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 ovoga 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 ovoga 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. ovoga 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. ovoga Zakona, mogu zatražiti nadležno tijelo da privremeno suspendira ovlaštenje izdano ključnom subjektu za pružanje usluga ili obavljanje djelatnosti iz Priloga I. odnosno Priloga II. ovoga Zakona te zahtijevati od nadležnog tijela privremenu zabranu obavljanja upravljačkih dužnosti u ključnom subjektu fizičkim osobama iz članka 29. ovoga Zakona. Stavkom 2. utvrđuje se kako se privremene suspenzije i privremene zabrane iz stavka 1. ovoga članka primjenjuju samo dok ključni subjekt ne postupi sukladno izrečenim korektivnim mjerama iz članka 82. ovoga 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. ovoga Zakona odnosno podnošenju zahtjeva sukladno članku 84. ovoga 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. ovoga 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 ovoga Zakona, ako je nadziranom subjektu tijelo nadležno za zaštitu osobnih podataka za povrede osobnih podataka koje proizlaze iz istog postupanja subjekta izreklo upravnu novčanu kaznu sukladno Uredbi (EU) 2016/679. Ovim člankom posebno se ne propisuju isključenja prekršajne odgovornosti koja su člankom 62. Prekršajnog zakona („Narodne novine”, br. 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 ovoga Zakona i uredbe iz članka 24. ovoga 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. ovoga

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 ovoga Zakona i uredbe iz članka 24. ovoga 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 ovoga 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. ovoga 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 članke 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 ovoga 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 ovoga Zakona provodili mjere za postizanje visoke razine kibernetičke sigurnosti prema odredbama Zakona o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga („Narodne novine“, broj 64/18.) i Uredbe o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga („Narodne novine“, broj 68/18.), 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 ovoga 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 76/22.), 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 ovoga Zakona provodili sigurnosne zahtjeve u svrhu zaštite sigurnosti usluga povjerenja prema odredbama Uredbe (EU) br. 910/2014 o elektroničkoj identifikaciji i uslugama povjerenja za elektroničke transakcije na unutarnjem tržištu i stavljanju izvan snage Direktive 1999/93/EZ i Zakona o provedbi Uredbe (EU) br. 910/2014 Europskog parlamenta i Vijeća od 23. srpnja 2014. o elektroničkoj identifikaciji i uslugama povjerenja za elektroničke transakcije na unutarnjem tržištu i stavljanju izvan snage Direktive 1999/93/EZ („Narodne novine“, broj 62/17.), 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 ovoga Zakona koji se odnose na upravljanje podacima o registraciji naziva domena te provesti provjere iz članka 47. stavka 2. ovoga 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 64/18.) 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 76/22.), 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 posrednika u 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. ovoga Zakona u roku od godinu dana od dana stupanja na snagu ovoga 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. ovoga Zakona donijeti u roku od devet mjeseci od dana stupanja na snagu ovoga Zakona, prijedlog nacionalnog akta strateškog planiranja iz članka 55. ovoga Zakona u roku od 24 mjeseca od dana stupanja na snagu ovoga Zakona, nacionalni program upravljanja kibernetičkim krizama iz članka 56. ovoga Zakona u roku od tri mjeseca od dana stupanja na snagu ovoga Zakona, a Plana provedbe vježbi kibernetičke sigurnosti iz članka 58. ovoga Zakona u roku od 12 mjeseci od dana stupanja na snagu ovoga 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 79/07.), članak 41. Zakona o elektroničkim komunikacijama, Uredba o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga („Narodne novine“, broj 68/18.), Odluka o osnivanju Nacionalnog vijeća za kibernetičku sigurnost i Operativno-tehničke koordinacije za kibernetičku sigurnost („Narodne novine“, br. 61/16., 28/18., 110/18., 79/19. i 136/20.) 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.

Uz članak 116.

Ovim se člankom određuje stupanje na snagu ovoga Zakona.

Uz Prilog I.

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

Uz Prilog IV.

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

PRILOZI
- **Izvješće o provedenom savjetovanju sa zainteresiranom javnošću**
- **Izjava o usklađenosti prijedloga propisa s pravnom stečevinom Europske unije**
- **Usporedni prikaz podudaranja odredbi propisa Europske unije s prijedlogom propisa**

OBRAZAC IZVJEŠĆA O PROVEDENOM SAVJETOVANJU SA ZAINTERESIRANOM JAVNOŠĆU	
Naslov dokumenta	Savjetovanje o Nacrtu prijedloga zakona o kibernetičkoj sigurnosti
Stvaratelj dokumenta, tijelo koje provodi savjetovanje	Ministarstvo hrvatskih branitelja
Svrha dokumenta	Izvješće
Datum dokumenta	12.9.2023.
Verzija dokumenta	-
Vrsta dokumenta	Izvješće
Naziv nacrta zakona, drugog propisa ili akta	Nacrt prijedloga zakona o kibernetičkoj sigurnosti
Jedinstvena oznaka iz Plana donošenja zakona, drugih propisa i akata objavljenog na internetskim stranicama Vlade	-
Naziv tijela nadležnog za izradu nacrta	Ministarstvo hrvatskih branitelja u suradnji sa Sigurnosno-obavještajnom agencijom
Koji su predstavnici zainteresirane javnosti bili uključeni u postupak izrade odnosno u rad stručne radne skupine za izradu nacrta?	U prilogu.
Je li nacrt bio objavljen na internetskim stranicama ili na drugi odgovarajući način? Ako jest, kada je nacrt objavljen, na kojoj internetskoj stranici i koliko je vremena ostavljeno za savjetovanje? Ako nije, zašto?	Putem portala https://esavjetovanja.gov.hr provedeno je savjetovanje u trajanju od 17.7. do 16.8.2023.
Koji su predstavnici zainteresirane javnosti dostavili svoja očitovanja?	U prilogu.
ANALIZA DOSTAVLJENIH PRIMJEDBI Primjedbe koje su prihvaćene	U prilogu.

Primjedbe koje nisu prihvaćene i obrazloženje razloga za neprihvaćanje	
Troškovi provedenog savjetovanja	Provedba savjetovanja nije imala financijskih troškova

Izvješće o provedenom savjetovanju - Savjetovanje o Nacrtu prijedloga zakona o kibernetičkoj sigurnosti

Redni broj	Korisnik	Isječak	Komentar	Status odgovora	Odgovor
1	Ana Balaško	NACRT PRIJEDLOGA ZAKONA O KIBERNETIČKOJ SIGURNOSTI	Uz konkretne komentare koje sam ostavila pored pojedinih članaka prijedloga Zakona o kibernetičkoj sigurnosti (uspoređujući isti sa odredbama NIS2 Direktive (2022/2555)), izdvajam slijedeće primjedbe: • Opis i obuhvat Uredbe kao važnog provedbenog akta predmetnog Zakona nije jasno definiran, već se Uredba indirektno spominje u čl. 24., a potom se u drugim člancima poziva na čl.24. koji sam po sebi nije dovoljno jasan. • NIS2 čl.34 ne propisuje iznos (odnosno postotak godišnjeg prometa) najmanje novčane kazne, dok je u prijedlogu Zakon isto navedeno (čl. 101 i 102.). Metodologija određivanja istog? • U prijedlogu Zakona (čl.103) predviđene novčane kazne koje nisu propisane odredbama NIS2 Direktive • Osim novčanih kazni za pravne subjekte prijedlogom Zakona propisane su novčane kazne i za odgovorne osobe subjekata (čl.101. st.2,č.102.st.2 i čl.103.st2.) što NIS2 Direktivom nije određeno. • Prijedlogom Zakona zakonska obaveza proširena i na jedinice lokalne samouprave unutar sektora javne uprave (Prilog I. točka 10.) što je šire od NIS2 koji ide do regionalne razine (Prilog I. točka 10.), obuhvat na subjekte javne uprave na lokalnoj razini ostavljen samo kao opcija (NIS2 čl.2.st.5). Obuhvaćeno temeljem napravljene procjene rizika, ili ? • Prijedlogom Zakona zakonska obaveza proširena generalno na sustav obrazovanja (privatni i javni subjekti), neovisno o provođenju ključnih istraživačkih aktivnosti, što NIS 2 ostavlja samo kao opciju (NIS2 čl.2.st.5). Obuhvaćeno temeljem napravljene procjene rizika, ili ?	Primljeno na znanje	Opis i obuhvat Uredbe iz čl. 24. napravljen je u skladu s nomotehničkim pravilima te se zainteresirani mogu uputiti na aktualni Zakon i Uredbu o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga (NN 64 i 68 /2018) u kojima je primijenjen isti pristup u nešto užem opsegu NIS1 transpozicije. NIS direktiva se ne primjenjuje direktno već se transponira i usklađuje s nacionalnim zakonodavstvom u kojemu je nužno pratiti maksimalne iznose kazni definirane u NIS2 direktivi, ali i nacionalno odrediti raspone tih kazni odnosno utvrditi i minimalne iznose kazni. Navedeno je provedeno u skladu s nacionalnim pristupom definiranim Prekršajnim zakonom („Narodne novine“, broj: 107/07, 39/13, 157/13, 110/15, 70/17, 118/18 i 114/22) koji predstavlja opći propis kojim se propisuju odredbe koje se odnose na sve prekršaje propisane u drugim zakonima. Budući da je provedba kategorizacije subjekata elementarni postupak o kojem ovise brojni drugi važni aspekti provedbe zahtjeva NIS2 direktive odnosno slijedno i nacionalnog transpozicijskog zakona, člankom 103. utvrđuju se pravila o sankcijama kako bi se osigurala pravovremena i potpuna provedba postupaka kategorizacije odnosno utvrđivanja i ažuriranja popisa ključnih i važnih subjekata. Vezano uz mogućnost izricanja novčanih kazni odgovornim osobama subjekta, napominje se kako je člankom 32. stavkom 6. i člankom 33. stavkom 5. NIS2 direktive utvrđena obveza država članica osigurati da fizičke osobe koje su odgovorne za ključni i važni subjekt mogu smatrati odgovornim za kršenje svojih dužnosti da osiguraju usklađenost s NIS2 direktivom. Proces kategorizacije (procjena rizika) će odrediti subjekte obveznike na lokalnoj razini, dok je samo centralna razina uprave, odnosno tijela državne uprave, obuhvaćena u cijelosti, neovisno o veličini subjekata, upravo kako je to zahtijevano na razini NIS2

					direktive. NIS2 opcija uključenja obrazovnog sustava je prihvaćena nacionalno, u suradnji s nadležnim tijelima za obrazovni sektor, te uz pristup kroz provedbu procjene rizika u okviru procesa kategorizacije, što znači da se ne uključuju svi subjekti, već subjekti prema procjeni rizika koja će se provesti prilikom procesa kategorizacije.
2	Antonija Hinckel Osojnik	NACRT PRIJEDLOGA ZAKONA O KIBERNETIČKOJ SIGURNOSTI	"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." Ovaj rok je nerealan iz više razloga: 1. države članice poput Njemačke i Francuske s puno jačim kapacitetima ne postavljaju tako kratak rok 2. koje privatne tvrtke su uključene u implementaciju i prema kojem natječaju? 3. u slučaju da direktiva nije ispravno implementirana, tko je odgovoran, da li Ministarstvo branitelja? (iz ovog Zakona to nije razvidno) 4. donošenje podzakonskih akata je predvidjeno naknadno izvan tog roka, što implementaciju direktive čini posebno problematičnom zamale subjekte.	Primljeno na znanje	Ovaj rok (17.10.2024.) je definiran na razini EU i prihvatile su ga sve države članice. Rok podrazumijeva donošenje propisa i funkcionalnost nadležnih tijela dok se ostali procesi poput kategorizacije, provedbe mjera, revizije i nadzora pokreću postupno tijekom mjeseci i godina nakon donošenja Zakona, a prema rokovima u Prijelaznim i završnim odredbama Zakona. Provedba Zakona u dijelu ključnih i važnih subjekata provodit će se tek nakon kategorizacije subjekata, u Zakonom utvrđenim rokovima. Pri tome je svaki subjekt odgovoran za svoju vlastitu provedbu mjera na temelju vlastite procjene rizika i taj proces može provoditi samostalno ili uz angažiranje trećih strana. Privatne tvrtke se, između ostalog, planiraju uključiti kao autorizirana tijela za ocjenu sukladnosti (čl. 40). Formalni predlagatelj Zakona je član Vlade zadužen za nacionalnu sigurnost (danas potpredsjednik Vlade i ministar hrvatskih branitelja Tomo Medved), jednako kao što je to bio slučaj i prilikom NIS1 transpozicije 2018. godine. Stručno-administrativne poslove uobičajeno vodi ministarstvo člana Vlade zaduženog za nacionalnu sigurnost, a danas je to Ministarstvo hrvatskih branitelja. Nacionalno potvrđivanje sukladnosti s NIS2 direktivom u nadležnosti je Ministarstva vanjskih i europskih poslova. Donošenje podzakonskih akata predviđeno je u rokovima iz Zakona, a planira se prije 17.10.2024., jer se Zakon planira donijeti na prijelazu 2023. u 2024. godinu.
3	Diverto d.o.o.	NACRT PRIJEDLOGA ZAKONA O KIBERNETIČKOJ SIGURNOSTI	Zakon o kibernetičkoj sigurnosti je još jedan evolucijski korak u osiguravanju hrvatskog, a tako i europskog kibernetičkog prostora. Svakako treba pozdraviti ovakvu važnu inicijativu koja za cilj ima učinkovito upravljanje organizacijom i sigurnosnim procesima. Ovaj Zakon prepoznaje važnost upravljačkih organizacijskih kontrola, ali u manjoj mjeri ističe važnost kontinuiranog nadzora kontrola sigurnosti, preventivne zaštite IKT sustava i obranu od prijetnji u što bliže realnom vremenu.	Primljeno na znanje	Zakon predviđa tehničke, operativne i organizacijske mjere, utemeljene na procjeni rizika svakog pojedinog subjekta obveznika. Nezavisna kontrola usklađenosti je predviđena kroz revizije odnosno provedbu ocjena sukladnosti sa zahtjevima kibernetičke sigurnosti najmanje jednom u dvije godine (obavljaju autorizirane pravne osobe), a dodatno provodit će se i stručni nadzor nadležnog tijela za

			Dio sigurnosnih kontrola odnosno mjera koji mogu pomoći smo predložili kroz komentare na konkretne članke. S obzirom na ciljeve NIS 2 direktive, predlažemo da se gore navedeno propagira kroz ostale relevantne dijelove Zakona i daljnje podzakonske akte.		provedbu zahtjeva kibernetičke sigurnosti svakih tri do pet godina, ovisno o procjeni rizičnosti subjekta. Kontinuirana kontrola usklađenosti moguća je putem dobrovoljnih mjera kibernetičke zaštite definiranih u Zakonu (Nacionalni sustav za otkrivanje kibernetičkih prijetnji i zaštitu kibernetičkog prostora) i/ili putem korištenja pružatelja upravljanih sigurnosnih usluga iz Priloga I., točka 9.
4	Ivan Zidarević - Europska civilna inicijativa Zagreb	NACRT PRIJEDLOGA ZAKONA O KIBERNETIČKOJ SIGURNOSTI	Poštovani, Na internet stranicama Ministarstva hrvatskih branitelja navedeno je da je misija Ministarstva negovanje i čuvanje vrednosti odbrambenog i osloboditeljskog Domovinskog rata, ratnih stradalnika i svih građana Republike Hrvatske. Glavni ciljevi su zaštita interesa i digniteta svih učesnika Domovinskog rata i sprovođenje javnih politika radi osiguravanja adekvatne zdravstvene i socijalne zaštite hrvatskih branitelja i njihovih članova porodica. S tim u vezi postavlja se pitanje zašto predlagatelj ovog Zakona nije Ministarstvo unutarnjih poslova, koje ima više iskustva i adekvatnog kadra za bavljenje ovom izazovnom temom.	Primljeno na znanje	Formalni predlagatelj Zakona je član Vlade zadužen za nacionalnu sigurnost (danas potpredsjednik Vlade i ministar hrvatskih branitelja Tomo Medved), jednako kao što je to bio slučaj i prilikom NIS1 transpozicije 2018. godine. Stručno-administrativne poslove uobičajeno vodi ministarstvo člana Vlade zaduženog za nacionalnu sigurnost, a danas je to Ministarstvo hrvatskih branitelja. Nacrt prijedloga Zakona izrađen je na razini Nacionalnog vijeća za kibernetičku sigurnost koje je u tu svrhu uspostavilo međuresornu radnu skupinu u kojoj su bili aktivno uključeni predstavnici 15 državnih tijela i pravnih osoba s javnim ovlastima, a dodatno je u fazi usklađivanja uključen i niz drugih institucija.
5	Krešimir Kristić	NACRT PRIJEDLOGA ZAKONA O KIBERNETIČKOJ SIGURNOSTI	Meni se ovaj prijedlog čini dovoljno dobrim za usvajanje/donošenje Zakona. Zašto se uopće smatram relevantnim dati ovaj komentar? Od samoga početka važenja transponirane NIS direktive 2018. u ZKS, vodim i odgovoran sam za sukladnost poslovanja sa ZKS-om (NIS direktivom) dva od tri prva operatora ključnih usluga po ZKS-u. Pročitao sam ovaj prijedlog, sve 132 stranice i temeljem bogatoga iskustva u provedbi ZKS-a mislim da je prijedlog dobar, zaokružen, da je Zakon ovakav dobro definiran i što je najvažnije - da je provediv!	Primljeno na znanje	Provedivost Zakona, ali i promjena nacionalnog pristupa u odnosu na neke segmente koji nisu zadovoljavajuće provedeni rješenjima iz nacionalne transpozicije NIS1 direktive, bili su temelj izrade ovog Zakona.
6	Zoran Sambol	NACRT PRIJEDLOGA ZAKONA O KIBERNETIČKOJ SIGURNOSTI	Nacrt Prijedloga Zakona o kibernetičkoj sigurnosti valjalo je napraviti u suradnji s Ministarstvom znanosti i obrazovanja, Ministarstvom obrane i Ministarstvom unutarnjih poslova kako bi se dobio "sveobuhvatni pregled" problematike. Kibernetički izazovi ne mogu se promatrati u "manjem broju dimenzija".	Primljeno na znanje	Nacrt prijedloga Zakona izrađen je na razini Nacionalnog vijeća za kibernetičku sigurnost koje je u tu svrhu uspostavilo međuresornu radnu skupinu u kojoj su bili uključeni predstavnici 15 državnih tijela i pravnih osoba s javnim ovlastima, a dodatno je u fazi usklađivanja uključen i niz drugih institucija. Sva tri, u komentaru navedena ministarstva, sudjelovala su u pojedinim fazama izrade ovog Zakona.
7	ivo bakalić	NACRT PRIJEDLOGA ZAKONA O KIBERNETIČKOJ SIGURNOSTI , I. USTAVNA OSNOVA ZA DONOŠENJE ZAKONA	Ivo Bakalić Pridružujem se primjedbi da je prijedlog zakona po svom značaju trebao biti rezultat suradnje više ministarstava, prvenstveno MUP, Ministarstva znanosti, Ministarstva obrane, Ministarstva pravosuđa. U odnosu na Ministarstvo branitelja kao predlagatelja ne mogu pronaći poveznicu sa sadržajem zakona. Ivo Bakalić, sudac Trgovačkog suda u Splitu	Primljeno na znanje	Nacrt prijedloga Zakona izrađen je na razini Nacionalnog vijeća za kibernetičku sigurnost koje je u tu svrhu uspostavilo međuresornu radnu skupinu u kojoj su bili uključeni predstavnici 15 državnih tijela i pravnih osoba s javnim ovlastima, a dodatno je u fazi usklađivanja uključen i niz drugih institucija. Sva četiri, u komentaru navedena ministarstva, sudjelovala su u pojedinim fazama

					izrade ovog Zakona. Formalni predlagatelj Zakona je član Vlade zadužen za nacionalnu sigurnost (danas potpredsjednik Vlade i ministar hrvatskih branitelja Tomo Medved), jednako kao što je to bio slučaj i prilikom NIS1 transpozicije 2018. godine. Stručno-administrativne poslove uobičajeno vodi ministarstvo člana Vlade zaduženog za nacionalnu sigurnost, a danas je to Ministarstvo hrvatskih branitelja.
8	MARKO RAKAR	NACRT PRIJEDLOGA ZAKONA O KIBERNETIČKOJ SIGURNOSTI , IV. TEKST PRIJEDLOGA ZAKONA	NIS2 direktiva u svojoj preambuli (točka 15), upozorava na potrebi „osiguranja pravedne ravnoteže između zahtjeva i obveza utemeljenih na procjeni rizika s jedne strane te administrativnog opterećenja koje proizlazi iz nadzora usklađenosti s druge strane“. Nacrt zakona kakav je ovdje prezentiran ne predviđa, niti govori o osiguranju ravnoteže nego na istovjetni način kreira zahtjeve i obveze usklađenosti za sve subjekte, neovisno o njihovoj relativnoj veličini i/ili riziku – što će rezultirati nerazmjernim opterećenjem za niz subjekata, uključivo i za središnje državno tijelo koje će istim mjerilima morati promatrati sve zahvaćene subjekte. Nadalje, iako u se u NIS2 direktivi na više mjesta spominje potreba koordinacije različitih javnih tijela, u nacrtu zakona kakvog vidimo ovdje cjelokupna regulacija je svedena na središnje državno tijelo za kibernetičku sigurnost koje je smješteno u Sigurnosnu obavještajnu agenciju. Za razliku od ostalih sastavnica (nacionalne) sigurnosti koje često zahtijevaju različite razine tajnosti ili opskurnosti, kibernetička sigurnost je, po svojoj prirodi, osobito zbog svoje sveobuhvatnosti u cijelosti u javnoj sferi. Stoga smatram da je za središnje tijelo za kibernetičku sigurnost nužno imenovati ured ili agenciju koja je, poput Europske ENISA-e, u cijelosti civilna organizacija.	Ne prihvaća se	Subjekti obveznici Zakona dužni su provoditi mjere kibernetičke sigurnosti proporcionalno vlastitoj procjeni rizika, pri čemu trebaju razmatrati rizike u svim segmentima koje Zakon utvrđuje te koristiti neku od standardiziranih metoda za upravljanje rizikom. Na taj način postiže se primjena mjera koja je u potpunosti u skladu s procjenom rizika, a procjena rizika prati veličinu i vrstu subjekta, odnosno njegove poslovne karakteristike. Cijelo jedno poglavlje Zakona (Poglavlje II.), utvrđuje obveze suradnje nadležnih tijela na nacionalnoj razini. Kibernetička sigurnost je integralni dio nacionalne sigurnosti u svim članicama EU. Odabir središnjeg tijela, odnosno izgradnja nacionalnog centra za kibernetičku sigurnost, u svim državama provodi se na temelju tradicije razvoja i raspoloživih sposobnosti i resursa. U RH je sigurnosno-obavještajni sustav bio nositelj izrade Nacionalne strategije kibernetičke sigurnosti 2014. godine, NIS1 transpozicije 2018. godine, pa je kroz Nacionalno vijeće za kibernetičku sigurnost nastavljen isti pristup i sa NIS2 transpozicijom. Odabir SOA-e je rezultat već razvijenih kapaciteta te procjene da će se interni Centar za kibernetičku sigurnost SOA-e moći najbrže i najučinkovitije transformirati u nužno potrebni Nacionalni centar za kibernetičku sigurnost (NCSC). Ne postoji jednoobrazno rješenje oko osnivanja NCSC-a na razini EU i svaka članica osnivanje NCSC-a regulira temeljem vlastitih specifičnosti, potreba i već razvijenih kapaciteta, a veći broj članica EU je za osnivanje NCSC-a koristila sigurnosno-obavještajne sustave. Primjerice, u Danskoj, Španjolskoj, Grčkoj (članice EU), kao i Velikoj Britaniji, Kanadi, Južnoj Koreji i drugim razvijenim demokratskim

					državama, NCSC je dio sigurnosnih i obavještajnih sustava, dok su neke zemlje poput Njemačke i Italije proces osnivanja NCSC-a započele u okvirima sigurnosno-obavještajnog sustava (navedene dvije članice EU su naknadno provodile daljnju organizacijsku transformaciju NCSC tijela u samostalne agencije, ali su godinama njihova NCSC tijela funkcionirala unutar sigurnosno-obavještajnih sustava tih država). U Francuskoj se središnje tijelo za kibernetičku sigurnost (ANSSI) nalazi unutar sustava obrane i nacionalne sigurnosti te odgovara državnom tajniku za obranu i nacionalnu sigurnost. Dodatno napominjemo kako u onim državama, u kojima su nacionalni centri kibernetičke sigurnosti smješteni u ministarstvima, postoji zakonska obveza njihove uske suradnje i koordinacije sa sigurnosno-obavještajnim tijelima. Formalni predlagatelj Zakona je član Vlade zadužen za nacionalnu sigurnost (danas potpredsjednik Vlade i ministar hrvatskih branitelja Tomo Medved), jednako kao što je to bio slučaj i prilikom NIS1 transpozicije 2018. godine. Stručno-administrativne poslove uobičajeno vodi ministarstvo člana Vlade zaduženog za nacionalnu sigurnost, a danas je to Ministarstvo hrvatskih branitelja. Nacrt prijedloga Zakona izrađen je na razini Nacionalnog vijeća za kibernetičku sigurnost koje je u tu svrhu uspostavilo internu međuresornu radnu skupinu u kojoj su bili uključeni predstavnici 15 državnih tijela i pravnih osoba s javnim ovlastima, a dodatno je u fazi usklađivanja Nacrta zakona uključen i niz drugih institucija. Radna skupina nije formalno imenovana donošenjem posebne odluke, već je radila pod ingerencijama Nacionalnog vijeća za kibernetičku sigurnost i redovito izvještavala Vijeće o napretku. Izvješća o radu Nacionalnog vijeća za kibernetičku sigurnost s popisom uključenih institucija i članova Vijeća dostupna su na sljedećoj poveznici: https://www.uvns.hr/hr/informacijska-sigurnost/kiberneticka-sigurnost
			Kao i drugi sudionici savjetovanja, upozorio bi i na nelogičnost Ministarstva hrvatskih branitelja kao predlagača (u smislu da ne posjeduje kadrove koji su kompetentni za izradu ovakvog nacrta zakona, kao i činjenicu da je ovaj zakon sasvim očigledno izvan djelokruga djelovanja ministarstva kako je ono definirano u Zakonu o ustrojstvu i djelokrugu tijela državne uprave, članak 19.), te činjenice da je predlagač prekšio Zakon o pravu na pristup informacijama članak 11. stavak 2. samom činjenicom da nije objavio sastav radne skupine odnosno autore nacrta prijedloga zakonskog teksta.		
9	Zoran Sambol	IV. TEKST PRIJEDLOGA ZAKONA, Članak 1.	Stavak (1) Nedostaje definicija "visoke zajedničke razine kibernetičke sigurnosti". Koja je metrika, tko je određuje i tko bira procjenitelje metrike "razine kibernetičke sigurnosti"?	Primljeno na znanje	NIS2 direktiva predstavlja „metriku“ visoke zajedničke razine kibernetičke sigurnosti, usuglašenu na razini EU i 27 država članica. U tu svrhu sve države članice transponiraju NIS2 direktivu te preko zajedničke baze podataka, u organizaciji nadležnih ministarstava vanjskih poslova, dokazuju sukladnost, koju u konačnici provjerava Europska komisija.

10	Hrvatska udruga menadžera sigurnosti (HUMS)	IV. TEKST PRIJEDLOGA ZAKONA, Članak 4.	Točka 31. predlažemo da se ne naglašavaju primjeri jer isti isključuju neke druge jednakovažne primjere osobnih podataka, odnosno, stavlja se naglasak na neke primjere koji nisu temeljeni na bilo kojoj analizi rizika ili praksi. Također, dio vezan za IP može biti krivo interpretiran. S tim u vezi, predlažemo da točka 31. glasi: "„ 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)."	Ne prihvaća se	Intencija predlagatelja Zakona bila je ukazati na to da je korištenje osobnih podataka u okviru ovog Zakona izuzetak, a ne pravilo. Stoga je GDPR definicija prilagođena konkretnim slučajevima iz područja primjene ovog Zakona.
11	Hrvatska udruga menadžera sigurnosti (HUMS)	IV. TEKST PRIJEDLOGA ZAKONA, Članak 4.	Predlažemo da se, gdjegod je to moguće i kad se ne radi o direktnoj transpoziciji definicije iz Direktive (EU) 2022/2555, odnosno kad nadogradnja definicije ne bi bila u sukobu s Direktivom, definicija pojmova što je moguće detaljnije razloži. Naime, iz sigurnosne je prakse poznato da do čestih nerazumijevanja i grešaka dolazi upravo radi primjene različitih metodologija i/ili standarda koje se vežu iz različite pojmove. S tim u vezi, naglašavamo važnost pojmova vezanih za sigurnost, usluge, incidente i upravljanje incidentima, te rizike i ranjivosti.	Ne prihvaća se	Člankom 4. Prijedloga zakona preuzimaju se odredbe članka 6. NIS2 direktive, pa tako i u dijelu koji se odnosi na pojmove vezane za sigurnost, usluge, incidente i upravljanje incidentima, te rizike i ranjivosti. Definicije pojmova iz članka 6. NIS2 direktive potrebno je u potpunosti ispravno preuzeti, što znači da je odredbe uredbi EU zabranjeno prepisivati u nacionalne propise, a pojmove iz direktiva EU potrebno je preuzeti u tekstu kakav je sadržan u dotičnoj direktivi odnosno u transpozicijskom propisu kojim su dotična direktiva i pojam preuzeti u nacionalno zakonodavstvo.
12	A1 Hrvatska d.o.o.	IV. TEKST PRIJEDLOGA ZAKONA, Članak 4.	Čl.4.st.1.t.16. umjesto riječi informacija potrebno koristiti riječ podataka s obzirom na čl.5.st.1.t.27 Zakona o elektroničkim komunikacijama, a sve u svrhu usklađivanja sektorski specifičnih definicija.	Prihvaća se	
13	HGK	IV. TEKST PRIJEDLOGA ZAKONA, Članak 4.	U skladu s čl. 4. st.1 toč. 17. Nacrta, Hrvatska gospodarska komora potpada pod javne subjekte jer je nositelj pojedinih javnih ovlasti koje obavlja u okviru svoje službene dužnosti. S obzirom na nedostupnost određenih informacija o pojedinim fizičkim, odnosno pravnim osobama te trošak izvještavanja naglašavamo da se HGK smatra obveznom izvještavati isključivo taksativno navedena tijela u točki 28. ovoga članka, pri čemu predlažemo da se dodatno precizira o kojim se tijelima radi.	Ne prihvaća se	Pretpostavljamo da se komentar odnosi na čl. 21. Zakona te upućujemo na Prilog III., u kojem su popisana sva tijela nadležna za provedbu zahtjeva kibernetičke sigurnosti, kao i sektori za koja su nadležni.
14	Porobija & Špoljarić d.o.o.	IV. TEKST PRIJEDLOGA ZAKONA, Članak 4.	Smatramo određivanjem SOA-e kao središnjeg državnog tijela za područje kibernetičke sigurnosti, odnosno, de facto određivanjem kao regulatornog tijela koje nadzire primjenu ZKS, te koji ujedno provodi neposredni nadzor na adresatima nepogodnim budući da bi se time potencijalno kompromitiralo opće djelovanje SOA-e kao središnjeg i ključnog obavještajnog tijela Republike Hrvatske, dok bi se istovremeno od strane reguliranih subjekata, ali i drugih nadzornih tijela država članica EU, mogla proizvesti nevoljkost i otpor suradnji i dijeljenju informacija, čime bi se potencijalno smanjila efikasnost primjene ZKS, kao i opće smanjenje razine kibernetičke sigurnosti. SOA je Zakonom o sigurnosno-obavještajnom sustavu Republike Hrvatske određena kao jedno od ključnih obavještajnih tijela za zaštitu nacionalne sigurnosti Republike Hrvatske i nacionalnih interesa Republike Hrvatske. Bez obzira na bilo kakve druge ovlasti koje bi SOA-i bila dodijeljena, centralna svrha i cilj djelovanja	Ne prihvaća se	Kibernetička sigurnost je integralni dio nacionalne sigurnosti u svim članicama EU. Odabir središnjeg tijela, odnosno izgradnja nacionalnog centra za kibernetičku sigurnost, u svim državama se provodi na temelju tradicije razvoja i raspoloživih sposobnosti i resursa. U RH je sigurnosno-obavještajni sustav bio nositelj izrade Nacionalne strategije kibernetičke sigurnosti 2014. godine, NIS1 transpozicije 2018. godine, pa je kroz Nacionalno vijeće za kibernetičku sigurnost nastavljen isti pristup i sa NIS2 transpozicijom. Odabir SOA-e je rezultat procjene da će se interni Centar za kibernetičku sigurnost SOA-e moći najbrže i najučinkovitije transformirati u nužno potrebni Nacionalni centar za kibernetičku

			SOA-e je uvijek i bez iznimke zaštita nacionalne sigurnosti Republike Hrvatske, dok je centralni interes koji se štiti prije svih interes Republike Hrvatske. S druge strane tijela-regulatori, bez obzira na polje koje se regulira, kao primarnu svrhu imaju osiguravanje provođenja propisa koji uređuju pojedino polje te ostvarenje šire svrhe i ciljeva koji su određeni propisima koji uređuju djelovanje regulatora. Navedeni se cilj se postiže kroz izravnu suradnju sa reguliranim subjektima, što vrlo često podrazumijeva i određenu dozu povjerenja i transparentnosti u međusobnom odnosu. SOA bi se kao regulatorno tijelo moglo naći u vrlo nezavidnoj situaciji, tj. sukobu interesa da mora birati između interesa subjekata koje regulira i povjerljivosti informacija koje postanu dostupne prilikom provođenja regulatornih ovlasti s jedne strane i prikupljanja, analize i korištenja istih povjerljivih informacija ako bi takve informacije potencijalno predstavljale informacije koje bi mogle koristiti u svrhu zaštite interesa Republike		sigurnost (NCSC). Ne postoji jednoobrazno rješenje oko osnivanja NCSC-a na razini EU i svaka članica osnivanje NCSC-a regulira temeljem vlastitih specifičnosti, potreba i već razvijenih kapaciteta, a veći broj članica EU je za osnivanje NCSC-a koristila sigurnosno-obavještajne sustave. Primjerice, u Danskoj, Španjolskoj, Grčkoj (članice EU), kao i Velikoj Britaniji, Kanadi, Južnoj Koreji i drugim razvijenim državama, NCSC je dio sigurnosnih i obavještajnih sustava, dok su neke zemlje poput Njemačke i Italije proces osnivanja NCSC-a započele u okvirima sigurnosno-obavještajnog sustava (navedene dvije članice EU su naknadno provodile daljnju organizacijsku transformaciju NCSC tijela u samostalne agencije, ali su godinama njihova NCSC tijela funkcionirala unutar sigurnosno-obavještajnih sustava tih država). U Francuskoj se središnje tijelo za kibernetičku sigurnost (ANSSI) nalazi unutar sustava obrane i nacionalne sigurnosti te odgovara državnom tajniku za obranu i nacionalnu sigurnost. Dodatno napominjemo kako u onim državama, u kojima su nacionalni centri kibernetičke sigurnosti smješteni u ministarstvima, postoji zakonska obveza njihove uske suradnje i koordinacije sa sigurnosno-obavještajnim tijelima. Tijela-regulatori kako su opisana u komentaru predstavljaju regulatore pojedinih vertikalnih sektora kao što su to primjerice sektori telekomunikacija ili bankarstva. NIS2 direktiva, jednako kao ni ovaj Zakon, ne bave se reguliranjem vertikalnih sektora, već stvaraju preduvjete za veću zajedničku razinu kibernetičke sigurnosti na razini EU. Sve mjere NIS2 direktive su horizontalne i predstavljaju sigurnosno-organizacijske mjere. Prostor za buduće uvođenje jače normizacije i pratećih akreditacijskih i certifikacijskih zahtjeva u području kibernetičke sigurnosti može se tek očekivati kroz druge EU propise (npr. Cyber Resiliancy Act predložen 2022. godine), ali ni to neće biti proces usporediv s reguliranim vertikalnim sektorima gospodarstva već samo nešto više standardiziran pristup kibernetičkoj sigurnosti i njenim najboljim praksama. Sukob interesa sigurnosno-obavještajnih tijela nije do sada zabilježen niti u jednoj od niza država u kojima su nacionalni centri za

			Hrvatske ili čak zaštitu nacionalne sigurnosti Republike Hrvatske. Smatramo da u tom slučaju ne smije biti dvojbe da bi SOA morala izabrati interes Republike Hrvatske iznad interesa reguliranih subjekata, jer bi u suprotnom došlo do neizvršavanja primarne zadaće SOA-e. No problem je da navedena činjenica ne može ostati nepoznata budućim reguliranim subjektima, ali i regulatornim tijelima drugih država članica koje nisu dio obavještajne zajednice drugih država članica EU (koliko nam je poznato, niti jedno drugo regulatorno tijelo, prema trenutačnim najavama, neće biti sigurnosno-obavještajna agencija države EU). Osim toga, kao što smo već istaknuli, primarna zadaća SOA-e je zaštita nacionalne sigurnosti i nacionalnih interesa RH. U tu svrhu SOA provodi određen skup radnji i mjera koji su, po svojoj prirodi, tajne i nejavne. Transparentnost i otvorenost djelovanja predstavljaju nužan element postupanja svakog regulatora budući da se konačna svrha i cilj postižu kroz suradnju sa reguliranim subjektima. Baš iz razloga takvog (očekivanog i razumljivog) tajnovitog i netransparentnog djelovanja, smatramo da postoji opasnost od korištenja regulatornih ovlasti u ostvarivanje svrha koje nisu primarno regulatorne prirode, a što bi se vrlo lako moglo shvatiti od strane reguliranih subjekata kao potencijalna zlouporaba regulatornih ovlasti na njihovu štetu te bi moglo rezultirati značajnim otporom suradnji sa regulatorom. Iz navedenog razloga smatramo da je SOA po svojoj prirodi nepogodan regulator za polje kibernetičke sigurnosti, te bi ustrajanje u određivanju SOA-e kao regulatora moglo rezultirati: a. Dovođenjem SOA-e u položaj gdje mora birati između izvršavanja svoje primarne zadaće zaštite nacionalne sigurnosti i interesa RH i zaštite tajnosti i povjerljivosti informacija nadziranih subjekata koje jamči zakon. b. Nevoljkošću reguliranih subjekata, a posebice multi-nacionalnih subjekata koji u poslovanju koriste povjerljive informacije vrlo visoke vrijednosti, da surađuju sa regulatorom u RH. c. Nevoljkošću drugih EU regulatora da dijele određene informacije za regulatorom u RH. Iako je jasno da bi bilo potrebno da SOA ima svoje mjesto u nacionalnoj mreži tijela koja osiguravaju i nadziru razinu kibernetičke sigurnosti u RH, smatramo da bi bilo pogodnije sa aspekta izbjegavanja potencijalnih dvojbi o primarnoj svrsi i misiji SOA-e, ali i sa aspekta percepcije regulatora (pa time i provedbi odredaba ZKS) da se kao regulatorno tijelo za ZKS odredi ili zasnova novi subjekt koji nije formalni dio sigurnosno-obavještajne zajednice.		kibernetičku sigurnost pozicionirani u sigurnosno-obavještajnim tijelima. Također, niti jedan od nacionalnih centara kibernetičke sigurnosti na globalnoj razini nema regulatorne ovlasti. NIS2 direktiva ne postavlja zahtjev državama članicama za određivanje regulatornih tijela, tako da niti jedno tijelo u državama članicama, određeno za nadležno tijelo u okviru NIS2 transpozicije, nije regulatorno tijelo i nema regulatorne ovlasti, a to je slučaj i s Nacionalnim centrom za kibernetičku sigurnost u okviru predloženog Zakona.
15	Karlo Paljug	IV. TEKST PRIJEDLOGA ZAKONA, Članak 4.	Prijedlog je da se definicija osobnih podataka iz točke 31. ostavi jednakom onoj iz članka 4. stavka 1. točke 1. GDPR: „osobni podaci” znače svi podaci koji se odnose na pojedinca čiji je identitet utvrđen ili se može utvrditi („ispitanik”); pojedinac čiji se identitet može utvrditi jest osoba koja se može identificirati izravno ili neizravno, osobito uz pomoć identifikatora kao što su ime, identifikacijski broj, podaci o lokaciji, mrežni identifikator ili uz pomoć jednog ili više čimbenika svojstvenih za fizički,	Ne prihvaća se	Intencija predlagatelja Zakona bila je ukazati na to da je korištenje osobnih podataka u okviru ovog Zakona izuzetak, a ne pravilo. Stoga je GDPR definicija prilagođena konkretnim slučajevima iz područja primjene ovog Zakona.

			fiziološki, genetski, mentalni, ekonomski, kulturni ili socijalni identitet tog pojedinca." Ovakvim dodavanjem/izmjenama može stovit će se pravna nesigurnost. Smisao definicije osobnih podataka iz GDPR je da se da dovoljno široka definicija kako bi se obuhvatili svi oni podaci kojima se može pridodati atribut "osobni". Navođenje posebnih podataka kao osobnih podataka, je adekvatna praksa za smjernice, ali ne i u ovom slućaju za zakon budući nije nužno da u svim nabrojanim situacijama će se stvarno raditi o osobnim podacima (npr. IP adresa može biti adresa društva). Također, samim upućivanjem na članak drugog akta, ne spada u najbolju praksu kod pisanja zakona.		
16	Diverto d.o.o.	IV. TEKST PRIJEDLOGA ZAKONA, Članak 4.	U nastavku navodimo komentare na postojeće pojmove za koje smatramo da ih je potrebno detaljnije pojasniti, izmijeniti ili izbrisati: Aktivna kibernetička zaštita - preporučamo da se u definiciju uz Nacionalni sustav za otkrivanje kibernetičkih prijetnji dodaju i "pružatelji usluga otkrivanja i zaštite kibernetičke sigurnosti koje pružaju javna tijela ili privatne tvrtke". Digitalna usluga - preporučamo dopunu definicije s obzirom na postojanje slobodnog softvera i besplatnih rješenja. IKT usluga - predlažemo da se jasnije i detaljnije definira pojam IKT usluge. IKT uslugu čini skup procesa, ljudi i tehnologija i zbog toga smatramo da postojeća definicija nije sveobuhvatna. Postupanje s incidentom - korištenje riječi "sprečavanje" u opisu pojma podrazumijeva da do incidenta neće niti doći. Predlažemo da se definicija promijeni na način da se umjesto "sprečavanje" navede "sprečavanje novih incidenata". Pružatelji usluga povjerenja - definicija je nedovoljno opisana te iz nje nije moguće jasno utvrditi što su to pružatelji usluga povjerenja. Ranjivost - predlažemo da se definicija dopuni sa slabostima, osjetljivošću i nedostacima u organizacijskim i operativnim postupcima koji su uz IKT čest izvor ranjivosti. Rizik - predlažemo da se definicija pojma "rizik" obriše sukladno prijedlogu na razini EU (Amandman 39, unutar dokumenta https://www.europarl.europa.eu /doceo/document/A-9-2021-0313-AM-001-280_HR.pdf) Sistemski rizik - sistemski rizik je prema ovoj definiciji šireg opsega i obuhvaća više subjekata. Predlažemo da se jasno definira tko je odgovoran za sistemski rizik. Jesu li to nadležna tijela ili netko drugi? Usluga računalstva u oblaku - definicija je nejasna i nedovoljno opisana. Postoji li razlog zbog kojeg pojam nije definiran kao i u NIS 2 direktivi? Dodatno, preporučamo dodati definiciju pojmova: - Upravljana usluga i - Sigurnosno upravljana usluga (ukoliko se prihvati komentar da se subjekti "sigurnosno upravljana usluga" dodaju kao vrsta subjekta unutar Priloga I., sektor 9. Upravljanje uslugama	Djelomično se prihvaća	Pojam aktivne kibernetičke zaštite će se prikladno skratiti, dok je u slučaju definicija koje se preuzimaju iz NIS2 direktive te definicija potrebno u potpunosti ispravno preuzeti, što znači da je odredbe uredbi EU zabranjeno prepisivati u nacionalne propise, a pojmove iz direktiva EU potrebno preuzeti u tekstu kakav je sadržan u dotičnoj direktivi odnosno u transpozicijskom propisu kojim su dotična direktiva i pojam preuzeti u nacionalno zakonodavstvo. Vezano za upit o sistemskom riziku molimo pogledati čl. 12. Zakona, iz kojeg je razvidno kako se koristi u nadležnim tijelima za proces kategorizacije i pripadnu procjenu rizika.

			IKT-a (B2B))		
17	Span d.d.	IV. TEKST PRIJEDLOGA ZAKONA, Članak 4.	Molimo Vas za pojašnjenje. Koja je razlika između „javnih subjekata“ koji su definirani u članku 4. stavku 1. točki 17. i „subjekata javnog sektora“ koji su definirani u članku 4. stavku 1. točki 53. prijedloga zakona? Zašto nam je ta razlika bitna?	Primljeno na znanje	Definicije „javnog subjekta“ i „subjekata javnog sektora“ u članku 4. daju se u smislu potreba predmetnog Zakona, kako bi se osiguralo različite opsege primjene u pojedinim propisanim zakonskim instrumentima. Definicija „javnog subjekta“ naknadno je izmijenjena na način da se izbjegnu nepotrebna preklapanja s obuhvatom pojma „subjekata javnog sektora“.
18	Span d.d.	IV. TEKST PRIJEDLOGA ZAKONA, Članak 4.	Predlažemo da se u definiciji 'osobni podaci' (Članak 4. stavak 1. točka 31.) gdje se navode konkretni primjeri osobnih podataka (URL, IP adresa, adresa e-pošte, nazivi domena itd.), naglasi da je riječ samo o primjerima koji mogu ali i ne moraju biti osobni podaci, ovisno o situaciji. Tim više što se u dosta situacija neki od tih podataka uopće neće smatrati osobnim podatkom (npr. adresa e-pošte može glasiti samo info@lmeOrg.hr, što nije osobni podatak). Ovakva zakonska definicija 'osobnih podataka' koja navodi konkretne primjere osobnih podataka (koje sam GDPR ne navodi) mogla bi dovesti do problema u primjeni jer bi se ti podaci mogli paušalno uzeti kao osobni, bez sagledavanja konkretne situacije. Inače, NIS 2 ne sadrži definiciju 'osobnih podataka' već samo navodi primjere u točki 121 preambule, pa bih alternativno predložili i da se još jednom razmotri svrsishodnost samog članka 4. stavka 1. točke 31. predmetnog prijedloga zakona odnosno njegovo brisanje.	Ne prihvaća se	Intencija predlagatelja Zakona bila je ukazati na to da je korištenje osobnih podataka u okviru ovog Zakona izuzetak, a ne pravilo. Stoga je GDPR definicija prilagođena konkretnim slučajevima iz područja primjene ovog Zakona.
19	Stjepan Groš	IV. TEKST PRIJEDLOGA ZAKONA, Članak 4.	U definiciji istraživačke oragnizacije izuzimate, primjerice, fakultete koji su istovremeno i obrazovne i istraživačke organizacije, ali koje se bave i stručnim radom - i sve tri djelatnosti bi trebali raditi podjednako. Dodatno, MZO ima registar znanstvenih organizacija: https://mzo.gov.hr/istaknute-teme/znanost/znanstvenici-i-znanstvene-organizacije/upisnik-znanstvenih-organizacija-674/674	Ne prihvaća se	Člankom 4. preuzimaju se odredbe članka 6. NIS2 direktive, pa tako i u dijelu koji se odnosi na definiciju pojma „istraživačka organizacija“. Samu definiciju predmetnog pojma iz članka 6. NIS2 direktive potrebno je u potpunosti ispravno preuzeti, što u odnosu na pojam „istraživačka organizacija“ znači obvezu preuzimanja definicije u tekstu sadržanom u članku 6. stavku 1. točki 41. NIS2 direktive. Nadalje, Zakonom se uvodi preporuka NIS2 direktive i uključuje se uz istraživački sektor i obrazovni sektor. Razlog tome je da se istraživački sektor kroz NIS2 direktivu smatra skupom organizacija koje se primarno bave istraživanjem. Upravo zato je prihvaćena mogućnost proširenja na obrazovni sektor, u kojemu će biti moguće procesom kategorizacije uključiti u okvir Zakona subjekte kao što su određeni fakulteti. NIS2 direktiva postavlja zahtjev provedbe mjera kibernetičke sigurnosti u cijelosti poslovanja kategoriziranog subjekta, tako da će obuhvatiti i istraživačke i obrazovne i stručne segmente na opisani način kategoriziranog fakulteta i to neovisno o području u kojem je kategoriziran. Navedeno je usuglašeno sa sektorski nadležnim Ministarstvom znanosti i obrazovanja

20	Zoran Sambol	IV. TEKST PRIJEDLOGA ZAKONA, Članak 4.	Točka 2. Mislili se na Nacionalni hrvatski CERT: https://www.cert.hr/onama/? Ako se misli, onda se to i treba napisati.	Ne prihvaća se	U članku 4. dana je opća definicija pojma CSIRT jer se isti koristi u Zakonu.
21	NINO ŠETUŠIĆ	IV. TEKST PRIJEDLOGA ZAKONA, Članak 5.	Potrebno je razjasniti što su klasificirani podaci ili se pozvati ne neki dokument koji to definira. Također o kojim/čijim klasificiranim podacima se radi, samo Republike Hrvatske, drugih zemalja članica i EU? Što podacima koje kompanije smatraju klasificiranim.	Ne prihvaća se	Zakon se ne bavi kategorijama podataka jer se to ne može jednostavno definirati za veliki broj vrlo raznorodnih sektora, podsektora i vrsta subjekata. Ti pojmovi se koriste samo u smislu jasnijeg utvrđivanja opsega ovog Zakona i njegovog odnosa prema drugim propisima, a isti su definirani već dugi niz godina u različitim temeljnim propisima koji uređuju određenu materiju, primjerice klasificirani podaci u Zakonu o tajnosti podataka (NN 79/07, 86/12).
22	Porobija & Špoljarić d.o.o.	IV. TEKST PRIJEDLOGA ZAKONA, Članak 9.	Članak 9. st. 1. t. 3. Formulacija navedenog kriterija za razvrstavanje koja se poziva na odredbe Zakona o poticanju razvoja malog gospodarstva izrazito je nejasna i može rezultirati pravnom nesigurnošću kod budućeg tumačenja zakona i klasifikacije subjekta sukladno zakonu. Naime, subjekti (u konkretnom podstavku to su pružatelji javnih elektroničkih komunikacijskih usluga i javno dostupnih elektroničkih komunikacijskih usluga) koji bi bili razvrstani kao ključni subjekti bi bili tzv. subjekti malog gospodarstva koji se sukladno odredbama čl. 2. st. 1. t. 1. i 3. određuju kao subjekti koji: - imaju manje od 250 zaposlenih i - ostvaruju ukupni godišnji poslovni prihod u iznosu protuvrijednosti do 50.000.000,00 EUR ili imaju ukupnu aktivu ako su obveznici poreza na dobit, odnosno imaju dugotrajnu imovinu ako su obveznici poreza na dohodak u iznosu protuvrijednosti do 43.000.000,00 EUR. No, unutar iste odredbe dodaje se da će se kao ključne subjekte razvrstati i svi subjekti koji prelaze gornje granice subjekta malog gospodarstva. Predmetna odredba se može tumačiti da obuhvaća sve subjekte sa manje ili više od 250 zaposlenih i poslovnim prihodom manjim ili većim od 50.000.000,00 EUR. Drugim riječima, odnosi se na sve subjekte koji pružaju usluge javnih elektroničkih komunikacijskih mreža i javno dostupnih elektroničkih komunikacijskih usluga, te se pozivanjem na predmetnu odredbu Zakona o poticanju razvoja malog gospodarstva uopće ne postiže razlikovanje subjekata prema kriterijima veličine ili ekonomske snage. Nejasna je namjera predlagatelja zakona u svezi sa navedenom formulacijom, no s obzirom da se u prethodnoj točci istog stavka jasno i nedvosmisleno određuje da u odnosu na pružatelje TSP usluga, top level domain pružatelje usluga i DNS pružatelje usluga razvrstavanje provodi bez obzira na veličinu, nejasno je zašto je u odnosu na pružatelje usluga javnih elektroničkih komunikacijskih mreža i javno dostupnih elektroničkih komunikacijskih usluga nije korištena ista formulacija kada iz trenutačnog teksta proizlazi isti tretman. Smatramo bitnim ukazati da je NIS 2 direktiva u članku 2. st. 1. upućuje na javne ili privatne subjekte koji se smatraju srednjim poduzećima na temelju članka 2. Priloga Preporuci 2003/361/EZ	Prihvaća se	

			(a ne upućuje na sve subjekte malog gospodarstva tzv. SME) i onima koji prelaze tu granicu, a što znači da je NIS 2 kao kriterij veličine uzeo srednja poduzeća koja se, prema čl. 3. st. 4. Zakona o poticanju razvoja malog gospodarstva imaju smatrati poduzećima koja zapošljavaju između 51-250 ljudi i prema financijskim izvješćima za prethodnu godinu ostvaruju godišnji poslovni prihod u iznosu protuvrijednosti između 10.000.001,00 EUR i 50.000.000,00 EUR, ili imaju ukupnu aktivu ako su obveznici poreza na dobit, odnosno imaju dugotrajnu imovinu ako su obveznici poreza na dohodak, u iznosu protuvrijednosti od 10.000.001,00 EUR do 43.000.000,00 EUR. Ukoliko je namjera predlagatelja zakona bila da ipak odredi određene kriterije veličine u odnosu na navedene subjekte, predlažemo pozivanje na odredbe članka 3. Zakona o poticanju razvoja malog gospodarstva u kojem se određuju kriteriji za razlikovanje mikro, malih i srednjih subjekata malog gospodarstva prema veličini, kao pogodniju odredbu za segmentaciju prema veličini subjekta.		
23	Porobija & Špoljarić d.o.o.	IV. TEKST PRIJEDLOGA ZAKONA, Članak 10.	Članak 10. st. 1. t. 1. Jednako kao i komentar na čl. 9. st. 1. t. 3., ovdje se koristi nejasna formulacija iz koje proizlazi da bi se kao važne subjekte moglo razvrstati sve javne i privatne subjekte iz Priloga II Zakona (one koji jesu subjekti malog gospodarstva, kao i one koji prelaze gornju granicu, dakle sve subjekte) Smatramo bitnim ukazati da je NIS 2 direktiva u članku 2. st. 1. upućuje na javne ili privatne subjekte koji se smatraju srednjim poduzećima na temelju članka 2. Priloga Preporuci 2003/361/EZ (a ne upućuje na sve subjekte malog gospodarstva tzv. SME) i onima koji prelaze tu granicu, a što znači da je NIS 2 kao kriterij veličine uzeo srednja poduzeća koja se, prema čl. 3. st. 4. Zakona o poticanju razvoja malog gospodarstva imaju smatrati poduzećima koja zapošljavaju između 51-250 ljudi i prema financijskim izvješćima za prethodnu godinu ostvaruju godišnji poslovni prihod u iznosu protuvrijednosti između 10.000.001,00 EUR i 50.000.000,00 EUR, ili imaju ukupnu aktivu ako su obveznici poreza na dobit, odnosno imaju dugotrajnu imovinu ako su obveznici poreza na dohodak, u iznosu protuvrijednosti od 10.000.001,00 EUR do 43.000.000,00 EUR. Ukoliko je namjera predlagatelja zakona bila da ipak odredi određene kriterije veličine u odnosu na navedene subjekte, predlažemo pozivanje na odredbe članka 3. Zakona o poticanju razvoja malog gospodarstva u kojem se određuju kriteriji za razlikovanje mikro, malih i srednjih subjekata malog gospodarstva prema veličini, kao pogodniju odredbu za segmentaciju prema veličini subjekta.	Prihvaća se	
24	Diverto d.o.o.	IV. TEKST PRIJEDLOGA ZAKONA, Članak 12.	Vezano za stavak 2, slažemo se s prethodnim komentarom i smatramo da je potrebno pojašnjenje o odgovornostima i načinu provođenja procjene, te definiranje roka.	Primljeno na znanje	Kriteriji za procjenu koja se provodi u procesu kategorizacije temeljem članaka 11. do 13. Prijedloga zakona, neovisno od općih kriterija za kategorizaciju (članci 9. i 10. Prijedloga zakona), dodatno će se razraditi za sve potrebne sektore Uredbom iz članka 24. Zakona. Rok za kategorizaciju subjekata propisan je čl. 110. Zakona i traje godinu dana od stupanja na snagu Zakona.
25	Jurica Čular	IV. TEKST PRIJEDLOGA	Tko i na koji način provodi procjenu važnosti za nesmetano obavljanje ključnih društvenih ili	Primljeno na znanje	Procjenu važnosti provodi nadležno tijelo za provedbu zahtjeva

		ZAKONA, Članak 12.	gospodarskih djelatnosti za jedinice lokalne i područne (regionalne) samouprave?		kibernetičke sigurnosti prema podjeli nadležnosti iz Priloga III.
26	Stjepan Groš	IV. TEKST PRIJEDLOGA ZAKONA, Članak 13.	Fakulteti i visokoškolske ustanove su obrazovne ustanove, za razliku od osnovnih škola i srednjih škola koje su odgojno-obrazovne. Jesu li u ovom članku namjerno isključene visokoškolske ustanove?	Prihvaća se	
27	Jurica Čular	IV. TEKST PRIJEDLOGA ZAKONA, Članak 14.	Da li se Zakon odnosi i na infrastrukturu subjekta koja se ne nalazi na prostoru RH? Ako da, na koji način nadležna tijela misle provoditi izravan nadzor na teritoriju druge države?	Primljeno na znanje	NIS2 direktiva uvodi alat uzajamne pomoći za slučajeve kada subjekt 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. U pitanju je članak 37. NIS2 direktive i isti se odnosi upravo na provedbu nadzornih aktivnosti u gore opisanim slučajevima, a sve u cilju osiguranja provedbe obveza iz NIS2 direktive (recital 134. NIS2 direktive). Članak 37. NIS2 direktive preuzima se u nacionalno zakonodavstvo člancima 94. do 96. Nacrta (DIO OSMI, STRUČNI NADZOR NAD PROVEDBOM ZAHTJEVA KIBERNETIČKE SIGURNOSTI, POGLAVLJE V. UZAJAMNA POMOĆ U PROVEDBI STRUČNIH NADZORA S NADLEŽNIM TIJELIMA DRUGIH DRŽAVA ČLANICA).
28	Porobija & Špoljarić d.o.o.	IV. TEKST PRIJEDLOGA ZAKONA, Članak 15.	Nastavno na prethodne komentare na čl. 9. i 10., smatramo da se predmetnim člankom uvodi dodatna nejasnoća i nesigurnost u odnosu na kriterij veličine koji će se koristiti za razvrstavanje subjekata. Stavak 2. predmetnog članka koji bi trebao pružiti dodatnu jasnoću vezano uz primjenu kriterija veličine, odnosno, na koje bi se vrste subjekata malog gospodarstva primjenjivala klasifikacija sukladno zakonu, u trenutačnoj formulaciji proizvodi dodatnu sumnju jer navodi da će se prilikom kategorizacije „voditi računa“ o smjernicama Europske komisije (konkretan dokument koji uređuje navedenu materiju naziva se Preporuka 2003/361/EZ i odredbe su, u bitnom, već prenesene u Zakon o poticanju razvoja malog gospodarstva). Budući da je razumno očekivati da će usklađivanje poslovanja subjekata koji su obveznici ovog zakona biti skup i kompliciran proces, smatramo da bi se morao propisati jasan kriterij veličine (osim u slučaju primjene posebnih kriterija iz članka 11. ovog zakona) temeljem kojih se provodi kategorizacija jer se potencijalno reguliranim subjektima mora omogućiti određena razina izvjesnosti da će prelaskom objektivno određenih pragova postati obveznici ovog zakona.	Primljeno na znanje	Člankom 15. Prijedloga zakona se potvrđuje odrednica Zakona kako se svi zahtjevi i kriteriji odnose na poslovanje subjekta u cijelosti. Pri tome se samo upućuje na to kako se kriteriji veličine promatraju kumulativno u odnosu na cjelokupno poslovanje subjekta, jednako kao što se i mjere kibernetičke sigurnosti primjenjuju na cjelokupno poslovanje. Stavak 2. ovog članka odnosi se primarno na smjernice koje bi Europska komisija, u suradnji sa Skupinom za suradnju i relevantnim dionicima, trebala izraditi nastavno na recital 20. NIS2 direktive. Provedba obveza ne bi trebala biti niti složen, a niti skup proces za tvrtke koje danas primjenjuju najbolje prakse kibernetičke sigurnosti u svom poslovanju. Postupnost uvođenja šire EU standardizacije donijet će u srednjoročnom razdoblju svim subjektima puno stabilnije upravljanje informacijskim i komunikacijskim sustavima i veću sigurnost njihovih poslovnih procesa, kao i ispomoć u rješavanju kibernetičkih incidenata i napada, a pri tome ne nužno veća financijska ulaganja.
29	NINO ŠETUŠIĆ	IV. TEKST PRIJEDLOGA	S obzirom da klasifikacija i/ili reklasifikacija znatno utječu na obveze subjekta bitno je da subjekt	Primljeno na znanje	Kategorizacija podrazumijeva početak suradnje i uspostavu obostrane

		ZAKONA, Članak 19.	potvrdi primitak obavijesti tj. u slučaju da potvrda nije primljena da ga se pokuša kontaktirati putem nekog drugog kanala.		komunikacije između nadležnog tijela za provedbu zahtjeva kibernetičke sigurnosti i ključnog subjekta.
30	Span d.d.	IV. TEKST PRIJEDLOGA ZAKONA, Članak 19.	Budući da se radi o promjeni kategorizacije subjekta i samim time obveza subjekta, kako se i navodi u članku, svrsishodno bi bilo subjektima dati određeni rok za prilagodbu novim obvezama, umjesto da se njihove obveze mijenjaju odmah po primitku obavijesti. Rok bi trebalo odrediti od slučaja do slučaja i definirati ga u obavijesti subjektu, a minimalan rok bi trebao biti 60 dana. (komentar na stavak 2. ovog članka)	Prihvaća se	
31	Hrvatska udruga menadžera sigurnosti (HUMS)	IV. TEKST PRIJEDLOGA ZAKONA, Članak 20.	Predlažemo definirati na što se odnosi "IP adresni prostor" te dodatno navedeno odvojiti u zasebnu natuknicu, odvojeno od kontakt podataka. Vezano za "druge podatke", razmotriti navođenje primjera ili obavezu nadležnim tijelima da definiraju ili upute subjekte koji bi im drugi podaci bili potrebni za potrebu kategorizacije.	Primljeno na znanje	Ovaj dio teksta prenesen je iz NIS2 direktive te će biti dalje razrađen, pojašnjen i strukturiran u okviru Uredbe iz članka 24. Zakona, vodeći računa i o članku 3. stavku 4. podstavku 3. NIS2 direktive kojim je utvrđeno da Europska komisija uz pomoć Europske agencije za kibernetičku sigurnost (ENISA) bez nepotrebne odgode pruža smjernice i predloške u svezi s obvezama dostave predmetnih podataka.
32	A1 Hrvatska d.o.o.	IV. TEKST PRIJEDLOGA ZAKONA, Članak 20.	Čl.20.st.1. alineja 2 -pojasniti detaljnije na što se konkretno odnosi pojedina stavka posebno u dijelu IP adresnih raspona	Primljeno na znanje	Ovaj dio teksta prenesen je iz NIS2 direktive (članak 3. stavak 1. podstavak 1.) te će biti dalje razrađen, pojašnjen i strukturiran u okviru Uredbe iz članka 24. Zakona, vodeći računa i o članku 3. stavku 4. podstavku 3. NIS2 direktive kojim je utvrđeno da Europska komisija uz pomoć Europske agencije za kibernetičku sigurnost (ENISA) bez nepotrebne odgode pruža smjernice i predloške u svezi s obvezama dostave predmetnih podataka.
33	NINO ŠETUŠIĆ	IV. TEKST PRIJEDLOGA ZAKONA, Članak 20.	Potrebno je detaljnije definirati tražene podatke pogotovo u vidu multi-nacionalnih kompanija tj. da li se dostavljaju podaci samo koji se tiču lokalnih ureda ili za cijelu tvrtku. Također tražiti sve adrese e-pošte lokalnih ili globalnih zaposlenika nije najsigurnije rješenje zbog rizika gubitka tih podataka. Što se IP adresa trebalo bi definirati točno koje IP adrese – sve ili samo vezane za neke servise, ponovno pitanje vezano uz multinacionalne kompanije da li su potrebne i adrese koje nisu vezane za lokalnu ispostavu, što je s uporabom cloud rješenja gdje se te adrese znaju mijenjati. U velikim tvrtkama često se neke stranice, najčešće marketing, kupuju kao gotova rješenja od raznih agencija koje se odgovorne za njih te naručilac usluge nije upoznat s svim adresama koje se vežu uz takvu stranicu iz takvih i sličnih razloga kod multinacionalnih kompanije gotovo ako ne i praktički je nemoguće prikupiti sve IP adrese, stoga bi bilo potrebno u zahtjevu definirati koje sve IP adrese je potrebno priložiti.	Primljeno na znanje	Ovaj dio teksta prenesen je iz NIS2 direktive (članak 3. stavak 1. podstavak 1.) te će biti dalje razrađen, pojašnjen i strukturiran u okviru Uredbe iz članka 24. Zakona, vodeći računa i o članku 3. stavku 4. podstavku 3. NIS2 direktive kojim je utvrđeno da Europska komisija uz pomoć Europske agencije za kibernetičku sigurnost (ENISA) bez nepotrebne odgode pruža smjernice i predloške u svezi s obvezama dostave predmetnih podataka.
34	Stjepan Groš	IV. TEKST PRIJEDLOGA ZAKONA, Članak 20.	Pod "IP adresnim rasponima" se vjerojatno misli na javne IP adrese, ali s obzirom da to nije jasno rečeno, može označavati i privatne IP adrese. Također, nejasno je radi li se o dodijeljenim IP adresama, ili korištenim IP adresama.	Primljeno na znanje	Ovaj dio teksta prenesen je iz NIS2 direktive (članak 3. stavak 1. podstavak 1.) te će biti dalje razrađen, pojašnjen i strukturiran u okviru Uredbe iz članka 24. Zakona, vodeći računa i o članku 3. stavku 4. podstavku 3. NIS2 direktive kojim je utvrđeno da Europska komisija uz pomoć Europske agencije za kibernetičku sigurnost (ENISA) bez nepotrebne odgode pruža smjernice i predloške u svezi s obvezama dostave

					predmetnih podataka.
35	Jurica Čular	IV. TEKST PRIJEDLOGA ZAKONA, Članak 20.	Ako je obveznik globalni provider s data centrima diljem svijeta, da li mora prijaviti sve globalno korištene IP raspone?	Primljeno na znanje	Potrebni su rasponi IP adresa koje davatelj koristi za potrebe davanja usluga u RH.
36	HGK	IV. TEKST PRIJEDLOGA ZAKONA, Članak 21.	U skladu s čl. 21. st. 1. Nacrta, javni subjekti dužni su bez naknade dostavljati popise subjekata i omogućiti pristup registrima te dostavljati i druge podatke. Skrećemo pozornost kako je za omogućavanje pristupa registrima, odnosno evidenciji potrebno izvršiti dodatne zahvate tehničke prirode te je nužno da trošak u vezi s navedenim snosi podnositelj zahtjeva.	Primljeno na znanje	Članak 21. ostavlja mogućnost dostave traženih podataka ili odgovarajućeg pristupa registrima, a s obzirom da se radi o periodičkom procesu kategorizacije, a ne operativnom pristupu na dnevnoj bazi, mišljenja smo kako je članak jasan i lako primjenjiv u praksi.
37	MARKO RAKAR	IV. TEKST PRIJEDLOGA ZAKONA, 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, a uz prethodno mišljenje nadležnih tijela za provedbu posebnih zakona dužna su redovito.	Ne prihvaća se	Prilikom donošenja uredbi Vlade, pa tako i Uredbe iz članka 24. Prijedloga zakona primjenjuje se poslovnička procedura utvrđena Poslovnikom Vlade RH („Narodne novine“, broj: 154/11, 121/12, 7/13, 61/15, 99/16, 57/17, 87/19 i 88/20), sukladno kojoj nacrtu prijedloga Uredbe iz članka 24. Prijedloga zakona moraju biti priložena mišljenja širokog kruga relevantnih dionika, a kako je to slučaj i s Nacrtom prijedloga predmetnog zakona.
38	MARKO RAKAR	IV. TEKST PRIJEDLOGA ZAKONA, Članak 24.	Članak 24. vrlo široko i bez jasnih kriterija opisuje kako Vlada donosi mjerila za razvrstavanje ključnih odnosno važnih subjekata i to isključivo na prijedlog središnjeg državnog tijela za kibernetičku sigurnost. Ovom definicijom se odluka o tome koji će subjekt biti obveznik zakona svodi na diskrecijsku odluku tijela koje po svojoj prirodi nije transparentno. Ovaj članak je u značajnom raskoraku s NIS2 direktivom, koja u svojem članku 13. stavak 5. predviđa da sva nadležna tijela (kako su definirana u članku 13. stavak 4.) redovno surađuju i razmjenjuju informacije kako bi identificirali kritične subjekte, prijetnje i dr., što znači da bi kao donji minimum u zakonski tekst trebalo uvrstiti obvezu suradnje s nadležnim tijelima (sektorskim, regulatornim) poput HAKOM, HERA, HNB, HANFA, Ministarstvo financija, Ministarstvo gospodarstva i održivog razvoja, Ministarstvo mora, prometa i infrastrukture (i druge po potrebi). Napominjem također, da se ovaj članak zakona bavi posebnim kriterijima, te se razlikuje od obveze definirane člankom 17. prijedloga iako za to nema argumenta.	Ne prihvaća se	Uredbu donosi Vlada na prijedlog središnjeg državnog tijela za kibernetičku sigurnost, priprema ju međuresorna stručna radna skupina, mišljenje na uredbu će davati niz tijela kao i na Zakon, a proces kategorizacije provodi više nadležnih tijela za zahtjeve kibernetičke sigurnosti iz priloga III. Zakona, svako od tih tijela za sektore iz svoje nadležnosti prema ovome prilogu. Napominjemo kako SOA ne bi bila jedino tijelo koje prijedlogom zakonom dobiva nadležnosti u području kibernetičke sigurnosti već su to i druga tijela: Hrvatska narodna banka (HNB) za sektor bankarstva; Hrvatska agencija za nadzor financijskih usluga (HANFA) za infrastrukture financijskog sektora; Hrvatska agencija za civilno zrakoplovstvo (HACZ) za sektor zračnog prometa; Hrvatska regulatorna agencija za mrežne djelatnosti (HAKOM) za telekomunikacijski sektor; Ured Vijeća za nacionalnu sigurnost (UVNS) za javni sektor; Središnji državni ured za razvoj digitalnog društva (SDURDD) za pružatelje usluga povjerenja; Ministarstvo znanosti i obrazovanja (MZO) za sektor istraživanja, sektor sustava obrazovanja te za registar naziva vršne nacionalne internetske domene i registrare; Nacionalni CERT ustrojen u CARNET-u kao drugi nadležni CSIRT, uz NCSC. Slijedom ovog opisa i niza drugih dijelova Zakona, jasno je da su kriteriji

					definirani i usklađeni te da više nadležnih tijela postupa po tim kriterijima u sektorima definiranim Prilogom III. Zakona. Nacionalno vijeće za kibernetičku sigurnost (https://www.uvns.hr/hr/informacijska-sigurnost/kiberneticka-sigurnost) već godinama se sastaje na mjesečnoj razini i trenutno obuhvaća predstavnike 16 institucija, a od 2021. godine postoji i međuresorna radna skupina za upravljanje kibernetičkim krizama koja se sastaje na kvartalnoj razini i obuhvaća više državnih tijela, sigurnosno-obavještajnih tijela i sektorskih regulatora. Donošenjem ovog Zakona ta će se suradnja nadležnih tijela dodatno razviti i strukturirati u skladu s EU zahtjevima iz NIS2 direktive odnosno iz ovog Zakona.
39	Hrvatska udruga menadžera sigurnosti (HUMS)	IV. TEKST PRIJEDLOGA ZAKONA, Članak 26.	Čl. 26, st.1: "Ključni i važni subjekti dužni su provoditi ODGOVARAJUĆE I RAZMJERNE mjere upravljanja kibernetičkim sigurnosnim rizicima." Navedeni prijedlog je u skladu s preambulom 93. te člankom 21. st1. Direktive.	Prihvaća se	
40	Hrvatska udruga menadžera sigurnosti (HUMS)	IV. TEKST PRIJEDLOGA ZAKONA, Članak 27.	S obzirom na to da države članice osiguravaju da subjekti poduzimaju mjere za upravljanje rizicima, predlažemo da radi očuvanja pravne sigurnosti država pobliže definira na koji način se provodi procjena rizika i mjera, bilo na način da propiše obavezu korišenja neke od javno dostupnih i besplatnih metodologija, bilo na način da dodatno definira neke od obaveznih elemenata, a kako bi se ujednačio pristup među subjektima.	Primljeno na znanje	Uredbom iz članka 24. Zakona planira se dodatno razraditi niz elemenata Zakona pa tako i metode za upravljanje rizikom.
41	Hrvatska udruga menadžera sigurnosti (HUMS)	IV. TEKST PRIJEDLOGA ZAKONA, Članak 27.	Čl. 27. točka 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 društveni i gospodarski UČINAK." Navedeni prijedlog je u skladu s Direktivom i značenju riječi učinak koji nije istoznačica riječi utjecaj.	Prihvaća se	
42	Stjepan Groš	IV. TEKST PRIJEDLOGA ZAKONA, Članak 27.	Ako subjekt radi procjenu rizika, tada mora uzeti u obzir točku jedan stavka 2 te dijelom i točku 3 istog stavka. S druge strane, veličina subjekta i njegov mogući društveni i gospodarski utjecaj nisu nešto s čim se subjekt treba "zamarati" već nadzorno tijelo koje temeljem tih parametara odlučuje tko je ključan, a tko važan subjekt. Obveza upravljanja rizicima podrazumijeva i njihovo ovladavanje - ako su rizici neprihvatljivi. Potpuno drugo pitanje je kako će pojedini subjekt definirati razinu prihvatljivog rizika te da se može doći u situaciju u kojoj subjekt ima preveliki apetit za rizik. Tu bi na nacionalnoj razini trebalo imati procjenu rizika za društvo koje svaki subjekt donosi.	Primljeno na znanje	Procjenu rizika provodi subjekt obveznik Zakona, ali se ta procjena provjerava u sklopu ocjene sukladnosti (revizije), kao i pri stručnom nadzoru tijela nadležnog za zahtjeve kibernetičke sigurnosti. U tom smislu subjekt mora biti svjestan svoje uloge u gospodarstvu i društvu kako bi pravilno procijenio rizike. Upravo ta uloga subjekta razlog je za njegovu kategorizaciju kao ključni ili važni subjekt.
43	Diverto d.o.o.	IV. TEKST PRIJEDLOGA ZAKONA, Članak 27.	Kako bi se izbjeglo manipuliranje u procesu procjene rizika, predlažemo da se propiše obveza korištenja okvira za procjenu rizika koji je donijela ENISA (ENISA Risk Management/Risk	Primljeno na znanje	Uredbom iz članka 24. Zakona planira se dodatno razraditi niz elemenata Zakona pa tako i metode za

			Assessment (RM/RA) Framework).		upravljanje rizikom.
44	Jurica Čular	IV. TEKST PRIJEDLOGA ZAKONA, Članak 27.	Što je utvrđeni rizik, tko i na koji način ga procjenjuje i vrednuje? Ako je to zadaća samog obveznika, da li isti može utvrditi niske ili nepostojeće rizike i prihvatiti ih?	Primljeno na znanje	Procjenu rizika provodi subjekt obveznik Zakona, ali se ta procjena provjerava u sklopu ocjene sukladnosti (revizije), kao i pri stručnom nadzoru tijela nadležnog za zahtjeve kibernetičke sigurnosti. U tom smislu subjekt mora biti svjestan svoje uloge u gospodarstvu i društvu kako bi pravilno procijenio rizike. Upravo ta uloga subjekta razlog je za njegovu kategorizaciju kao ključni ili važni subjekt.
45	Hrvatska udruga menadžera sigurnosti (HUMS)	IV. TEKST PRIJEDLOGA ZAKONA, Članak 28.	Direktiva, kao i neke druge regulative EU (primjerice, Opća uredba o zaštiti podataka), ne navodi obavezu korištenja najnovijih dostignuća što se može zaključiti iz stavka 1. članka 28., već naglašava da se najnovija dostignuća trebaju uzeti u obzir. Predlažemo stavak preformulirati u skladu s time.	Prihvaća se	
46	A1 Hrvatska d.o.o.	IV. TEKST PRIJEDLOGA ZAKONA, Članak 28.	Čl.28.st1. - potrebno pojasniti kroz Uredbu iz čl.24. ovog Zakona kako bi se izbjegla mogućnost širokog tumačenja obveza, njihovog ispunjenja te potencijalnog kažnjavanja adresata Zakona.	Prihvaća se	
47	MARKO RAKAR	IV. TEKST PRIJEDLOGA ZAKONA, Članak 28.	(1) Mjere upravljanja kibernetičkim sigurnosnim rizicima provode se na način da se koriste najnovija tehnička dostignuća koja se koriste u okviru najbolje sigurnosne prakse u području kibernetičke sigurnosti i, kada je to primjenjivo, relevantne europske i međunarodne norme te 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, 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. (3) Ključni i važni subjekti dužni su zamijeniti IKT proizvode, IKT usluge i IKT procese te upravljane sigurnosne usluge, a koji nisu sukladni sa stavkom (2) ovog članka, u roku koji ne može biti duži od 5 godina. (4) U slučaju da nadležno tijelo izda nalog za hitnu zamjenu IKT proizvoda, IKT usluga i IKT procesa te upravljanih sigurnosnih usluga, a koji nisu sukladni sa stavkom (2) ovog članka, troškove zamjene snosi državni proračun.	Ne prihvaća se	Procesi certifikacije su tek u pripremi na EU razini, a mjerodavna postupanja po možebitnim obvezama zamjene moraju u svakom slučaju biti praćena uvjetima i rokovima koji se propisuju mjerodavnim aktima EU (predviđen rok od 5 godina) odnosno relevantnim nacionalnim propisima, odnosno onim propisima koji će za subjekte uvesti obvezu korištenja točno određenih certificiranih IKT proizvoda, IKT usluga, IKT procesa ili upravljanih sigurnosnih usluga. Prijedlogom zakona se takva obveza za ključne i važne subjekte ne uvodi, već se njime uvodi pravni temelj za slučaj ako, odnosno kada, takva obveza bude utvrđena drugim relevantnim propisima.
48	MARKO RAKAR	IV. TEKST PRIJEDLOGA ZAKONA, Članak 28.	U stavku 1. taksativno se navode „najnovija tehnička dostignuća“ koja se koriste u okviru „najbolje sigurnosne prakse u području kibernetičke sigurnosti“. Obzirom da za sukladnost s člankom 28. zakona postoje prekršajne odredbe (članak 101. prijedloga), postavlja se pitanje kako nadzirani subjekt može nedvosmisleno znati da se nalazi u prekršaju uz subjektivno postavljeni cilj sukladnosti, a što je suprotno temeljnom načelu da bilo koji prekršaj mora jasno utvrđen da bi bio kažnjiv.	Ne prihvaća se	Stavak 1. je odgovarajuće preformuliran slijedom prijedloga HUMS-a iz točke 30. i A1 iz točke 46. te je jasniji i u skladu je s NIS2 zahtjevima.

			Nadalje, ovaj članak je u raskoraku s NIS2 direktivom i to na način da je u stavku 2. dodana formulacija „ili nacionalnih shema kibernetičke sigurnosne certifikacije“, a koja ne postoji u članku 24. NIS2 direktive. Nadalje, taj dodatak je u direktnoj suprotnosti s EU uredbom o kibernetičkoj sigurnosti (EU2019/881), koji u članku 57. stavak 2. eksplicitno naređuje kako „članice EU neće uvoditi nove nacionalne kibernetičke certifikacijske sheme za ICT proizvode, ICT servise i ICT procese koji su već pokriveni Europskom kibernetičkom certifikacijskom shemom koja je na snazi“. Također, potrebno je detaljno razraditi što se događa sa subjektom u kojem je zatečena oprema, servisi ili procesi a za koje je propisana EU certifikacija, ali oprema, servisi ili procesi je ne posjeduju. Nužno je propisati prijelazne rokove tj. rokove zamjene (npr. do kraja amortizacijskog roka, ili vremenskog roka npr. 5 godina), te u slučaju da postoji utemeljeni razlog za žurnu zamjenu, tko će podmiriti nastalu štetu (trošak zamjene opreme, servisa ili procesa, odnosno trošak nabavke i implementacije nove opreme, servisa ili procesa). Ovo je nužno razraditi i zbog primjene prekršajnih odredbi članka 101. i 102. nacrta. Predlaže se brisanje dijela koji glasi „ili nacionalnih shema kibernetičke sigurnosne certifikacije“ obzirom da nepotrebno izlazi iz prostora NIS2 direktive, te je u direktnoj suprotnosti s obvezama koje proizlaze iz EU uredbe o kibernetičkoj sigurnosti.		Nacionalne certifikacijske sheme su omogućene u svim slučajevima u kojima ne postoji EU certifikacijska shema. S tim u svezi, skreće se pozornost na Uredbu (EU) 2019/881 (Akt o kibernetičkoj sigurnosti) i Zakon o provedbi Uredbe (EU) 2019/881 („Narodne novine“, broj: 63/22). Procesi certifikacije su tek u pripremi na EU razini, a mjerodavna postupanja po možebitnim obvezama zamjene moraju u svakom slučaju biti praćena uvjetima i rokovima koji se propisuju mjerodavnim aktima EU (predviđen rok od 5 godina) odnosno relevantnim nacionalnim propisima, odnosno onim propisima koji će za subjekte uvesti obvezu korištenja točno određenih certificiranih IKT proizvoda, IKT usluga, IKT procesa ili upravljanih sigurnosnih usluga. Prijedlogom zakona se takva obveza za ključne i važne subjekte ne uvodi, već se njime uvodi pravni temelj za slučaj ako, odnosno kada, takva obveza bude utvrđena drugim relevantnim propisima.
49	Stjepan Groš	IV. TEKST PRIJEDLOGA ZAKONA, Članak 28.	Ako netko provodi upravljanje rizicima prema nekoj od međunarodno prihvaćenih normi, ne bi li trebao već raditi prema onome što definira stavak 1 ovog članka? Isto tako, umanjenje rizika nije samo korištenje tehničkih dostignuća već i drugih, primjerice organizacijskih. Nadalje, ako se umanjuje rizik, je li potrebno definirati kako se to treba napraviti? Ako je rizik smanjen, je li bitno kako je to učinjeno - pod uvijetom da je doista rizik manji? Ovaj članak kao da ide u definiranje metoda procjene i upravljanja rizicima.	Primljeno na znanje	Svi budući subjekti koji danas koriste najbolje prakse kibernetičke sigurnosti, imat će vrlo malo promjena u provođenju zahtjeva iz ovog Zakona, koje će se svoditi na izvještavanje određenog CSIRT-a o kibernetičkim incidentima te na korištenje nezavisne revizije i periodičkog stručnog nadzora nadležnog tijela.
50	Span d.d.	IV. TEKST PRIJEDLOGA ZAKONA, Članak 28.	S obzirom da nam još nije poznata količina i vrsta IKT proizvoda i usluga koji će biti certificirani i čija će primjena biti obvezna ključnim i važnim subjektima, predlažemo da se razmotri opcionalno korištenje certificiranih IKT proizvoda i usluga (a ne obvezno). Tako bi subjekti koji se odluče na korištenje certificiranih IKT proizvoda i usluga puno lakše dokazali usklađenost, a istovremeno bi se izbjegle komplikacije koje za sobom povlači obvezno korištenje certificiranih IKT proizvoda i usluga (monopol, gubitak certifikacije, prelazak na drugi proizvod ili uslugu). Time bi se ostvario namjeravani cilj jer će se većina subjekata na tržištu sigurno opredijeliti za certificirane IKT proizvode i usluge ukoliko oni budu dostupni na tržištu uz slične/jednake uvjete kao i proizvodi i usluge bez certifikata. (komentar na stavak 2. ovog članka)	Ne prihvaća se	Procesi certifikacije su tek u pripremi na EU razini, a mjerodavna postupanja po možebitnim obvezama zamjene moraju u svakom slučaju biti praćena uvjetima i rokovima koji se propisuju mjerodavnim aktima EU (predviđen rok od 5 godina) odnosno relevantnim nacionalnim propisima, odnosno onim propisima koji će za subjekte uvesti obvezu korištenja točno određenih certificiranih IKT proizvoda, IKT usluga, IKT procesa ili upravljanih sigurnosnih usluga. Prijedlogom zakona se takva obveza za ključne i važne subjekte ne uvodi, već se njime uvodi pravni temelj za slučaj ako, odnosno kada, takva obveza bude utvrđena drugim relevantnim propisima.
51	Jurica Čular	IV. TEKST PRIJEDLOGA ZAKONA, Članak 28.	U skladu s ovim člankom, moguć je scenarij u kojem će obveznicima Zakona obveznim propisati korištenje „određenih IKT proizvoda, IKT usluga i IKT procesa te upravljanih sigurnosnih usluga, koje su certificirane na temelju europskih programa kibernetičke sigurnosne certifikacije ili	Primljeno na znanje	Procesi certifikacije su tek u pripremi na EU razini, a mjerodavna postupanja po možebitnim obvezama zamjene moraju u svakom slučaju biti praćena uvjetima i rokovima koji se propisuju

			nacionalnih shema kibernetičke sigurnosne certifikacije“. Da li postoje podaci o tome koji proizvodi, usluge i procesi su certificirani i što se događa u situaciji ako obveznik već koristi određene proizvode, usluge i procese koji nisu certificirani? Što ako određeni proizvodi, usluge i procesi izgube certifikat, a obveznici Zakona ih koriste?		mjerodavnim aktima EU (predviđen rok od 5 godina) odnosno relevantnim nacionalnim propisima, odnosno onim propisima koji će za subjekte uvesti obvezu korištenja točno određenih certificiranih IKT proizvoda, IKT usluga, IKT procesa ili upravljanih sigurnosnih usluga. Prijedlogom zakona se takva obveza za ključne i važne subjekte ne uvodi, već se njime uvodi pravni temelj za slučaj ako, odnosno kada, takva obveza bude utvrđena drugim relevantnim propisima.
52	Porobija & Špoljarić d.o.o.	IV. TEKST PRIJEDLOGA ZAKONA, Članak 29.	U odnosu na stavak 1. Izraz „članovi upravljačkih tijela“ nije pravno-tehnički izraz koji se koristi u pravnom sustavu RH budući da se time neadekvatno označavaju odgovorne osobe u trgovačkim društvima u određenim oblicima uređenja trgovačkog društva. Naime, problematično je u slučaju kada se radi o tzv. monističkom uređenju društva gdje društvo umjesto nadzornog odbora kao nadzornog tijela koje imenuje upravu i uprave kao upravljačkog tijela postoji tek jedno tijelo - upravni odbor koji imenuje određene članove upravnog odbora izvršnim direktorima - osobama koje neposredno upravljaju društvom. S druge strane postoje i članovi upravnog odbora - neizvršni direktori koji nemaju izravnu mogućnost donositi odluke i upravljati poslovanjem društva. Trenutačna formulacija bi obuhvatila i neizvršne direktore u društvima sa monističkim uređenjem, a što smatramo pogrešnim i protivnim smislu NIS 2 direktive. Predlažemo zamijeniti izraz „članovi upravljačkih tijela“ sa „osobe ovlaštene za zastupanje subjekata“ ili „zakonski zastupnici subjekata“. U odnosu na stavak 4. Odredba je nejasna te se može tumačiti vrlo široko. Izraz „pravni predstavnik“ je nejasan i nije moguće utvrditi odnosi li se na pravnu ili fizičku osobu. S obzirom na ozbiljne posljedice koje zakon propisuje za odgovorne osobe, smatramo da je potrebno dodatno razraditi navedenu odredbu na način da se jasnije odredi tko sve i na temelju čega može biti pravni predstavnik subjekta.	Djelomično se prihvaća	Zbog velikog broja vrlo različitih sektora i subjekata koje Zakon pokriva teško je iznaći zajednički prihvatljivu formulaciju. U Prijedloga zakona je u pojmovnik uveden pojam „upravljačkog tijela ključnog i važnog subjekta“ (tijelo ili tijela imenovana u skladu sa zakonom kojim se uređuje osnivanje i poslovanje subjekta, a koja raspolažu ovlastima za upravljanje i vođenje subjekta). Također, radi jasnoće i dodatnog usklađivanja sa člankom 32. stavkom 6. i člankom 33. stavkom 5. NIS2 direktive, izmijenjen je i stavak 4. članka 29. Prijedloga zakona na način da iz njega sada izrijekom proizlazi kako se članak 29. odnosi na fizičke osobe koje, između ostalog, u svojstvu pravnog predstavnika na temelju punomoći ili 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.
53	Diverto d.o.o.	IV. TEKST PRIJEDLOGA ZAKONA, Članak 29.	Vezano uz stavak 1., članovi upravljačkih tijela u hrvatskom jeziku predstavljaju širok pojam. Predlažemo da se izraz "članovi upravljačkih tijela" zamijeni s "članovi upravljačkih tijela u upravljačkoj funkciji" kako bi bilo jasno da se misli na članove uprava/direktore najviših razina odgovornosti. Dodatno, predlažemo da se u ovaj članak, nakon stavka 3. dodaju dodatna dva stavka važna za odgovornost za provedbu mjera: 1. Osobe odgovorne za upravljanje mjerama obvezne su imenovati voditelja informacijske sigurnosti koji će direktno njima odgovarati po pitanjima vezanim uz sigurnost IKT sustava i povezanih organizacijskih i operativnih postupaka. Obrazloženje: Zbog važnosti ovog Zakona, nužno je imenovati osobu koja će obnašati funkciju voditelja informacijske sigurnosti i jasno definirati odgovornosti te funkcije. S obzirom na posljedice	Djelomično se prihvaća	Zbog velikog broja vrlo različitih sektora i subjekata koje Zakon pokriva teško je iznaći zajednički prihvatljivu formulaciju. U Prijedloga zakona je u pojmovnik uveden pojam „upravljačkog tijela ključnog i važnog subjekta“ (tijelo ili tijela imenovana u skladu sa zakonom kojim se uređuje osnivanje i poslovanje subjekta, a koja raspolažu ovlastima za upravljanje i vođenje subjekta). Sličan problem je i s propisivanjem imenovanja „voditelja informacijske sigurnosti“ jer se u različitim sektorima koriste vrlo različite prakse i

			koje mogu nastati u slučaju ne poštivanja odredbi ovog Zakona, ključno je da voditelj informacijske sigurnosti o stanju sigurnosti odgovara direktno osobi odgovornoj za upravljanje mjerama unutar subjekta. Na primjer, Opća uredba o zaštiti podataka definira imenovanje službenika za zaštitu podataka i njegove odgovornosti u sklopu. 2. Osobe odgovorne za upravljanje mjerama obvezne su za uspostavu, odobrenje i praćenje provedbe strategije informacijske sigurnosti. Obrazloženje: Strategija informacijske sigurnosti je dokument kojim se na najvišim razinama definira način razvoja informacijske sigurnosti te ciljevi sigurnosti vezani uz IKT i povezane organizacijske i operativne postupke. Strategijom se na najvišoj razini osigurava usklađenost s poslovnim ciljevima. S obzirom na navedeno, smatramo da strategija mora postojati kako bi subjektima osigurala smisleno i plansko usklađivanje sa Zakonom koje će osigurati željenu razinu otpornosti.		nazivi ovakvih radnih mjesta, tako da je prihvatljivo rješenje opisno i obvezuje na određivanje odgovornih osoba, ali nazivi radnih mjesta ostaju u ingerenciji svakog pojedinog sektora/subjekta.
54	ZLATAN MORIĆ	IV. TEKST PRIJEDLOGA ZAKONA, Članak 29.	Predpostavljam da će biti potrebno osmisliti osposobljavanja koje polaznicima daje znanja i vještine da mogu napraviti sve iz članka 30.	Primljeno na znanje	Članak 29. stavak 3. Prijedloga zakona uvodi obvezu 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, a kako to određuje članak 20.stavak 2. NIS2 direktive. Vezano uz pitanje osposobljavanja napominje se kako je odredbom članka 30. stavkom 1. podstavkom 7. Prijedloga zakona propisano da mjere upravljanja kibernetičkim sigurnosnim rizicima moraju uključivati i osposobljavanje o kibernetičkoj sigurnosti, a kako to određuje i članak 21. stavak 2. točka g) NIS2 direktive. Prema članku 38. Prijedloga zakona, mjere upravljanja kibernetičkim sigurnosnim rizicima i način njihove provedbe, propisuju se uredbom iz članka 24. ovog Zakona. Također, napominje se kako se, sukladno obvezama država članica iz članka 7. NIS2 direktive, člankom 55. stavkom 2. i Prilogom IV. Nacrta, utvrđuje obvezni sadržaj nacionalnog akta strateškog planiranja iz područja kibernetičke sigurnosti, a koji, između ostalog, obuhvaća obvezu razraditi tim aktom politiku 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.
55	Jurica Čular	IV. TEKST PRIJEDLOGA ZAKONA, Članak 29.	Što se smatra odgovarajućim osposobljavanjem?	Primljeno na znanje	Članak 29. stavak 3. Prijedloga zakona uvodi obvezu 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, a kako to određuje članak 20.stavak 2. NIS2 direktive. Vezano uz pitanje osposobljavanja napominje se kako je odredbom članka 30. stavkom 1. podstavkom 7. Prijedloga zakona propisano da mjere upravljanja kibernetičkim sigurnosnim rizicima moraju uključivati i osposobljavanje o kibernetičkoj sigurnosti, a kako to određuje i članak 21. stavak 2. točka g) NIS2 direktive. Prema članku 38. Prijedloga zakona, mjere upravljanja kibernetičkim sigurnosnim rizicima i način njihove provedbe, propisuju se uredbom iz članka 24. ovog Zakona. Također, napominje se kako se, sukladno obvezama država članica iz članka 7. NIS2 direktive, člankom 55. stavkom 2. i Prilogom IV. Nacrta, utvrđuje obvezni sadržaj nacionalnog akta strateškog planiranja iz područja kibernetičke sigurnosti, a koji, između ostalog, obuhvaća obvezu razraditi tim aktom politiku 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.
56	Hrvatska udruga menadžera sigurnosti (HUMS)	IV. TEKST PRIJEDLOGA ZAKONA, Članak 30.	(1) Mjere upravljanja kibernetičkim sigurnosnim rizicima uključuju najmanje sljedeće: - politike analize rizika i sigurnosti informacijskih sustava - postupanje s incidentima - kontinuitet poslovanja, kao što je upravljanje sigurnosnim kopijama i oporavak od katastrofe, te upravljanje krizama - sigurnost lanca opskrbe, uključujući sigurnosne aspekte u pogledu odnosa između svakog subjekta i njegovih izravnih dobavljača ili pružatelja usluga - sigurnost u nabavi, razvoju i održavanju mrežnih i informacijskih sustava, uključujući rješavanje ranjivosti i njihovo otkrivanje - politike i postupke za procjenu djelotvornosti mjera upravljanja kibernetičkim sigurnosnim rizicima - osnovne prakse kibernetičke higijene i osposobljavanje o kibernetičkoj sigurnosti - politike i postupke u pogledu kriptografije i, prema potrebi, kriptiranja - sigurnost ljudskih resursa, politike kontrole pristupa i upravljanje imovinom - korištenje višefaktorske provjere autentičnosti ili rješenja kontinuirane provjere autentičnosti, zaštićene glasovne, video i tekstualne komunikacije te sigurnih komunikacijskih sustava u hitnim slučajevima unutar subjekta, prema potrebi Prijedlog je u skladu s čl. 21 Direktive jer transpozicija u trenutnom prijedlogu ne bi bila pravilna radi greške u prvoj rečenici iz čega se može protumačiti kako su taksativno nabrojene politike, a ne mjere.	Prihvaća se	

			Također, Direktiva naglašava da se neke od mjera provode prema potrebi što u trenutnom prijedlogu teksta nije uzeto u obzir.		
57	A1 Hrvatska d.o.o.	IV. TEKST PRIJEDLOGA ZAKONA, Članak 30.	Čl.30.st.1. alineja 5- potrebno pojasniti da li se radi o nabavi svih sustava ili samo kritičnih sustava?	Primljeno na znanje	Odnosi se na sve mrežne i informacijske sustave u cijelosti poslovanja kategoriziranog subjekta.
58	Ana Balaško	IV. TEKST PRIJEDLOGA ZAKONA, Članak 30.	Članak se odnosi na odredbe NIS2 Direktive čl.21.st.2. koji je u prijedlogu Zakona bespotrebno modificiran dodavanjem termina"sigurnosne politike" prije dvotočke, čime su neke odredbe izgubile smisao, kao npr. sigurnosne politike u pogledu kriptografije i, prema potrebi, kriptiranja Zadnja crtica u st.1:- korištenja višefaktorske provjere autentičnosti ili rješenja kontinuirane provjere autentičnosti, zaštićene glasovne, video i tekstualne komunikacije te sigurnih komunikacijskih sustava u hitnim slučajevima unutar subjekta. Dodati na kraj rečenice "prema potrebi" kako je i definirano u NIS2 (čl.21.st.2. točka (j)) Prijedlog: Uskladiti sa NIS2 (čl.21.st2.)	Prihvaća se	
59	Diverto d.o.o.	IV. TEKST PRIJEDLOGA ZAKONA, Članak 30.	Predlažemo da se unutar stavka 1. podstavak 5. "- sigurnosti u nabavi, razvoju i održavanju mrežnih i informacijskih sustava, uključujući otklanjanje ranjivosti i njihovo otkrivanje" podijeli na dva dijela na slijedeći način: - sigurnosti u nabavi, razvoju i održavanju mrežnih i informacijskih sustava - upravljanje ranjivostima uključujući otklanjanje ranjivosti i njihovo otkrivanje Obrazloženje: Umjesto otklanjanja i otkrivanja ranjivosti predlažemo da se propiše obveza upravljanja ranjivostima koja je nešto širi pojam i podrazumijeva proaktivan i kontinuiran proces prepoznavanja, procjenjivanja i otklanjanja potencijalnih sigurnosnih slabosti vezanih uz IKT, te organizacijske i operativne postupke pri upravljanju IKT-om. Također, s obzirom da ranjivosti ne moraju biti nužno vezane samo za mrežne i informacijske sustave već i za organizacijske i operativne postupke, predlažemo da se upravljanje ranjivostima izdvoji kao zasebni podstavak. Dodatno, predlažemo da se u stavak 1. dodaju i sljedeće mjere: - sigurnost u upravljanju, izgradnji i pružanju aplikativnih rješenja Obrazloženje: Sigurnost aplikativnih rješenja važna je jer aplikacije često sadrže osjetljive podatke i podržavaju rad poslovnih procesa zbog čega je važno osigurati njihov nesmetan rad. Uvođenjem sigurnosti u upravljanje aplikacijama osigurava se minimiziranje ranjivosti koje mogu proizaći iz ne upravljanja aplikacijskom sigurnošću, neprovedenog testiranja promjene i sl. Iako ostale točke indirektno govore o sigurnosti na svim razinama što uključuje i aplikacije, mislimo da je važno istaknuti ovu točku kako bi nedvojbeno istaknulo važnost aplikacijske sigurnosti i sve važniji element u osiguravanju informacijskih sustava. - osvješćivanje i izgradnja sigurnosnih kompetencija ljudskih resursa Obrazloženje: Jačanje svijesti o kibernetičkoj sigurnosti jedan je od ciljeva NIS 2 direktive i ovog Zakona. Također, nedovoljna razina osviještenosti ljudskih resursa jedna je od najčešći ranjivosti organizacija. - jačanje IKT sustava Obrazloženje: Jačanje IKT sustava je potrebno	Primljeno na znanje	Članak je prikladno i dodatno usklađen isključivo prema sadržaju članka 21. stavka 2. NIS2 direktive koji se člankom 30. stavkom 1. prenosi u nacionalno zakonodavstvo.

			navesti jer predstavlja proces podizanja razine sigurnosti sustava smanjenjem njegove površine ranjivosti, a uključuje kontinuirano popravljanje sigurnosnih propusta, uključujući zakrpe na sustavima, konfiguracije, identifikaciju zlonamjernog koda, nadzor nad kontrolama pristupa, itd.		
60	A1 Hrvatska d.o.o.	IV. TEKST PRIJEDLOGA ZAKONA, Članak 31.	Čl.31.st.2. alineja 2- arbitrarno određeni kriteriji – mogućnost širokog tumačenja što će rezultirati pravnom nesigurnošću za obveznika ovog Zakona	Ne prihvaća se	Radi se odgovornosti subjekta za korisnike njegovih usluga koja je na EU razini usklađena NIS2 zahtjevima. Člankom 31. Prijedloga zakona prenosi se u nacionalno zakonodavstvo članak 23. stavci 1. i 3. NIS2 direktive. Ovim odredbama opisno se određuje koji incident se smatra značajnim incidentom. Sukladno članku 38. Prijedloga zakona, kriteriji za utvrđivanje značajnih incidenata, uključujući kriterijske pragove ako su potrebni zbog specifičnosti pojedinog sektora, propisat će se uredbom iz članka 24. Zakona.
61	NINO ŠETUŠIĆ	IV. TEKST PRIJEDLOGA ZAKONA, Članak 31.	U prijedlogu stoji: „- ako je uzrokovao ili može uzrokovati ozbiljne poremećaje u funkcioniranju usluga koje subjekt pruža odnosno djelatnosti koju obavlja ili financijske gubitke za subjekt“ Potrebno bi bilo izmijeniti „financijske gubitke“ za subjekt u „značajne financijske gubitke“ ili nešto slično. Npr. financijski gubitak od 100€ zbog ne dostupnosti web shopa ne bih okarakterizirao kao značajni incident ali bih se iz ovog uvjeta tako mogao shvatiti.	Ne prihvaća se	Poslovni subjekti gubitke stavljaju u relaciju sa svojim ukupnim prometom i dobiti te su oni u tom smislu vrlo različiti po iznosu u različitim sektorima i subjektima, ali svi subjekti imaju u tom smislu dobro razrađenu financijsku praksu. Člankom 31. Prijedloga zakona prenosi se u nacionalno zakonodavstvo članak 23. stavci 1. i 3. NIS2 direktive. Ovim odredbama opisno se određuje koji incident se smatra značajnim incidentom. Sukladno članku 38. Prijedloga zakona, kriteriji za utvrđivanje značajnih incidenata, uključujući kriterijske pragove ako su potrebni zbog specifičnosti pojedinog sektora, propisat će se uredbom iz članka 24. Zakona.
62	Karlo Paljug	IV. TEKST PRIJEDLOGA ZAKONA, Članak 31.	Direktiva kao sekundarni izvor prava EU je tu da pruži određeni cilj državama članicama, koje onda u implementacijskom roku trebaju nači način kako taj cilj zadovoljiti. S obzirom da se radi o prepisanom tekstu u pogledu kada se incident smatra značajnim iz NIS2, nužno je dodati jasnije kriterije. Npr. termin znatna materijalna šteta bi koja bila za pojedinca - 1000EUR? Također, znatna nematerijalna šteta kod povrede podataka fizičkih osoba teško da bi prelazila 500 EUR sukladno sudskoj praksi njemačkih sudova. Teško da bi se iznos mogao smatrati znatnim pa bi samim time, termin značajnog invidenta postao incident koji se često i ne prijavljuje. Takvo bi postupanje imalo bi negativan daljnji utjecaj na prava i slobode pojedinaca.	Ne prihvaća se	NIS2 direktiva ide za tim da osigura opći okvir za prepoznavanje incidenata koji se smatraju značajnim, što će se u određenoj mjeri dodatno razraditi u Uredbi iz članka 24. Zakona, kao i kroz praksu rada nadležnih CSIRT tijela i najbolje prakse u drugim državama članicama. Člankom 31. Prijedloga zakona prenosi se u nacionalno zakonodavstvo članak 23. stavci 1. i 3. NIS2 direktive. Ovim odredbama opisno se određuje koji incident se smatra značajnim incidentom. Sukladno članku 38. Prijedloga zakona, kriteriji za utvrđivanje značajnih incidenata, uključujući kriterijske pragove ako su potrebni zbog specifičnosti pojedinog sektora, propisat će se uredbom iz članka 24.

					Zakona. Sukladno članku 66. Prijedloga zakona, nadležni CSIRT donosi smjernice za ujednačavanje i unaprjeđenje stanja obveze obavještavanja iz članka 31. Zakona.
63	Jurica Čular	IV. TEKST PRIJEDLOGA ZAKONA, Članak 31.	Tko i sukladno kojim mjerilima procjenjuje da je incident značajan, odnosno da „je uzrokovao ili može uzrokovati ozbiljne poremećaje u funkcioniranju usluga“. Ako je to sam obveznik Zakona, ostavlja se sloboda da svatko „procjeni“ da nešto ipak nije ozbiljan poremećaj. U prvotnoj verziji Zakona postojali su jasni pragovi narušavanja usluge koji ukazuju da se radi o značajnom incidentu. Ovaj komentar se odnosi i na sve naredne članke kojima se propisuju obveze vezano za prijavu značajnih incidenata – ako subjekt sam procjenjuje značaj, da li je slobodan sve proglasiti „bez značajnim“ i da li zbog toga može biti kažnjen?	Ne prihvaća se	Člankom 31. Prijedloga zakona prenosi se u nacionalno zakonodavstvo članak 23. stavci 1. i 3. NIS2 direktive. Ovim odredbama opisno se određuje koji incident se smatra značajnim incidentom. Sukladno članku 38. Prijedloga zakona, kriteriji za utvrđivanje značajnih incidenata, uključujući kriterijske pragove ako su potrebni zbog specifičnosti pojedinog sektora, propisat će se uredbom iz članka 24. Zakona. Sukladno članku 66. Prijedloga zakona, nadležni CSIRT donosi smjernice za ujednačavanje i unaprjeđenje stanja obveze obavještavanja iz članka 31. Zakona.
64	Karlo Paljug	IV. TEKST PRIJEDLOGA ZAKONA, Članak 33.	Predlažem doradu ćlanka na način da se u istome doda: (2) Nadležni CSIRT će o incidentima i prijetnjama iz stavka 1. ovog članka uspostaviti registar kako bi se kotinuirano pratilo stanje kibernetičke sigurnosti na nacionalnoj razini. (3) Nadležni CSIRT će obavještavati o kibernetičkim prijetnjama ostale ključne i važne subjekte u najkraćem mogućem roku, a najkasnije u roku od 3 dana od dana zaprimanja obavjesti iz stavka 1. ovog članka.	Ne prihvaća se	CSIRT tijela imaju odgovornost za praćenje i rješavanje značajnih kibernetičkih incidenata i prijetnji, kao i za evidentiranje prijavljenih incidenata, njihovo rješavanje, odnosno pružanje pomoći subjektu u rješavanju incidenta. Člankom 33. otvorena je dodatna mogućnost subjektima za prijavu svih incidenata pa i onih izbjegnutih, a kako se to zahtjeva člankom 30. stavkom 1. točkom a) NIS2 direktive. Vrste i sadržaj obavijesti iz članka 33., kao i rokovi za njihovu dostavu propisat će se uredbom iz članka 24. Zakona (utvrđeno člankom 38. Prijedloga zakona).
65	Karlo Paljug	IV. TEKST PRIJEDLOGA ZAKONA, Članak 35.	Razmisliti o načinu obavještavanja javnosti. Možda u slučaju značajnog incidenta obavijestiti javnost i putem javne televizije kako bi se samim time podigla razina svjesti i kod građana o važnosti kibernetičke sigurnosti.	Primljeno na znanje	Pored članka 35., obavještavanje javnosti redovna je procedura u programima razvoja sigurnosne svijesti koji postoje u nizu Zakonom obuhvaćenih sektora. Također, to je dio područja upravljanja kibernetičkim krizama, a i redovitih izvješća koje nadležna CSIRT i druga tijela redovito komuniciraju s javnosti.
66	Diverto d.o.o.	IV. TEKST PRIJEDLOGA ZAKONA, Članak 37.	Naše razumijevanje ovog članka je da će se informacije o incidentima ključnih i važnih subjekata, uključujući i tajne podatke koje takve informacije mogu sadržavati prikupljati unutar CARNET-a, bez obzira je li CARNET nadležno tijelo subjekta ili nije. Ako je navedena tvrdnja točna, potrebno je uzeti u obzir potencijalne probleme koji mogu nastati vezano uz klasifikaciju informacija.	Primljeno na znanje	CARNET je upravitelj nacionalne platforme za prikupljanje, analizu i razmjenu podataka o kibernetičkim prijetnjama i incidentima, kao jedinstvene ulazne točke za obavještavanje o kibernetičkim prijetnjama i incidentima. Sva nadležna tijela i ključni subjekti iz Zakona su korisnici ove platforme, pri čemu svatko ima pravo pristupa podacima na platformi u skladu s nadležnostima iz Zakona i to se odnosi i na CARNET. Ova platforma (PiXi) je realizirana i danas radi na ovaj način, ali prema zahtjevima NIS1 transpozicije.

67	A1 Hrvatska d.o.o.	IV. TEKST PRIJEDLOGA ZAKONA, Članak 38.	Čl.38. -u izradu Uredbe potrebno uključiti sve bitne dionike radi transparentnosti i preciznosti obveza i njihovog ispunjenja s obzirom na bitnost teme i mogućnosti kažnjavanja	Primljeno na znanje	Prilikom izrade Uredbe planira se primijeniti međuresorni pristup te uključiti sve relevantne dionike.
68	Ana Balaško	IV. TEKST PRIJEDLOGA ZAKONA, Članak 38.	S obzirom da se članak 38. kao i članak 24. odnose na istu Uredbu, prijedlog da se članci objedine u jedan u kojem će jasnije biti definirano što će sve biti dodatno propisano predmetnom Uredbom, tko će ju donijeti i u kojem roku.	Ne prihvaća se	Opis i obuhvat Uredbe iz čl. 24. napravljen je u skladu s nomotehničkim pravilima. Zainteresirani se mogu uputiti na aktualni Zakon i Uredbu o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga (NN 64 i 68 /2018) u kojima je primijenjen isti pristup u nešto užem opsegu NIS1 transpozicije.
69	A1 Hrvatska d.o.o.	IV. TEKST PRIJEDLOGA ZAKONA, Članak 39.	Čl.39.st.2. Potrebno pojasniti kako će provoditi postupci ocjene sukladnosti ili samoocjena s obzirom na dosadašnju praksu u sektoru elektroničkih komunikacija koja je bila propisana Pravilnikom o načinu i rokovima provedbe mjera zaštite sigurnosti mreža i usluga i koji se sada, prema našem razumijevanju, kao dio članka 41. ZEK-a stavlja van snage?	Primljeno na znanje	Uredbom iz članka 24. će se dodatno razraditi niz aspekata iz Zakona pa i zahtjevi za provedbu postupka ocjene sukladnosti i mogućnost autorizacije pravnih osoba za obavljanje ovih poslova. Za ključne subjekte provodit će se ocjena sukladnosti, a za važne samoocjena sukladnosti. Ove odredbe obvezuju i sektor elektroničkih komunikacija, s obzirom da se te odredbe u ZEK-u stavljaju izvan snage. Sukladno članku 41. stavku 2. Prijedloga zakona, ocjene sukladnosti u sektoru elektroničkih komunikaciji provodit će privatni subjekti koji ispunjavaju organizacijske i stručne zahtjeve za autorizaciju propisane Uredbom iz članka 24. Zakona.
70	A1 Hrvatska d.o.o.	IV. TEKST PRIJEDLOGA ZAKONA, Članak 41.	Čl.41.st.6. Potrebno je pojasniti proces nakon što ključni subjekti izrade ocjenu sukladnosti – kojem se tijelu dostavlja ocjena sukladnosti, koje tijelo sastavlja izvješće, kojem tijelu se dostavlja izvješće u roku od 8 dana koji možda neće biti moguće ispuniti ukoliko zatraženi izvješće neko drugo nadležno tijelo nije sastavilo?	Primljeno na znanje	U slučaju ključnih subjekata ocjenu sukladnosti izrađuje tijelo za ocjenu sukladnosti, odnosno autorizirana pravna osoba. Izvješće se dostavlja ključnom subjektu koji je dužan jedan primjerak izvješća dostaviti nadležnom tijelu za provedbu zahtjeva kibernetičke sigurnosti (u slučaju A1 to je HAKOM).
71	A1 Hrvatska d.o.o.	IV. TEKST PRIJEDLOGA ZAKONA, Članak 41.	Čl.41.st.3. Koja je razlika između samostalnog provođenja ocjene sukladnosti i samoocjene sukladnosti iz članka 42. Zakona ?	Djelomično se prihvaća	Radi jasnoće, stavak 3. na koji se odnosi upit izmijenjen na način da je riječ „samostalno“ zamijenjena riječima „kao zaseban postupak“.
72	Ana Balaško	IV. TEKST PRIJEDLOGA ZAKONA, Članak 41.	Stavak 8. nejasno definiran: "Troškove provedbe ocjene sukladnosti snose ključni i važni subjekti, ako nije drugačije propisano ovim Zakonom.",	Primljeno na znanje	Troškove snose ključni i važni subjekti osim u slučaju iz članka 80. stavka 3. ovog Zakona.
73	Diverto d.o.o.	IV. TEKST PRIJEDLOGA ZAKONA, Članak 41.	Predlažemo da se definira predložak (format i sadržaj) izvješća o ocjeni sukladnosti kako bi izvješća bila unificirana za sve subjekte. Predlošci bi omogućili bržu provedbu ocjene sukladnosti te bi kasnije olakšali analizu rezultata i olakšali praćenje trendova kroz vremenski period.	Primljeno na znanje	Razrada i unificiranje procesa ocjene sukladnosti predviđena je člankom 44. Prijedloga zakona.
74	Jurica Čular	IV. TEKST PRIJEDLOGA ZAKONA, Članak 42.	Na koji način i tko može provoditi samoocjenu sukladnosti? Iako se radi o samoocjeni, ipak je riječ o svojevrsnoj reviziji provođenja mjera sigurnosti koje se provodi, a za što su potrebna određena stručna znanja. Da li se očekuje da u svim subjektima koji provode samoocjenu postoje ti resursi? Jer ne postoje. A u skladu s time postupak samoocjene će se svesti na jednostavno potpisivanje checkliste od strane odgovorne osobe. Time će se i ti subjekti i javnost i država u cjelini zapravo samozavaravati da su	Primljeno na znanje	Kako je Zakonom definirano, samoocjenu provode važni subjekti i snose troškove te procjene bilo da ju rade samostalno ili da angažiraju treću stranu. Za proces samoocjene odgovorni su subjekti koji su ju dužni provoditi te u slučaju incidenta za koji se nadzorom utvrdi da je nastao uslijed loše provedbe mjera koja nije utvrđena samoocjenom, važni subjekt podliježe

			usklađeni.		prekršajnoj odgovornosti.
75	Diverto d.o.o.	IV. TEKST PRIJEDLOGA ZAKONA, Članak 44.	Predlažemo da se popravi konzistentnost u člancima 24. i 44. U članku 24. navodi se da će se uredbom donijeti mjerila za procjenu, a u članku 44. navodi se da će se uredbom iz članka 24. urediti 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.	Ne prihvaća se	Takav pristup je rezultat nomotehničkih pravila i sve članke koji se povezuju s člankom 24. potrebno je promatrati kumulativno, vodeći računa o tome da svaki za sebe predstavljaju poseban sadržaj koji će se razraditi Uredbom iz članka 24.
76	MARKO RAKAR	IV. TEKST PRIJEDLOGA ZAKONA, 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 pristupiti ključni i važni subjekti, kao i privatni i javni subjekti koji nisu kategorizirani kao ključni i 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 pojedine kategorije ključnih subjekata, 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. (6) Nacionalnim sustavom prati se isključivo imovina subjekta koja je izložena internetu (imovina subjekta s internetskim sučeljem), te nacionalni sustav nema pravo pristupa lokalnim resursima subjekta, osim ako to nije određeno drugim zakonom.	Ne prihvaća se	Članak 51. dio je dobrovoljnih mehanizama Zakona, a izričaj o obvezivanju određenih tijela javnog sektora na pristupanje sustavu iz članka 52. dodatno je prilagođen i pojašnjen.
77	MARKO RAKAR	IV. TEKST PRIJEDLOGA ZAKONA, Članak 51.	Ovim člankom se propisuje kako će subjekt, a koji je diskrecijskom odlukom definiranom u članku 24. ovog prijedloga morati pristupiti „nacionalnom sustavu za otkrivanje kibernetičkih prijetnji i zaštitu kibernetičkog prostora“. Sustav SK@UT koji predstavlja nacionalni „kibernetički kišobran“ (gore spomenuti nacionalni sustav) sastoji se od nekoliko komponenti (alata), od kojih su neki invazivne prirode na način da podrazumijevaju pristup lokalnoj mreži/komunikaciji nadziranog subjekta. Obzirom da je sukladno zakonu, nadležni CSIRT obavještajna agencija, postavlja se pitanje prekomjernosti dosega obavještajne agencije prema podacima kojima subjekt raspolaže (osobnim podacima, poslovnim tajnama i sl.) pod krinkom zakonske obveze. NIS2 direktiva (točka 44. preambule), precizno navodi kako bi CSIRT-ovi trebali imati „mogućnost na zahtjev ključnog ili važnog subjekta pratiti imovinu subjekta s internetskim sučeljem“. Nadalje, u NIS2 direktivi nema naznake da bi CSIRT (sa svojim alatima) mogao ili smio imati pristup lokalnim resursima subjekta koji je kategoriziran kao ključni ili važni.	Ne prihvaća se	Izuzev određenih tijela javnog sektora, svi ostali ključni i važni subjekti nisu obavezni na pristupanje sustavu iz članka 51. Prijedloga zakona. Svi subjekti koji dobrovoljno odluče pristupiti sustavu iz članka 51. potpisuju sporazum o utvrđenim međusobnim pravima i odgovornostima te načinu uvida u podatke na sustavu i njihovom korištenju. Ovaj pristup se primjenjuje na potpuno isti način već nekoliko godina temeljem odluke Vlade iz 2021. godine te sustav pod imenom SK@UT danas štiti više od 60 državnih tijela, operatora ključnih usluga i pravnih osoba od posebnog interesa za RH, pri čemu su svi operatori ključnih usluga i druge pravne osobe uključeni dobrovoljno, na njihov zahtjev i na temelju sigurnosne procjene SOA-e.

			Predlaže se da se članak 51. preformulira na način da se precizno navede kako je primjena dopuštena na zahtjev ključnog ili važnog subjekta isključivo pratiti imovinu subjekta s internetskim sučeljem, a kako bi se spriječile buduće zlouporabe obavještajnog sustava.		
78	JAGOR ČAKMAK	IV. TEKST PRIJEDLOGA ZAKONA, Članak 51.	Zastrašujuće je da SOA kao dio obavještajnog aparata ima pravo nadgledati privatni promet kompanija i pristup njihovim podatcima (i podatcima svih zaposlenika) bez ikakvog sudskog naloga. Dodatno jedan takav alat (SK@UT) bi sam po sebi stvarao ogromnu ugrozu cijele IT infrastrukture u RH ako se taj sustav kompromitira, pogotovo s obzirom na to da je to sustav dijelom rađen na bazi projekta otvorenog koda. Također vrlo praktično pitanje se postavlja i tko podnosi troškove toga ako je predmet nadzora u cloudu i ne posjeduje vlastitu fizičku infrastrukturu?	Ne prihvaća se	Sustav iz članka 51. Prijedloga zakona predstavlja nacionalnu SOC (Security Operations Centre) mrežu, koja se sastoji od distribuiranih senzora i centralnog SOC-a. Takvi sustavi su raspoloživi u najmanje polovini EU država članica, a Europska komisija kroz prijedlog Cyber Solidarity Acta iz travnja 2023. godine potiče njihovo daljnje širenje i međusobno povezivanje. Aktualno španjolsko EU predsjedništvo stavilo je prioritet kibernetičkih aktivnosti upravo na nacionalne SOC mreže država članica te je SOA ispred RH dala doprinos u traženju daljnjeg EU puta razvoja ovakvih nacionalnih rješenja. Sustav SK@UT je izgrađen u okviru Centra za kibernetičku sigurnost SOA-e te služi za otkrivanje i zaštitu od državno-sponzoriranih kibernetičkih napada, APT kampanja (*Advanced Persistent Threat*) te drugih kibernetičkih ugroza. SK@UT tako predstavlja kibernetički kišobran RH koji trenutno pokriva više od 60 državnih tijela, operatora ključnih usluga i pravnih osoba od posebnog interesa za RH. Centar za kibernetičku sigurnost SOA-e putem sustava SK@UT štiti, a ne nadzire, ministarstva i ključna državna tijela, niz operatora ključne infrastrukture, uključujući i privatne tvrtke koje su se dobrovoljno uključile u sustav SK@UT.
79	Jurica Čular	IV. TEKST PRIJEDLOGA ZAKONA, Članak 51.	Vezano uz moj komentar na članak 64., proizlazi da SOA-a (kao nadležno tijelo za provedbu zahtjeva kibernetičke sigurnosti) može obveznicima naložiti pristupanje sustavu i postavljanje senzora sustava SK@UT (koji razvija SOA, kao središnje državno tijelo za kibernetičku sigurnost) u informacijski sustav privatnih gospodarskih subjekata koji su definirani kao ključni ili važni. Primjeri takvih pružatelja su pružatelji usluga podatkovnog centra, pružatelji usluga računalstva u oblaku, pružatelji platformi za usluge društvenih mreža, subjekti koji obavljaju djelatnosti istraživanja i razvoja lijekova, itd. Obzirom na ovlasti SOA-e za provođenjem tajnih postupaka i mjera prikupljanja podataka sukladno Zakonu o sigurnosno-obavještajnom sustavu Republike Hrvatske, smatram da ovakve ovlasti dodijeljene SOA-i nisu razmjerne potrebama te mogu dovesti do zloupotreba i nepovjerenja obveznika ovog Zakona te javnosti u SOA-u kao Nadležno tijelo za provedbu zahtjeva	Ne prihvaća se	Izuzev određenih tijela javnog sektora svi ostali ključni i važni subjekti nisu obavezni na pristupanje ovom sustavu iz članka 51. Prijedloga zakona. Svi subjekti koji dobrovoljno odluče pristupiti sustavu iz članka 51. potpisuju sporazum o utvrđenim međusobnim pravima i odgovornostima te načinu uvida u podatke na sustavu i njihovog korištenja,. Ovaj način se primjenjuje na potpuno isti način već nekoliko godina te sustav danas štiti više od 60 državnih tijela, operatora ključnih usluga i pravnih osoba od posebnog interesa za RH., pri čemu su svi operatori ključnih usluga i druge privatne pravne osobe uključene dobrovoljno, na njihov zahtjev i na temelju sigurnosne procjene SOA-e.

80	Jurica Čular	IV. TEKST PRIJEDLOGA ZAKONA, Članak 51.	Da li Zakon predviđa i pristupanje nacionalnom sustava dijelova infrastrukture subjekta koja se nalazi izvan RH? Ako da, ovo bi moglo biti vrlo problematično iz aspekta sukoba nadležnosti zakonodavnih sustava različitih zemalja.	Primljeno na znanje	Ne.
81	Stjepan Groš	IV. TEKST PRIJEDLOGA ZAKONA, Članak 53.	Koji je smisao ovog članka? Bez obzira pisalo u zakonu da bilo tko može razmjenjivati podatke, to je uvijek moguće. Dakle, ovo se čini redundantnim? Tim više što se članak odnosi i na one koji nisu obveznici ovog zakona.	Primljeno na znanje	Svaka razmjena sigurnosno osjetljivih podataka mora imati pravila, čak i kada je dobrovoljna. Upravo ta pravila su definirana ovim člankom, a dobrovoljni način razmjene se kao takav potiče, ali uz svijest o potrebi korištenja međusobnih pravila u razmjeni podataka. Člankom 53. prenosi se u nacionalno zakonodavstvo članak 59. NIS2 direktive.
82	A1 Hrvatska d.o.o.	IV. TEKST PRIJEDLOGA ZAKONA, Članak 58.	čl.58. Da li su operatori elektroničkih komunikacija adresati vježbe i ako da u kojem opsegu jer je potrebno znati unaprijed scenarije vježbe?	Primljeno na znanje	Zakonom se propisuje samo opći okvir za održavanje nacionalnih i međunarodnih vježbi. Scenariji se u svakom pojedinom slučaju planiranih vježbi utvrđuju i organiziraju više mjeseci ili po godinu dana unaprijed i pravovremeno se koordiniraju sa svim planiranim sudionicima.
83	Stjepan Groš	IV. TEKST PRIJEDLOGA ZAKONA, Članak 58.	Tijekom pripreme vježbe Kibernetički štit 2020 (koja zbog pandemije nije održana), a i tijekom provođenja drugih vježbi, stečena su iskustva temeljem kojih bi bilo dobro doraditi ovaj članak. Prije svega, kriza nastaja kao posljedica nemogućnosti odgovora na incident unutar jednog ili više kritičnih subjekata što se onda prelijeva na nacionalnu razinu.Prema tome, da bi se složila dobra vježba NUŽNO je imati u ekipi i eksperte koji dolaze iz kritičnih ili važnih subjekata koji pomažu tijekom izrade vježbe. To je bio problem jer nije postojala nikakva obaveza sudjelovanja kritičnih subjekata u vježbi ili u pripremi vježbe. Alternativno, kriza nije posljedica incidenta u kibernetičkom prostoru, ali kroz kibernetički prostor se takva kriza dodatno amplificira. Međutim, priprema za takve slučajeve vjerojatno ne spada u okvire ovog zakona. Nadalje, bilo bi dobro da kritični i važni subjekti provode vježbe koje bi se koristile kao ulazi u planiranje nacionalne vježbe - barem na razini uprava. Nigdje nije propisano da bi oni to trebali raditi, ali tijekom vježbi koje su obavljene ispostavlja se da vježbe nisu samo korisne za pripremu odgovornih osoba za incident, VEĆ SU I JAKO DOBAR ALAT ZA OSVJEŠTAVANJE, POSEBNO UPRAVA.	Primljeno na znanje	Zakonom se po prvi puta na nacionalnoj zakonskoj razini propisuje instrument vježbi kibernetičke sigurnosti, a provedba samih vježbi razrađivat će se kroz planove i scenarije budućih vježbi. Što plan provedbe vježbi treba sadržavati propisano je člankom 58. stavkom 4. Prijedloga zakona.
84	Stjepan Groš	IV. TEKST PRIJEDLOGA ZAKONA, Članak 59.	Prva točka prvog stavka - popis ključnih i važnih subjekata bi morao biti PRIORITIZIRAN. Nisu svi jednaki, niti svi zahtjevaju istu pažnju, niti svi imaju jednaku slobodu. Kritični subjekt čiji incident može napraviti incident na nacionalnoj razini sigurno nije jednako vrijedan kao i kritični subjekt na regionalnoj razini. O tome je već bilo riječi kod članka koji se bavi procjenama rizika. Dodatno, resursa da se država bavi sa svima na isti način gotovo sigurno nema. Sve se to može riješiti prioritetnom listom (koja može biti različitih oblika - što bi se vjerojatno definiralo kroz uredbu iz članka 24). U članku 75, stavku 4 se govori da se to može napraviti i to prema "kategoriji rizičnosti".	Ne prihvaća se	Prioriteti se postavljaju kod procjene rizika u svrhu kraćeg ili dužeg razdoblja za provedbu redovitog nadzora (3 do 5 godina), čime se postiže mogućnost boljeg nadzora rizičnijih ključnih subjekata.
85	Ana Balaško	IV. TEKST PRIJEDLOGA ZAKONA,	Zamijeniti stavak 1. i stavak 2.	Ne prihvaća se	Korišten pristup u raspoređivanju odredbi kakav je korišten i u članku 59. Prijedloga zakona odnosno prvim

		Članak 61.			stavkom se utvrđuju poslovi, a stavkom 2. koje tijelo ih obavlja.
86	MARKO RAKAR	IV. TEKST PRIJEDLOGA ZAKONA, Članak 61.	Mandat SOA-e (članak 23. Zakona o sigurnosno obavještajnom sustavu RH) eksplicitno definira kako SOA brine o neovlaštenom ulasku u zaštićene informacijske i komunikacijske sustave državnih tijela. Definiranjem SOA-e kao središnjeg državnog tijela za kibernetičku sigurnost izlazi se iz zakonom definiranog djelokruga rada SOA-e. Nadalje, SOA je kao obavještajna agencija u svojem radu zaštićena tajnom, izuzeta je iz zakona o javnoj nabavi, te ne podliježe većini demokratskih mehanizama za nadzor svojeg poslovanja, nema gotovo nikakve obveze za transparentnim djelovanjem. Istovremeno, u smislu NIS2 direktive biti će zadužena za redovitu komunikaciju, te postaje regulatorno tijelo za vrlo veliki broj pravnih subjekata (državnih, javnih i privatnih) što je suprotno samoj prirodi funkcioniranja obavještajne agencije. Osim toga, u okviru koordinacije i izvještavanja koje proizlaze iz primjene NIS2 direktive, SOA će komunicirati s drugim EU tijelima, a koja su redom civilna. Istovremeno, Zavod za sigurnost informacijskih sustava (ZSIS) u svojem mandatu (članak 14. Zakona o sigurnosno obavještajnom sustavu RH) eksplicitno navodi kako ZSIS obavlja poslove u područjima sigurnosti informacijskih sustava. Stoga je sasvim jasno i logično kako je ZSIS tijelo koje je trebalo biti imenovano središnjim državnim tijelom za kibernetičku sigurnost. Širina obuhvata NIS2 direktive će posljedično u redovima veličine proširiti prostor na kojem SOA djeluje, a značajno izvan zakonskog okvira koji je za SOA-u definiran, ali i definicije koja je sadržana u NIS2 direktivi. Predlaže se stoga da se središnjim državnim tijelom za kibernetičku sigurnost proglasi ZSIS, te da se ZSIS izdvoji iz obavještajnog sustava RH i pretvori u Vladin ured ili Agenciju, a koji u cijelosti djeluje kao civilni subjekt. Alternativno, moguće je (neovisno o nepopularnosti takve odluke), osnovati sasvim novi ured ili agenciju koja će se baviti ovim iznimno značajnim aspektom funkcioniranja društva. I svakako treba spomenuti i problem financiranja, SOA za svoje cjelokupno djelovanje ima 55mil EUR, a ZSIS nešto manje od 3mil EUR godišnje; istovremeno i usporedbe radi, HAKOM kao regulator telekomunikacijskog sektora ima 15mil EUR proračuna.	Ne prihvaća se	Kibernetička sigurnost je integralni dio nacionalne sigurnosti u svim članicama EU. Odabir središnjeg tijela, odnosno izgradnja nacionalnog centra za kibernetičku sigurnost, u svim državama provodi se na temelju tradicije razvoja i raspoloživih sposobnosti i resursa. U RH je sigurnosno-obavještajni sustav bio nositelj izrade Nacionalne strategije kibernetičke sigurnosti 2014. godine, NIS1 transpozicije 2018. godine, pa je kroz Nacionalno vijeće za kibernetičku sigurnost nastavljen isti pristup i sa NIS2 transpozicijom. Odabir SOA-e je rezultat procjene da će se interni Centar za kibernetičku sigurnost SOA-e moći najbrže i najučinkovitije transformirati u nužno potrebni Nacionalni centar za kibernetičku sigurnost (NCSC). Ne postoji jednoobrazno rješenje oko osnivanja NCSC-a na razini EU i svaka članica osnivanje NCSC-a regulira temeljem vlastitih specifičnosti, potreba i već razvijenih kapaciteta, a veći broj članica EU je za osnivanje NCSC-a koristila sigurnosno-obavještajne sustave. Primjerice, u Danskoj, Španjolskoj, Grčkoj (članice EU), kao i Velikoj Britaniji, Kanadi, Južnoj Koreji i drugim razvijenim državama, NCSC je dio sigurnosnih i obavještajnih sustava, dok su neke zemlje poput Njemačke i Italije proces osnivanja NCSC-a započele u okvirima sigurnosno-obavještajnog sustava (navedene dvije članice EU su naknadno provodile daljnju organizacijsku transformaciju NCSC tijela u samostalne agencije, ali su godinama njihova NCSC tijela funkcionirala unutar sigurnosno-obavještajnih sustava tih država). U Francuskoj se središnje tijelo za kibernetičku sigurnost (ANSSI) nalazi unutar sustava obrane i nacionalne sigurnosti te odgovara državnom tajniku za obranu i nacionalnu sigurnost.
87	Jurica Čular	IV. TEKST PRIJEDLOGA ZAKONA, Članak 64.	Ne dovodeći u pitanje kompetencije koje postoje u SOA-i za obavljanje ovih zadaća, smatram da, sa stajališta mogućih zloupotreba i narušavanja povjerenja javnosti, nije prihvatljivo SOA-i dodijeliti sve 3 uloge: (1) Nadležno tijelo za provedbu zahtjeva kibernetičke sigurnosti (2) Središnje državno tijelo za kibernetičku sigurnost i (3) Jedinstvena kontaktna točka. Naime, ovlasti primjene tajnih postupaka i mjera prikupljanja podataka kakve su Zakonom o sigurnosno-obavještajnom sustavu Republike Hrvatske dodijeljene SOA-i te temeljne zadaće SOA-e definirane istim zakonom nisu u skladu s karakteristikama koje su nužne za obavljanje navedene 3 uloge. Dodjela ovih uloga SOA-i može spriječiti učinkovitu suradnju i razmjenu	Ne prihvaća se	Kibernetička sigurnost je integralni dio nacionalne sigurnosti u svim članicama EU. Odabir središnjeg tijela, odnosno izgradnja nacionalnog centra za kibernetičku sigurnost, u svim državama provodi se na temelju tradicije razvoja i raspoloživih sposobnosti i resursa. U RH je sigurnosno-obavještajni sustav bio nositelj izrade Nacionalne strategije kibernetičke sigurnosti 2014. godine, NIS1 transpozicije 2018. godine, pa je kroz Nacionalno vijeće za kibernetičku sigurnost nastavljen isti pristup i sa NIS2 transpozicijom. Odabir SOA-e je

			informacija, a potreba za učinkovitijom suradnjom nadležnih tijela posebno je naglašena kao razlog donošenja NIS2 direktive. Ovlasti SOA-e za provođenjem tajnih postupaka i mjera prikupljanja podataka također mogu dovesti do zloupotreba i nepovjerenja obveznika ovog Zakona u SOA-u kao Nadležno tijelo za provedbu zahtjeva. Vidite i komentar na članak 51. Sukladno Zakonu o sigurnosno-obavještajnom sustavu Republike Hrvatske, dio zadaća iz ovog Zakona dodijeljenih SOA-i bolje bi ispunjavao Zavod za sigurnost informacijskih sustava (ZSIS), obzirom na svoje temeljne zadaće i kompetencije.		rezultat procjene da će se interni Centar za kibernetičku sigurnost SOA-e moći najbrže i najučinkovitije transformirati u nužno potrebni Nacionalni centar za kibernetičku sigurnost (NCSC). Ne postoji jednoobrazno rješenje oko osnivanja NCSC-a na razini EU i svaka članica osnivanje NCSC-a regulira temeljem vlastitih specifičnosti, potreba i već razvijenih kapaciteta, a veći broj članica EU je za osnivanje NCSC-a koristila sigurnosno-obavještajne sustave. Primjerice, u Danskoj, Španjolskoj, Grčkoj (članice EU), kao i Velikoj Britaniji, Kanadi, Južnoj Koreji i drugim razvijenim državama, NCSC je dio sigurnosnih i obavještajnih sustava, dok su neke zemlje poput Njemačke i Italije proces osnivanja NCSC-a započele u okvirima sigurnosno-obavještajnog sustava (navedene dvije članice EU su naknadno provodile daljnju organizacijsku transformaciju NCSC tijela u samostalne agencije, ali su godinama njihova NCSC tijela funkcionirala unutar sigurnosno-obavještajnih sustava tih država). U Francuskoj se središnje tijelo za kibernetičku sigurnost (ANSSI) nalazi unutar sustava obrane i nacionalne sigurnosti te odgovara državnom tajniku za obranu i nacionalnu sigurnost.
88	Hrvatska udruga menadžera sigurnosti (HUMS)	IV. TEKST PRIJEDLOGA ZAKONA, Članak 67.	Predlažemo uvesti obavezu informiranja subjekata kako bi se na strani subjekta mogli eliminirati lažno pozitivni pokazatelji kao indikatori aktivnosti neprepoznatih trećih strana/lažno pozitivne prijetnje.	Primljeno na znanje	Zakonom se otvaraju velike mogućnosti međusobne suradnje i razmjene informacija između niza nadležnih tijela i ključnih i važnih subjekata. Informacije o kibernetičkim ugrozama i indikatorima kompromitacije, kao i o taktikama, tehnikama i procedurama državno-sponzoriranih APT grupa i drugih sofisticiranih i organiziranih kibernetičkih napadača, SOA je do sada u određenoj mjeri razmjenjivala samo s pravnim osobama uključenima u nacionalni sustav iz članka 51. (sustav SK@UT), dok će kroz ovlasti iz Zakona takvo informiranje nadležnih tijela i subjekata biti puno šire.
89	A1 Hrvatska d.o.o.	IV. TEKST PRIJEDLOGA ZAKONA, Članak 67.	Čl.67. Svrha ovakve aktivnosti trebala bi biti detekcija ranjivosti i ostavljanje prostora za poboljšanje razine sigurnosti obveznika. Ona ne bi trebala inicirati provođenje inspekcija već bi trebala biti usmjerena na davanje informacija isključivo obvezniku nad kojim je aktivnost provedena o detektiranoj ranjivosti.Navedeno je sukladno i Direktivi 2022/2555.	Primljeno na znanje	Da, smisao ove odredbe je da omogući CSIRT tijelima u NIS2 direktivi iste mogućnosti kakve koristi i niz globalnih komercijalnih tvrtki, kao i niz malicioznih aktera u svijetu. Aktivnosti ove vrste imaju za cilj preventivno i kontinuirano upozoravanje subjekata na potencijalne ranjivosti vidljive u javnom kibernetičkom prostoru i njihovo brzo uklanjanje.
90	Ana	IV. TEKST	Stavak 2. u raskoraku s odredbom NIS2 Direktive	Ne prihvaća	Članak 68. odnosi se na rješavanje

	Balaško	PRIJEDLOGA ZAKONA, Članak 68.	(čl.11., st.2.) gdje je navedeno da CSIRT-ovi mogu provoditi proaktivno neintruzivno skeniranje javno dostupnih mrežnih i informacijskih sustava ključnih i važnih subjekata, te da takvo skeniranje ne smije imati negativan učinak na funkcioniranje usluga subjekata. Dali je u redu da se CSIRT zakonski ograđuje od snošenja odgovornosti za štetu uzrokovanu incidentom na mrežnim i informacijskim sustavima ključnih i važnih subjekata uslijed obavljanja svojih zadaća?	se	kibernetičkih incidenata i u tom dijelu postoji odgovornost subjekta za suradnju s CSIRT tijelom, ovisno o razini pomoći koja mu je potrebna, ili minimalno za izvještavanje kada se radi o značajnom kibernetičkom incidentu. U slučaju prijavljenog kibernetičkog incidenta i traženja pomoći od CSIRT-a, CSIRT ne može biti odgovoran za incident već jedino može pomoći u odgovoru na incident. Članak 67. odnosi se na proaktivno neintruzivno skeniranje javno dostupnih mrežnih i informacijskih sustava ključnih i važnih subjekata s ciljem brzog uklanjanja ranjivosti vidljivih u javnom kibernetičkom prostoru.
91	Span d.d.	IV. TEKST PRIJEDLOGA ZAKONA, Članak 68.	S obzirom da je riječ o dužnosti/obvezi ključnih i važnih subjekata da sa nadležnim CSIRT-om razmjenjuju potrebne informacije u postupku rješavanja incidenta, predlažemo da se umjesto „incidenta“ napiše „značajnog incidenta“. Naime, jasno je iz teksta prijedloga zakona da obveze za subjekte proizlaze kada je riječ o značajnom incidentu, dok se kod (običnog) incidenta može ali i ne mora komunicirati sa CSIRT-om.	Ne prihvaća se	Članak 68. odnosi se na odgovor na incident koji je na obaveznoj ili dobrovoljnoj osnovi prijavljen CSIRT-u, jer i za dobrovoljnu osnovu prijave incidenta iz nekog subjekta CSIRT pruža pomoć i sudjeluje u njegovom otklanjanju, osim u iznimnim okolnostima kada mora vlastite resurse uskladiti s prioritetima rješavanja većeg broja značajnih incidenata koji su se dogodili u isto vrijeme.
92	Stjepan Groš	IV. TEKST PRIJEDLOGA ZAKONA, Članak 69.	Nisu li CSIRT-ovi kritični subjekti? I ako jesu, ne bi li onda trebali primjenjivati sve što se definira zakonom i uredbom i na taj način postići sve - a i više - nego što piše u ovom članku?	Ne prihvaća se	CSIRT-ovi su nadležna tijela iz Priloga III. te imaju posebno određene zahtjeve s obzirom na specifičnost posla kojim se bave.
93	Elizabeta Montan	IV. TEKST PRIJEDLOGA ZAKONA, Članak 73.	Nepotreban članak s ovakvim tekstom, svi su obavezni na obradu osobnih podataka u skladu s Općom uredbom o zaštiti podataka. Nigdje nije navedena obaveza prijenosa osobnih podataka sudionika u incidentima kod prijave incidenata (napadač ili napadnut). Prijava detalja o incidentima bez da je u zakonu navedeno koje/čije osobne podatke je obavezno prikupiti i prijaviti predstavlja time kršenje Uredbe za prijavitelje incidenta. Nije navedeno koliko je potrebno čuvati i koje podatke u svrhe koje obuhvaća ovaj zakon, razuman rok bi bio 2 godine.	Ne prihvaća se	Osobni podaci u ovom Zakonu predstavljaju izuzetak koji se u nekim slučajevima može pojaviti te su odredbe povezane s osobnim podacima u Prijedlogu zakona dodatno dorađene i dopunjene u suradnji s Agencijom za zaštitu osobnih podataka.
94	Stjepan Groš	IV. TEKST PRIJEDLOGA ZAKONA, Članak 75.	Možda je umjesto "kategoriji rizičnosti" bolje napisati "prema značenju za sustav/državu", "mogućem (štetnom) utjecaju na društvo/državu/regiju" ili tako nešto?	Ne prihvaća se	Radi se o korištenju kriterija za procjenu rizika i metode kojom se na temelju te procjene razvrstavaju tijela u različite kategorije, odnosno o formaliziranom procesu upravljanja rizikom koji se dinamički prati i procjenjuje.
95	Hrvatska udruga menadžera sigurnosti (HUMS)	IV. TEKST PRIJEDLOGA ZAKONA, Članak 77.	Predlažemo da se rok najave definira kao tri radna dana.	Djelomično se prihvaća	Promijenjeno na „najkasnije u roku od pet dana prije početka nadzora“.
96	A1 Hrvatska d.o.o.	IV. TEKST PRIJEDLOGA ZAKONA, Članak 77.	Čl.77.st.2. Pozdravljamo uvođenje roka najave, međutim predlažemo da umjesto tri dana budu tri radna dana kako bi se nadzirani subjekti pravovremeno pripremili za najavljeni nadzor.	Djelomično se prihvaća	Promijenjeno na „najkasnije u roku od pet dana prije početka nadzora“.
97	Diverto d.o.o.	IV. TEKST PRIJEDLOGA ZAKONA, Članak 77.	Vezano za stavak 2., predlažemo da se jasnije navede misli li se na tri radna ili tri kalendarska dana. S obzirom da nije jasno definirano koja će se dokumentacija tražiti na uvid, predlažemo da se obavijest o nadzoru pošalje minimalno 3 (ili više) radna dana prije kako bi se subjekti mogli bolje pripremiti za nadzor.	Djelomično se prihvaća	Promijenjeno na „najkasnije u roku od pet dana prije početka nadzora“.

98	Span d.d.	IV. TEKST PRIJEDLOGA ZAKONA, Članak 77.	Molimo da se razmotri produljenje roka za najavljeni stručni nadzor. Predlažemo da rok bude minimalno 5 radnih dana. Naime, nadležnim tijelima uvijek ostaje mogućnost provedbe nenajavljenog nadzora iz članka 77. stavka 3. kada se za to pokaže potreba. S druge strane najavljeni nadzor trebao bi subjektu nadzora dati dovoljno vremena za pripremu, za što su 3 dana premalo (pogotovo ako se u obzir uzme da bi tu mogli ući vikendi i drugi neradni dani).	Djelomično se prihvaća	Promijenjeno na „najkasnije u roku od pet dana prije početka nadzora“.
99	Stjepan Groš	IV. TEKST PRIJEDLOGA ZAKONA, Članak 78.	Treća točka - što ako je određen dio sustava pod kontrolom treće strane? U tom slučaju do njih se ne može jer oni nisu "nadležne i odgovorne osobe nadziranog subjekta".	Ne prihvaća se	Ključni i važni subjekti su odgovorni za korištenje usluga trećih strana u sklopu svojih mrežnih i informacijskih sustava te se nadzire samo način i uvjeti pod kojima ta treća strana obavlja svoj posao unutar opsega nadležnosti nadziranog subjekta.
100	Hrvatska udruga menadžera sigurnosti (HUMS)	IV. TEKST PRIJEDLOGA ZAKONA, Članak 83.	Ukoliko se radi o transpoziciji iz čl. 32. Direktive, službenik je na strani nadležnog tijela, a ne na strani subjekta. Ukoliko je pak ideja imenovanja unutar samog subjekta, predlažemo dodatno definirati mehanizme zaštite zaposlenika, njegove kompetencije te pozicije koje su u potencijalnom sukobu interesa unutar subjekta.	Prihvaća se	
101	Stjepan Groš	IV. TEKST PRIJEDLOGA ZAKONA, Članak 83.	Nije li ovo poprilično nedorečeno? Nigdje se ne kaže koje su kompetencije, ovlasti i odgovornosti službenika za praćenje usklađenosti.	Primljeno na znanje	Izmijenjeno temeljem prijedloga iz točke 100.
102	Diverto d.o.o.	IV. TEKST PRIJEDLOGA ZAKONA, Članak 85.	Molimo pojašnjenje nadležnih tijela koja se spominju u članku. Iz načina kako je opisano, nije jasno radi li se o istom ili više različitih nadležnih tijela.	Primljeno na znanje	Nadležna tijela za provedbu zahtijeva kibernetičke sigurnosti pobrojana su u Prilogu III. Zakona, zajedno sa sektorima svojih nadležnosti.
103	Diverto d.o.o.	IV. TEKST PRIJEDLOGA ZAKONA, Članak 86.	Predlažemo da se prilikom donošenja odluka o izricanju korektivnih mjera u obzir uzme potencijalno nesavjesna procjena rizika. Nesavjesno i preblago procjenjivanje rizika koje ne odražava stvarno stanje bi se uz navedene u stavku 2. ovog članka trebalo smatrati ozbiljnom povredom.	Ne prihvaća se	Pobrojane su opće kategorije korektivnih mjera koje su primjenjive i na proces upravljanja rizikom, odnosno na njegove rezultate i stanje mjera kibernetičke sigurnosti u nekom subjektu, a kako to zahtijevaju članci 32. stavak 7. i članak 33. stavak 5. NIS2 direktive.
104	Stjepan Groš	IV. TEKST PRIJEDLOGA ZAKONA, Članak 90.	Laičko pitanje. Nije li po definiciji pravo nadziranog subjekta zatražiti sudsku zaštitu?	Primljeno na znanje	Članak 90. regulira stvarnu nadležnost sudova u ovim predmetima i vrstu pravnog lijeka koji se može koristiti.
105	Stjepan Groš	IV. TEKST PRIJEDLOGA ZAKONA, Članak 92.	Laičko pitanje. Ako nema obaveze pokazivanja očevidnika van nadležnog tijela nije li to nešto što se uređuje internim pravilnicima, i prema tome ne spominje u zakonu?	Primljeno na znanje	Zakonom se uređuje provedba stručnog nadzora koji prema Prijedlogu zakona provodi više različitih tijela nadležnih za provedbu zahtjeva kibernetičke sigurnosti prema podjeli nadležnosti iz Priloga III. Zakona. Intencija članka 92. Prijedloga zakona uskladiti postupanja svih nadležnih tijela u vođenju očevidnika o obavljenim stručnim nadzorima.
106	A1 Hrvatska d.o.o.	IV. TEKST PRIJEDLOGA ZAKONA, Članak 101.	Članak 101. Zakona potrebno je u cijelosti uskladiti sa čl.34. Direktive (EU) 2022/2555 uključivo i čl. 32.s.t.7. Direktive koji se navodi u čl.34. st.3. Direktive. Dodatno , čl.32. Direktive nije u cijelosti i valjano transponiran u čl.85 i 86. Zakona te je stoga potrebno uskladiti te odredbe te ih povezati sa čl.101 i 102 Zakona na način kako je to definirano uz čl.34. Direktive. Poveznica prema čl. 101 Zakona je čl.34. Direktive koji se primjenjuje u slučaju kršenja čl.21. i 23. Direktive. Čl .101.st.1. puno šire definira mogućnost kažnjavanja najvećim	Djelomično se prihvaća	Članci 101. i 102. dopunjeni su odgovarajućim stavcima prema zahtjevima članka 34. stavka 3. NIS2 direktive.

			kaznama te na taj način ne slijedi pravila transponiranja Direktive u nacionalno zakonodavstvo. Ovaj članaka dodatno je upitan s obzirom da je čl.21.st.5. Direktive propisano da EU komisija do 17. listopada 2024. donosi provedbene akte kojima se utvrđuju tehnički i metodološki zahtjevi za mjere iz stavka 2. čl.21. u pogledu pružatelja usluga DNS-a, registara naziva vršnih domena, 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 i pružatelja usluga povjerenja. Drugim riječima, čl.101. Zakona netransparentno transponira čl.34. Direktive te s obzirom na očekivane nove provedben akte stvara pravnu nesigurnost za obveznike Zakona.		
107	MARKO RAKAR	IV. TEKST PRIJEDLOGA ZAKONA, Članak 101.	Ovaj članak navodi niz prekršajnih kazni za subjekte, no nigdje nije definirano što se događa sa subjektom u kojem je zatečena oprema, servisi ili procesi a za koje je propisana EU certifikacija, ali oprema, servisi ili procesi je ne posjeduju. Nužno je propisati prijelazne rokove tj. rokove zamjene (npr. do kraja amortizacijskog roka, ili vremenskog roka npr. 5 godina), te u slučaju da postoji utemeljeni razlog za žurnu zamjenu, tko će podmiriti nastalu štetu (trošak zamjene opreme, servisa ili procesa, odnosno trošak nabavke i implementacije nove opreme, servisa ili procesa).	Ne prihvaća se	Procesi certifikacije su tek u pripremi na EU razini, a mjerodavna postupanja po možebitnim obvezama zamjene moraju u svakom slučaju biti praćena uvjetima i rokovima koji se propisuju mjerodavnim aktima EU (predviđen rok od 5 godina) odnosno relevantnim nacionalnim propisima, odnosno onim propisima koji će za subjekte uvesti obvezu korištenja točno određenih certificiranih IKT proizvoda, IKT usluga, IKT procesa ili upravljanih sigurnosnih usluga. Prijedlogom zakona se takva obveza za ključne i važne subjekte ne uvodi, već se njime uvodi pravni temelj za slučaj ako odnosno kada takva obveza bude utvrđena drugim relevantnim propisima.
108	Stjepan Groš	IV. TEKST PRIJEDLOGA ZAKONA, Članak 101.	Stavak 2, ovog članka. Nije li to smiješan iznos za predsjednike uprava velikih subjekata, posebno privatnih koji zarađuju daleko veće iznose? Posebno kada se uzme u obzir inflacija? Ne bi li bilo bolje to definirati kroz prosječne dohodke, dohodke odgovorne osobe, ukupna primanja u godini, ili tako nekako?	Ne prihvaća se	Usklađeno s okvirima definiranim Prekršajnim zakonom („Narodne novine“, broj: 107/07, 39/13, 157/13, 110/15, 70/17, 118/18 i 114/22) koji predstavlja opći propis kojim se propisuju odredbe koje se odnose na sve prekršaje propisane u drugim zakonima.
109	MARKO RAKAR	IV. TEKST PRIJEDLOGA ZAKONA, Članak 102.	Ovaj članak navodi niz prekršajnih kazni za subjekte, no nigdje nije definirano što se događa sa subjektom u kojem je zatečena oprema, servisi ili procesi a za koje je propisana EU certifikacija, ali oprema, servisi ili procesi je ne posjeduju. Nužno je propisati prijelazne rokove tj. rokove zamjene (npr. do kraja amortizacijskog roka, ili vremenskog roka npr. 5 godina), te u slučaju da postoji utemeljeni razlog za žurnu zamjenu, tko će podmiriti nastalu štetu (trošak zamjene opreme, servisa ili procesa, odnosno trošak nabavke i implementacije nove opreme, servisa ili procesa).	Ne prihvaća se	Procesi certifikacije su tek u pripremi na EU razini, a mjerodavna postupanja po možebitnim obvezama zamjene moraju u svakom slučaju biti praćena uvjetima i rokovima koji se propisuju mjerodavnim aktima EU (predviđen rok od 5 godina) odnosno relevantnim nacionalnim propisima, odnosno onim propisima koji će za subjekte uvesti obvezu korištenja točno određenih certificiranih IKT proizvoda, IKT usluga, IKT procesa ili upravljanih sigurnosnih usluga. Prijedlogom zakona se takva obveza za ključne i važne subjekte ne uvodi, već se njime uvodi pravni temelj za slučaj ako odnosno kada takva obveza bude utvrđena drugim relevantnim propisima.
110	Ana Balaško	IV. TEKST PRIJEDLOGA	NIS2 Direktivom nije predviđena kazna za navedeno.	Primljeno na znanje	Budući da je provedba kategorizacije subjekata elementarni postupak o

		ZAKONA, Članak 103.			kojem ovise brojni drugi važni aspekti provedbe zahtjeva NIS2 direktive odnosno slijedno i nacionalnog transpozicijskog zakona, člankom 103. Prijedloga zakona utvrđuju se pravila o sankcijama kako bi se osigurala pravovremena i potpuna provedba postupaka kategorizacije odnosno utvrđivanja i ažuriranja popisa ključnih i važnih subjekata.
111	A1 Hrvatska d.o.o.	IV. TEKST PRIJEDLOGA ZAKONA, Članak 106.	Pružatelji javnih elektroničkih komunikacijskih usluga ne samo da bi trebali nastaviti s provedbe zahtjeva do trenutka dostave popisa već i do trenutka donošenja Uredbe iz čl.24. ovog Zakona jer čl.41. ZEK-a detaljno opisuje proces provođenja sigurnosti elektroničkih komunikacijskih mreža i usluga što uključuje ne samo proces obavještavanja HAKOM-a o sigurnosnim incidentima već i proces obavještavanja krajnjih korisnika te primjenu Pravilnika o načinu i rokovima provedbe mjera zaštite sigurnosti i cjelovitosti mreža i usluga kojim su detaljno propisani način i rokovi u kojima operatori javnih elektroničkih komunikacijskih mreža i usluga te mreža koje se upotrebljavaju kao potpora sustavima kritičnih infrastruktura moraju poduzeti odgovarajuće tehničke i ustrojstvene mjere kako bi se zaštitila sigurnost njihovih mreža i usluga, način i rokovi izvješćivanja Hrvatske regulatorne agencije za mrežne djelatnosti o sigurnosnim incidentima od značajnog utjecaja na rad mreža operatora ili obavljanje njihovih usluga, obveza provedbe godišnje revizije mjera sigurnosti mreža i usluga operatora te mjerila i način certificiranja pravnih osoba koje je za provedbu te revizije ovlastio HAKOM. Operatori su sukladno navedenom Pravilniku i kriterijima iz Pravilnika implementirali procese i interne sustave upozorenja temeljem kojih obavještavaju HAKOM o incidentima te implementirali sigurnosne mjere uz provođenje propisanih revizija. Uredba iz čl.24. ovog Zakona trebala bi voditi računa o obvezama i kriterijima propisanim Pravilnikom u svrhu osiguranja kontinuiteta već uspostavljenih sigurnosnih i incidentnih procesa kod operatora	Primljeno na znanje	Svi podzakonski akti ovog Zakona bit će doneseni prije provedbe kategorizacije subjekata iz ovog sektora, koji će do te kategorizacije provoditi pravila koja su sada na snazi prema ZEK-u.
112	Ana Balaško	IV. TEKST PRIJEDLOGA ZAKONA, Članak 115.	Nedostaje broj zakona u NN kod Zakona o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga pod prvom točkom, kao i kod Zakona o elektroničkim komunikacijama pod točkom 3.	Prihvaća se	
113	Vodovod d.o.o. Makarska	IV. TEKST PRIJEDLOGA ZAKONA, PRILOG I.	Ovim prijedlogom su svi javni isporučitelji vodnih usluga (toč 6 . – Voda za ljudsku potrošnju i toč.7 Otpadne vode) su u Prilogu I svrstani u sektor visoke rizičnosti. Zakonom o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga (NN 64/18) Prilogom I - Popis ključnih usluga s kriterijima i pragovima za donošenje ocjene o važnosti negativnog učinka incidenta, kao obveznici su određeni Isporučitelji vodnih usluga koji isporučuju više od 10.000.000 m3/godišnje. Predlaže se po uzoru na Zakon iz 2018.godine odrediti pragove zavisno o veličini Javnog isporučitelja vodnih usluga prema kojima se isti svrstavaju u kategoriju rizičnosti. Također različiti Isporučitelji vodnih usluga koriste različite vrste obrade pitke vode. Tako primjerice dok je na određenom području dovoljno samo kloriranje ili filtracija i kloriranje , određeni isporučitelji provode i dodatnu obradu pitke vode u vidu izdvajanja metala i sl. Stoga različite tehnologije obrade	Ne prihvaća se	NIS2 direktiva napustila je pristup kategorizacije subjekata preko popisa ključnih usluga i definiranja kriterija i pragova za donošenje ocjene o važnosti negativnog učinka incidenta, prvenstveno zato što se kategorizacija subjekata provodi u puno širem opsegu subjekata i za cjelokupno poslovanje tih subjekata, a ne više samo za ključne usluge, kao što je bio slučaj u NIS1 direktivi.

			nose i različite rizike koji se mogu dogoditi, a što predloženom kategorizacijom nije vrednovano, već su svi stavljeni u sektor visoke rizičnosti. Vodovod d.o.o. Makarska Direktor Ivica Nuić		
114	IZVOR PLOČE d.o.o.	IV. TEKST PRIJEDLOGA ZAKONA, PRILOG I.	Ovim prijedlogom Zakona o kibernetičkoj sigurnosti su svi javni isporučitelji vodnih usluga (točke 6 i 7 u Prilogu I.) svrstani u sektor visoke rizičnosti. Zakonom o kibernetičkoj sigurnosti operatera ključnih usluga i davatelja digitalnih usluga (NN64/18) Prilogom I - Popis ključnih usluga s kriterijima i pragovima za donošenje ocjene o važnosti negativnog učinka incidenta, kao obveznici su određeni isporučitelji vodnih usluga koji isporučuju više od 10.000.000 m3/godišnje. Isto tako, člankom 4, točka 10., Uredbe o posebnim uvjetima za obavljanje djelatnosti vodnih usluga, propisani su uvjeti vezani za kibernetičku sigurnost samo za isporučitelje koji isporučuju najmanje 10.000.000 m3/godišnje. Predlaže se po uzoru na Zakon iz 2018. godine odrediti pragove ovisno o veličini Javnog isporučitelja vodnih usluga prema kojima se isti svrstavaju u kategoriju rizičnosti. Također, različiti isporučitelji vodnih usluga koriste različite obrade pitke i otpadne vode. Dok je na određenom području dovoljno samo kloriranje na nekom drugom je potrebna dodatna predobrada. Isto tako, pojedini isporučitelji provode pročišćavanje otpadne vode različitim stupnjevima pročišćavanja. Različiti tehnološki procesi nose i različite rizike koji se mogu dogoditi, a što predloženom kategorizacijom nije vrednovano, već su svi stavljeni u sektor visoke rizičnosti.	Ne prihvaća se	NIS2 direktiva napustila je pristup kategorizacije subjekata preko popisa ključnih usluga i definiranja kriterija i pragova za donošenje ocjene o važnosti negativnog učinka incidenta, prvenstveno zato što se kategorizacija subjekata provodi u puno širem opsegu subjekata i za cjelokupno poslovanje tih subjekata, a ne više samo za ključne usluge, kao što je bio slučaj u NIS1 direktivi.
115	NINO ŠETUŠIĆ	IV. TEKST PRIJEDLOGA ZAKONA, PRILOG I.	Pod pružatelje zdravstvene zaštite bi pripali i obiteljski liječnici u RH koji se sastoje od najčešće od timova od dvoje ljudi. Ministarstvo zdravstva bi se trebalo obvezati da pruži podršku, savjetovanje i praktičnu realizaciju tih zahtjeva jer bi to moglo predstavljati veliki izazov za brojne ordinacije.	Primljeno na znanje	Vrste subjekata iz sektora zdravstva kategoriziraju se primarno temeljem kriterija veličine subjekta (članak 9. stavak 1. i članak 10. stavak 2. Prijedloga zakona), a neovisno o veličini mogu se kategorizirati temeljem posebnih kriterija iz članka 11. Prijedloga zakona. Pitanja vezana uz podršku kategoriziranim subjektima iz sektora zdravstva su u ingerenciji nadležnog ministarstva te će se razmatrati prilikom provedbe procesa kategorizacije subjekata.
116	Diverto d.o.o.	IV. TEKST PRIJEDLOGA ZAKONA, PRILOG I.	Predlažemo unifikaciju pojmova u Zakonu. Kroz Zakon se koriste izrazi „ključni subjekti“, a u nazivu priloga I. su SEKTORI VISOKE KRITIČNOSTI. Dodatno: - unutar sektora 9. Upravljanje uslugama IKT-a (B2B), uz subjekte pružatelje upravljanih usluga nedostaju subjekti koji su pružatelji sigurnosno upravljanih usluga - unutar sektora 5. Zdravstvo, pod vrstom sektora u opsegu navode se subjekti koji obavljaju gospodarske djelatnosti iz Nacionalne klasifikacije djelatnosti 2007. – NKD 2007., a poznato je da sudski registar ne funkcionira prema NKD-u 2007.	Djelomično se prihvaća	Terminologija je prenesena iz NIS2 direktive, gdje su ključni subjekti oni koji pripadaju sektorima visoke kritičnosti. Prilog I. dopunjen u točki 9. Budući da se NIS2 direktiva referira na NACE Rev 2., u Prijedlogu zakona obvezno je pozivanje na nacionalni akt kojim je preuzeta klasifikacija iz NACE Rev 2., a to je NKD 2007.
117	Hrvatska udruga menadžera sigurnosti (HUMS)	IV. TEKST PRIJEDLOGA ZAKONA, PRILOG II.	Umjesto pozivanja na NKD 2007., predlažemo taksativno navesti trenutne djelatnosti, a s obzirom na nedavno savjetovanje o novoj klasifikaciji NKD 2025.	Ne prihvaća se	Budući da se NIS2 direktiva referira na NACE Rev 2., u Prijedlogu zakona obvezno je pozivanje na nacionalni akt kojim je preuzeta klasifikacija iz NACE Rev 2., a to je NKD 2007.

118	Diverto d.o.o.	IV. TEKST PRIJEDLOGA ZAKONA, PRILOG II.	Predlažemo unifikaciju pojmova u Zakonu. Kroz Zakon se koristi izraz važni subjekti, a u nazivu priloga II su DRUGI KRITIČNI SEKTORI. Dodatno: - unutar sektora 5. Proizvodnja, pod vrstom sektora u opsegu navode se subjekti koji obavljaju gospodarske djelatnosti iz Nacionalne klasifikacije djelatnosti 2007. – NKD 2007., a poznato je da sudski registar ne funkcionira prema NKD-u 2007.	Ne prihvaća se	Terminologija je prenesena iz NIS2 direktive, gdje su važni subjekti oni koji pripadaju drugim kritičnim sektorima. Budući da se NIS2 direktiva referira na NACE Rev 2., u Prijedlogu zakona obvezno je pozivanje na nacionalni akt kojim je preuzeta klasifikacija iz NACE Rev 2., a to je NKD 2007.
119	A1 Hrvatska d.o.o.	IV. TEKST PRIJEDLOGA ZAKONA, PRILOG III.	Potrebno precizirati koje tijelo/tijela provode nadzor nad operatorima elektroničkih komunikacija s obzirom da se isti bave ne samo djelatnostima koje su navedene pod nadležnosti HAKOM-a već i drugim djelatnostima poput usluga računalstva u oblaku i usluga podatkovnog centra, upravljanje uslugama IKT-a (B2B). Prema tablici iz Priloga III proizlazi da bi nadležno tijelo za navedene usluge bila SOA. A1 predlaže da se centralizira regulatorna funkcija u jedno tijelo koje bi u slučaju operatora elektroničkih komunikacija bilo HAKOM, a koje je u cijelosti upoznato sa djelatnostima koje pružaju operatori, te koje već danas provodi nadzor nad operatorima u području kibernetičke sigurnosti.	Primljeno na znanje	Primarne nadležnosti određene u Prilogu III. vezane su na glavnu djelatnost subjekata prema definicijama svake pojedine vrste subjekta, a u slučaju da subjekt obavlja više vrsta djelatnosti iz različitih sektora obuhvaćenih Zakonom, u suradnji svih nadležnih tijela provest će se koordinacija i dogovor prema članku 59. stavcima 3. i 4. Prijedloga zakona.

IZJAVA O USKLAĐENOSTI PRIJEDLOGA PROPISA S PRAVNOM STEČEVINOM EUROPSKE UNIJE

1. Naziv prijedloga propisa

Zakon o kibernetičkoj sigurnosti

2. Stručni nositelj izrade prijedloga propisa

MINISTARSTVO HRVATSKIH BRANITELJA

3. Veza s Programom Vlade Republike Hrvatske za preuzimanje i provedbu pravne stečevine Europske unije

Predviđeno Programom Vlade Republike Hrvatske za preuzimanje i provedbu pravne stečevine Europske unije za 2023. godinu.
Rok: III. kvartal 2023.

4. Preuzimanje odnosno provedba pravne stečevine Europske unije

a) Odredbe primarnih izvora prava Europske unije

Ugovor o funkcioniranju Europske unije
članak/članci 114.

b) Sekundarni izvori prava Europske unije

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 NIS 2) (Tekst značajan za EGP) (SL L 333, 27.12.2022.)

32022L2555

- Članci 21., 23., 30. i 41. bit će preuzeto: Uredba o kibernetičkoj sigurnosti (12.09.2024)

c) Ostali izvori prava Europske unije

-

5. Prilog: tablice usporednih prikaza za propise kojima se preuzimaju odredbe sekundarnih izvora prava Europske unije u zakonodavstvo Republike Hrvatske

Da.

Potpis EU koordinatora stručnog nositelja izrade prijedloga propisa, datum i pečat

Darko Nekić

Državni tajnik

(potpis)

REPUBLIKA HRVATSKA 11 ZAGREB MINISTARSTVO HRVATSKIH BRANITELJA

7. 9. 2023.

(datum i pečat)

Potpis EU koordinatora Ministarstva vanjskih i europskih poslova, datum i pečat

Andreja Metelko-Zgombić

Državna tajnica za Europu

(potpis)

REPUBLIKA HRVATSKA 29 ZAGREB MINISTARSTVO VANJSKIH I EUROPSKIH POSLOVA

7.9.2023.

(datum i pečat)

USPOREDNI PRIKAZ PODUDARANJA ODREDBI PROPISA EUROPSKE UNIJE S PRIJEDLOGOM PROPISA

1. **Naziv propisa Europske unije**
   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 NIS 2) (Tekst značajan za EGP)

2. **Naziv prijedloga propisa**
   Zakon o kibernetičkoj sigurnosti

3. Usklađenost odredbi propisa Europske unije (sekundarni izvori prava) s odredbama prijedloga propisa

a)	b)	c)	d)
Odredbe propisa Europske unije	**Odredbe prijedloga propisa**	**Je li sadržaj odredbe propisa Europske unije u potpunosti preuzet u odredbu prijedloga propisa?**	**Obrazloženje (ako sadržaj odredbe propisa Europske unije nije preuzet ili je djelomično preuzet u odredbu prijedloga propisa)**

Članak 1. Predmet 1. Ovom se Direktivom utvrđuju mjere čiji je cilj postići visoku zajedničku razinu kibersigurnosti širom Unije kako bi se poboljšalo funkcioniranje unutarnjeg tržišta. 2. U tu svrhu, ovom se Direktivom utvrđuju: (a) obveze kojima se zahtjeva da države članice donesu nacionalne strategije za kibersigurnost i imenuju ili uspostave nadležna tijela, tijela za upravljanje kiberkrizama, jedinstvene kontaktne točke za kibersigurnost (jedinstvene kontaktne točke) i timove za odgovor na računalne sigurnosne incidente (CSIRT-ovi); (b) mjere upravljanja kibersigurnosnim rizicima i obveze izvješćivanja za subjekte koji pripadaju vrstama navedenim u Prilogu I. i u Prilogu II kao i za subjekte utvrđene kao kritični subjekti na temelju Direktive (EU) 2022/2557; (c) pravila i obveze u pogledu razmjene informacija o kibersigurnosti;	**Članak 1. NIS2 direktive preuzima se sljedećim člankom:** **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 potpunosti preuzeto	

(d)	obveze nadzora i izvršavanja za države članice.	u sektorima od posebne važnosti za nesmetano obavljanje ključnih društvenih i gospodarskih aktivnosti i pravilno funkcioniranje unutarnjeg tržišta. **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. **Dopunjen članak 1. Nacrta zakona, radi potpunijeg preuzimanja dijela članka 1. NIS2 direktive koji se referira na svrhu provedbe postupaka i mjera za postizanje visoke razine kibernetičke sigurnosti u odnosu na funkcioniranje unutarnjeg tržišta**		

Članak 2. Područje primjene 1. Ova se Direktiva primjenjuje na javne ili privatne subjekata koji pripadaju vrstama navedenim u Prilogu I. ili u Prilogu II. koji se smatraju srednjim poduzećima na temelju članka 2. Priloga Preporuci 2003/361/EZ, ili koji prelaze gornje granice za srednja poduzeća iz stavka 1. tog članka i pružaju svoje usluge ili obavljaju svoje djelatnosti unutar Unije. Članak 3. stavak 4. Priloga toj Preporuci ne primjenjuje se za potrebe ove Direktive. 2. Ova se Direktiva primjenjuje i na subjekte koji pripadaju vrstama navedenim u Prilogu I. ili u Prilogu II, neovisno o njihovoj veličini: (a) ako usluge pružaju: i. pružatelji javnih elektroničkih komunikacijskih mreža ili javno dostupnih elektroničkih komunikacijskih usluga; ii. pružatelji usluga povjerenja; iii. registri naziva vršnih domena i pružatelji usluga sustava naziva domena;	**Članak 2. stavci 1. do 9. NIS2 direktive preuzimaju se sljedećim člancima:** **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. **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	U potpunosti preuzeto	

(b) ako je subjekt u nekoj državi članici jedini pružatelj usluge koja je ključna za održavanje ključnih društvenih ili gospodarskih djelatnosti; (c) ako bi poremećaj u funkcioniranju usluge koju pruža subjekt mogao imati znatan učinak na javnu sigurnost, javnu zaštitu ili javno zdravlje; (d) ako bi poremećaj u funkcioniranju usluge koju pruža subjekt mogao uzrokovati znatne sistemske rizike, posebno u sektorima u kojima bi takav poremećaj mogao imati prekogranični učinak; (e) ako je subjekt ključan zbog svoje posebne važnosti na nacionalnoj ili regionalnoj razini za određeni sektor ili vrstu usluge ili za druge međuovisne sektore u državi članici; (f) ako se radi o subjektu javne uprave: i. na razini državne uprave kako ga definira država članica u skladu s nacionalnim pravom; ili ii. na regionalnoj razini kako ga definira država članica u skladu s nacionalnim pravom koji nakon procjene utemeljene na riziku pruža usluge čiji bi poremećaj mogao imati znatan	– Prilog IV. Obvezni sadržaj nacionalnog akta strateškog planiranja iz područja kibernetičke sigurnosti (u daljnjem tekstu: Prilog IV. ovog Zakona). **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 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 vršne nacionalne internetske domene te pružatelji usluga DNS-a, neovisno o njihovoj veličini - pružatelji javnih elektroničkih komunikacijskih mreža ili javno dostupnih elektroničkih komunikacijskih usluga koji predstavlja subjekt malog gospodarstva na temelju zakona kojim se uređuju osnove za primjenu poticajnih mjera gospodarske politike usmjerenih razvoju, restrukturiranju i tržišnom prilagođavanju maloga gospodarstva 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.**		

učinak na ključne društvene ili gospodarske djelatnosti. 3. Neovisno o njihovoj veličini, ova se Direktiva primjenjuje na subjekte utvrđene kao kritične subjekte na temelju Direktive (EU) 2022/2557. 4. Neovisno o njihovoj veličini, ova se Direktiva primjenjuje na subjekte utvrđene kao kritične subjekte koji pružaju usluge registracije naziva domena. 5. Države članice mogu predvidjeti da se ova Direktiva primjenjuje na: (a) subjekte javne uprave na lokalnoj razini; (b) obrazovne ustanove, posebno ako provode ključne istraživačke aktivnosti. 6. Ovom Direktivom ne dovodi se u pitanje odgovornost država članica za zaštitu nacionalne sigurnosti ili njihove ovlasti za zaštitu drugih ključnih državnih funkcija, uključujući osiguravanje teritorijalne cjelovitosti države i održavanje javnog poretka. 7. Ova se Direktiva ne primjenjuje na subjekte javne uprave koji obavljaju svoje aktivnosti u području nacionalne sigurnosti, javne sigurnosti, obrane ili	U kategoriju važnih subjekata razvrstavaju se: - privatni i javni subjekti iz Priloga II. ovog Zakona koji predstavljaju subjekt malog gospodarstva na temelju zakona kojim se uređuju osnove za primjenu poticajnih mjera gospodarske politike usmjerenih razvoju, restrukturiranju i tržišnom prilagođavanju maloga gospodarstva- privatni i javni subjekti iz Priloga I. ovog Zakona koji nisu utvrđeni kao ključni subjekti temeljem članka 9. ovog Zakona, a predstavljaju subjekt malog gospodarstva na temelju zakona kojim se uređuju osnove za primjenu poticajnih mjera gospodarske politike usmjerenih razvoju, restrukturiranju i tržišnom prilagođavanju maloga gospodarstva - pružatelji usluga povjerenja koji nisu kategorizirani kao ključni subjekti, 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		

izvršavanja zakonodavstva, uključujući sprečavanje, istragu, otkrivanje i progon kaznenih djela. 8. Države članice mogu izuzeti određene subjekte koji obavljaju aktivnosti u području nacionalne sigurnosti, javne sigurnosti, obrane ili izvršavanja zakonodavstva, uključujući sprečavanje, istragu, otkrivanje i progon kaznenih djela, ili koji pružaju usluge isključivo subjektima javne uprave iz stavka 7. ovog članka od obveza iz članka 21 ili članka 23. u pogledu tih aktivnosti ili usluga. U takvim se slučajevima nadzorne mjere i mjere izvršavanja iz poglavlja VII. ne primjenjuju na te posebne aktivnosti ili usluge. Ako subjekti obavljaju aktivnosti ili pružaju usluge isključivo one vrste koja je navedena u ovom stavku, države članice mogu i odlučiti izuzeti te subjekte od obveza utvrđenih u člancima 3. i 27. 9. Stavci 7. i 8. ne primjenjuju se ako subjekt djeluje kao pružatelj usluga povjerenja. 10. Ova se Direktiva ne primjenjuje na subjekte koje su države članice izuzele iz područja primjene Uredbe (EU)	- bi poremećaj u funkcioniranju usluge koju pruža subjekt, odnosno poremećaj u obavljanju djelatnosti subjekta, mogao imati znatan utjecaj 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:		

2022/2554 u skladu s člankom 2. stavkom 4. te Uredbe. 11. Obveze utvrđene u ovoj Direktivi ne podrazumijevaju dostavu informacija čije bi otkrivanje bilo u suprotnosti s osnovnim interesima u pogledu nacionalne sigurnosti, javne sigurnosti ili obrane država članica. 12. Ova se Direktiva primjenjuje ne dovodeći u pitanje Uredbu (EU) 2016/679, Direktivu 2002/58/EZ, direktive 2011/93/EU (27) i 2013/40/EU (28) Europskog parlamenta i Vijeća te Direktivu 2022/2557. 13. Ne dovodeći u pitanje članak 346. UFEU-a, informacije koje se smatraju povjerljivima u skladu s pravilima Unije ili nacionalnim pravilima, kao što su pravila o poslovnoj tajni, razmjenjuju se s Komisijom i drugim relevantnim tijelima u skladu s ovom Direktivom samo u slučaju kad je takva razmjena nužna za primjenu ove Direktive. Razmijenjene informacije ograničuju se na ono što je relevantno i razmjerno svrsi te razmjene. Pri razmjeni informacija čuva se njihova povjerljivost te se štite sigurnost i komercijalni interesi predmetnih subjekata.	- 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 u kategoriju važnih subjekata, ovisno o rezultatima provedene procjene njihove posebne važnosti na nacionalnoj ili regionalnoj razini za obavljanje odgojno-obrazovnog rada. **Članak 2. stavci 11. do 13. NIS2 direktive preuzimaju se sljedećim člancima:** **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. **Ograničenja u korištenju i pravima pristupa informacijama** **Članak 72.** (1) Popisi ključnih i važnih subjekata, kao i svi ostali zapisi koji nastaju u okviru provedbe ovoga Zakona koriste se i razmjenjuju		

14. Subjekti, nadležna tijela, jedinstvene kontaktne točke i CSIRT-ovi obrađuju osobne podatke u mjeri u kojoj je to potrebno za svrhe ove Direktive i u skladu s Uredbom (EU) 2016/679, a takva obrada posebno se oslanja na njezin članak 6. Obradu osobnih podataka na temelju ove Direktive provode pružatelji javnih elektroničkih komunikacijskih mreža ili pružatelji javno dostupnih elektroničkih komunikacijskih usluga u skladu s pravom Unije o zaštiti podataka i pravom Unije o zaštiti privatnosti, a posebno s Direktivom 2002/58/EZ.	isključivo u svrhu izvršavanja zahtjeva iz ovoga Zakona, uz poštivanje potrebe ograničavanja pristupa tim zapisima kada je to potrebno u svrhu sprječavanja, otkrivanja, provođenja istraživanja i vođenja kaznenog postupka. (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 o pravu na pristup informacijama. **Članak 2. stavak 14. NIS2 direktive preuzima se sljedećim člancima:** **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. **Zadaće od javnog interesa** **Članak 71.** Izvršavanje zadaća 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 i međunarodnoj razini, smatra se izvršavanjem zadaća od javnog interesa. **Zaštita i obrada osobnih podataka** **Članak 73.** 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. **Članak 2. stavci 1. do 9. i stavci 11. do 14. NIS2 direktive u potpunosti preuzeti.** **Nije potrebno preuzimanje članka 2. stavka 10. NIS2 Direktive.** **Sukladno članku 2. stavku 4. Uredbe (EU) 2022/2554 države članice mogu iz područja primjene te Uredbe isključiti subjekte iz članka 2. stavka 5. točaka od 4. do 23. Direktive 2013/36/EU koji se nalaze na njihovu državnom području.** **Budući da se članak 2. stavak 5. točke 4. do 23. Direktive 2013/36/EU ne odnosi na Republiku Hrvatsku odnosno subjekte s državnog područja Republike Hrvatske, preuzimanje članka 2. stavka 10. NIS2 direktive nije potrebno.** ***Izmijenjen dio relevantnih odredbi Nacrta zakona, prema danom komentaru.***		

Članak 3. Ključni i važni subjekti 1. Za potrebe ove Direktive sljedeći subjekti smatraju se ključnim subjektima: (a) subjekti koji pripadaju vrstama iz Priloga I. koji premašuju gornje granice za srednja poduzeća iz članka 2. stavka 1. Priloga Preporuci 2003/361/EZ; (b) kvalificirani pružatelji usluga povjerenja i registri naziva vršnih domena te pružatelji usluga DNS-a, neovisno o njihovoj veličini; (c) pružatelji javnih elektroničkih komunikacijskih mreža ili javno dostupnih elektroničkih komunikacijskih usluga koji se smatraju srednjim poduzećima na temelju članka 2. Priloga Preporuci 2003/361/EZ; (d) subjekti javne uprave iz članka 2. stavka 2. točke (f) podtočke (i);	**Članak 3. stavci 1. i 2. NIS2 direktive preuzimaju se sljedećim člancima:** **Pojmovi** **Članak 4.** (1) U smislu ovog Zakona pojedini pojmovi imaju sljedeće značenje: 17. "javni subjekti" su tijela državne uprave, druga državna tijela, jedinice lokalne i područne (regionalne) samouprave, pravne osobe i druga tijela koja imaju javne ovlasti, 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 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	U potpunosti preuzeto	

(e) svi drugi subjekti koji pripadaju vrstama iz priloga I. ili II. koje je država članica utvrdila kao ključne subjekte na temelju članka 2. stavka 2. točaka od (b) do (e); (f) subjekti koji su utvrđeni kao kritični subjekti na temelju Direktive (EU) 2022/2557, iz članka 2. stavka 3. ove Direktive; (g) ako država članica tako odredi, subjekti koje je ta država članica utvrdila prije 16. siječnja 2023. kao operatore ključnih usluga u skladu s Direktivom (EU) 2016/1148 ili nacionalnim pravom. 2. Za potrebe ove Direktive, svi subjekti koji pripadaju vrstama iz priloga I. ili II. koji se ne smatraju ključnim subjektima na temelju stavka 1. ovog članka smatraju se važnim subjektima. To uključuje subjekte koje je država članica utvrdila kao važne subjekte na temelju članka 2. stavka 2. točaka od (b) do (e). 3. Do 17. travnja 2025. države članice utvrđuju popis ključnih i važnih subjekata te subjekata koji pružaju usluge registracije naziva domena. Države članice redovito, a najmanje svake dvije godine, preispituju taj popis te ga prema potrebi ažuriraju.	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“ je subjekt koji pruža usluge registracije naziva domena odnosno pravna ili fizička osoba koja obavlja samostalnu djelatnost ovlaštena za registraciju i administraciju .hr domena u ime registra naziva vršne nacionalne internetske domene **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 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 vršne nacionalne internetske domene te pružatelji usluga DNS-a, neovisno o njihovoj veličini - pružatelji javnih elektroničkih komunikacijskih mreža ili javno dostupnih elektroničkih komunikacijskih usluga koji predstavlja subjekt malog gospodarstva na temelju zakona kojim se uređuju osnove za primjenu poticajnih mjera gospodarske politike usmjerenih razvoju, restrukturiranju i tržišnom prilagođavanju maloga gospodarstva i - subjekti koji su utvrđeni kao kritični subjekti na temelju zakona kojim se uređuje područje kritičnih infrastruktura, neovisno o njihovoj veličini.		

4. Za potrebe utvrđivanja popisa iz stavka 3. države članice zahtijevaju od subjekata iz tog stavka da nadležnim tijelima dostave barem sljedeće informacije: (a) naziv subjekta; (b) adresu i ažurirane podatke za kontakt, uključujući adrese e-pošte, IP raspone i telefonske brojeve; (c) ako je to primjenjivo, relevantni sektor i podsektor iz priloga I. ili II.; i (d) ako je to primjenjivo, popis država članica u kojima pružaju usluge obuhvaćene područjem primjene ove Direktive. Subjekti iz stavka 3. bez odgode, a u svakom slučaju u roku od dva tjedna od datuma promjene, obavješćuju o svim promjenama podataka koje su dostavili u skladu s prvim podstavkom ovog stavka. Komisija uz pomoć Agencije Europske unije za kibersigurnost (ENISA) bez nepotrebne odgode pruža smjernice i predloške u vezi s obvezama utvrđenim u ovom stavku.	**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 subjekt malog gospodarstva na temelju zakona kojim se uređuju osnove za primjenu poticajnih mjera gospodarske politike usmjerenih razvoju, restrukturiranju i tržišnom prilagođavanju maloga gospodarstva - privatni i javni subjekti iz Priloga I. ovog Zakona koji nisu utvrđeni kao ključni subjekti temeljem članka 9. ovog Zakona, a predstavljaju subjekt malog gospodarstva na temelju zakona kojim se uređuju osnove za primjenu poticajnih mjera gospodarske politike usmjerenih razvoju, restrukturiranju i tržišnom prilagođavanju maloga gospodarstva - pružatelji usluga povjerenja koji nisu kategorizirani kao ključni subjekti, 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		

Države članice mogu uspostaviti nacionalne mehanizme za registraciju subjekata. 5. Do 17. travnja 2025. i svake dvije godine nakon toga nadležna tijela obavješćuju: (a) Komisiju i skupinu za suradnju o broju svih ključnih i važnih subjekata navedenih u skladu sa stavkom 3. za svaki sektor i podsektor iz priloga I. ili II.; i (b) Komisiju o relevantnim informacijama o broju ključnih i važnih subjekata utvrđenih na temelju članka 2. stavka 2. točaka od (b) do (e), sektoru i podsektoru iz priloga I. ili II. kojima pripadaju, vrsti usluge koju pružaju i odredbama iz članka 2. stavka 2. točaka od (b) do (e), na temelju kojih su utvrđeni. 6. Do 17. travnja 2025. i na zahtjev Komisije države članice mogu obavijestiti Komisiju o nazivima ključnih i važnih subjekata iz stavka 5. točke (b).	- bi poremećaj u funkcioniranju usluge koju pruža subjekt, odnosno poremećaj u obavljanju djelatnosti subjekta, mogao imati znatan utjecaj 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: - 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 u kategoriju važnih subjekata, ovisno o rezultatima provedene procjene njihove posebne važnosti na nacionalnoj ili regionalnoj razini za obavljanje odgojno-obrazovnog rada. **Članak 3. stavak 3. NIS2 direktive preuzima se sljedećim člancima:** **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 kriterija iz članaka 9., 10. i 12. stavka 1. podstavka 1. i stavka 2. ovog Zakona, za svaki sektor i podsektor iz Priloga I. I Priloga II. ovog Zakona, osim za sektor iz Priloga II. točke 8. ovog Zakona - Europskoj komisiji podatke o broju ključnih i važnih subjekata razvrstanih temeljem kriterija iz 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. **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. **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). **Članak 3. stavak 4. NIS2 direktive preuzima se sljedećim člancima:** 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** **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).		

	Članak 3. stavci 5. i 6. NIS2 direktive preuzimaju se sljedećim člankom: 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 kriterija iz članaka 9., 10. i 12. stavka 1. podstavka 1. i stavka 2. ovog Zakona, za svaki sektor i podsektor iz Priloga I. I Priloga II. ovog Zakona, osim za sektor iz Priloga II. točke 8. ovog Zakona - Europskoj komisiji podatke o broju ključnih i važnih subjekata razvrstanih temeljem kriterija iz 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. **Izmijenjen dio relevantnih odredbi Nacrta Zakona sukladno prijedlogu da se dio odredbi prijedloga propisa kojima se na ukazuje na konkretan hrvatski propis izmjeni, imajući na umu učestale izmjene navedenog zakonskog teksta.** **Odredba predmetne Direktive: „Subjekti iz stavka 3. bez odgode, a u svakom slučaju u roku od dva tjedna od datuma promjene, obavješćuju o svim promjenama podataka koje su dostavili u skladu s prvim podstavkom ovog stavka.“, preuzeta člankom 20. st.3. Nacrta Zakona.** **18.8.2023.:** **Kako je pojašnjeno u telefonskom razgovoru 17.8.2023., u**		

	pitanju je prijelazna odredba predmetnog Zakona u kojoj je pozivanje na konkretan naziv zakona i broj NN bitno s aspekta njezine provedbe. Dodatno, u pitanju je pozivanje na NIS1 transpozicijski zakon iz 2018. godine, za koji se predmetnim Zakonom predviđa stavljanje van snage, što znači da ne postoji mogućnost njegovih promjena. S obzirom na prethodno navedeno, članak se vraća na provjeru bez intervencija u tekst Nacrta zakona i UP-a u dijelu koji se odnosi na članak 110. stavak 2. Nacrta zakona. **Čanak 20. stavak 3. Nacrta zakona izmijenjen – umjesto rok od „15 dana" propisan rok od „dva tjedna", kako je to izrijekom propisano NIS2 direktivom. Kako je napomenuto u telefonskom razgovoru od 17.8.2023., budući da se u RH rokovi uobičajeno računaju na dane, mjesece i godine moguće su primjedbe u daljnjem postupku nomotehničke prirode. U tom slučaju koristit će se gore dano obrazloženje o stavu Europske komisije o propisivanju rokova na identičan način kako je to učinjeno direktivama EU.**		
Članak 4. Sektorski pravni akti Unije 1. Ako se sektorskim pravnim aktima Unije od ključnih ili važnih subjekata zahtijeva donošenje mjera upravljanja kibersigurnosnim rizicima ili obavješćivanje o značajnim incidentima i ako su ti zahtjevi po učinku barem jednakovrijedni obvezama utvrđenima u ovoj Direktivi, relevantne odredbe ove Direktive, uključujući odredbe o	**Članak 4. NIS2 direktive preuzima se sljedećim člankom:** **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	U potpunosti preuzeto	

nadzoru i izvršavanju iz poglavlja VII., ne primjenjuju se na te subjekte. Ako sektorski pravni akti Unije ne obuhvaćaju sve subjekte u određenom sektoru koji su obuhvaćeni područjem primjene ove Direktive, relevantne odredbe ove Direktive i dalje se primjenjuju na subjekte koji nisu obuhvaćeni tim sektorskim pravnim aktima Unije. 2. Zahtjevi iz stavka 1. ovog članka smatraju se po učinku jednakovrijednim obvezama utvrđenima u ovoj Direktivi ako: (a) mjere upravljanja kibersigurnosnim rizicima po učinku su barem jednakovrijedne mjerama utvrđenima u članku 21. stavcima 1. i 2.; ili (b) sektorskim pravnim aktom Unije predviđa se neposredan, prema potrebi automatski i izravan, pristup obavijestima o incidentima od strane CSIRT-ova, nadležnih tijela ili jedinstvenih kontaktnih točaka na temelju ove Direktive te kada su zahtjevi za obavješćivanje o značajnim incidentima po učinku barem jednakovrijedni onima utvrđenima u članku 23. stavcima od 1. do 6. ove Direktive.	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. **Odredba preuzeta člankom 8. Nacrta zakona. Radi izričitijeg preuzimanja teksta članka 4. NIS2 direktive u gore citiranom dijelu, stavak 1. članka 8. Nacrta zakona dopunjen na način da je dio rečenice koji je glasio „Ako su za subjekte iz pojedinih sektora iz Priloga I. ovog Zakona i Priloga II. ovog Zakona posebnim zakonima ...“ zamijenjen sljedećim riječima „Ako su za *ključne i važne* subjekte iz pojedinih sektora iz Priloga I. ovog Zakona i Priloga II. ovog Zakona posebnim zakonima.“.**		

3. Komisija do 17. srpnja 2023. pruža smjernice kojima se pojašnjava primjena stavaka 1. i 2. Komisija redovito preispituje te smjernice. Kod pripreme tih smjernica Komisija uzima u obzir primjedbe skupine za suradnju i ENISA-e.			
Članak 5. Minimalno usklađivanje Ovom Direktivom ne sprečava se države članice da donesu ili zadrže odredbe kojima se osigurava viša razina kibersigurnosti, pod uvjetom da su te odredbe u skladu s obvezama država članica utvrđenih pravom Unije.		Nije potrebno preuzimanje	Predmetnom odredbom NIS2 Direktive propisana je mogućnost uvođenja strožih zahtjeva nacionalnim propisima te kao takva ne zahtijeva izravno prenošenje same odredbe u tekst predmetnog Nacrta zakona.

Članak 6. Definicije Za potrebe ove Direktive primjenjuju se sljedeće definicije: 1. „mrežni i informacijski sustav" znači: (a) elektronička komunikacijska mreža kako je definirana u članku 2. točki 1. Direktive (EU) 2018/1972; (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 točkama (a) i (b) u svrhu njihova rada, uporabe, zaštite i održavanja; 2. „sigurnost mrežnih i informacijskih sustava" znači 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	**Članak 6. NIS2 direktive preuzima se sljedećim člankom:** **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, kao što je slučaj s nacionalnim sustavom za otkrivanje kibernetičkih prijetnji i zaštitu kibernetičkog prostora iz ovog Zakona 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:	U potpunosti preuzeto	

usluga koje ti mrežni i informacijski sustavi nude ili kojima omogućuju pristup; 3. „kibersigurnost" znači kibersigurnost kako je definirana u članku 2. točki 1. Uredbe (EU) 2019/881; 4. „nacionalna strategija za kibersigurnost" znači koherentan okvir države članice kojim se predviđaju strateški ciljevi i prioriteti u području kibersigurnosti i upravljanje za njihovo postizanje u toj državi članici; 5. „izbjegnuti incident" znači 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; 6. „incident" znači 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; 7. „kibersigurnosni incident velikih razmjera" znači incident koji uzrokuje razinu poremećaja koja premašuje sposobnost države članice da na njega odgovori ili koji ima	- „na daljinu" znači da se usluga pruža bez da su strane istodobno prisutne - „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 - „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: - „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 - „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		

znatan učinak na najmanje dvije države članice; 8. „postupanje s incidentom” znači sve radnje i postupci čiji je cilj sprečavanje, otkrivanje, analiza, zaustavljanje incidenta ili odgovor na njega te oporavak od incidenta; 9. „rizik” znači mogućnost gubitka ili poremećaja uzrokovana incidentom i treba ga izražavati kao kombinaciju opsega takvog gubitka ili poremećaja i vjerojatnosti pojave tog incidenta; 10. „kiberprijetnja” znači kiberprijetnja kako je definirana u članku 2. točki 8. Uredbe (EU) 2019/881; 11. „ozbiljna kiberprijetnja” znači kiberprijetnja 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; 12. „IKT proizvod” znači IKT proizvod kako je definiran u članku 2. točki 12. Uredbe (EU) 2019/881; 13. „IKT usluga” znači IKT usluga kako je definirana u članku 2. točki 13. Uredbe (EU) 2019/881; 14. „IKT proces” znači IKT proces kako je definiran u članku 2. točki 14. Uredbe (EU) 2019/881;	- 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) 2019/88110. „*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		

15. „ranjivost” znači slabost, osjetljivost ili nedostatak IKT proizvoda ili IKT usluga koje kiberprijetnja može iskoristiti; 16. „norma” znači norma kako je definirana u članku 2. točki 1. Uredbe (EU) br. 1025/2012 Europskog parlamenta i Vijeća (29); 17. „tehnička specifikacija” znači tehnička specifikacija kako je definirana u članku 2. točki 4. Uredbe (EU) br. 1025/2012; 18. „središte za razmjenu internetskog prometa” znači 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; 19. „sustav naziva domena” ili „(DNS)” znači hijerarhijsko raspoređeni sustav imenovanja koji omogućuje utvrđivanje internetskih usluga i resursa, čime se krajnjim	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 informacija među završnim točkama mreže 17. “*javni subjekti*” su tijela državne uprave, druga državna tijela, jedinice lokalne i područne (regionalne) samouprave, pravne osobe i druga tijela koja imaju javne ovlasti, 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		

	korisnicima uređaja omogućuje da korištenje internetskim uslugama usmjeravanja i povezivosti za pristupanje tim uslugama i resursima; 20. „pružatelj usluga DNS-a" znači subjekt koji pruža: (a) javno dostupne rekurzivne usluge razlučivanja naziva domena krajnjim korisnicima interneta; ili (b) mjerodavne usluge razlučivanja naziva domena za upotrebu trećih strana, uz iznimku korijenskih poslužitelja naziva; 21. „registar naziva vršnih domena" znači subjekt kojem je delegirana određena vršna 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 njihovo obavljanje eksternalizira, ali su isključene situacije u kojima registar koristi	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 utjecaj 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 utjecaj 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)		

nazive vršnih domena samo za vlastitu upotrebu; 22. „subjekt koji pruža usluge registracije naziva domena" znači registrar ili zastupnik koji djeluje u ime registrara, kao što je pružatelj ili preprodavatelj usluga zaštite privatnosti i proxy registracije; 23. „digitalna usluga" znači usluga kako je definirana u članku 1. stavku 1. točki (b) Direktive (EU) 2015/1535 Europskog parlamenta i Vijeća (30); 24. „usluga povjerenja" znači usluga povjerenja kako je definirana u članku 3. točki 16. Uredbe (EU) br. 910/2014; 25. „pružatelj usluga povjerenja" znači pružatelj usluga povjerenja kako je definiran u članku 3. točki 19. Uredbe (EU) br. 910/2014; 26. „kvalificirana usluga povjerenja" znači kvalificirana usluga povjerenja kako je definirana u članku 3. točki 17. Uredbe (EU) br. 910/2014; 27. „kvalificirani pružatelj usluga povjerenja" znači kvalificirani pružatelj usluga povjerenja kako je definiran u članku 3. točki 20. Uredbe (EU) br. 910/2014; 28. „internetsko tržište" znači internetsko tržište kako je definirano u članku 2. točki (n)	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 pružateljâ sadržaja i usluga 25. *"mrežni i informacijski sustav"* čine: - "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 - svaki uređaj ili skupina povezanih ili srodnih uređaja, od kojih jedan ili više njih programski izvršava automatsku obradu digitalnih podataka ili - 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		

	Direktive 2005/29/EZ Europskog parlamenta i Vijeća (31); 29. „internetska tražilica" znači internetska tražilica kako je definirana u članku 2. točki 5. Uredbe (EU) 2019/1150 Europskog parlamenta i Vijeća (32); 30. „usluga računalstva u oblaku" znači 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; 31. „usluga podatkovnog centra" znači 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; 32. „mreža za isporuku sadržaja" znači mreža zemljopisno raspoređenih poslužitelja u svrhu osiguravanja visoke dostupnosti, pristupačnosti ili brze isporuke digitalnog sadržaja i usluga korisnicima	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		

	interneta u ime pružateljâ sadržaja i usluga; 33. „platforma za usluge društvenih mreža” znači platforma koja krajnjim korisnicima omogućuje da se međusobno povežu, dijele i otkrivaju sadržaj te da komuniciraju na više uređaja, posebno preko razgovora, objava, videozapisa i preporuka; 34. „predstavnik” znači fizička ili pravna osoba koja ima poslovni nastan u 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 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 ove Direktive; 35. „subjekt javne uprave” znači subjekt koji je kao takav priznat u	(EU) 2016/679), a osobito informacije potrebne za identifikaciju nositelja naziva 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		

državi članici u skladu s nacionalnim pravom, ne uključujući sudstvo, parlamente ili središnje banke i koji ispunjava sljedeće kriterije: (a) uspostavljen je u svrhu zadovoljavanja potreba od općeg interesa i nije industrijske ili komercijalne naravi; (b) ima pravnu osobnost ili ima zakonsko pravo djelovati u ime drugog subjekta s pravnom osobnošću; (c) većim dijelom financiraju ga državna, regionalna ili druga javnopravna tijela, ili podliježe upravljačkom nadzoru tih tijela, ili ima upravni, upravljački ili nadzorni odbor u kojem su više od polovine članova imenovala državna, regionalna ili druga javnopravna tijela; (d) ovlašten je fizičkim ili pravnim osobama upućivati upravne ili regulatorne odluke koje utječu na njihova prava u prekograničnom kretanju osoba, robe, usluga ili kapitala.	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: - javno dostupne rekurzivne usluge razlučivanja naziva domena krajnjim korisnicima interneta i/ili - 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		

36. „javna elektronička komunikacijska mreža” znači javna elektronička komunikacijska mreža kako je definirana u članku 2. točki (8) Direktive (EU) 2018/1972; 37. „elektronička komunikacijska usluga” znači elektronička komunikacijska usluga kako je definirana u članku 2. točki (4) Direktive (EU) 2018/1972; 38. „subjekt” znači fizička ili pravna osoba osnovana i priznata kao takva na temelju nacionalnog prava mjesta svojeg poslovnog nastana, koja može, djelujući u vlastito ime, ostvarivati prava i preuzimati obveze; 39. „pružatelj upravljanih usluga” znači 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; 40. „pružatelj upravljanih sigurnosnih usluga” znači pružatelj upravljanih usluga koji provodi ili pruža pomoć za aktivnosti povezane s	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“* je subjekt koji pruža usluge registracije naziva domena odnosno pravna ili fizička osoba koja obavlja samostalnu djelatnost ovlaštena za registraciju i administraciju .hr domena u ime registra naziva vršne nacionalne internetske domene 44. *„regulatorno tijelo za mrežne djelatnosti“* je Hrvatska regulatorna agencija za mrežne djelatnosti 45. „*rizik*” je mogućnost gubitka ili poremećaja uzrokovana incidentom, koji se izražava kao kombinacija utjecaja 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 utjecaj 48. *„Skupina za suradnju*“ je skupina osnovana u svrhu podupiranja i olakšavanja strateške suradnje i razmjene informacija među		

upravljanjem kibersigurnosnim rizicima; 41. „istraživačka organizacija" znači 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.	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 i privatni subjekt kako su oni definirani u točki 17. i 36. ovog stavka 54. *„subjekti javnog sektora"* su tijela državne uprave, druga državna tijela, pravne osobe s javnim ovlastima, tijela 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"* je Ministarstvo znanosti i obrazovanja 60. „*tijelo nadležno za zaštitu osobnih podataka*" je Agencija za zaštitu osobnih podataka ili drugo nadzorno tijelo iz članaka 55. i 56. Uredbe (EU) 2016/679 61. *„treća strana pružatelj IKT usluga"* je pružatelj IKT usluga kako je definiran u članku 3. 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. *„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		

	63. *„usluga povjerenja"* je usluga povjerenja kako je definirana u članku 3. točki 16. Uredbe (EU) br. 910/2014 64. *„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 65. *„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. Sukladno komentaru: *"Zabranjeno je prepisivanje odredbi uredbi EU, pa ljubazno molimo da ispravite definiciju u čl. 4. st. 1. t. 21. (kibernatička sigurnost), t. 19. (kibernetička prijetnja), t. 8., 9. i 10. (IKT proizvod, usluga i proces), t. 30. (norma), t. 60. (usluga povjerenja), t. 40. (pružatelj usluga povjerenja), t. 23. (kvalificirana usluga povjerenja), t. 22. (kvalificirani pružatelj usluga povjerenja), t. 12. (internetska tražilica)."*- **Izmijenjene navedene točke članka 4. Nacrta zakona, prema gornjem prijedlogu.** U svezi komentara: *"Ljubazno molimo preuzmite definicije ovih odredbi predmetne Direktive: „nacionalna strategija za kibersigurnost", „ozbiljna kiberprijetnja", „tehnička specifikacija", „subjekt koji pruža usluge registracije naziva domena", „subjekt"."* - **ističemo da su definicije već preuzete – članak 4. stavak 1. točke 26., 32., 36. i 43. Nacrta zakona, osim pojma tehnička**		

	specifikacije (pojam naknadno preuzet - dopunjen članak 4. Nacrta zakona, točka 57.). **Vezano uz pojam „nacionalna strategija za kibernetičku sigurnost“ ukazuje se kako se u predmetnom Nacrtu zakona radi usklađivanja sa Zakonom o sustavu strateškog planiranja i upravljanja razvojem Republike Hrvatske koristi pojam „nacionalni akt strateškog planiranja iz područja kibernetičke sigurnosti“.** **Sama NIS2 definicija predmetnog pojma, kao i druge obveze DČ koje proizlaze iz NIS2 direktive u odnosu na donošenje akta strateškog planiranja iz područja kibernetičke sigurnosti ugrađene su u tekst Nacrta zakona (članak 4. stavak 1. točka 26., članak 55.), vodeći pri tome računa o nacionalnom okviru koji uređuje pitanje strateškog planiranja u Republici Hrvatskoj.** **Umjesto pojma „subjekt koji pruža usluge registracije naziva domena“ u Nacrtu zakona se, radi usklađivanja s nacionalnim okvirom koji uređuje pitanje upravljanja registracijama nazivima domena, koristi pojam „registrar“ u definiciji kako je dana u članku 4. stavku 1. točki 43. Nacrta zakona (vidi članak 138. Zakona o elektroničkim komunikacijama i odredbe pratećeg Pravilnika o ustrojstvu i upravljanju vršnom nacionalnom internetskom domenom).** **NIS2 definicija pojma „subjekt“ preuzeta je točkom 36. stavkom 1. člankom 4. Nacrta zakona – pojmom „privatni subjekt“. Naime, radi jasnoće i potpunosti pri propisivanju i razumijevanju na koje sve vrste subjekata se odnosi NIS2 direktiva odnosno predmetni transpozicijski zakon, u Nacrtu zakona koriste se pojmovi „privatni“ i „javni“ subjekt te odgovarajuće definiraju ti pojmovi. Pojam „subjekt“ u**		

	nacionalnom kontekstu obuhvaća i javne i privatne subjekte. (dopunjen stavak 4. stavak 1. – točka 53.). U svezi komentara: "*u potpunosti ispravno preuzmite definiciju pojma „subjekt javne uprave".*- **ističemo da se umjesto pojma „subjekt javne uprave" u Nacrtu zakona koristi pojam „subjekti javnog sektora" budući da se taj pojam cijeni prikladnijim izričaju koji se nacionalno koristi i ustaljeniji je u primjeni (javni sektor, a ne javna uprava).** **Dodatno, definicija pojma „subjekta javne uprave" daje se u Pojmovniku NIS2 direktive u kontekstu uporabe tog pojma u samoj NIS2 direktivi i to kako bi se razjasnilo koje sve vrste subjekata je nacionalno potrebno obuhvatiti kada je sektor „javne uprave" u pitanju, neovisno o različitostima koje u organizacijskom smislu postoje u državama članicama kada je „obuhvat javne uprave" u pitanju.** **Transpozicijskim zakonom potrebno je osigurati da se isti primjenjuje i na obveznike iz domene „javne uprave" odnosno „javnog sektora" kako to proizlazi iz NIS2 direktive, uključujući njezinog PRILOGA I (točka 10., sektor „javna uprava"). Navedeno je predmetnim Nacrtom zakona osigurano. Naime, Nacrtom zakona se jasno propisuje koji subjekti „javnog sektora" su obuhvaćeni primjenom transpozicijskog zakona i to u okvirima zahtjeva NIS2 direktive te je i povezani pojam („subjekti javnog sektora) definiran prema potrebama samog sadržaja transpozicijskog zakona i njegove provedbe u praksi u tom segmentu. S obzirom na izneseno, opća definicija pojma takvih subjekata koja govori o njihovim svojstvima, odnosno kako je to propisano u točki 35. članka 5. NIS2 direktive, nije potrebna.** U svezi komentara: *"Ljubazno molimo pojasnite razlikovanje pojma „registar naziva vršnih domena" u odnosu na čl. 4. st. 1. t. 42. (registar*		

	naziva vršne nacionalne internetske domene), odnosno zašto se sami nazivi navedenih pojmova razlikuju."- **Sadržajno razlikovanje pojmova ne postoji, ali je naziv pojma bilo potrebno prilagoditi nacionalnim okolnostima i uskladiti s nacionalnim okvirom koji uređuje pitanje upravljanja vršnom domenom (članak 138. Zakona o elektroničkim komunikacijama).**		
Članak 7. Nacionalna strategija za kibersigurnost 1. Svaka država članica donosi nacionalnu strategiju za kibersigurnost u kojoj se utvrđuju strateški ciljevi, resursi potrebni za postizanje tih ciljeva i odgovarajuće mjere politike i regulatorne mjere radi postizanja i održavanja visoke razine kibersigurnosti. Nacionalna strategija za kibersigurnost uključuje: (a) ciljeve i prioritete strategije za kibersigurnost države članice koji posebno obuhvaćaju sektore i podsektore iz priloga I. i II.; (b) upravljački okvir za postizanje ciljeva i prioriteta iz točke (a) ovog stavka, uključujući politike iz stavka 2. ; (c) upravljački okvir kojim se pojašnjavaju uloge i odgovornosti relevantnih dionika na nacionalnoj razini, kojim se podupire suradnja i	**Članak 7. NIS2 direktive preuzima se sljedećim člancima i Prilogom (IV.) Zakonu:** **Pojmovi** **Članak 4.** (1) U smislu ovog Zakona pojedini pojmovi imaju sljedeće značenje: 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 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:	U potpunosti preuzeto	

koordinacija na nacionalnoj razini među nadležnim tijelima, jedinstvenim kontaktnim točkama i CSIRT-ovima na temelju ove Direktive, kao i koordinacija i suradnja između tih tijela i nadležnih tijela na temelju sektorskih pravnih akata Unije; (d) mehanizam za utvrđivanje relevantne imovine i procjenu rizika u toj državi članici; (e) određivanje mjera za osiguravanje pripravnosti i sposobnosti reagiranja na incidente i oporavka od incidenata, uključujući suradnju javnog i privatnog sektora; (f) popis različitih tijela i dionika koji su uključeni u provedbu nacionalne strategije za kibersigurnost; (g) okvir politike za bolju koordinaciju između nadležnih tijela na temelju ove Direktive i nadležnih tijela na temelju Direktive (EU) 2022/2557 u svrhu razmjene informacija o rizicima, kiberprijetnjama i incidentima te o rizicima, prijetnjama i incidentima izvan kiberprostora i izvršavanja nadzornih zadaća, prema potrebi; (h) plan, uključujući potrebne mjere, za povećanje opće razine osviještenosti o kibersigurnosti među građanima.	- 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 3 mjeseca od dana njegovog donošenja, odnosno u roku od 3 mjeseca od dana donošenja njegovih izmjena i/ili dopuna. PRILOG IV. Obvezni sadržaj nacionalnog akta strateškog planiranja iz područja kibernetičke sigurnosti I. Nacionalnim aktom strateškog planiranja iz članka 55. ovog Zakona utvrđuju se:		

2. U okviru nacionalne strategije za kibersigurnost države članice posebno donose politike: (a) za rješavanje kibersigurnosnih pitanja u lancu opskrbe za IKT proizvode i IKT usluge kojima se koriste subjekti za pružanje svojih usluga; (b) za uključivanje i definiranje kibersigurnosnih zahtjeva za IKT proizvode i IKT usluge u području javne nabave, uključujući u odnosu na kibersigurnosnu certifikaciju, kriptiranje i upotrebu kibersigurnosnih proizvoda otvorenog koda; (c) za upravljanje ranjivostima, uključujući promicanje i olakšavanje koordiniranog otkrivanja ranjivosti u skladu s člankom 12. stavkom 1.; (d) koje se odnose na održavanje opće dostupnosti, cjelovitosti i povjerljivosti javne jezgre otvorenog interneta, uključujući, ako je to potrebno, kibersigurnost podmorskih komunikacijskih kabela; (e) za promicanje razvoja i integracije relevantnih naprednih tehnologija radi provedbe najsuvremenijih	- 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		

mjera upravljanja kibersigurnosnim rizicima; (f) za promicanje i razvoj obrazovanja i osposobljavanja u području kibersigurnosti, vještina u području kibersigurnosti, informiranja te istraživačkih i razvojnih inicijativa u području kibersigurnosti, kao i smjernica o dobroj praksi i kontrolama kiberhigijene namijenjenih građanima, dionicima i subjektima; (g) za potporu akademskim i istraživačkim institucijama u razvoju, unapređivanju i poticanju uvođenja alata za kibersigurnost i sigurne mrežne infrastrukture; (h) koje uključuju relevantne postupke i odgovarajuće alate za razmjenu informacija u cilju podupiranja dobrovoljne razmjene informacija o kibersigurnosti među subjektima u skladu s pravom Unije; (i) za jačanje kiberotpornosti i osnovne razine kiberhigijene malih i srednjih poduzeća, osobito onih koji su izuzeti iz područja primjene ove Direktive, pružanjem lako dostupnih smjernica i pomoći za njihove specifične potrebe; (j) za promicanje aktivne kiberzaštite.	- 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		

3. Države članice obavješćuju Komisiju o svojim nacionalnim strategijama za kibersigurnost u roku od tri mjeseca od njihova donošenja. Države članice mogu iz takvih obavijesti izostaviti informacije koje se odnose na njihovu nacionalnu sigurnost. 4. Države članice redovito, a najmanje svakih pet godina ocjenjuju svoje nacionalne strategije za kibersigurnost na temelju ključnih pokazatelja uspješnosti te ih prema potrebi ažuriraju. ENISA pomaže državama članicama, na njihov zahtjev u razvoju ili ažuriranju nacionalne strategije za kibersigurnost i ključnih pokazatelja uspješnosti za ocjenjivanje te strategije kako bi je uskladila sa zahtjevima i obvezama utvrđenim u ovoj Direktivi.	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. **Definicija iz čl. 4. st. 1. t. 26. (nacionalni akt strateškog planiranja iz područja kibernetičke sigurnosti) već ranije unesena uz prethodni odnosno članak 6. Usporednog prikaza.** **Izmijenjen članak 55. stavak 5. prema danom prijedlogu.**		

Članak 8. Nadležna tijela i jedinstvene kontaktne točke 1. Svaka država članica imenuje ili uspostavlja jedno ili više nadležnih tijela odgovornih za kibersigurnost i za nadzorne zadaće iz poglavlja VII. (nadležna tijela). 2. Nadležna tijela iz stavka 1. prate provedbu ove Direktive na nacionalnoj razini. 3. Svaka država članica imenuje ili uspostavlja jedinstvenu kontaktnu točku. Ako država članica imenuje ili uspostavi samo jedno nadležno tijelo u skladu sa stavkom 1., to nadležno tijelo ujedno je jedinstvena kontaktna točka te države članice. 4. Svaka jedinstvena kontaktna točka izvršava funkciju povezivanja kako bi osigurala prekograničnu suradnju tijela svoje države članice s relevantnim tijelima u drugim državama članicama, i prema potrebi s Komisijom i ENISA-om, te međusektorsku suradnju s drugim nadležnim tijelima u svojoj državi članici. 5. Države članice osiguravaju da njihova nadležna tijela i jedinstvene	**Članak 8. NIS2 direktive preuzima se sljedećim člancima i Prilogom (III.) Zakonu:** **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, 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. **Popis priloga koji su sastavni dio Zakona**	U potpunosti preuzeto	

kontaktne točke imaju odgovarajuće resurse za učinkovitu i efikasnu provedbu zadaća koje su im dodijeljene te da time ispune ciljeve ove Direktive. 6. Svaka država članica bez nepotrebne odgode obavješćuje Komisiju o identitetu nadležnog tijela iz stavka 1. i jedinstvene kontaktne točke iz stavka 3., o zadaćama tih tijela i o svim naknadnim promjenama. Svaka država članica objavljuje identitet svojeg nadležnog tijela. Komisija javno objavljuje popis jedinstvenih kontaktnih točaka.	**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). **Pojmovi** **Članak 4.** (1) U smislu ovog Zakona pojedini pojmovi imaju sljedeće značenje: 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 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 44. *„regulatorno tijelo za mrežne djelatnosti“* je Hrvatska regulatorna agencija za mrežne djelatnosti 49. *„središnje državno tijelo za informacijsku sigurnost“* je Ured Vijeća za nacionalnu sigurnost 50. „*središnje državno tijelo za kibernetičku sigurnost*“ je Sigurnosno-obavještajna agencija 56. *„tijelo državne uprave nadležno za razvoj digitalnog društva“* je Središnji državni ured za razvoj digitalnog društva 57. *„tijelo državne uprave nadležno za znanost i obrazovanje“* je Ministarstvo znanosti i obrazovanja **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 provedbe zahtjeva kibernetičke sigurnosti sukladno ovom Zakonu i propisu donesenom na temelju 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 - surađuju i razmjenjuju relevantne informacije s tijelom za zaštitu osobnih podataka, kada su osobni podaci ugroženi zbog incidenata na mrežnim i informacijskim sustavima, odnosno s tijelima kaznenog progona, kada je takav incident 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 privatni ili javni 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. **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 - 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: - izvještava Europsku komisiju o nazivima nadležnih tijela iz ovog Zakona i njihovim zadaćama te 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. **PRILOG III.** **Popis nadležnosti u području kibernetičke sigurnosti**		

R. br.	Sektor	Podsektor	Vrsta subjekta	Nadležno tijelo za provedbu zahtjeva kibernetičke sigurnosti	Nadležno tijelo za provedbu posebnih zakona		Nadležni CSIRT
1.	Energetika	Svi	Svi	Središnje državno tijelo za kibernetičku sigurnost	-		Nacionalni centar za kibernetičku sigurnost
2.	Promet	Zračni promet	Svi	-	Hrvatska agencija za civilno zrakoplovstvo		Nacionalni centar za kibernetičku sigurnost
3.	Promet	Željeznički Vodeni Cestovni	Svi	Središnje državno tijelo za kibernetičku sigurnost	-		Nacionalni centar za kibernetičku sigurnost
4.	Bankarstvo	-	Svi	-	Hrvatska narodna banka		Nacionalni CERT
5.	Infrastruktura financijs	-	Svi	-	Hrvatska agencija za nadzor		Nacionalni CERT

	kog tržišta				financijskih usluga			
6.	Zdravstvo	-	Svi	Središnje državno tijelo za kibernetičku sigurnost	-		Nacionalni centar za kibernetičku sigurnost	
7.	Voda za ljudsku potrošnju	-	Svi	Središnje državno tijelo za kibernetičku sigurnost	-		Nacionalni centar za kibernetičku sigurnost	
8.	Otpadne vode	-	Svi	Središnje državno tijelo za kibernetičku sigurnost	-		Nacionalni centar za kibernetičku sigurnost	
9.	Digitalna infrastruktura	-	Pružatelji usluga povjerenja	Tijelo državne uprave nadležno za razvoj digitalnog društva	-		Nacionalni centar za kibernetičku sigurnost	
10.	Digitalna infrastruktura	-	Pružatelji javnih elektroničkih komunikacijskih mreža	Hrvatska regulatorna agencija za mrežne djelatnosti	-		Nacionalni centar za kibernetičku sigurnost	

				Pružatelji javno dostupnih elektroničkih komunikacijskih usluga					
	11.	Digitalna infrastruktura	-	Pružatelji središta za razmjenu internetskog 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 podatkovnog 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 kibernetič	-		Nacionalni centar za kibernetič	

					ku sigurnost			ku 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	Svi	Središnje državno tijelo za kibernetičku sigurnost	-		Nacionalni centar za kibernetičku sigurnost

				proizvoda						
				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	

Članak 9. Nacionalni okviri za upravljanje kiberkrizama 1. Svaka država članica imenuje ili uspostavlja jedno ili više nadležnih tijela odgovornih za upravljanje kibersigurnosnim incidentima velikih razmjera i krizama (tijela za upravljanje kiberkrizama). Države članice osiguravaju da ta tijela imaju odgovarajuće resurse za učinkovito i efikasno obavljanje zadaća koje su im dodijeljene. Države članice osiguravaju koherentnost s postojećim nacionalnim okvirima za opće upravljanje krizama. 2. Ako pojedina država članica imenuje ili uspostavi više od jednog tijela za upravljanje kiberkrizama u skladu sa stavkom 1., jasno navodi koje od tih tijela treba služiti kao koordinator za upravljanje kibersigurnosnim incidentima velikih razmjera i krizama.	**Članak 9. NIS2 direktive preuzima se sljedećim člancima:** **Pojmovi** **Članak 4.** (1) U smislu ovog Zakona pojedini pojmovi imaju sljedeće značenje: 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 utjecaj 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 utjecaj 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 **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	U potpunosti preuzeto	

3. Svaka država članica utvrđuje kapacitete, sredstva i postupke koji se mogu primijeniti u slučaju krize za potrebe ove Direktive. 4. Svaka država članica donosi nacionalni plan za odgovor na kibersigurnosne incidente velikih razmjera i krize u kojem se utvrđuju ciljevi i načini upravljanja kibersigurnosnim incidentima velikih razmjera i krizama. U tom planu se konkretno utvrđuju: (a) ciljevi mjera i aktivnosti za nacionalnu pripravnost; (b) zadaće i odgovornosti tijela za upravljanje kiberkrizama; (c) postupci upravljanja kiberkrizama, uključujući njihovu integraciju u opći nacionalni okvir za upravljanje krizama, i kanali za razmjenu informacija; (d) nacionalne mjere pripravnosti, uključujući vježbe i aktivnosti osposobljavanja; (e) relevantni javni i privatni dionici i uključena infrastruktura; (f) nacionalni postupci i dogovori između relevantnih nacionalnih tijela i drugih tijela kako bi se osiguralo učinkovito sudjelovanje država članica u koordiniranom upravljanju kibersigurnosnim	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. **(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. **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).		

incidentima velikih razmjera i krizama na razini Unije i njihova potpora takvom upravljanju. 5. U roku od tri mjeseca od imenovanja ili uspostave tijela za upravljanje kiberkrizama iz stavka 1. svaka država članica obavješćuje Komisiju o identitetu svojeg tijela i o svim naknadnim promjenama. Države članice dostavljaju Komisiji i Europskoj mreži organizacija za vezu za kiberkrize (mreža EU-CyCLONe) relevantne informacije u vezi sa zahtjevima iz stavka 4. o svojim nacionalnim planovima za odgovor na kibersigurnosne incidente velikih razmjera i krize u roku od tri mjeseca od donošenja tih planova. Države članice mogu izostaviti određene informacije ako je to potrebno i u mjeri u kojoj je takvo izostavljanje potrebno za nacionalnu sigurnost.	(2) Vlada, na prijedlog tijela odgovornog za upravljanje kibernetičkim krizama, donosi nacionalni plan upravljanja kibernetičkim krizama. (3) Nacionalnim planom 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 plana 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 plana iz stavka 2. ovog članka u roku od tri mjeseca od njegova donošenja odnosno njegovih izmjena i dopuna ili donošenja novog plana.		
Članak 10. Timovi za odgovor na računalne sigurnosne incidente (CSIRT-ovi) 1. Svaka država članica imenuje ili uspostavlja jedan ili više CSIRT-ova. CSIRT-ovi se mogu imenovati ili uspostaviti u okviru nadležnog tijela. CSIRT-ovi ispunjavaju zahtjeve utvrđene u članku 11. stavku 1. i obuhvaćaju barem sektore, podsektore ili vrste subjekata iz priloga I. i II. te su odgovorni za postupanje s incidentima u skladu s točno propisanim postupkom. 2. Države članice osiguravaju da svaki CSIRT ima odgovarajuće resurse za učinkovito izvršavanje zadaća utvrđenih u članku 11. stavku 3. 3. Države članice osiguravaju da svaki CSIRT raspolaže odgovarajućom, sigurnom i otpornom komunikacijskom	**Članak 10. NIS2 direktive preuzima se sljedećim člancima i Prilogom (III.) Zakonu:** **Pojmovi** **Članak 4.** (1) U smislu ovog Zakona pojedini pojmovi imaju sljedeće značenje: 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) 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 **Zadaće jedinstvene kontaktne točke** **Članak 62.**	U potpunosti preuzeto	

i informacijskom infrastrukturom za razmjenu informacija s ključnim i važnim subjektima te drugim relevantnim dionicima. Države članice u tu svrhu osiguravaju da svaki CSIRT doprinosi uvođenju sigurnih alata za razmjenu informacija. 4. CSIRT-ovi surađuju i, prema potrebi, razmjenjuju relevantne informacije u skladu s člankom 29. sa sektorskim ili međusektorskim zajednicama ključnih i važnih subjekata. 5. CSIRT-ovi sudjeluju u istorazinskim ocjenjivanjima organiziranima u skladu s člankom 19. 6. Države članice osiguravaju učinkovitu, efikasnu i sigurnu suradnju svojih CSIRT-ova u mreži CSIRT-ova. 7. CSIRT-ovi mogu uspostaviti odnose suradnje s nacionalnim timovima za odgovor na računalne sigurnosne incidente iz trećih zemalja. Kao dio takvih odnosa suradnje, države članice olakšavaju učinkovitu, efikasnu i sigurnu razmjenu informacija s tim nacionalnim timovima za odgovor na računalne sigurnosne incidente iz trećih zemalja koristeći se odgovarajućim protokolima za razmjenu informacija, uključujući Protokol o semaforu. CSIRT-	Jedinstvena kontaktna točka obavlja sljedeće poslove: - obavještava bez odgode Europsku komisiju o nazivima nadležnih tijela iz članka 54. stavka 9., članka 56. stavka 2., 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. **Zadaće CSIRT-a**		

ovi mogu razmjenjivati relevantne informacije s nacionalnim timovima za odgovor na računalne sigurnosne incidente iz trećih zemalja, uključujući osobne podatke u skladu s pravom Unije o zaštiti podataka. 8. CSIRT-ovi mogu surađivati s nacionalnim timovima za odgovor na računalne sigurnosne incidente iz trećih zemalja ili istovjetnim tijelima iz trećih zemalja, posebno kako bi im se pružila pomoć u području kibersigurnosti. 9. Svaka država članica bez nepotrebne odgode obavješćuje Komisiju o identitetu CSIRT-a iz stavka 1. ovog članka i CSIRT-a koji je imenovan koordinatorom u skladu s člankom 12. stavkom 1., o zadaćama u odnosu na ključne i važne subjekte i o svim naknadnim promjenama. 10. Države članice mogu zatražiti podršku ENISA-e u razvijanju svojih CSIRT-ova.	**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 utjecaje 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. **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 sve druge javne subjekte te sve privatne subjekte, uključujući građanstvo.

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**
1.	Energetika	Svi	Svi	Središnje državno tijelo za kibernetičku sigurnost	-
2.	Promet	Zračni promet	Svi	-	Hrvatska agencija za

					civilno zrakoplovstvo		ku sigurnost
3.	Promet	Željeznički Vodeni Cestovni	Svi	Središnje državno tijelo za kibernetičku sigurnost	-		Nacionalni centar za kibernetičku sigurnost
4.	Bankarstvo	-	Svi	-	Hrvatska narodna banka		Nacionalni CERT
5.	Infrastruktura financijskog tržišta	-	Svi	-	Hrvatska agencija za nadzor financijskih usluga		Nacionalni CERT
6.	Zdravstvo	-	Svi	Središnje državno tijelo za kibernetičku sigurnost	-		Nacionalni centar za kibernetičku sigurnost
7.	Voda za ljudsku potrošnju	-	Svi	Središnje državno tijelo za kibernetičku sigurnost	-		Nacionalni centar za kibernetičku sigurnost
8.	Otpadne vode	-	Svi	Središnje državno tijelo za kibernetič	-		Nacionalni centar za kibernetič

					ku sigurnost			ku sigurnost	
	9.	Digitalna infrastruktura	-	Pružatelji usluga povjerenja	Tijelo državne uprave nadležno za razvoj digitalnog društva	-		Nacionalni centar za kibernetičku sigurnost	
	10.	Digitalna infrastruktura	-	Pružatelji javnih elektroničkih komunikacijskih mreža Pružatelji javno dostupnih elektroničkih komunikacijskih usluga	Hrvatska regulatorna agencija za mrežne djelatnosti	-		Nacionalni centar za kibernetičku sigurnost	
	11.	Digitalna infrastruktura	-	Pružatelji središta za razmjenu internet-	Središnje državno tijelo za kibernetičku sigurnost	-		Nacionalni centar za kibernetičku sigurnost	

					skog prometa					
					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	Tijelo državne uprave nadležno za znanost	-		Nacionalni CERT	

				internetske domene	i obrazovanje				
	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 računalate elektroničkih i optičkih						

				proizvoda					
				Proizvodnja električne opreme					
				Proizvodnja strojeva i uređaja, d. n.					
				Proizvodnja motornih vozila, prikolica i polupriko lica					
				Proizvodnja ostale opreme za prijevoz					
	21.	Pružatelji digitalnih usluga	-	Svi	Središnje državno tijelo za kibernetič ku sigurnost	-		Nacionalni centar za kibernetič ku sigurnost	
	22.	Istraživanj e	-	Svi	Tijelo državne uprave	-		Nacionalni CERT	

					nadležno za znanost i obrazovanje			
	23.	Sustav obrazovanja	-	Svi	Tijelo državne uprave nadležno za znanost i obrazovanje	-		Nacionalni CERT

U odnosu na dio komentara koji glasi: Potrebno je izrijekom preuzeti i iduću odredbu predmetne Direktive: „Države članice osiguravaju da svaki CSIRT ima odgovarajuće resurse za učinkovito izvršavanje zadaća utvrđenih u članku 11. stavku 3., kao i „3. Države članice osiguravaju da svaki CSIRT raspolaže odgovarajućom, sigurnom i otpornom komunikacijskom i informacijskom infrastrukturom za razmjenu informacija s ključnim i važnim subjektima te drugim relevantnim dionicima.“ **napominje se da je, radi potpunijeg preuzimanja, dopunjen članak 69. Nacrta zakona (dodani podstavci 5. i 6.).**

U odnosu na dio komentara koji glasi: Potrebno je izrijekom preuzeti i iduću odredbu predmetne Direktive: .. kao i „3. .. Države članice u tu svrhu osiguravaju da svaki CSIRT doprinosi uvođenju sigurnih alata za razmjenu informacija.“ **napominje se da ovaj dio predmetne odredbe NIS2 direktive već preuzet člankom 66. stavkom 1. podstavkom 14. Nacrta zakona.**

	U odnosu na dio komentara koji glasi: Potrebno je izrijekom preuzeti i iduću odredbu predmetne Direktive: „9. Svaka država članica bez nepotrebne odgode obavješćuje Komisiju o identitetu CSIRT-a iz stavka 1. ovog članka i CSIRT-a koji je imenovan koordinatorom u skladu s člankom 12. stavkom 1., o zadaćama u odnosu na ključne i važne subjekte i o svim naknadnim promjenama.“ **napominje se da ovaj dio predmetne odredbe NIS2 direktive već preuzet člankom 62. stavkom 1. podstavkom 1. koji se inicijalno generički odnosio na sva imenovanja o kojima je potrebno obavijestiti Europsku komisiju sukladno NIS2 direktivi odnosno temeljem transpozicijskog zakona. Radi jasnoće i veće preciznosti, dopunjena je spomenuta odredba Nacrta zakona na način da se sada ista izrijekom referira na konkretne odredbe Zakona odnosno nadležna tijela i njihove zadaće na koje se obveza obavještavanja odnosi.** **18.8.2023.:** **Članak 66. stavak 1. podstavak 14. Nacrta zakona dopunjen na način da isti glasi:** „- doprinosi ***uvođenju i*** korištenju alata za sigurnu razmjenu informacija“. **Napominje se kako se člankom 66. stavkom 1. podstavkom 14. Nacrta zakona preuzima i članak 11. stavak 2. točka h) NIS2 direktive. Ta odredba i odredba članka 10. stavka 3. NIS2 direktive (u dijelu koji je predmet dorade), odnose se na isto pitanje, s tim da je u engleskoj verziji NIS2 direktive korišten isti pojam „deployment“, dok se u hrvatskoj verziji u članku 10. stavku 3. NIS2 direktive koristi pojam „uvođenje“, a u članku 11. stavku 2. točki h) „korištenje“.**		

	Radi pravne sigurnosti, a u konačnici i potpunijeg reguliranja ovog pitanja u kontekstu osiguranja angažmana CSIRT-ova i pri uvođenju i pri korištenju alata za sigurnu komunikaciju, u Nacrtu zakona predlaže se dalje koristiti tekst odredbe kako je gore citiran. **Vraćeno na provjeru uz opisanu intervenciju u tekst Nacrta zakona i UP-a u dijelu koji se odnosi na članak 66. stavak 1. podstavak 14. Nacrta zakona.** **Članak 62. stavak 1. podstavak 1. Nacrta zakona dopunjen prema prijedlogu.**		
Članak 11. Zahtjevi, tehničke sposobnosti u pogledu CSIRT-ova i njihove zadaće 1. CSIRT-ovi moraju ispunjavati sljedeće zahtjeve: (a) CSIRT-ovi osiguravaju visoku razinu dostupnosti svojih komunikacijskih kanala izbjegavanjem jedinstvenih točki prekida te u svakom trenutku imaju na raspolaganju više sredstava za dvosmjerno kontaktiranje; oni jasno određuju komunikacijske kanale i o njima obavješćuju klijente i suradnike;	**Članak 11. NIS2 direktive preuzima se sljedećim člancima Zakona:** **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	U potpunosti preuzeto	

(b) prostori CSIRT-ova i informacijski sustavi za potporu smješteni su na sigurnim lokacijama; (c) CSIRT-ovi su opremljeni odgovarajućim sustavom za upravljanje zahtjevima i njihovim usmjeravanjem, posebno kako bi se olakšale učinkovite i efikasne primopredaje; (d) CSIRT-ovi osiguravaju povjerljivost i pouzdanost svojih operacija; (e) CSIRT-ovi imaju dovoljno osoblja kako bi se osigurala dostupnost njihovih usluga u svako doba i osiguravaju da je njihovo osoblje osposobljeno na odgovarajući način; (f) CSIRT-ovi su opremljeni redundantnim sustavima i rezervnim radnim prostorom kako bi se osigurao kontinuitet njihovih usluga. CSIRT-ovi mogu sudjelovati u međunarodnim mrežama za suradnju. 2. Države članice osiguravaju da njihovi CSIRT-ovi zajedno imaju tehničke sposobnosti potrebne za izvršavanje zadaća iz stavka 3. Države članice osiguravaju da se njihovim CSIRT-ovima dodijele dostatni resursi za osiguravanje dovoljno osoblja kako bi se CSIRT-ovima	- 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 utjecaje 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		

omogućilo da razviju svoje tehničke sposobnosti. 3. CSIRT-ovi obavljaju sljedeće zadaće: (a) praćenje i analiziranje kiberprijetnji, ranjivosti i incidenata na nacionalnoj razini i, na zahtjev, pružanje pomoći predmetnim ključnim i važnim subjektima u vezi s praćenjem njihovih mrežnih i informacijskih sustava u stvarnom ili gotovo stvarnom vremenu; (b) pružanje ranih upozorenja i najava te informiranje predmetnih ključnih i važnih subjekata, kao i nadležnih tijela i drugih relevantnih dionika o kiberprijetnjama, ranjivostima i incidentima, ako je moguće u gotovo stvarnom vremenu; (c) odgovaranje na incidente i, ako je to primjenjivo, pružanje pomoći predmetnim ključnim i važnim subjektima; (d) prikupljanje i analiziranje forenzičkih podataka te osiguravanje dinamičke analize rizika i incidenata te informiranosti o stanju u pogledu kibersigurnosti; (e) osiguravanje, na zahtjev predmetnog ključnog ili važnog	- 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 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.		

subjekta, proaktivnog skeniranja mrežnih i informacijskih sustava predmetnog subjekta radi otkrivanja ranjivosti s potencijalno znatnim učinkom; (f) sudjelovanje u mreži CSIRT-ova i pružanje uzajamne pomoći u skladu sa svojim kapacitetima i kompetencijama drugim članovima mreže CSIRT-ova na njihov zahtjev; (g) ako je to primjenjivo, djelovanje u svojstvu koordinatora za potrebe postupka koordiniranog otkrivanja ranjivosti iz članka 12. stavka 1.; (h) doprinošenje korištenju alata za sigurnu razmjenu informacija na temelju članka 10. stavka 3. CSIRT-ovi mogu provoditi proaktivno neintruzivno skeniranje javno dostupnih mrežnih i informacijskih sustava ključnih i važnih subjekata. Takvo skeniranje provodi se kako bi se otkrili ranjivi ili nesigurno konfigurirani mrežni i informacijski sustavi te kako bi se obavijestili dotični subjekti. Takvo skeniranje ne smije imati negativan učinak na funkcioniranje usluga subjekata. Pri obavljanju zadaća iz prvog podstavka CSIRT-ovi mogu dati prednost određenim zadaćama na	**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. 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		

temelju pristupa utemeljenog na procjeni rizika. 4. CSIRT-ovi uspostavljaju odnose suradnje s relevantnim dionicima u privatnom sektoru radi ostvarenja ciljeva ove Direktive. 5. Kako bi olakšali suradnju iz stavka 4., CSIRT-ovi promiču donošenje i primjenu zajedničkih ili standardiziranih praksi, planova za klasifikaciju i taksonomija u odnosu na: (a) postupke za postupanje s incidentima; (b) upravljanje krizama; i (c) koordinirano otkrivanje ranjivosti na temelju članka 12. stavka 1.	- 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. **Predmetna odredba NIS2 direktive preuzeta člankom 69. Nacrta zakona (Osiguravanje uvjeta za obavljanje zadaća nadležnog CSIRT-a). Radi potpunijeg preuzimanja članka 11. u citiranim dijelovima, dorađena je spomenuta odredba Nacrta zakona.**		

Članak 12. Koordinirano otkrivanje ranjivosti i europska baza podataka o ranjivosti 1. Svaka država članica imenuje jednog od svojih CSIRT-ova koordinatorom za potrebe koordiniranog otkrivanja ranjivosti. CSIRT koji je imenovan koordinatorom 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-a koji je imenovan koordinatorom uključuju: (a) utvrđivanje predmetnih subjekata i kontaktiranje s njima; (b) pomaganje fizičkim ili pravnim osobama koje prijavljuju ranjivost; i (c) pregovaranje o vremenskom okviru za otkrivanje i upravljanje ranjivostima koje utječu na više subjekata. Države članice osiguravaju da fizičke ili pravne osobe, kad to zatraže, mogu anonimno prijaviti ranjivost CSIRT-u koji je imenovan koordinatorom. CSIRT koji je imenovan koordinatorom	**Članak 12. stavak 1. NIS2 direktive preuzima se sljedećim člankom Zakona:** **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 dostavlja informacije o novootkrivenim ranjivostima nadležnim CSIRT-ovima iz ovog Zakona, zajedno s uputom o načinu daljnjeg obavještavanja o ranjivostima subjekata u njihovoj nadležnosti. (7) Nadležni CSIRT-ovi izrađuju smjernice namijenjene korisnicima ranjivih IKT proizvoda ili IKT usluga o načinu na koji se mogu ublažiti	U potpunosti preuzeto	

osigurava provedbu pažljivih daljnjih mjera u pogledu prijavljene ranjivosti i osigurava anonimnost fizičke ili pravne osobe koja prijavljuje ranjivost. Ako bi prijavljena ranjivost mogla imati znatan učinak na subjekte u više od jedne države članice, CSIRT koji je imenovan koordinatorom svake dotične države članice, prema potrebi, surađuje s drugim CSIRT-ovima koji su imenovani koordinatorima u okviru mreže CSIRT-ova. 2. ENISA nakon savjetovanja sa skupinom za suradnju razvija i vodi europsku bazu podataka o ranjivosti. U tu svrhu ENISA uspostavlja i održava odgovarajuće informacijske sustave, politike i postupke te usvaja potrebne tehničke i organizacijske mjere za osiguravanje sigurnosti i cjelovitosti europske baze podataka o ranjivosti, osobito kako bi omogućila subjektima, neovisno jesu li obuhvaćeni područjem primjene ove Direktive, kao i njihovim dobavljačima mrežnih i informacijskih sustava, da, na dobrovoljnoj osnovi, otkriju i registriraju javno poznate ranjivosti u IKT proizvodima ili IKT uslugama. Svim dionicima omogućuje se pristup informacijama o ranjivostima sadržanima u europskoj bazi podataka o ranjivosti. Ta baza podataka uključuje:	rizici koji proizlaze iz otkrivenih ranjivosti te dostavljaju obavijesti s najboljim praksama subjektima za koje su zaduženi temeljem ovog Zakona. (8) 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. (9) Zadaće CSIRT koordinatora za otkrivanje ranjivosti obavlja CSIRT pri središnjem državnom tijelu za kibernetičku sigurnost. **Nije potrebno preuzimanje stavka 2. U pitanju su obveze koje se odnose na ENISA-u.**		

(a) informacije koje opisuju ranjivost; (b) IKT proizvode ili IKT usluge na koje ona utječe i ozbiljnost ranjivosti s obzirom na okolnosti u kojima se može iskoristiti; (c) dostupnost odgovarajućih popravaka i ako nisu dostupni popravci, smjernice koje pružaju nadležna tijela ili CSIRT-ovi namijenjene korisnicima ranjivih IKT proizvoda i IKT usluga o načinu na koji se mogu ublažiti rizici koji proizlaze iz otkrivenih ranjivosti.			
Članak 13. Suradnja na nacionalnoj razini 1. Ako su različiti, nadležna tijela, jedinstvena kontaktna točka i CSIRT-ovi iste države članice surađuju u ispunjavanju obveza utvrđenih u ovoj Direktivi. 2. Države članice osiguravaju da njihovi CSIRT-ovi ili, ako je to primjenjivo, njihova nadležna tijela, primaju obavijesti o značajnim incidentima u skladu s člankom 23. i incidentima, kiberprijetnjama i izbjegnutim incidentima u skladu s člankom 30. 3. Države članice osiguravaju da njihovi CSIRT-ovi ili, ako je to primjenjivo, njihova nadležna tijela obavješćuju	**Članak 13. stavak 1. NIS2 direktive preuzima se sljedećim člancima Zakona:** **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 provedbe zahtjeva kibernetičke sigurnosti sukladno ovom Zakonu i propisu donesenom na temelju 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	U potpunosti preuzeto	

njezinu jedinstvenu kontaktnu točku o obavijestima o incidentima, kiberprijetnjama i izbjegnutim incidentima koje su im dostavljene skladu s ovom Direktivom. 4. Kako bi se osiguralo učinkovito obavljanje zadaća i obveza nadležnih tijela, jedinstvenih kontaktnih točaka i CSIRT-ova, države članice, u mjeri u kojoj je to moguće, osiguravaju odgovarajuću suradnju između tih tijela i tijela za izvršavanje zakonodavstva, tijela za zaštitu podataka, nacionalnih tijela na temelju uredaba (EZ) br. 300/2008 i (EU) 2018/1139, nadzornih tijela na temelju Uredbe (EU) br. 910/2014, nadležnih tijela na temelju Uredbe (EU) 2022/2554, nacionalnih regulatornih tijela na temelju Direktive (EU) 2018/1972, nadležnih tijela na temelju Direktive (EU) 2022/2557, kao i nadležnih tijela na temelju drugih sektorskih pravnih akta Unije, unutar te države članice. 5. Države članice osiguravaju da njihova nadležna tijela na temelju ove Direktive i njihova nadležna tijela na temelju Direktive (EU) 2022/2557 redovito surađuju i razmjenjuju informacije u pogledu utvrđivanja kritičnih subjekata, o rizicima, kiberprijetnjama i incidentima, kao i o	- surađuju i razmjenjuju relevantne informacije s tijelom za zaštitu osobnih podataka, kada su osobni podaci ugroženi zbog incidenata na mrežnim i informacijskim sustavima, odnosno s tijelima kaznenog progona, kada je takav incident 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 privatni ili javni 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		

rizicima, prijetnjama i incidentima izvan kiberprostora koji utječu na ključne subjekte koji su utvrđeni kao kritični subjekti na temelju Direktive (EU) 2022/2557, kao i o poduzetim mjerama kao odgovor na takve rizike, prijetnje i incidente. Države članice osiguravaju i da njihova nadležna tijela u skladu s ovom Direktivom i njihova nadležna tijela na temelju Uredbe (EU) br. 910/2014, Uredbe (EU) 2022/2554 i Direktive (EU) 2018/1972 redovito razmjenjuju relevantne informacije, među ostalim o bitnim incidentima i kiberprijetnjama. 6. Države članice pojednostavnjuju izvješćivanje tehničkim sredstvima za obavijesti iz članaka 23. i 30.	dužnosti, na prijedlog jednog od nadležnih tijela prema Prilogu III. ovog Zakona ili na prijedlog subjekta. **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 - 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: - izvještava Europsku komisiju o nazivima nadležnih tijela iz ovog Zakona i njihovim zadaćama te 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. **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 utjecaje 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 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. **Članak 13. stavci 2. i 3. NIS2 direktive preuzima se sljedećim člankom Zakona:** **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. **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 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. **Članak 13. stavak 4. NIS2 direktive preuzima se sljedećim člankom Zakona:** **Pojmovi** **Članak 4.**		

	(1) U smislu ovog Zakona pojedini pojmovi imaju sljedeće značenje: 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 49. *„središnje državno tijelo za informacijsku sigurnost“* je Ured Vijeća za nacionalnu sigurnost 50. „*središnje državno tijelo za kibernetičku sigurnost*“ je Sigurnosno-obavještajna agencija 56. *„tijelo državne uprave nadležno za razvoj digitalnog društva“* je Središnji državni ured za razvoj digitalnog društva 57. *„tijelo državne uprave nadležno za znanost i obrazovanje“* je Ministarstvo znanosti i obrazovanja 58. „*tijelo nadležno za zaštitu osobnih podataka*“ je Agencija za zaštitu osobnih podataka **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 provedbe zahtjeva kibernetičke sigurnosti sukladno ovom Zakonu i propisu donesenom na temelju 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 **- surađuju i razmjenjuju relevantne informacije s tijelom za zaštitu osobnih podataka, kada su osobni podaci ugroženi zbog incidenata na mrežnim i informacijskim sustavima, odnosno s tijelima kaznenog progona, kada je takav incident 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 privatni ili javni 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. **Suradnja s nadležnim tijelima za provedbu posebnih zakona** **Članak 64.** (1) Središnje državno tijelo za kibernetičku sigurnost i 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. **Članak 13. stavak 5. NIS2 direktive preuzima se sljedećim člankom Zakona:** **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. **Članak 13. stavak 6. NIS2 direktive preuzima se sljedećim člankom 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).		

Članak 14. Skupina za suradnju 1. Kako bi se podupirala i olakšavala strateška suradnja i razmjena informacija među državama članicama te jačalo povjerenje, osniva se skupina za suradnju. 2. Skupina za suradnju izvršava svoje zadaće na temelju dvogodišnjih programa rada iz stavka 7. 3. Skupina za suradnju sastoji se od predstavnika država članica, Komisije i ENISA-e. Europska služba za vanjsko djelovanje sudjeluje u aktivnostima skupine za suradnju kao promatrač. Europska nadzorna tijela i nadležna tijela na temelju Uredbe (EU) 2022/2554 mogu sudjelovati u aktivnostima skupine za suradnju u skladu s člankom 47. stavkom 1. te uredbe. Skupina za suradnju može, prema potrebi, pozvati Europski parlament i predstavnike relevantnih dionika da sudjeluju u njezinu radu. Komisija osigurava tajništvo. 4. Zadaće su skupine za suradnju:	**Članak 14. stavak 3. NIS2 direktive preuzima se sljedećim člancim Zakona:** **Pojmovi** **Članak 4.** (1) U smislu ovog Zakona pojedini pojmovi imaju sljedeće značenje: 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 **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	U potpunosti preuzeto	

(a) pružanje smjernica nadležnim tijelima za prenošenje i provedbu ove Direktive; (b) pružanje smjernica nadležnim tijelima u vezi s razvojem i provedbom politika o koordiniranom otkrivanju ranjivosti, kako je navedeno u članku 7. stavku 2. točki (c); (c) razmjena najbolje prakse i informacija povezanih s provedbom ove Direktive, među ostalim u pogledu kiberprijetnji, incidenata, ranjivosti, izbjegnutih incidenata, inicijativa za informiranje, osposobljavanja, vježbi i vještina, izgradnje kapaciteta, normi i tehničkih specifikacija te utvrđivanja ključnih i važnih subjekata na temelju članka 2. stavka 2. točaka od (b) do (e); (d) savjetovanje i suradnja s Komisijom u pogledu novih inicijativa kibersigurnosne politike i ukupne dosljednosti sektorskih kibersigurnosnih zahtjeva; (e) savjetovanje i suradnja s Komisijom u pogledu nacrta delegiranih ili provedbenih akata donesenih u skladu s ovom Direktivom; (f) razmjena najbolje prakse i informacija s relevantnim	- 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:		

institucijama, tijelima, uredima i agencijama Unije; (g) razmjena mišljenja o provedbi sektorskih pravnih akata Unije koji sadržavaju odredbe o kibersigurnosti; (h) ako je to relevantno, rasprava o izvješćivanju o istorazinskom ocjenjivanju iz članka 19. stavka 9. te donošenje zaključaka i preporuka; (i) provedba koordinirane procjene sigurnosnih rizika kritičnih lanaca opskrbe u skladu s člankom 22. stavkom 1.; (j) rasprava o slučajevima uzajamne pomoći, uključujući iskustva i rezultate prekograničnih zajedničkih nadzornih aktivnosti iz članka 37.; (k) na zahtjev jedne ili više dotičnih država članica, rasprava o posebnim zahtjevima za uzajamnu pomoć iz članka 37.; (l) pružanje strateških smjernica mreži CSIRT-ova i mreži EU-CyCLONe o određenim novonastalim pitanjima; (m) razmjena mišljenja o politici daljnjih mjera nakon kibersigurnosnih incidenata velikih razmjera i kriza na temelju iskustava stečenih u okviru mreže CSIRT-ova i mreže EU-CyCLONe;	- izvještava Europsku komisiju o nazivima nadležnih tijela iz ovog Zakona i njihovim zadaćama te 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. **Članak 14. st. 3. u potpunosti preuzet.** **Nije potrebno preuzimanje ostalih odredbi članka 14. NIS2 direktive.** **U pitanju su obveze koje su provedene na razini nadležnih EU institucija. Predstavnici RH već sudjeluju u radu Skupine za suradnju, dok je predmetnim Nacrtom zakona isto uključeno kroz zadaće jedinstvene nacionalne kontaktne točke odnosno središnjeg državnog tijela za kibernetičku sigurnost.**		

(n) doprinos kibersigurnosnim kapacitetima širom Unije olakšavanjem razmjene nacionalnih službenika putem programa za izgradnju kapaciteta koji uključuje osoblje iz nadležnih tijela ili CSIRT-ova; (o) organiziranje redovitih zajedničkih sastanaka s relevantnim privatnim dionicima iz cijele Unije u svrhu rasprave o aktivnostima skupine za suradnju i prikupljanja informacija o novim izazovima u pogledu politike; (p) rasprava o radu obavljenom u vezi s vježbama u području kibersigurnosti, uključujući rad ENISA-e; (q) utvrđivanje metodologije i organizacijskih aspekata istorazinskog ocjenjivanja iz članka 19. stavka 1. te utvrđivanje metodologije samoocjene za države članice u skladu s člankom 19. stavkom 5. uz pomoć Komisije i ENISA-e te, u suradnji s Komisijom i ENISA-om, izrađivanje kodeksa ponašanja na kojima se temelje metode rada imenovanih stručnjaka za kibersigurnost u skladu s člankom 19. stavkom 6.; (r) priprema izvješća u svrhu preispitivanja iz članka 40. o iskustvu stečenom na strateškoj i			

operativnoj razini te iz istorazinskih ocjenjivanja; (s) rasprava i redovita provedba procjene stanja kiberprijetnji ili kiberincidenata, kao što su ucjenjivački softveri. Izvješća iz prvog podstavka točke (r) skupina za suradnju podnosi Komisiji, Europskom parlamentu i Vijeću. 5. Države članice osiguravaju učinkovitu, djelotvornu i sigurnu suradnju svojih predstavnika u skupini za suradnju. 6. Skupina za suradnju može od mreže CSIRT-ova zatražiti tehničko izvješće o odabranim temama. 7. Do 1. veljače 2024., a nakon toga svake dvije godine, skupina za suradnju sastavlja program rada u pogledu mjera koje treba poduzeti za provedbu svojih ciljeva i zadaća. 8. Komisija može donijeti provedbene akte kojima se utvrđuju postupovni aranžmani potrebni za funkcioniranje skupine za suradnju. Ti se provedbeni akti donose u skladu s postupkom ispitivanja iz članka 39. stavka 2.			

Komisija u skladu sa stavkom 4. točkom (e) razmjenjuje savjete i surađuje sa skupinom za suradnju na nacrtima provedbenih akata iz prvog podstavka ovog stavka. 9. Skupina za suradnju sastaje se redovito, a u svakom slučaju jednom godišnje, sa skupinom za otpornost kritičnih subjekata, osnovanom na temelju Direktive (EU) 2022/2557 radi promicanja i olakšavanja strateške suradnje i razmjene informacija.			
Članak 15. Mreža CSIRT-ova 1. Kako bi se doprinijelo razvoju povjerenja i pouzdanja te promicanja brze i učinkovite operativne suradnje među državama članicama, osniva se mreža nacionalnih CSIRT-ova. 2. Mreža CSIRT-ova sastoji se od predstavnika CSIRT-ova imenovanih ili uspostavljenih u skladu s člankom 10. i tima za hitne računalne intervencije za institucije, tijela i agencije Unije (CERT-EU). Komisija u mreži CSIRT-ova sudjeluje kao promatrač. ENISA osigurava tajništvo i aktivno	**Članak 15. stavak 2. NIS2 direktive preuzima se sljedećim člancim Zakona:** **Pojmovi** **Članak 4.** (1) U smislu ovog Zakona pojedini pojmovi imaju sljedeće značenje: 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) **Zadaće CSIRT-a** **Članak 66.**	U potpunosti preuzeto	

pruža pomoć za suradnju među CSIRT-ovima. 3. Zadaće su mreže CSIRT-ova: (a) razmjena informacija o kapacitetima CSIRT-ova; (b) olakšavanje dijeljenja, prijenosa i razmjene tehnologije i relevantnih mjera, politika, alata, procesa, najbolje prakse i okvira među CSIRT-ovima; (c) razmjena relevantnih informacija o incidentima, izbjegnutim incidentima, kiberprijetnjama, rizicima i ranjivostima; (d) razmjena informacija o publikacijama i preporukama u području kibersigurnosti; (e) osiguravanje interoperabilnosti u pogledu specifikacija i protokola za razmjenu informacija; (f) na zahtjev člana mreže CSIRT-ova na koju bi incident mogao utjecati, razmjena i rasprava o informacijama o tom incidentu te povezanim kiberprijetnjama, rizicima i ranjivostima; (g) na zahtjev člana mreže CSIRT-ova, razmatranje te, ako je moguće, i provedba koordiniranog odgovora na incident koji je utvrđen u području za koje je nadležna ta država članica;	(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		

(h) pružanje pomoći državama članicama u rješavanju prekograničnih incidenata u skladu s ovom Direktivom; (i) suradnja, razmjena najbolje prakse i pružanje pomoći CSIRT-ovima koji su imenovani koordinatorima u skladu s člankom 12. stavkom 1. u pogledu upravljanja koordiniranim otkrivanjem ranjivosti koje bi mogle imati znatan učinak na subjekte u više od jedne države članice; (j) rasprava o daljnjim oblicima operativne suradnje te njihovo utvrđivanje, među ostalim u odnosu na: i. kategorije kiberprijetnji i incidenata; ii. rana upozorenja; iii. uzajamnu pomoć; iv. načela i načine koordinacije u odgovoru na prekogranične rizike i incidente; v. doprinos nacionalnom planu za odgovor na kibersigurnosne incidente velikih razmjera i krize iz članka 9. stavka 4. na zahtjev države članice; (k) obavješćivanje skupine za suradnju o svojim aktivnostima i daljnjim oblicima operativne suradnje razmotrenima na temelju	- u suradnji s nadležnim tijelom za provedbu zahtjeva kibernetičke sigurnosti, određuje prekogranične i međusektorske utjecaje 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 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		

točke (j) te prema potrebi traženje smjernica u tom pogledu; (l) razmatranje vježbi u području kibersigurnosti, među ostalim onih koje organizira ENISA; (m) na zahtjev pojedinačnog CSIRT-a, rasprava o kapacitetima i pripravnosti tog CSIRT-a; (n) suradnja i razmjena informacija s centrima za sigurnosne operacije (SOC-ovi) na regionalnoj razini i na razini Unije kako bi se poboljšala zajednička informiranost o stanju u pogledu na incidenata i kiberprijetnji širom Unije; (o) ako je to relevantno, rasprava o izvješćima o istorazinskom ocjenjivanju iz članka 19. stavka 9.; (p) pružanje smjernica radi olakšavanja konvergencije operativnih praksi u cilju primjene odredaba ovog članka o operativnoj suradnji. 4. U svrhu preispitivanja iz članka 40. mreža CSIRT-ova do 17. siječnja 2025., a nakon toga svake dvije godine, ocjenjuje napredak ostvaren u operativnoj suradnji i donosi izvješće. U izvješću se posebno donose zaključci i preporuke na temelju ishoda istorazinskih ocjenjivanja iz članka 19. provedenih u	- 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. **Članak 15. st. 1. u potpunosti preuzet.** **Nije potrebno preuzimanje ostalih odredbi članka 15. NIS2 direktive. U pitanju su obveze koje se provode na razini nadležnih EU institucija. Predstavnici RH već sudjeluju u radu Mreže CSIRT-ova, dok je predmetnim Nacrtom zakona isto uključeno kroz definirane zadaće nadležnih CSIRT-ova.**		

pogledu nacionalnih CSIRT-ova. To se izvješće dostavlja skupini za suradnju. 5. Mreža CSIRT-ova donosi svoj poslovnik. 6. Mreža CSIRT-a i mreža EU-CyCLONe dogovaraju postupovne aranžmane na temelju kojih surađuju.			
Članak 16. Europska mreža organizacija za vezu za kiberkrize (mreža EU-CyCLONe) 1. Mreža EU-CyCLONe osniva se kako bi se poduprlo koordinirano upravljanje kibersigurnosnim incidentima velikih razmjera i krizama na operativnoj razini i osigurala redovita razmjena relevantnih informacija među državama članicama te institucijama, tijelima, uredima i agencijama Unije.	**Članak 16. stavak 2. NIS2 direktive preuzima se sljedećim člancim Zakona:** **Pojmovi** **Članak 4.** (1) U smislu ovog Zakona pojedini pojmovi imaju sljedeće značenje: 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 **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:	U potpunosti preuzeto	

	- 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 - kao tijelo odgovorno za upravljanje kibernetičkim krizama koordinira aktivnosti vezane za upravljanje kibernetičkim krizama na nacionalnoj razini - **s**udjeluje 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		

2. Mreža EU-CyCLONe čine predstavnici tijela država članica za upravljanje kiberkrizama te, u slučajevima kada potencijalni ili aktualni kibersigurnosni incident velikih razmjera ima ili bi mogao imati znatan učinak na usluge i djelatnosti obuhvaćene područjem primjene ove Direktive, Komisija. U drugim slučajevima Komisija u aktivnostima mreže EU-CyCLONe sudjeluje kao promatrač. ENISA osigurava tajništvo mreže EU-CyCLONe i podupire sigurnu razmjenu informacija te osigurava potrebne alate za potporu suradnji među državama članicama osiguravajući pritom sigurnu razmjenu informacija. Mreža EU-CyCLONe može, prema potrebi, pozvati predstavnike relevantnih dionika da u njegovu radu sudjeluju kao promatrači.	- 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. **Čl. 16. st. 2. preuzet.** **Nije potrebno preuzimanje ostalih odredbi članka 16. NIS2 direktive. U pitanju su obveze koje se provode na razini nadležnih EU institucija. Predstavnici RH već sudjeluju u radu EU-CyCLONe mreže, dok je predmetnim Nacrtom zakona isto uključeno kroz definirane zadaće središnjeg državnog tijela za kibernetičku sigurnost.**		

3. Mreža EU-CyCLONe ima sljedeće zadaće: (a) povećanje razine pripravnosti za upravljanje kibersigurnosnim incidentima velikih razmjera i krizama; (b) poboljšanje zajedničke informiranosti o kibersigurnosnim incidentima velikih razmjera i krizama; (c) procjena posljedica i učinka relevantnih kibersigurnosnih incidenata velikih razmjera i kriza te predlaganje mogućih mjera ublažavanja; (d) koordinacija upravljanja kibersigurnosnim incidentima velikih razmjera i krizama te pomoć pri odlučivanju na političkoj razini u pogledu takvih incidenata i kriza; (e) rasprava, na zahtjev dotične države članice, o nacionalnim planovima za odgovor na kibersigurnosne incidente velikih razmjera i krize iz članka 9. stavka 4. 4. Mreža EU-CyCLONe donosi svoj poslovnik. 5. Mreža EU-CyCLONe redovito izvješćuje skupinu za suradnju o upravljanju kibersigurnosnim			

incidentima velikih razmjera i krizama te o trendovima, posvećujući posebnu pažnju njihovu učinku na ključne i važne subjekte. 6. Mreža EU-CyCLONe surađuje s mrežom CSIRT-ova na temelju dogovorenih postupovnih aranžmana iz članka 15. stavka 6. 7. Mreža EU-CyCLONe do 17. srpnja 2024. i svakih 18 mjeseci nakon toga, Europskom parlamentu i Vijeću podnosi izvješće u kojem ocjenjuje svoj rad.			
Članak 17. Međunarodna suradnja Unija, prema potrebi, može sklapati međunarodne sporazume s trećim zemljama ili međunarodnim organizacijama, u skladu s člankom 218. UFEU-a, kojima im se dopušta i organizira sudjelovanje u određenim aktivnostima skupine za suradnju, mreže CSIRT-ova i mreže EU-CyCLONe. Takvi sporazumi moraju biti u skladu s pravom Unije o zaštiti podataka.		Nije potrebno preuzimanje	Nije potrebno preuzimanje. Odredba se odnosi na nadležne EU institucije.

Članak 18. Izvješće o stanju kibersigurnosti u Uniji 1. ENISA u suradnji s Komisijom i skupinom za suradnju donosi dvogodišnje izvješće o stanju kibersigurnosti u Uniji te podnosi i predstavlja to izvješće Europskom parlamentu. Izvješće se, među ostalim, čini dostupnim u strojno čitljivom formatu i obuhvaća sljedeće: (a) procjenu rizika u području kibersigurnosti na razini Unije, uzimajući u obzir kiberprijetnje; (b) ocjenu razvoja kibersigurnosnih kapaciteta u javnim i privatnim sektorima širom Unije; (c) procjenu opće razine informiranosti o kibersigurnosti i kiberhigijeni među građanima i subjektima, uključujući mala i srednja poduzeća; (d) skupnu ocjenu ishoda istorazinskih ocjenjivanja iz članka 19.; (e) skupnu ocjenu razine razvijenosti kibersigurnosnih kapaciteta i resursa širom Unije, uključujući one na sektorskoj razini, te do koje su mjere usklađene nacionalne strategije država članica za kibersigurnost.		Nije potrebno preuzimanje	Nije potrebno preuzimanje. Odredba se odnosi na nadležne EU institucije, Skupinu za suradnju i Mrežu CSIRT-ova.

2. Izvješće sadržava posebne preporuke o politikama u cilju rješavanja nedostataka i povećanja razine kibersigurnosti širom Unije te sažetak zaključaka za određeno razdoblje iz tehničkih izvješća o stanju kibersigurnosti u EU-u koje sastavlja ENISA u skladu s člankom 7. stavkom 6. Uredbe (EU) 2019/881. 3. ENISA u suradnji Komisijom, skupinom za suradnju i mrežom CSIRT-ova razvija metodologiju, uključujući relevantne varijable, kao što su kvantitativni i kvalitativni pokazatelji, skupnih ocjena iz stavka 1. točke (e).			
Članak 19. Istorazinska ocjenjivanja 1. Skupina za suradnju, uz pomoć Komisije i ENISA-e te, ako je to relevantno, mreže CSIRT-ova, do 17. siječnja 2025. utvrđuje metodologiju i organizacijske aspekte istorazinskih ocjenjivanja s ciljem učenja iz zajedničkih iskustava, jačanja uzajamnog povjerenja, postizanja visoke zajedničke razine kibersigurnosti te jačanja kibersigurnosnih kapaciteta i politika država članica potrebnih za	**Članak 19. stavak 1. NIS2 direktive preuzima se sljedećim člankom Zakona:** **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	U potpunosti preuzeto	

provedbu ove Direktive. Sudjelovanje u istorazinskim ocjenjivanjima je dobrovoljno. Istorazinska ocjenjivanja provode stručnjaci za kibersigurnost. Stručnjake za kibersigurnost imenuju najmanje dvije države članice, koje nisu država članica koja se ocjenjuje. Istorazinska ocjenjivanja obuhvaćaju barem jedno od sljedećeg: (a) razinu provedbe mjera upravljanja kibersigurnosnim rizicima i obveza izvješćivanja iz članaka 21. i 23.; (b) razinu kapaciteta, uključujući dostupne financijske, tehničke i ljudske resurse te djelotvornost izvršavanja zadaća nadležnih tijela; (c) operativni kapacitet CSIRT-ova; (d) razinu provedbe uzajamne pomoći iz članka 37.; (e) razinu provedbe mehanizama za razmjenu informacija o kibersigurnosti iz članka 29.; (f) posebne probleme prekogranične ili međusektorske prirode. 2. Metodologija iz stavka 1. uključuje objektivne, nediskriminirajuće, pravedne i transparentne kriterije na temelju kojih države članice imenuju stručnjake za kibersigurnost koji su kvalificirani za provedbu istorazinskih	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		

ocjenjivanja. ENISA i Komisija sudjeluju u istorazinskom ocjenjivanju kao promatrači. 3. Države članice mogu identificirati posebne probleme iz stavka 1. točke (f) koje treba ocijeniti za potrebe istorazinskog ocjenjivanja. 4. Prije početka istorazinskog ocjenjivanja iz stavka 1., države članice obavješćuju države članice koje sudjeluju o opsegu takvog ocjenjivanja, među ostalim o specifičnim problemima identificiranim u skladu sa stavkom 3. 5. Prije početka istorazinskog ocjenjivanja, država članica može provesti samoocjenu aspekata koji se ocjenjuju i tu samoocjenu dostaviti imenovanim stručnjacima za kibersigurnost. Skupina za suradnju uz pomoć Komisije i ENISA-e utvrđuje metodologiju za samoocjenu koju provode države članice. 6. Istorazinska ocjenjivanja uključuju fizičke ili virtualne posjete na lokaciji i razmjene informacija izvan lokacije. U skladu s načelom dobre suradnje, država članica za koju se provodi istorazinsko ocjenjivanje dostavlja imenovanim stručnjacima za kibersigurnost informacije potrebne za ocjenu, ne	istorazinskih ocjenjivanja iz stavka 2. ovog članka, o tome obavještava državu članicu koja provodi imenovanja. Članak 19. st. 1. preuzet u potpunosti. Nije potrebno preuzimanje ostalih odredbi članka 19. NIS2 direktive. Članak 19. NIS2 direktive se odnosi na provedbu aktivnosti na EU razini odnosno od strane nadležnih EU institucija, Skupine za suradnju i Mreže CSIRT-ova. Sudjelovanje država članice u istorazinskim ocjenjivanjima je dobrovoljno. **Dopunjen članak 57. Nacrta zakona (dodani stavci 6. i 7.).**		

dovodeći u pitanje pravo Unije ili nacionalno pravo u vezi sa zaštitom povjerljivih ili klasificiranih podataka i zaštitom ključnih državnih funkcija, kao što je nacionalna sigurnost. Skupina za suradnju, u suradnji s Komisijom i ENISA-om, razvija odgovarajuće kodekse ponašanja koji podupiru metode rada imenovanih stručnjaka za kibersigurnost. Sve informacije dobivene tijekom istorazinskog ocjenjivanja smiju se upotrebljavati isključivo u tu svrhu. Stručnjaci za kibersigurnost koji sudjeluju u istorazinskom ocjenjivanju ne smiju trećim stranama otkrivati osjetljive ili povjerljive informacije dobivene tijekom tog istorazinskog ocjenjivanja. 7. Nakon provedenog istorazinskog ocjenjivanja isti aspekti ocijenjeni u određenoj državi članici ne podvrgavaju se daljnjem istorazinskom ocjenjivanju u toj državi članici tijekom dvije godine nakon završetka tog istorazinskog ocjenjivanja, osim ako država članica to ne zatraži ili na to ne pristane nakon prijedloga skupine za suradnju. 8. Države članice osiguravaju da se druge države članice, skupina za suradnju, Komisija i ENISA-a prije početka istorazinskog ocjenjivanja budu obaviještene o svakom riziku od sukoba			

interesa imenovanih stručnjaka za kibersigurnost. Država članica za koju se provodi istorazinsko ocjenjivanje može se usprotiviti imenovanju pojedinih stručnjaka za kibersigurnost iz opravdanih razloga, o kojima obavještava državu članicu koja ih imenuje. 9. Stručnjaci za kibersigurnost koji sudjeluju u istorazinskim ocjenjivanjima sastavljaju izvješća o nalazima i zaključcima ocjenjivanja. Države članice za koje se provodi istorazinsko ocjenjivanje mogu dostaviti primjedbe na nacrte izvješća koja se na njih odnose, a takve se primjedbe prilažu izvješćima. Izvješća sadržavaju preporuke kako bi se omogućilo poboljšanje aspekata obuhvaćenih istorazinskim ocjenjivanjem. Izvješća se podnose skupini za suradnju i, ako je to relevantno, mreži CSIRT-ova. Država članica za koju se provodi istorazinsko ocjenjivanje može odlučiti javno objaviti svoje izvješće ili njegovu redigiranu verziju.			

Članak 20. Upravljanje 1. Države članice osiguravaju da upravljačka tijela ključnih i važnih subjekata odobravaju mjere upravljanja kibersigurnosnim rizicima koje su ti subjekti poduzeli radi usklađivanja s člankom 21., nadgledaju njegovu provedbu i mogu se smatrati odgovornima za povrede tog članka od strane subjekata. Primjenom ovog stavka ne dovodi se u pitanje nacionalno pravo u pogledu pravila o odgovornosti koja se primjenjuju na javne institucije ni odgovornosti javnih službenika te izabranih ili imenovanih dužnosnika. 2. Države članice osiguravaju da članovi upravljačkih tijela ključnih i važnih subjekata moraju pohađati osposobljavanja te potiču ključne i važne subjekte da slično osposobljavanje redovito nude svojim zaposlenicima kako bi stekli dovoljno znanja i vještina za prepoznavanje i procjenu praksi upravljanja kibersigurnosnim rizicima i njihova učinka na usluge koje taj subjekt pruža.	**Članak 20. NIS2 direktive preuzima se sljedećim člancima 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 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 te kontrolirati njihovu provedbu. (3) U svrhu stjecanja znanja i vještina u pitanjima upravljanja kibernetičkim sigurnosnim rizicima i njihova učinka na usluge koje subjekt pruža odnosno djelatnost koju obavlja, osobe odgovorne za upravljanje mjerama dužne su: - pohađati odgovarajuća osposobljavanja - zaposlenicima subjekta omogućiti pohađanje odgovarajućih osposobljavanja. (4) Odredbe ovog članka odnose se i na pravne predstavnike koji na temelju ovlasti za zastupanje ili donošenje odluka u ime subjekta, sudjeluje u donošenju odluka o mjerama upravljanja kibernetičkim sigurnosnim rizicima i/ili njihovoj provedbi.	U potpunosti preuzeto	

	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 (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 86. 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 (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 86. ovog Zakona.		

	Predmetna odredba NIS2 direktive preuzeta člancima 29., 101. i 102. Nacrta Zakona. Članci 101. i 102. naknadno dodani u Usporedni prikaz uz njegov članak 20.		
Članak 21. Mjere upravljanja kibersigurnosnim rizicima 1. Države članice osiguravaju da ključni i važni subjekti poduzimaju odgovarajuće i razmjerne tehničke, operativne i organizacijske mjere za upravljanje rizicima kojima su izloženi mrežni i informacijski sustavi kojima se ti subjekti služe u svom poslovanju ili u pružanju svojih usluga te za sprečavanje ili smanjivanje na najmanju moguću mjeru učinka incidenata na primatelje njihovih usluga i na druge usluge. Uzimajući u obzir najnovija dostignuća i, ako je to primjenjivo, relevantne europske i međunarodne norme te trošak provedbe, mjerama iz stavka	**Članak 21. stavci 1., 2. i 3. NIS2 direktive preuzimaju se sljedećim člancima Zakona:** **Primjena mjera** **Članak 26.** (1) Ključni i važni subjekti dužni su provoditi 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	Djelomično preuzeto	Bit će preuzeto u: Uredba o kibernetičkoj sigurnosti (12.09.2024)

prvog podstavka osigurava se razina sigurnosti mrežnih i informacijskih sustava primjerena postojećem riziku. Pri procjeni proporcionalnosti tih mjera u obzir se uzima stupanj izloženosti subjekta rizicima, veličina subjekta, vjerojatnost pojave incidenata i njihova ozbiljnost, uključujući njihov društveni i gospodarski učinak. 2. Mjere iz stavka 1. temelje se 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 te uključuju najmanje sljedeće: (a) politike analize rizika i sigurnosti informacijskih sustava; (b) postupanje s incidentima; (c) kontinuitet poslovanja, kao što je upravljanje sigurnosnim kopijama i oporavak od katastrofe, te upravljanje krizama; (d) sigurnost lanca opskrbe, uključujući sigurnosne aspekte u pogledu odnosa između svakog subjekta i njegovih izravnih dobavljača ili pružatelja usluga; (e) sigurnost u nabavi, razvoju i održavanju mrežnih i informacijskih sustava, uključujući rješavanje ranjivosti i njihovo otkrivanje;	- mjere za sprečavanje ili smanjivanje na najmanju moguću mjeru utjecaja incidenata na mrežne i informacijske sustave ključnih i važnih subjekta, primatelje njihovih usluga ili na druge sektore, subjekte i usluge u kibernetičkom prostoru. (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. **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 utjecaj. **Način provedbe mjera upravljanja kibernetičkim sigurnosnim rizicima** **Članak 28.**		

(f) politike i postupke za procjenu djelotvornosti mjera upravljanja kibersigurnosnim rizicima; (g) osnovne prakse kiberhigijene i osposobljavanje o kibersigurnosti; (h) politike i postupke u pogledu kriptografije i, prema potrebi, kriptiranja; (i) sigurnost ljudskih resursa, politike kontrole pristupa i upravljanje imovinom; (j) korištenje višefaktorske provjere autentičnosti ili rješenja kontinuirane provjere autentičnosti, zaštićene glasovne, video i tekstualne komunikacije te sigurnih komunikacijskih sustava u hitnim slučajevima unutar subjekta, prema potrebi. 3. Države članice osiguravaju da subjekti, kada razmatraju koje su mjere iz stavka 2. točke (d) ovog članka primjerene, uzimaju u obzir ranjivosti specifične za svakog izravnog dobavljača i pružatelja usluge te opću kvalitetu proizvoda i kibersigurnosnu praksu svojih dobavljača i pružatelja usluga, uključujući njihove sigurne razvojne postupke. Države članice također osiguravaju da se od subjekata zahtijeva da, kada razmatraju koje su mjere iz te točke primjerene, uzmu u obzir rezultate koordiniranih procjena	(1) Mjere upravljanja kibernetičkim sigurnosnim rizicima provode se na način da se koriste najnovija tehnička dostignuća koja se koriste u okviru najbolje sigurnosne prakse u području kibernetičke sigurnosti i, kada je to primjenjivo, relevantne europske i međunarodne norme te 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. **Mjere upravljanja kibernetičkim sigurnosnim rizicima** **Članak 30.** (1) Mjere upravljanja kibernetičkim sigurnosnim rizicima uključuju najmanje sljedeće sigurnosne politike: - analize rizika i sigurnosti informacijskih sustava - postupanja s incidentima, uključujući njihovo praćenje, evidentiranje i prijavljivanje		

sigurnosnih rizika ključnih lanaca opskrbe provedenih u skladu s člankom 22. stavkom 1.	- osiguranja kontinuiteta poslovanja, kao što je upravljanje sigurnosnim kopijama i oporavak od nesreća, prekida rada i kibernetičkih napada, te upravljanje kibernetičkim krizama - sigurnosti lanca opskrbe, uključujući sigurnosne aspekte u pogledu odnosa između subjekta i njegovih izravnih dobavljača ili pružatelja usluga - sigurnosti u nabavi, razvoju i održavanju mrežnih i informacijskih sustava, uključujući otklanjanje ranjivosti i njihovo otkrivanje - provođenja procjene djelotvornosti mjera upravljanja kibernetičkim sigurnosnim rizicima - osnovne prakse kibernetičke higijene i osposobljavanja o kibernetičkoj sigurnosti - u pogledu kriptografije i, prema potrebi, kriptiranja - sigurnosti ljudskih resursa, 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. (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,		

4. Države članice osiguravaju da subjekt koji utvrdi da ne poštuje mjere iz stavka 2. bez nepotrebne odgode poduzme sve potrebne, primjerene i razmjerne korektivne mjere. 5. Komisija do 17. listopada 2024. donosi provedbene akte kojima se utvrđuju tehnički i metodološki zahtjevi za mjere iz stavka 2. u pogledu pružatelja usluga DNS-a, registara naziva vršnih domena, 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	IKT sustavima ili IKT proizvodima, koje provodi Skupina za suradnju zajedno s Europskom komisijom i ENISA-om. **Provedbeni propis o zahtjevima kibernetičke sigurnosti** **Članak 38.** Mjere upravljanja kibernetičkim sigurnosnim rizicima, način njihove provedbe, utvrđivanje značajnih incidenata, 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. **Članak 21. stavak 4. NIS2 direktive preuzima se sljedećim člancima Zakona:** **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 - izdati obvezujuće upute ili naloge kojima se zahtijeva da otklone utvrđene nedostatke ili povrede ovoga Zakona, uz navođenje mjera		

društvenih mreža i pružatelja usluga povjerenja. Komisija može donijeti provedbene akte kojima se utvrđuju tehnički i metodološki zahtjevi te, prema potrebi, sektorski zahtjevi za mjere iz stavka 2. i u pogledu ključnih i važnih subjekata koji nisu navedeni u prvom podstavku ovog stavka. U pripremi provedbenih akata iz prvog i drugog podstavka ovog stavka Komisija, u mjeri u kojoj je to moguće, prati europske i međunarodne norme te relevantne tehničke specifikacije. Komisija razmjenjuje savjete i surađuje sa skupinom za suradnju i ENISA-om na nacrtima provedbenih akata u skladu s člankom 14. stavkom 4. točkom (e). Ti se provedbeni akti donose u skladu s postupkom ispitivanja iz članka 39. stavka 2.	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 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 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 ključnim subjektima naložiti da na određeno razdoblje imenuju službenika za praćenje usklađenosti subjekta sa zahtjevima kibernetičke sigurnosti. (2) Nalog iz stavka 1. ovog članka mora sadržavati rok za imenovanje službenika za praćenje usklađenosti subjekta sa zahtjevima kibernetičke sigurnosti, razdoblje za koje trebaju imenovati takvog službenika, uputu o definiranju njegovih zadaća te rok za obavještavanje o provedbi mjere imenovanja. **Članak 21. stavci 1., 3. i 4. NIS2 direktive u potpunosti preuzeti.** **Stavak 3. djelomično preuzet.** **Stavak 5. nije preuzet.** **Stavak 3. bit će preuzet Uredbom o kibernetičkoj sigurnosti.** **Provedbeni akt iz stavka 5. bit će preuzet Uredbom o kibernetičkoj sigurnosti.**		
Članak 22. Koordinirane procjene rizika ključnih lanaca opskrbe na razini Unije 1. Skupina za suradnju, zajedno s Komisijom i ENISA-om, može provoditi koordinirane procjene sigurnosnih rizika za određene ključne lance opskrbe IKT uslugama, IKT sustavima ili IKT proizvodima, uzimajući u obzir		Nije potrebno preuzimanje	Odredba se odnosi na nadležne EU institucije i Skupinu za suradnju.

tehničke i, ako je to relevantno, netehničke čimbenike rizika. 2. Komisija, nakon savjetovanja sa skupinom za suradnju i ENISA-om i, ako je to potrebno, relevantnim dionicima, utvrđuje određene ključne IKT usluge, IKT sustave ili IKT proizvode koji mogu biti predmet koordinirane procjene sigurnosnih rizika iz stavka 1.			
Članak 23. Obveze izvješćivanja 1. Svaka država članica osigurava da ključni i važni subjekti bez nepotrebne odgode obavješćuju svoj CSIRT ili, ako je to primjenjivo, svoje nadležno tijelo u skladu sa stavkom 4. o svakom incidentu koji ima znatan učinak na pružanje njihovih usluga kako se navodi u stavku 3. (značajan incident). Prema potrebi, dotični subjekti bez nepotrebne odgode obavješćuju primatelje svojih usluga o značajnim incidentima koji bi mogli negativno utjecati na pružanje tih usluga. Svaka država članica osigurava da ti subjekti, među ostalim, izvješćuju o svim informacijama koje CSIRT-u ili, ako je to primjenjivo, nadležnom tijelu omogućuju da utvrde sve prekogranične učinke incidenta. Subjekt koji	**Članak 23. stavci 1. do 10. NIS2 direktive preuzimaju se sljedećim člancima Zakona:** **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.	Djelomično preuzeto	Bit će preuzeto u: Uredba o kibernetičkoj sigurnosti (12.09.2024)

obavješćuje ne podliježe samo zbog toga povećanoj odgovornosti. Ako dotični subjekti obavijeste nadležno tijelo o značajnom incidentu u skladu s prvim podstavkom, država članica osigurava da to nadležno tijelo obavijest po primitku proslijedi CSIRT-u. U slučaju prekograničnog ili međusektorskog značajnog incidenta, države članice osiguravaju da njihove jedinstvene kontaktne točke pravodobno dobiju relevantne informacije podnesene u skladu sa stavkom 4. 2. Države članice, ako je to primjenjivo, osiguravaju da ključni i važni subjekti primatelje svojih usluga na koje bi mogla utjecati ozbiljna kiberprijetnja bez nepotrebne odgode obavješćuju o svim mjerama ili pravnim sredstvima koje ti primatelji mogu poduzeti kao odgovor na prijetnju. Prema potrebi, subjekti te primatelje obavješćuju i o samoj ozbiljnoj kiberprijetnji. 3. Incident se smatra značajnim: (a) ako je uzrokovao ili može uzrokovati ozbiljne poremećaje u funkcioniranju usluga ili	(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. **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. **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		

financijske gubitke za predmetni subjekt; (b) ako je utjecao ili bi mogao utjecati na druge fizičke ili pravne osobe uzrokovanjem znatne materijalne ili nematerijalne štete. 4. Države članice osiguravaju da, za potrebe obavješćivanja iz stavka 1., predmetni subjekti CSIRT-u ili, ako je to primjenjivo, nadležnom tijelu podnose: (a) bez nepotrebne odgode, a u svakom slučaju u roku od 24 sata od kad su saznali za značajan incident, rano upozorenje u kojem se, ako je to primjenjivo, navodi sumnja li se da je značajan incident uzrokovan nezakonitim ili zlonamjernim djelovanjem te bi li mogao imati prekogranični učinak; (b) bez nepotrebne odgode, a u svakom slučaju u roku od 72 sata od kad su saznali za značajan incident, obavijest o incidentu kojom se, ako je to primjenjivo, ažuriraju informacije iz točke (a) i navodi početna procjena značajnog incidenta, uključujući njegovu ozbiljnosti i učinak te, ako su dostupni, pokazatelje ugroženosti; (c) na zahtjev CSIRT-a ili, ako je to primjenjivo, nadležnog tijela,	učinkom obavještava tijela državne uprave nadležna za pogođene sektore. **Obavještavanje javnosti o značajnom incident** **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.		

privremeno izvješće o relevantnim ažuriranjima statusa; (d) završno izvješće najkasnije mjesec dana nakon podnošenja obavijesti o incidentu iz točke (b), koje uključuje sljedeće: i. detaljan opis incidenta, uključujući njegovu ozbiljnost i učinak; ii. vrstu prijetnje ili temeljni uzrok koji je vjerojatno uzrokovao incident; iii. primijenjene i tekuće mjere ublažavanja; iv. ako je to primjenjivo, prekogranični učinak incidenta; (e) u slučaju incidenta koji je u tijeku u trenutku podnošenja završnog izvješća iz točke (d), države članice osiguravaju da dotični subjekti dostave izvješće o napretku u tom trenutku te završno izvješće u roku od mjesec dana od postupanja s incidentom. Odstupajući od prvog podstavka točke (b), pružatelj usluga povjerenja bez nepotrebne odgode, a u svakom slučaju u roku od 24 sata od kada je saznao za značajan incident, obavješćuje CSIRT ili, ako je to primjenjivo, nadležno tijelo o	**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, utvrđivanje značajnih incidenata, 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. **Suradnja s nadležnim tijelima za provedbu posebnih zakona** **Članak 64.**		

značajnim incidentima koji imaju učinak na pružanje njegovih usluga povjerenja. 5. CSIRT ili nadležno tijelo bez nepotrebne odgode i ako je moguće u roku od 24 sata od primitka ranog upozorenja iz stavka 4. točke (a) dostavlja odgovor subjektu koji obavješćuje, uključujući početne povratne informacije o značajnom incidentu i, na zahtjev subjekta, smjernice ili operativne savjete o provedbi mogućih mjera ublažavanja. Ako CSIRT nije prvi primatelj obavijesti iz stavka 1., smjernice pruža nadležno tijelo u suradnji s CSIRT-om. CSIRT pruža dodatnu tehničku potporu ako to zatraži predmetni subjekt. Ako se sumnja da je značajan incident kriminalne naravi, CSIRT ili nadležno tijelo pruža i smjernice o prijavi tog značajnog incidenta tijelima za izvršavanje zakonodavstva. 6. CSIRT, nadležno tijelo ili jedinstvena kontaktna točka o značajnom incidentu bez nepotrebne odgode obavješćuje ostale pogođene države članice i ENISA-u prema potrebi, a osobito ako se značajan incident odnosi na dvije države članice ili više njih. Takve informacije obuhvaćaju vrstu informacija primljenih u skladu sa stavkom 4. Pritom CSIRT, nadležno tijelo ili jedinstvena kontaktna	(1) Središnje državno tijelo za kibernetičku sigurnost i 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. **Članak 23. stavci 1. do 10. NIS2 direktive djelomično preuzeti. Stavak 11. nije preuzet.** **Članak 23. stavci 1. do 10. NIS2 direktive bit će preuzeti Uredbom o kibernetičkoj sigurnosti.** **Provedbeni akt iz stavka 11. bit će preuzet Uredbom o kibernetičkoj sigurnosti.**		

točka, u skladu s pravom Unije ili nacionalnim pravom, čuvaju sigurnost i komercijalne interese subjekta te povjerljivost dostavljenih informacija. 7. Ako je za sprečavanje značajnog incidenta ili rješavanje značajnog incidenta koji je u tijeku nužno obavijestiti javnost ili ako je otkrivanje značajnog incidenta u javnom interesu iz nekog drugog razloga, CSIRT ili, ako je to primjenjivo, njegovo nadležno tijelo te, prema potrebi, CSIRT-ovi ili nadležna tijela drugih pogođenih država članica mogu, nakon savjetovanja s predmetnim subjektom, obavijestiti javnost o značajnom incidentu ili zatražiti od subjekta da to učini. 8. Na zahtjev CSIRT-a ili nadležnog tijela jedinstvena kontaktna točka prosljeđuje obavijesti primljene na temelju stavka 1. jedinstvenim kontaktnim točkama drugih pogođenih država članica. 9. Jedinstvena kontaktna točka svaka tri mjeseca podnosi ENISA-i sažeto izvješće koje uključuje anonimizirane i agregirane podatke o značajnim incidentima, incidentima, ozbiljnim kiberprijetnjama i izbjegnutim incidentima o kojima je obaviješteno u skladu sa stavkom 1. ovog članka i			

člankom 30. Kako bi se doprinijelo dostavljanju usporedivih podataka, ENISA može donijeti tehničke smjernice o parametrima za informacije koje su uključene u sažeto izvješće. ENISA svakih šest mjeseci obavješćuje skupinu za suradnju i mrežu CSIRT-ova o svojim zaključcima o primljenim obavijestima. 10. CSIRT-ovi ili, ako je to primjenjivo, nadležna tijela dostavljaju nadležnim tijelima na temelju Direktive (EU) 2022/2557 informacije o značajnim incidentima, incidentima, kiberprijetnjama i izbjegnutim incidentima o kojima su u skladu sa stavkom 1. ovog članka i člankom 30. obavijestili subjekti koji su utvrđeni kao kritični subjekti na temelju Direktive (EU) 2022/2557 11. Komisija može donijeti provedbene akte kojima se dodatno utvrđuju vrsta informacija te oblik i postupak podnošenja obavijesti u skladu sa stavkom 1. ovog članka i člankom 30. te obavijest podnesena u skladu sa stavkom 2. ovog članka. Komisija do 17. listopada 2024. donosi provedbene akte u pogledu pružatelja usluga DNS-a, registara naziva vršnih domena, 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, kojima se dodatno utvrđuju slučajevi u kojima se incident smatra značajnim, kako je navedeno u stavku 3. Komisija takve provedbene akte može donijeti u pogledu drugih ključnih i važnih subjekata. Komisija razmjenjuje savjete i surađuje sa skupinom za suradnju na nacrtima provedbenih akata iz prvog i drugog podstavka ovog stavka u skladu s člankom 14. stavkom 4. točkom (e). Ti se provedbeni akti donose u skladu s postupkom ispitivanja iz članka 39. stavka 2.			
Članak 24. Primjena europskih programa kibersigurnosne certifikacije 1. Kako bi dokazale usklađenost s pojedinim zahtjevima iz članka 21., države članice mogu od ključnih i važnih subjekata zahtijevati korištenje određenim IKT proizvodima,	**Članak 24. stavak 1. NIS2 direktive preuzima se sljedećim člankom Zakona:** **Način provedbe mjera upravljanja kibernetičkim sigurnosnim rizicima** **Članak 28.** (1) Mjere upravljanja kibernetičkim sigurnosnim rizicima provode se na način da se koriste najnovija tehnička dostignuća koja se koriste u okviru najbolje sigurnosne prakse u području kibernetičke sigurnosti	U potpunosti preuzeto	

IKT uslugama i IKT procesima, koje je razvio ključni ili važni subjekt ili su nabavljeni od treće strane, koji su certificirani na temelju europskih programa kibersigurnosne certifikacije donesenih u skladu s člankom 49. Uredbe (EU) 2019/881. Nadalje, države članice potiču ključne i važne subjekte da se koriste kvalificiranim uslugama povjerenja. 2. Komisija je ovlaštena za donošenje delegiranih akata u skladu s člankom 38. radi dopune ove Direktive, kojima se određuje od kojih se kategorija ključnih i važnih subjekata treba zahtijevati korištenje određenim certificiranim IKT proizvodima, IKT uslugama i IKT procesima ili pribavljanje certifikata na temelju europskih programa kibersigurnosne certifikacije donesenih u skladu s člankom 49. Uredbe (EU) 2019/881. Ti delegirani akti donose se ako su utvrđene nedovoljne razine kibersigurnosti te obuhvaćaju razdoblje provedbe. Prije donošenja takvih delegiranih akata Komisija provodi procjenu učinka i organizira savjetovanja u skladu s člankom 56. Uredbe (EU) 2019/881. 3. Ako nije dostupan odgovarajući europski program kibersigurnosne	i, kada je to primjenjivo, relevantne europske i međunarodne norme te 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. **Članak 24. NIS2 direktive u cijelosti preuzet.** **Napominje se da nije potrebno preuzimanje članka 24. stavaka 2. i 3. NIS2 direktive.** **Stavkom 2. daje se ovlaštenje Europskoj komisiji za donošenje delegiranog akta, dok se odredba stavka 3. također odnosi na nadležne EU institucije.**		

certifikacije za potrebe stavka 2. ovog članka, Komisija može, nakon savjetovanja sa skupinom za suradnju i Europskom skupinom za kibersigurnosnu certifikaciju, zatražiti od ENISA-e da izradi prijedlog programa certifikacije u skladu s člankom 48. stavkom 2. Uredbe (EU) 2019/881.			
Članak 25. Normizacija 1. Države članice, u cilju promicanja konvergentne provedbe članka 21. stavaka 1. i 2., bez nametanja ili diskriminacije u korist upotrebe određene vrste tehnologije, potiču primjenu europskih i međunarodnih normi i tehničkih specifikacija relevantnih za sigurnost mrežnih i informacijskih sustava. 2. ENISA u suradnji s državama članicama i, prema potrebi, nakon savjetovanja s relevantnim dionicima, izrađuje savjete i smjernice u pogledu tehničkih područja koja treba razmotriti u odnosu na stavak 1. te u odnosu na postojeće norme, uključujući nacionalne norme, kojima bi se ta područja mogla obuhvatiti.	**Članak 25. stavak 1. NIS2 direktive preuzima se sljedećim člankom Zakona:** **Način provedbe mjera upravljanja kibernetičkim sigurnosnim rizicima** **Članak 28.** (1) Mjere upravljanja kibernetičkim sigurnosnim rizicima provode se na način da se koriste najnovija tehnička dostignuća koja se koriste u okviru najbolje sigurnosne prakse u području kibernetičke sigurnosti te, 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 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:	U potpunosti preuzeto	

	- mjerodavnim propisima Europske unije - posebnim propisima kojima se uređuje područje pružanja određenih usluga odnosno obavljanja određenih djelatnosti - uredbom iz članka 24. ovog Zakona. **Članak 25. NIS2 direktive u cijelosti preuzet.** **Napominje se da nije potrebno preuzimanje članka 25. stavka 2. NIS2 direktive.** **Odredba stavka 2. odnosi se na nadležne EU institucije.** **Sukladno danom komentaru, dopunjen članak 28. stavak 1. Nacrta zakona.**		
Članak 26. Nadležnost i teritorijalnost 1. Smatra se da su subjekti obuhvaćeni područjem primjene ove Direktive u nadležnosti države članice u kojoj imaju poslovni nastan, osim u sljedećim slučajevima: (a) pružatelji javnih elektroničkih komunikacijskih mreža ili pružatelji javno dostupnih elektroničkih komunikacijskih usluga, za koje se smatra da su u nadležnosti države članice u kojoj pružaju svoje usluge;	**Članak 26. NIS2 direktive preuzima se sljedećim člancima Zakona:** **Pojmovi** **Članak 4.** (1) U smislu ovog Zakona pojedini pojmovi imaju sljedeće značenje: 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	U potpunosti preuzeto	

(b) pružatelji usluga DNS-a, registri naziva vršnih domena, subjekti koji pružaju usluge registracije naziva domena, 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, za koje se smatra da su u nadležnosti države članice u kojoj imaju glavni poslovni nastan u Uniji u skladu sa stavkom 2.; (c) subjekti javne uprave, za koja se smatra da su u nadležnosti države članice koja ih je osnovala. 2. Za potrebe ove Direktive smatra se da subjekt iz stavka 1. točke (b) ima glavni poslovni nastan u Uniji u državi članici u kojoj se pretežno donose odluke povezane s mjerama upravljanja kibersigurnosnim rizicima. Ako se takva država članica ne može utvrditi ili ako se takve odluke ne donose u Uniji, smatra se da se glavni poslovni nastan nalazi u državi članici u kojoj se provode kibersigurnosne operacije. Ako se takva država članica ne može utvrditi, smatra se da se glavni poslovni nastan nalazi 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 **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:		

državi članici u kojoj subjekt ima poslovnu jedinicu s najvećim brojem zaposlenika u Uniji. 3. Ako subjekt iz stavka 1. točke (b) nema poslovni nastan u Uniji, ali nudi usluge unutar Unije, dužan je imenovati predstavnika u Uniji. Predstavnik mora imati poslovni nastan u jednoj od država članica u kojima se nude usluge. Smatra se da je takav subjekt u nadležnosti one države članice u kojoj njegov predstavnik ima poslovni nastan. Ako predstavnik u Uniji nije imenovan u skladu s ovim člankom, svaka država članica u kojoj subjekt pruža usluge može poduzeti pravne mjere protiv subjekta zbog povrede ove Direktive. 4. Imenovanjem predstavnika koje obavlja subjekt iz stavka 1. točke (b) ne dovode se u pitanje pravni postupci koji bi se mogli poduzeti protiv tog subjekta. 5. Države članice koje su primile zahtjev za uzajamnu pomoć u vezi sa subjektom iz stavka 1. točke (b) mogu, u okvirima zahtjeva, poduzeti odgovarajuće nadzorne mjere i mjere izvršavanja u odnosu na dotični subjekt koji pruža usluge ili koji ima mrežni i informacijski sustav na njihovu državnom području.	- 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. **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 u suradnji s nadležnim tijelima tih država članica te međusobnu uzajamnu pomoć u provedbi nadzora. **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.		
Članak 27. Registar subjekata 1. ENISA uspostavlja i vodi registar pružatelja usluga DNS-a, registra naziva vršnih domena, subjekata koji pružaju usluge registracije naziva domena, 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 ili pružatelja platformi za usluge društvenih mreža na temelju informacija dobivenih od jedinstvene kontaktne točke u skladu sa stavkom 4. ENISA na zahtjev nadležnim tijelima dopušta pristup tom registru,	**Članak 27. stavci 2. do 4. NIS2 direktive preuzimaju se sljedećim člancima Zakona:** **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	U potpunosti preuzeto	

osiguravajući pritom, ako je to primjenjivo, zaštitu povjerljivosti informacija. 2. Države članice do 17. siječnja 2025. zahtijevaju od subjekata iz stavka 1. da nadležnim tijelima dostavljaju sljedeće informacije: (a) naziv subjekta; (b) ako je to primjenjivo, relevantni sektor, podsektor i vrstu subjekta iz Priloga I. ili II.; (c) adresu glavnog poslovnog nastana subjekta i njegovih drugih zakonitih poslovnih jedinica u Uniji ili, ako nemaju poslovni nastan u Uniji, njegova predstavnika imenovanog u skladu s člankom 26. stavkom 3.; (d) ažurirane podatke za kontakt, uključujući adrese e-pošte i telefonske brojeve subjekta i, ako je to primjenjivo, njegova predstavnika imenovanog u skladu s člankom 26. stavkom 3.; (e) države članice u kojima subjekt pruža usluge; i (f) IP raspone subjekta. 3. Države članice osiguravaju da subjekti iz stavka 1. bez odgode, a u svakom slučaju u roku od tri mjeseca od datuma promjene, obavješćuju nadležno	- 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		

tijelo o svim promjenama informacija koje su dostavili na temelju stavka 2. 4. Po primitku informacija iz stavka 2. i stavka 3., osim informacija iz stavka 2. točke (f), jedinstvena kontaktna točka dotične države članice prosljeđuje ih bez nepotrebne odgode ENISA-i. 5. Informacije iz stavaka 2. i 3. ovog članka podnose se, ako je to primjenjivo, putem nacionalnog mehanizma iz članka 3. stavka 4. četvrtog podstavka.	- 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). **Članak 27. NIS2 direktive u cijelosti preuzet.** **Napominje se da nije potrebno preuzimanje članka 27. stavka 1. NIS2 direktive.** **Odredba stavka 1. odnosi se na ENISA-u.**		
Članak 28. Baza podataka o registraciji naziva domena 1. Kako bi se doprinijelo sigurnosti, stabilnosti i otpornosti DNS-a, države članice zahtijevaju od registara naziva vršnih domena i subjekata koji pružaju usluge registracije naziva domena da prikupljaju i održavaju točne i potpune podatke o registraciji naziva domena u posebnoj bazi podataka uz dužnu pažnju	**Članak 28. NIS2 direktive preuzima se sljedećim člancima Zakona:** **Pojmovi** **Članak 4.** (1) U smislu ovog Zakona pojedini pojmovi imaju sljedeće značenje: 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	U potpunosti preuzeto	

u skladu s pravom Unije o zaštiti osobnih podataka u pogledu podataka koji su osobni podaci. 2. Za potrebe stavka 1. države članice zahtijevaju da baza podataka o registraciji naziva domena sadržava informacije potrebne za identifikaciju nositelja naziva domena i kontaktnih točaka koje upravljaju nazivima domena u okviru vršnih domena te za kontakt s njima. Takve informacije uključuju: (a) naziv domene; (b) datum registracije; (c) ime korisnika domene te adresu njegove e-pošte i telefonski broj za kontakt; (d) adresu e-pošte i telefonski broj za kontakt kontaktne točke koja upravlja nazivom domene ako su različiti od podataka korisnika domene. 3. Države članice zahtijevaju da registri naziva vršnih domena i subjekti koji pružaju usluge registracije naziva domena uspostave politike i postupke, uključujući postupke provjere, kojima se osigurava da baze podataka iz stavka 1. sadržavaju točne i potpune informacije. Države članice zahtijevaju da se takve politike i postupci javno objavljuju.	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*“ je subjekt koji pruža usluge registracije naziva domena odnosno pravna ili fizička osoba koja obavlja samostalnu djelatnost ovlaštena za registraciju i administraciju .hr domena u ime registra naziva vršne nacionalne internetske domene **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.** **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		

4. Države članice zahtijevaju da registri naziva vršnih domena i subjekti koji pružaju usluge registracije naziva domena bez nepotrebne odgode nakon registracije naziva domene javno objavljuju podatke o registraciji naziva domena koji nisu osobni podaci. 5. Države članice zahtijevaju da registri naziva vršnih domena i subjekti koji pružaju usluge registracije naziva domena omoguće pristup određenim podacima o registraciji naziva domena na temelju zakonitih i opravdanih zahtjeva legitimnih tražitelja pristupa, u skladu s pravom Unije o zaštiti podataka. Države članice zahtijevaju da registri naziva vršnih domena i subjekti koji pružaju usluge registracije naziva domena odgovore bez nepotrebne odgode, a u svakom slučaju u roku od 72 sata nakon primitka svakog zahtjeva za pristup. Države članice zahtijevaju da se politike i postupci za otkrivanje takvih podataka javno objavljuju. 6. Usklađenost s obvezama utvrđenim u stavcima od 1. do 5. ne smije dovesti do dvostrukog prikupljanja podataka o registraciji naziva domena. U tu svrhu države članice zahtijevaju da registri naziva vršnih domena i subjekti koji	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 nositelja naziva domena 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 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		

pružaju usluge registracije naziva domena međusobno surađuju.	predstavlja temelj za uskratu registracije domene odnosno deaktivaciju domene. **Obveze registra naziva vršne nacionalne internetske domene i registrar** **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 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 deaktivirati. (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. **Obveza omogućavanja pristupa podacima o korisniku domene** **Članak 48.** (1) 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, u roku od 72 sata od primitka zahtjeva, dostaviti ili na drugi odgovarajući način omogućiti pristup podacima o korisniku domene. (2) 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 stavkom 1. ovog članka. **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.		

Članak 29. Mehanizmi za razmjenu informacija o kibersigurnosti 1. Države članice osiguravaju da subjekti obuhvaćeni područjem primjene ove Direktive i, prema potrebi, drugi subjekti koji nisu obuhvaćeni područjem primjene ove Direktive mogu međusobno dobrovoljno razmjenjivati relevantne informacije o kibersigurnosti, uključujući informacije koje se odnose na kiberprijetnje, izbjegnute incidente, ranjivosti, tehnike i postupke, pokazatelje ugroženosti, neprijateljske taktike, informacije o počinitelju prijetnje, kibersigurnosna upozorenja i preporuke o konfiguraciji kibersigurnosnih alata za otkrivanje kibernapada, ako takva razmjena informacija: (a) ima za cilj sprečavanje ili otkrivanje incidenata, odgovaranje na njih, oporavljanje od incidenata ili ublažavanje njihova učinka; (b) povećava razinu kibersigurnosti, posebno povećanjem informiranosti o kiberprijetnjama, ograničavanjem ili ometanjem mogućnosti širenja takvih prijetnji, podupiranjem niza obrambenih sposobnosti, otklanjanjem i	**Članak 29. stavci 1. do 4. NIS2 direktive preuzima se sljedećim člancima Zakona:** **Dobrovoljna razmjena informacija o kibernetičkoj sigurnosti** **Članak 53.** (1) Ključni i važni subjekti, kao i privatni i javni subjekti koji nisu kategorizirani kao ključni i 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	U potpunosti preuzeto	

otkrivanjem ranjivosti, tehnikama otkrivanja, zaustavljanja i sprečavanja prijetnji, strategijama ublažavanja ili fazama odgovora i oporavka ili promicanjem suradničkog istraživanja kiberprijetnji između javnih i privatnih subjekata. 2. Države članice osiguravaju da se razmjena informacija odvija unutar zajednica ključnih i važnih subjekata te, prema potrebi, njihovih dobavljača ili pružatelja usluga. S obzirom na potencijalno osjetljivu prirodu informacija koje se razmjenjuju, takva se razmjena provodi putem mehanizama za razmjenu informacija o kibersigurnosti. 3. Države članice olakšavaju uspostavu mehanizama za dijeljenje informacija o kibersigurnosti iz stavka 2. ovog članka. Takvim mehanizmima mogu se utvrditi operativni elementi, među ostalim upotreba namjenskih IKT platformi i alata za automatizaciju, sadržaj i uvjeti mehanizama za razmjenu informacija. Utvrđivanjem pojedinosti o sudjelovanju tijela javne vlasti u takvim mehanizmima države članice mogu odrediti uvjete za informacije koje nadležna tijela ili CSIRT-ovi stavljaju na raspolaganje. Države članice nude	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. **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		

potporu primjeni takvih mehanizama u skladu sa svojim politikama iz članka 7. stavka 2. točke (h). 4. Države članice osiguravaju da ključni i važni subjekti obavješćuju nadležna tijela o svojem sudjelovanju u mehanizmima za razmjenu informacija o kibersigurnosti iz stavka 2. nakon početka sudjelovanja u takvim mehanizmima ili, ako je primjenjivo, o svojem povlačenju iz takvih mehanizama nakon što povlačenje stupi na snagu. 5. ENISA pruža potporu uspostavi mehanizama za razmjenu informacija o kibersigurnosti iz stavka 2. razmjenom najboljih praksi i pružanjem smjernica.	- 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. **Članak 29. NIS2 direktive u cijelosti preuzet.** **Napominje se da nije potrebno preuzimanje članka 29. stavka 5. NIS2 direktive.**		

	Odredba stavka 5. odnosi se na ENISA-u. **Stavak 3. preuzet člankom 53. stavcima 3. do 6. Nacrta zakona. Radi potpunijeg preuzimanja stavka 3. članka 29. NIS2 direktive u dijelu koji glasi: „Države članice olakšavaju uspostavu mehanizama za dijeljenje informacija o kibersigurnosti iz stavka 2. ovog članka.“ dopunjen članak 61. Nacrta zakona.** **18.8.2023.:** **Članak 61. stavak 1. podstavak 5. Nacrta zakona dopunjen prema prijedlogu odnosno izmijenjen na način da isti glasi:** „- 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“		
Članak 30. Dobrovoljno obavješćivanje o relevantnim informacijama 1. Države članice osiguravaju da, uz obvezu obavješćivanja iz članka 23., CSIRT-ovima ili, ako je to primjenjivo, nadležnim tijelima obavijesti mogu dobrovoljno podnositi: (a) ključni i važni subjekti u pogledu incidenata, kiberprijetnji i izbjegnutih incidenata; (b) subjekti koji nisu subjekti iz točke (a), neovisno o tome jesu li obuhvaćeni područjem primjene ove Direktive, u pogledu značajnih	**Članak 30. NIS2 direktive preuzima se sljedećim člancima Zakona:** **Obavještavanje na dobrovoljnoj osnovi** **Članak 33.** Ključni i važni subjekti mogu nadležni CSIRT dobrovoljno obavijestiti o svakom incidentu, kibernetičkoj prijetnji i izbjegnutom incidentu. **Provedbeni propis o zahtjevima kibernetičke sigurnosti** **Članak 38.** Mjere upravljanja kibernetičkim sigurnosnim rizicima, način njihove provedbe, utvrđivanje značajnih incidenata, **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**	Djelomično preuzeto	Bit će preuzeto u: Uredba o kibernetičkoj sigurnosti (12.09.2024)

incidenata, kiberprijetnji ili izbjegnutih incidenata. 2. Države članice obrađuju obavijesti iz stavka 1. ovog članka u skladu s postupkom utvrđenim u članku 23. Države članice obradi obveznih obavijesti mogu dati prednost pred obradom obavijesti na dobrovoljnoj osnovi. Prema potrebi, CSIRT-ovi i, ako je primjenjivo, nadležna tijela, pružaju jedinstvenim kontaktnim točkama, informacije o obavijestima primljenim na temelju ovog članka, uz istovremeno osiguravanje povjerljivosti i odgovarajuće zaštite informacija koje je dostavio subjekt koji obavješćuje. Ne dovodeći u pitanje sprečavanje, istragu, otkrivanje i progon kaznenih djela, dobrovoljno izvješćivanje ne smije dovesti do nametanja dodanih obveza subjektu koji obavješćuje kojima ne bi podlijegao da nije podnio obavijest.	**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. **Članak 50.** (1) Svaki privatni ili javni 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 članka.** (2) Mogućnost provedbe samoocjena sukladnosti i dobrovoljnog obavještavanja iz stavka 1. ovog članka uredit će se uredbom iz članka 24. ovog Zakona. **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 utjecaje 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 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.		

Članak 31. Opći aspekti nadzora i izvršavanje 1. Države članice osiguravaju da njihova nadležna tijela djelotvorno nadziru i poduzimaju mjere potrebne za osiguravanje usklađenosti s ovom Direktivom. 2. Države članice mogu dopustiti svojim nadležnim tijelima da daju prednost nadzornim zadaćama. Takvo davanje prednosti utemeljeno je na pristupu koji se temelji na riziku. U tu svrhu, pri izvršavanju svojih nadzornih zadaća iz stavaka 32. i 33. nadležna tijela mogu uspostaviti nadzorne metodologije kojima se omogućuje određivanje tih zadaća kao prioriteta primjenom pristupa utemeljenog na procjeni rizika. 3. Nadležna tijela blisko surađuju s nadzornim tijelima na temelju Uredbe (EU) 2016/679 u rješavanju incidenata	**Članak 31. NIS2 direktive preuzima se slijedećim člancima Zakona:** **Pojmovi** **Članak 4.** (1) U smislu ovog Zakona pojedini pojmovi imaju sljedeće značenje: 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 49. „središnje državno tijelo za informacijsku sigurnost“ je Ured Vijeća za nacionalnu sigurnost 50. „središnje državno tijelo za kibernetičku sigurnost“ je Sigurnosno-obavještajna agencija	U potpunosti preuzeto	

koji za posljedicu imaju povrede osobnih podataka ne dovodeći u pitanje nadležnosti i zadaće nadzornih tijela na temelju te uredbe. 4. Ne dovodeći u pitanje nacionalne zakonodavne i institucionalne okvire, države članice osiguravaju da, pri nadzoru usklađenosti subjekata javne uprave s ovom Direktivom i određivanju mjera izvršavanja u odnosu na povrede ove Direktive, nadležna tijela imaju odgovarajuće ovlasti za izvršavanje takvih zadaća uz operativnu neovisnost u odnosu na subjekte javne uprave koji se nadziru. Države članice mogu odlučiti o određivanju odgovarajućih, proporcionalnih i djelotvornih nadzornih mjera i mjera izvršavanja u odnosu na te subjekte u skladu s nacionalnim zakonodavnim i institucionalnim okvirima.	58. „tijelo državne uprave nadležno za razvoj digitalnog društva“ je Središnji državni ured za razvoj digitalnog društva 59. „tijelo državne uprave nadležno za znanost i obrazovanje“ je Ministarstvo znanosti i obrazovanja 60. „tijelo nadležno za zaštitu osobnih podataka“ je Agencija za zaštitu osobnih podataka ili drugo nadzorno tijelo iz članaka 55. i 56. Uredbe (EU) 2016/679 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 provedbe zahtjeva kibernetičke sigurnosti sukladno ovom Zakonu i propisu donesenom na temelju 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 privatni ili javni 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. 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 zaprimi informacije 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 zaprimi informacije 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. **Izmijenjen članak 59. stavak 1. podstavak 4. Nacrta zakona.**		
Članak 32. Nadzorne mjere i mjere izvršavanja u odnosu na ključne subjekte 1. Države članice osiguravaju da su nadzorne mjere ili mjere izvršavanja određene ključnim subjektima u pogledu obveza utvrđenih u ovoj Direktivi učinkovite, proporcionalne i odvraćajuće, uzimajući u obzir okolnosti svakog pojedinog slučaja. 2. Države članice osiguravaju da nadležna tijela pri izvršavanju svojih nadzornih zadaća u odnosu na ključne subjekte imaju ovlasti da te subjekte obvežu barem na sljedeće: (a) inspekcije na lokaciji i neizravni nadzor, uključujući nasumične provjere, koji provode osposobljeni stručnjaci;	**Članak 32. stavci 1. do 8. NIS2 direktive preuzimaju se slijedećim člancima Zakona:** **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.	U potpunosti preuzeto	

(b) redovite i ciljane revizije sigurnosti koje provodi neovisno tijelo ili nadležno tijelo; (c) ad hoc revizije, među ostalim i u slučajevima kad je to opravdano na temelju značajnog incidenta ili povrede ove Direktive od strane ključnog subjekta; (d) analize sigurnosti na temelju objektivnih, nediskriminirajućih, pravednih i transparentnih kriterija za procjenu rizika, ako je to potrebno, u suradnji s dotičnim subjektom; (e) zahtjeve za informacije potrebne za ocjenjivanje mjera upravljanja kibersigurnosnim rizicima koje je donio dotični subjekt, uključujući dokumentirane kibersigurnosne politike, te usklađenosti s obvezom podnošenja informacija nadležnim tijelima u skladu s člankom 27. ; (f) zahtjeve za pristup podacima, dokumentima i informacijama potrebnima za izvršavanje njihovih nadzornih zadaća; (g) zahtjeve za dokaze o provedbi kibersigurnosnih politika, kao što su rezultati revizija sigurnosti koje je proveo kvalificirani revizor i odgovarajući temeljni dokazi. Ciljane revizije sigurnosti iz prvog podstavka točke (b) temelje se na	(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 samostalno ili u okviru revizije poslovanja, odnosno druge provjere sukladnosti subjekata koja se provodi temeljem posebnih propisa		

procjenama rizika koje provodi nadležno tijelo ili subjekt revizije, ili na drugim dostupnim informacijama u vezi s rizikom. Rezultati svake ciljane revizije sigurnosti stavljaju se na raspolaganje nadležnom tijelu. Troškove takve ciljane revizije sigurnosti koju provodi neovisno tijelo plaća subjekt nad kojim se provodi revizija, osim u propisno opravdanim slučajevima u kojima nadležno tijelo odluči drugačije. 3. Pri izvršavanju svojih ovlasti iz stavka 2. točaka od (e), (f) ili (g), nadležna tijela navode svrhu zahtjeva i pobliže određuju tražene informacije. 4. Države članice osiguravaju da njihova nadležna tijela pri izvršavanju svojih ovlasti izvršavanja u odnosu na ključne subjekte imaju barem sljedeće ovlasti: (a) izdavati upozorenja o povredama ove Direktive od strane dotičnih subjekata; (b) donositi obvezujuće upute, među ostalim u vezi s mjerama potrebnim za sprečavanje ili otklanjanje incidenta, kao i rokove za provedbu takvih mjera i za izvješćivanje o njihovoj provedbi,	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. **Suradnja s nadležnim tijelima za provedbu posebnih zakona** **Članak 64.** (1) Središnje državno tijelo za kibernetičku sigurnost i nadležna tijela za provedbu zahtjeva kibernetičke sigurnosti te nadležna tijela za provedbu posebnih zakona, međusobno surađuju i razmjenjuju relevantne informacije i iskustva.		

ili nalog kojim se od dotičnih subjekata zahtijeva da uklone utvrđene nedostatke ili povrede ove Direktive; (c) naložiti dotičnim subjektima da prestanu s postupanjem kojim se povređuje ova Direktiva i da ne ponavljaju takvo postupanje; (d) naložiti dotičnim subjektima da osiguraju da su njihove mjere upravljanja kibersigurnosnim rizicima u skladu s obvezama iz članka 21. ili da ispune obveze izvješćivanja iz članka 23. na utvrđeni način i u utvrđenom roku; (e) naložiti dotičnim subjektima da obavijeste fizičke ili pravne osobe u odnosu na koje pružaju usluge ili obavljaju djelatnosti na koje bi mogla utjecati ozbiljna kiberprijetnja o prirodi te prijetnje te o svim mogućim zaštitnim ili korektivnim mjerama koje te fizičke ili pravne osobe mogu poduzeti kao odgovor na tu prijetnju; (f) naložiti dotičnim subjektima da u razumnom roku provedu preporuke dane na temelju revizije sigurnosti; (g) imenovati službenika za praćenje s precizno definiranim zadaćama na određeno razdoblje kako bi	(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. (EU) 2022/2554 određeni kao ključna treća strana pružatelj IKT usluga. **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 zaprimi informacije 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		

nadgledao usklađenost dotičnih subjekata s člancima 21. i 23.; (h) naložiti dotičnim subjektima da objave aspekte povreda ove Direktive na određeni način; (i) izreći ili zahtijevati da relevantna tijela ili sudovi u skladu s nacionalnim pravom izreknu upravnu novčanu kaznu u skladu s člankom 34. uz sve mjere iz točaka od (a) do (h) ovog stavka. 5. Ako su mjere izvršavanja donesene u skladu sa stavkom 4. točkama od (a) do (d) i točkom (f) neučinkovite, države članice osiguravaju da njihova nadležna tijela imaju ovlast utvrditi rok u kojem se od ključnog subjekta zahtijeva da poduzme mjere potrebne za ispravljanje nedostataka ili da ispuni zahtjeve tih tijela. Ako zatražena mjera nije poduzeta u zadanom roku, države članice osiguravaju da nadležna tijela imaju ovlasti: (a) privremeno suspendirati ili zahtijevati od certifikacijskog tijela ili tijela koje izdaje ovlaštenja ili od suda, u skladu s nacionalnim pravom, da privremeno suspendira certifikat ili ovlaštenje za dio relevantnih usluga ili sve relevantne usluge koje ključni	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. **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		

subjekt pruža ili djelatnosti koje obavlja; (b) zahtijevati da relevantna tijela ili sudovi u skladu s nacionalnim pravom privremeno zabrane obavljanje upravljačkih dužnosti u ključnom subjektu svakoj fizičkoj osobi koja upravljačke dužnosti obavlja na razini glavnog izvršnog direktora ili pravnog zastupnika u tom ključnom subjektu. Privremene suspenzije ili zabrane izrečene u skladu s ovim stavkom primjenjuju se samo dok dotični subjekt ne poduzme potrebne mjere za otklanjanje nedostataka ili dok ne ispuni zahtjeve nadležnog tijela za koje su takve mjere izvršavanja primijenjene. Izricanje takvih privremenih suspenzija ili zabrana podliježe odgovarajućim postupovnim zaštitnim mjerama u skladu s općim načelima prava Unije i Poveljom, uključujući pravo na djelotvoran pravni lijek i pošteno suđenje, pretpostavku nedužnosti i prava na obranu. Mjere izvršavanja predviđene u ovom stavku ne primjenjuju se na subjekte javne uprave koji podliježu ovoj Direktivi.	članka obavijestiti nadzirani subjekt u roku od tri dana prije početka nadzora. (3) Iznimno od stavka 2. ovog članka, stručni nadzor može biti proveden bez prethodne obavijesti u slučaju postojanja opravdanih razloga za hitno postupanje. **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. **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		

6. Države članice osiguravaju da svaka fizička osoba koja je odgovorna za ključni subjekt ili djeluje kao njegov pravni predstavnik na temelju ovlasti za zastupanje, ovlasti za donošenje odluka u njegovo ime ili ovlasti za izvršavanje kontrole nad tim subjektom ima ovlast osigurati njegovu usklađenost s ovom Direktivom. Države članice osiguravaju da se takve fizičke osobe mogu smatrati odgovornima za kršenje svojih dužnosti da osiguraju usklađenost s ovom Direktivom. U pogledu subjekata javne uprave, ovim stavkom ne dovodi se u pitanje nacionalno pravo država članica u pogledu odgovornosti javnih službenika te izabranih ili imenovanih dužnosnika. 7. Kada poduzimaju bilo koju mjeru izvršavanja iz stavka 4. ili 5., nadležna tijela poštuju prava na obranu i uzimaju u obzir okolnosti svakog pojedinačnog slučaja te propisno uzimaju u obzir barem: (a) ozbiljnost povrede i važnost prekršenih odredaba, pri čemu se ozbiljnim povredama, među ostalim, smatra sljedeće: i. opetovane povrede;	- 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.		

ii. neprijavljivanje ili neispravljanje značajnih incidenata; iii. neuklanjanje nedostataka u skladu s obvezujućim uputama nadležnih tijela; iv. ometanje revizija ili aktivnosti praćenja koje je naložilo nadležno tijelo nakon utvrđivanja povrede; v. pružanje lažnih ili izrazito netočnih informacija povezanih s mjerama upravljanja kibersigurnosnim rizicima ili obvezama izvješćivanja utvrđenim u člancima 21. i 23.; (b) trajanje povrede; (c) sve relevantne prethodne povrede koje je počinio dotični subjekt; (d) svaku materijalnu ili nematerijalnu štetu koja je uzrokovana, uključujući sve financijske ili gospodarske gubitke, učinke na druge usluge i broj pogođenih korisnika; (e) je li počinitelj povrede djelovao s namjerom ili nepažnjom; (f) sve mjere koje je subjekt poduzeo radi sprečavanja ili ublažavanja materijalne ili nematerijalne štete; (g) svako poštovanje odobrenih kodeksa ponašanja ili odobrenih mehanizama certificiranja;	**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		

(h) razinu suradnje fizičkih ili pravnih osoba koje se smatraju odgovornima s nadležnim tijelima. 8. Nadležna tijela detaljno obrazlažu svoje mjere izvršavanja. Prije donošenja takvih mjera nadležna tijela obavješćuju predmetne subjekte o svojim preliminarnim nalazima. Ona tim subjektima također daju razuman rok za podnošenje primjedaba, osim u valjano obrazloženim slučajevima u kojima bi inače bile spriječene hitne mjere za sprečavanje incidenata ili odgovor na njih. 9. Države članice osiguravaju da njihova nadležna tijela na temelju ove Direktive obavješćuju relevantna nadležna tijela unutar iste države članice na temelju Direktive 2022/2557 pri izvršavanju svojih nadzornih ovlasti i ovlasti izvršavanja kojima je cilj osigurati usklađenost subjekta koji je utvrđen kao kritični subjekt na temelju Direktive (EU) 2022/2557 s ovom Direktivom. Prema potrebi, nadležna tijela na temelju Direktive (EU) 2022/2557 mogu zatražiti od nadležnih tijela na temelju ove Direktive da izvršavaju svoje nadzorne ovlasti i ovlasti izvršavanja u vezi s subjektom	raspolaže informacijama da subjekt ne provodi zahtjeve kibernetičke sigurnosti sukladno ovom Zakonu. (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. točke 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. **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 - izdati obvezujuće upute ili naloge kojima se zahtijeva da otklone utvrđene nedostatke ili povrede ovoga Zakona, uz navođenje mjera koje subjekt treba provesti radi sprečavanja značajnih incidenata ili otklanjanja njihovih posljedica - naložiti da prestanu s postupanjem koje je u suprotnosti s ovim Zakonom i 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		

koji je utvrđen kao kritičan subjekt na temelju Direktive (EU) 2022/2557. 10. Države članice osiguravaju da njihova nadležna tijela na temelju ove Direktive surađuju s relevantnim nadležnim tijelima dotične države članice na temelju Uredbe (EU) 2022/2554. Posebno, države članice osiguravaju da njihova nadležna tijela na temelju ove Direktive obavješćuju Nadzorni forum osnovan na temelju članka 32. stavka 1. Uredbe (EU) 2022/2554 pri izvršavanju svojih nadzornih ovlasti i ovlasti izvršavanja usmjerenih na osiguravanje usklađenosti ključnog subjekta koji je određen kao kritična treća strana pružatelj IKT usluga na temelju članka 31. (EU) 2022/2554 s ovom Direktivom.	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 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 ključnim subjektima naložiti da na određeno razdoblje imenuju službenika za praćenje usklađenosti subjekta sa zahtjevima kibernetičke sigurnosti.		

	(2) Nalog iz stavka 1. ovog članka mora sadržavati rok za imenovanje službenika za praćenje usklađenosti subjekta sa zahtjevima kibernetičke sigurnosti, razdoblje za koje trebaju imenovati takvog službenika, uputu o definiranju njegovih zadaća te rok za obavještavanje o provedbi mjere imenovanja. **Izricanje novčanih kazni** **Članak 84.** (1) Uz korektivne mjere propisane ovim Zakonom, 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. **Privremene suspenzije i zabrane obavljanja djelatnosti** **Članak 85.** (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 i jedinice lokalne i područne (regionalne) samouprave. Okolnosti koje se uzimaju u obzir prilikom donošenja odluka o izricanju korektivnih mjera, predlaganju privremenih suspenzija i zabrane obavljanja djelatnosti **Članak 86.** (1) Prilikom donošenja odluka o izricanju korektivnih mjera iz članaka 82. i 83. ovog Zakona odnosno podnošenju zahtjeva sukladno članku 85. 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 propisa donesenih na temelju ovog Zakona. **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, 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, 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. **Članak 32. stavak 9. NIS2 direktive preuzima se slijedećim člankom Zakona:** **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. **Članak 32. stavak 10. NIS2 direktive preuzima se slijedećim člankom Zakona:** **Suradnja s nadležnim tijelima za provedbu posebnih zakona** **Članak 64.**		

	(1) Središnje državno tijelo za kibernetičku sigurnost i 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. **Kako bi se potpunije preuzeo članak 32., konkretno stavak 10. NIS2 direktive u dijelu koji se referira na Nadzorni forum, dopunjen članak 64. (dodan stavak 4.).**		

Članak 33. Nadzorne mjere i mjere izvršavanja u odnosu na važne subjekte 1. Kada dobiju dokaz, naznaku ili informaciju da važan subjekt navodno ne poštuje ovu Direktivu, a posebno njezine članke 21. i 23., države članice osiguravaju da nadležna tijela, ako je potrebno, poduzmu ex post nadzorne mjere. Države članice osiguravaju da su te mjere učinkovite, proporcionalne i odvraćajuće, uzimajući u obzir okolnosti svakog pojedinačnog slučaja. 2. Države članice osiguravaju da nadležna tijela pri izvršavanju svojih nadzornih zadaća u odnosu na važne subjekte imaju ovlasti da te subjekte obvežu barem na sljedeće: (a) inspekcije na lokaciji i neizravni ex post nadzor, koji provode osposobljeni stručnjaci; (b) ciljane revizije sigurnosti koje provodi neovisno tijelo ili nadležno tijelo; (c) analize sigurnosti na temelju objektivnih, nediskriminirajućih, pravednih i transparentnih kriterija za procjenu rizika, ako je to potrebno, u suradnji s dotičnim subjektom;	**Članak 33. stavci 1. do 5. NIS2 direktive preuzimaju se slijedećim člancima Zakona:** **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.	U potpunosti preuzeto	

(d) zahtjeve za informacije potrebne za ex post ocjenjivanje mjera upravljanja kibersigurnosnim rizicima koje je donio dotični subjekt, uključujući dokumentirane kibersigurnosne politike, te usklađenosti s obvezom dostavljanja informacija nadležnim tijelima u skladu s člankom 27.; (e) zahtjeve za pristup podacima, dokumentima i informacijama potrebnima za izvršavanje njihovih nadzornih zadaća; (f) zahtjeve za dokaze o provedbi kibersigurnosnih politika, kao što su rezultati revizija sigurnosti koje je proveo kvalificirani revizor i odgovarajući temeljni dokazi. Ciljane revizije sigurnosti iz prvog podstavka točke (b) temelje se na procjenama rizika koje provodi nadležno tijelo ili subjekt revizije, ili na drugim dostupnim informacijama u vezi s rizikom. Rezultati svake ciljane revizije sigurnosti stavljaju se na raspolaganje nadležnom tijelu. Troškove takve ciljane revizije sigurnosti koju provodi neovisno tijelo plaća subjekt nad kojim se provodi revizija, osim u propisno	(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 samostalno 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.		

opravdanim slučajevima u kojima nadležno tijelo odluči drugačije. 3. Pri izvršavanju svojih ovlasti iz stavka 2. točkama (d), (e) ili (f), nadležna tijela navode svrhu zahtjeva i pobliže određuju tražene informacije. 4. Države članice osiguravaju da nadležna tijela pri izvršavanju svojih ovlasti izvršavanja u odnosu na važne subjekte imaju barem sljedeće ovlasti: (a) izdavati upozorenja o povredama ove Direktive od strane dotičnih subjekata; (b) donositi obvezujuće upute ili nalog kojim se od dotičnih subjekata zahtijeva da uklone utvrđene nedostatke ili povredu ove Direktive; (c) naložiti dotičnim subjektima da prestanu s postupanjem kojim se povređuje ova Direktiva i da ne ponavljaju takvo postupanje; (d) naložiti dotičnim subjektima da osiguraju da su njihove mjere upravljanja kibersigurnosnim rizicima u skladu s obvezama iz članka 21. ili da ispune obveze izvješćivanja iz članka 23. na utvrđeni način i u utvrđenom roku; (e) naložiti dotičnim subjektima da obavijeste fizičke ili pravne osobe	(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. **Suradnja s nadležnim tijelima za provedbu posebnih zakona** **Članak 64.** (1) Središnje državno tijelo za kibernetičku sigurnost i nadležna tijela za provedbu zahtjeva kibernetičke sigurnosti te nadležna tijela za		

u odnosu na koje pružaju usluge ili obavljaju djelatnosti na koje bi mogla utjecati ozbiljna kiberprijetnja o prirodi te prijetnje te o svim mogućim zaštitnim ili korektivnim mjerama koje te fizičke ili pravne osobe mogu poduzeti kao odgovor na tu prijetnju; (f) naložiti dotičnim subjektima da u razumnom roku provedu preporuke dane na temelju revizije sigurnosti; (g) naložiti dotičnim subjektima da objave aspekte povrede ove Direktive na određeni način; (h) izreći ili zahtijevati da relevantna tijela ili sudovi u skladu s nacionalnim pravom izreknu upravnu novčanu kaznu u skladu s člankom 34. uz sve mjere iz točaka od (a) do (g) ovog stavka. 5. Članak 32. stavci 6., 7. i 8. primjenjuju se mutatis mutandis na nadzorne mjere i mjere izvršavanja predviđene ovim člankom za važne subjekte. 6. Države članice osiguravaju da njihova nadležna tijela na temelju ove Direktive surađuju s relevantnim nadležnim tijelima dotične države članice na temelju Uredbe (EU)	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. (EU) 2022/2554 određeni kao ključna treća strana pružatelj IKT usluga. **Provedba stručnog nadzora važnog subjekta** **Članak 76.** (1) Stručni nadzor važnog subjekta provodi se kada nadležno tijelo za provedbu zahtjeva kibernetičke sigurnosti zaprimi informacije 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		

2022/2554. Posebno, države članice osiguravaju da njihova nadležna tijela na temelju ove Direktive obavješćuju Nadzorni forum osnovan na temelju članka 32. stavka 1. Uredbe (EU) 2022/2554 pri izvršavanju svojih nadzornih ovlasti i ovlasti izvršavanja usmjerenih na osiguravanje usklađenosti važnog subjekta koji je određen kao kritična treća strana pružatelj IKT usluga na temelju članka 31. (EU) 2022/2554 s ovom Direktivom.	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 u roku od tri dana prije početka nadzora.		

	(3) Iznimno od stavka 2. ovog članka, stručni nadzor može biti proveden bez prethodne obavijesti u slučaju postojanja opravdanih razloga za hitno postupanje. **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. **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. **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 - izdati obvezujuće upute ili naloge kojima se zahtijeva da otklone utvrđene nedostatke ili povrede ovoga Zakona, uz navođenje mjera koje subjekt treba provesti radi sprečavanja značajnih incidenata ili otklanjanja njihovih posljedica - naložiti da prestanu s postupanjem koje je u suprotnosti s ovim Zakonom i 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 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. **Izricanje novčanih kazni** **Članak 84.** (1) Uz korektivne mjere propisane ovim Zakonom, 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. **Okolnosti koje se uzimaju u obzir prilikom donošenja odluka o izricanju korektivnih mjera, predlaganju privremenih suspenzija i zabrane obavljanja djelatnosti** **Članak 86.** (1) Prilikom donošenja odluka o izricanju korektivnih mjera iz članaka 82. i 83. ovog Zakona odnosno podnošenju zahtjeva sukladno članku 85. 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 propisa donesenih na temelju ovog Zakona. **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, 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, 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. **Članak 32. stavak 6. NIS2 direktive preuzima se slijedećim člankom Zakona:** **Suradnja s nadležnim tijelima za provedbu posebnih zakona** **Članak 64.** (1) Središnje državno tijelo za kibernetičku sigurnost i 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. **Kako bi se potpunije preuzeo članak 33., konkretno stavak 10. NIS2 direktive u dijelu koji se referira na Nadzorni forum, dopunjen članak 64. (dodan stavak 4.).**		
Članak 34. Opći uvjeti za izricanje upravnih novčanih kazni ključnim i važnim subjektima 1. Države članice osiguravaju da su upravne novčane kazne izrečene ključnim i važnim subjektima u skladu s ovim člankom u pogledu povreda ove Direktive učinkovite, proporcionalne i odvraćajuće, uzimajući u obzir okolnosti svakog pojedinog slučaja. 2. Upravne novčane kazne izriču se dodatno uz sve mjere iz članka 32. stavka 4. točaka od (a) do (h), članka 32. stavka 5. i članka 33. stavka 4. točaka od (a) do (g). 3. Pri odlučivanju o izricanju upravne novčane kazne i o njezinu iznosu dužna se pažnja u svakom pojedinom slučaju posvećuje barem elementima predviđenima u članku 32. stavku 7.	**Članak 34. NIS2 direktive preuzima se slijedećim člancima Zakona:** **Izricanje novčanih kazni** **Članak 84.** (1) Uz korektivne mjere propisane ovim Zakonom, 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. **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	U potpunosti preuzeto	

4. Države članice osiguravaju da u slučaju da povrijede članak 21. ili članak 23. ključni subjekti podliježu, u skladu sa stavcima 2. i 3. ovog članka, upravnim novčanim kaznama u najvećem iznosu od najmanje 10 000 000 EUR ili u najvećem iznosu od najmanje 2 % ukupnog godišnjeg prometa na svjetskoj razini u prethodnoj financijskoj godini poduzeća kojem pripada ključni subjekt, ovisno o tome koji je iznos veći. 5. Države članice osiguravaju da u slučaju da povrijede članak 21. ili članak 23. važni subjekti podliježu, u skladu sa stavcima 2. i 3. ovog članka, upravnim novčanim kaznama u najvećem iznosu od najmanje 7 000 000 EUR ili u najvećem iznosu od najmanje 1,4 % ukupnog godišnjeg prometa na svjetskoj razini u prethodnoj financijskoj godini poduzeća kojem pripada važni subjekt, ovisno o tome koji je iznos veći. 6. Države članice mogu predvidjeti ovlast izricanja periodičnih penala kako bi se ključni ili važni subjekt prisililo da prestane s povredom ove Direktive u skladu s prethodnom odlukom nadležnog tijela.	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 (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)		

7. Ne dovodeći u pitanje ovlasti nadležnih tijela u skladu s člancima 32. i 33., svaka država članica može utvrditi pravila o tome mogu li se i u kojoj mjeri subjektima javne uprave izreći upravne novčane kazne. 8. Ako pravnim sustavom pojedine države članice nisu predviđene upravne novčane kazne, ta država članica osigurava da se ovaj članak primjenjuje na način da novčanu kaznu pokreće nadležno tijelo, a izriču je nadležni nacionalni sudovi, osiguravajući pritom da su ta pravna sredstva djelotvorna i imaju jednakovrijedan učinak kao upravne novčane kazne koje izriču nadležna tijela. U svakom slučaju novčane kazne koje se izriču moraju biti učinkovite, proporcionalne i odvraćajuće. Država članica najkasnije do 17. listopada 2024. obavješćuje Komisiju o svojim zakonodavnim odredbama koje donese u skladu s ovim stavkom te, bez odgode, o svim daljnjim izmjenama tih zakonodavnih odredbi ili izmjeni koja na njih utječe.	- 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 86. 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 (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 86. ovog Zakona. **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 nacionalno 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. **NIS2 direktivom utvrđuje se minimalni iznos najvećeg mogućeg iznosa novčane kazne kojoj podliježu ključni i važni subjekti. Člankom 101. i 102. Nacrta zakona se osim maksimalnog (NIS2) iznosa novčane kazne koja se može izreći, utvrđuje i iznos minimalnih kazni koje se mogu izreći subjektima, pri tome vodeći računa u tom dijelu o okviru koji po tom pitanju postavlja Prekršajni zakon.**		
Članak 35. Povrede koje uključuju povredu osobnih podataka 1. Ako nadležna tijela tijekom nadzora ili izvršavanja saznaju da povreda obveza utvrđenih u člancima 21. i 23. ove Direktive koju je počinio ključni ili važni subjekt može uključivati povredu	**Članak 35. NIS2 direktive preuzima se slijedećim člancima Zakona:** **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	U potpunosti preuzeto	

osobnih podataka iz članka 4. stavka 12. Uredbe (EU) 2016/679 o kojoj se izvješćuje na temelju članka 33. te uredbe, ta nadležna tijela bez nepotrebne odgode obavješćuju nadzorna tijela iz članaka 55. i 56. te uredbe. 2. Ako nadzorna tijela kako su utvrđena u člancima 55. i 56. Uredbe (EU) 2016/679 izreknu upravnu novčanu kaznu u skladu s člankom 58. stavkom 2. točkom (i) te uredbe, nadležna tijela ne smiju izreći upravnu novčanu kaznu na temelju članka 34. ove Direktive za povredu iz stavka 1. ovog članka koja proizlazi iz istog postupanja koje je predmet upravne novčane kazne na temelju članka 58. stavka 2. točke (i) Uredbe (EU) 2016/679. Međutim, nadležna tijela mogu izreći mjere izvršavanja predviđene u članku 32. stavku 4. točkama od (a) do (h), članku 32. stavku 5. i članku 33. stavku 4. točkama od (a) do (g) ove Direktive. 3. Ako je nadzorno tijelo nadležno na temelju Uredbe (EU) 2016/679 osnovano u državi članici različitoj od one u kojoj je osnovano nadležno tijelo, nadležno tijelo obavještava nadzorno tijelo osnovano u svojoj vlastitoj državi	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 obavještava tijelo nadležno za zaštitu osobnih podataka osnovano u drugoj državi članici, nadležno tijelo za provedbu zahtjeva kibernetičke sigurnosti dužno je o istoj povredi obavijestiti i Agenciju za zaštitu osobnih podataka. **Izricanje novčanih kazni** **Članak 84.** (1) Uz korektivne mjere propisane ovim Zakonom, 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. **Dopunjen članak 74. (dodan stavak 2.)**		

članici o potencijalnoj povredi podataka iz stavka 1.			
Članak 36. Sankcije Države članice utvrđuju pravila o sankcijama koje se primjenjuju na kršenja nacionalnih mjera donesenih na temelju ove Direktive i poduzimaju sve potrebne mjere radi osiguranja njihove provedbe. Predviđene sankcije moraju biti učinkovite, proporcionalne i odvraćajuće. Države članice do 17. siječnja 2025. obavješćuju Komisiju o tim pravilima i tim mjerama te je bez odgode obavješćuju o svim naknadnim izmjenama koje na njih utječu.	**Članak 36. NIS2 direktive preuzima se slijedećim člancima Zakona:** **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 9., članka 56. stavka 2., 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	U potpunosti preuzeto	

	- 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. **Izricanje novčanih kazni** **Članak 84.** (1) Uz korektivne mjere propisane ovim Zakonom, 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. **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 (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 86. 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 (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 86. ovog Zakona. **Dopunjen članak 62. (novi podstavak 2.).** **18.8.2023.:** **Članak 62. stavak 1. podstavak 2. Nacrta zakona dopunjen prema prijedlogu.**		

Članak 37. Uzajamna pomoć 1. Ako subjekt 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, nadležna tijela dotičnih država članica surađuju i međusobno si pomažu ako je potrebno. Ta suradnja podrazumijeva najmanje sljedeće: (a) nadležna tijela koja primjenjuju nadzorne mjere ili mjere izvršavanja u državi članici preko jedinstvene kontaktne točke obavješćuju nadležna tijela u drugim dotičnim državama članicama o poduzetim nadzornim mjerama i mjerama izvršavanja te se savjetuju s njima; (b) nadležno tijelo može zatražiti od drugog nadležnog tijela da poduzme nadzorne mjere ili mjere izvršavanja; (c) nakon primitka potkrijepljenog zahtjeva drugog nadležnog tijela nadležno tijelo pruža tom drugom nadležnom tijelu uzajamnu pomoć razmjernu vlastitim resursima kako bi se nadzorne mjere ili mjere izvršavanja mogle provesti na	**Članak 37. NIS2 direktive preuzima se slijedećim člancima Zakona:** **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 u suradnji s nadležnim tijelima tih država članica te međusobnu uzajamnu pomoć u provedbi nadzora. **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	U potpunosti preuzeto	

djelotvoran, učinkovit i dosljedan način. Uzajamna pomoć iz prvog podstavka točke (c) može obuhvaćati zahtjeve za informacije i nadzorne mjere, uključujući zahtjeve za provođenje inspekcija na lokaciji ili neizravnog nadzora ili ciljanih revizija sigurnosti. Nadležno tijelo kojem je upućen zahtjev za pomoć ne smije odbiti taj zahtjev osim u slučaju da se utvrdi da to tijelo nema nadležnost za pružanje zatražene pomoći, da zatražena pomoć nije razmjerna nadzornim zadaćama nadležnog tijela ili da se zahtjev odnosi na informacije ili uključuje aktivnosti koje bi, u slučaju da se otkriju ili provedu, bile suprotne osnovnim interesima nacionalne sigurnosti, javne sigurnosti ili obrane države članice. Prije odbijanja takvog zahtjeva nadležno tijelo savjetuje se s drugim dotičnim nadležnim tijelima te, na zahtjev jedne od dotičnih država članica, Komisijom i ENISA-om. 2. Prema potrebi i uz međusobnu suglasnost, nadležna tijela iz različitih država članica mogu provoditi zajedničke nadzorne aktivnosti.	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.		
Članak 38. Izvršavanje delegiranja ovlasti 1. Ovlast za donošenje delegiranih akata dodjeljuje se Komisiji podložno uvjetima utvrđenima u ovom članku. 2. Ovlast za donošenje delegiranih akata iz članka 24. stavka 2. dodjeljuje se Komisiji na razdoblje od pet godina počevši od 16. siječnja 2023. 3. Europski parlament ili Vijeće u svakom trenutku mogu opozvati delegiranje ovlasti iz članka 24. stavka 2. Odlukom o opozivu prekida se delegiranje ovlasti koje je u njoj navedeno. Opoziv počinje proizvoditi učinke sljedećeg dana od dana objave spomenute odluke u Službenom listu Europske unije ili na kasniji dan naveden u spomenutoj odluci. On ne utječe na valjanost delegiranih akata koji su već na snazi.		Nije potrebno preuzimanje	Odredba se odnosi na ovlast Europske komisije za donošenje delegiranih akata.

4. Prije donošenja delegiranog akta Komisija se savjetuje sa stručnjacima koje je imenovala svaka država članica u skladu s načelima utvrđenima u Međuinstitucijskom sporazumu o boljoj izradi zakonodavstva od 13. travnja 2016. 5. Čim donese delegirani akt, Komisija ga istodobno priopćuje Europskom parlamentu i Vijeću. 6. Delegirani akt donesen na temelju članka 24. stavka 2. stupa na snagu samo ako ni Europski parlament ni Vijeće u roku od dva mjeseca od priopćenja tog akta Europskom parlamentu i Vijeću na njega ne podnesu prigovor ili ako su prije isteka tog roka i Europski parlament i Vijeće obavijestili Komisiju da neće podnijeti prigovore. Taj se rok produljuje za dva mjeseca na inicijativu Europskog parlamenta ili Vijeća.			
Članak 39. Postupak odbora 1. Komisiji pomaže odbor. Navedeni odbor je odbor u smislu Uredbe (EU) br. 182/2011.		Nije potrebno preuzimanje	Odredba se odnosi na nadležne EU institucije.

2. Pri upućivanju na ovaj stavak primjenjuje se članak 5. Uredbe (EU) br. 182/2011. 3. Kada se mišljenje odbora treba dobiti pisanim postupkom, navedeni postupak završava bez rezultata kada u roku za davanje mišljenja to odluči predsjednik odbora ili to zahtijeva član odbora.			
Članak 40. Preispitivanje Do 17. listopada 2027. i svakih 36 mjeseci nakon toga, Komisija preispituje funkcioniranje ove Direktive te o tome izvješćuje Europski parlament i Vijeće. U izvješću se posebno ocjenjuje relevantnost veličine dotičnih subjekata, te sektora, podsektora i vrsta subjekata iz priloga I. i II. za funkcioniranje gospodarstva i društva u pogledu kibersigurnosti. U tu svrhu te u cilju daljnjeg unapređivanja strateške i operativne suradnje, Komisija uzima u obzir izvješća skupine za suradnju i mreže CSIRT-ova o iskustvu stečenom na strateškoj i operativnoj razini. Uz to izvješće prilaže se, prema potrebi, zakonodavni prijedlog.		Nije potrebno preuzimanje	U pitanju je odredba NIS2 direktive koja se provodi od strane nadležnih EU institucija.

Članak 41. Prenošenje 1. Države članice do 17. listopada 2024. donose i objavljuju mjere potrebne radi usklađivanja s ovom Direktivom. One o tome odmah obavješćuju Komisiju. One primjenjuju te mjere od 18. listopada 2024. 2. Kada države članice donose mjere iz stavka 1, one sadržavaju upućivanje na ovu Direktivu ili se na nju upućuje prilikom njihove službene objave. Načine tog upućivanja određuju države članice.	**Članak 41. NIS2 direktive preuzima se slijedećim člankom 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.).	Djelomično preuzeto	Bit će preuzeto u: Uredba o kibernetičkoj sigurnosti (12.09.2024)
Članak 42. Izmjena Uredbe (EU) br. 910/2014 U Uredbi (EU) br. 910/2014 članak 19. briše se s učinkom od 18. listopada 2024.	**Članak 42. NIS2 direktive preuzima se slijedećim člankom 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 Zakona o elektroničkim komunikacijama („Narodne novine“, broj: 76/2022) nastavljaju s provedbom zahtjeva na temelju tog Zakona do dostave obavijesti o provedenoj kategorizaciji subjekta iz članka 19. stavka 1. ovog Zakona.	U potpunosti preuzeto	

	(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. **Nije potrebno cjelovito preuzimanje.** **Uredba (EU) br. 910/2014 se izravno primjenjuje u državama članicama.** **Izmjene i dopune 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 (NN, broj: 62/17) nisu potrebne, budući da se u Zakonu ne razrađuje članak 19. Uredbe (EU) br. 910/2014.** **Člancima 106. i 109. Nacrta zakona osigurava se provedba NIS2 direktive po pitanju pravovremene primjene „NIS2 pravila“ te prestanka važenja odnosno prestanka primjene u odgovarajućem roku onih sigurnosnih zahtjeva koji su bili utvrđeni brisanim člankom Uredbe (EU) br. 910/2014.**		

Članak 43. Izmjena Direktive (EU) 2018/1972 U Direktivi (EU) 2018/1972 članci 40. i 41. brišu se s učinkom od 18. listopada 2024.	**Članak 43. NIS2 direktive preuzima se slijedećim člancima 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 Zakona o elektroničkim komunikacijama („Narodne novine“, broj: 76/2022) nastavljaju s provedbom zahtjeva na temelju 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 109.** (1) Postupci započeti prema odredbama Zakona o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga	U potpunosti preuzeto	

	(„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 115.** Danom stupanja na snagu ovog Zakona prestaju 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.		

	Člankom 106. predviđa se stavljanje van snage relevantne odredbe Zakona o elektroničkim komunikacijama i to stupanjem na snagu Zakona o kibernetičkoj sigrnosnti, budući da odgodno stavljanje van snage (osobito s datumom u 2024.) nije nomotehnički prihvatljivo. **Člancima 106., 109. i 115. Nacrta zakona osigurava se provedba NIS2 direktive po pitanju pravovremene primjene „NIS2 pravila" te prestanka važenja odnosno prestanka primjene u odgovarajućem roku onih sigurnosnih zahtjeva koji su bili utvrđeni brisanim člancima Direktive (EU) 2018/1972.**		
Članak 44. Stavljanje izvan snage Direktiva (EU) 2016/1148 stavlja se izvan snage s učinkom od 18. listopada 2024. Upućivanja na direktivu stavljenu izvan snage smatraju se upućivanjima na ovu Direktivu i čitaju se u skladu s korelacijskom tablicom iz Priloga III.	**Članak 44. NIS2 direktive preuzima se sljedećim člancima Zakona:** **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 od tih propisa do dostave obavijesti o provedenoj kategorizaciji subjekta iz članka 19. stavaka 1. i 3. 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**	U potpunosti preuzeto	

	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 115.** **Danom stupanja na snagu ovog Zakona prestaju 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. **Člankom 106. predviđa se stavljanje van snage NIS1**		

	transpozicijskog zakona i prateće Uredbe i to stupanjem na snagu Zakona o kibernetičkoj sigurnosti, budući da odgodno stavljanje van snage (osobito s datumom u 2024.) nije nomotehnički prihvatljivo. **Člancima 106., 109. i 115. Nacrta zakona osigurava se provedba NIS2 direktive po pitanju pravovremene primjene „NIS2 pravila" te prestanka važenja odnosno prestanka primjene u odgovarajućem roku mjera kibernetičke sigurnosti koje su uvedene prenošenjem NIS1 direktove u nacionalno zakonodavstvo.**		
Članak 45. Stupanje na snagu Ova Direktiva stupa na snagu dvadesetog dana od dana objave u Službenom listu Europske unije.		Nije potrebno preuzimanje	Riječ je odredbi NIS2 direktive koja utvrđuje njezino stupanje na snagu, a koja nije predmet preuzimanja.
Članak 46. Adresati Ova je Direktiva upućena državama članicama.		Nije potrebno preuzimanje	Riječ je o odredbi NIS2 direktive koja utvrđuje adresate na koje se Direktiva odnosi.

PRILOG I. SEKTORI VISOKE KRITIČNOSTI Sektor 1. Energetika Podsektor (a) električna energija Vrsta subjekta — elektroenergetska poduzeća iz članka 2. točke 57. Direktive (EU) 2019/944 Europskog parlamenta i Vijeća (1), koja obavljaju funkciju „opskrbe” iz članka 2. točke 12. te direktive — operatori distribucijskog sustava kako su definirani u članku 2. točki 29. Direktive (EU) 2019/944 — operatori prijenosnog sustava kako su definirani u članku 2. točki 35.	PRILOG I. SEKTORI VISOKE KRITIČNOSTI **Sektor** / **Podsektor** / **Vrsta subjekta** 1. Energetika / (a) električna energija / - elektroenergetski subjekti koju obavljaju funkciju opskrbe električnom energijom, uključujući opskrbu električnom energijom koja se obavlja kao javna usluga Pojam „*elektroenergetski subjekt*“ u smislu 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.	U potpunosti preuzeto	

Direktive (EU) 2019/944 — proizvođači kako su definirani u članku 2. točki 38. Direktive (EU) 2019/944 —nominirani operatori tržišta električne energije kako su definirani u članku 2. točki 8. Uredbe (EU) 2019/943 Europskog parlamenta i Vijeća (2) — sudionici na tržištu kako su definirani u članku 2. točki 25. Uredbe (EU) 2019/943 koji pružaju usluge agregiranja, upravljanja potrošnjom ili skladištenja			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 sustava Pojam *„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		

	energije iz članka 2. točaka 18., 20. i 59. Direktive (EU) 2019/944 — 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 (centralizi — operator b rano sustava) grijanje i centraliziranog hlađenje grijanja ili centraliziranog hlađenja kako je definirano u članku 2. točki 19. Direktive			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 sustava Pojam „*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 energije Pojam *„proizvođač električne energije”* u smislu ovog Zakona znači fizička ili pravna osoba koja proizvodi električnu energiju.		

	(EU) 2018/2001 Europskog parlamenta i Vijeća (3) (c) nafta — operatori naftovoda — operatori proizvodnje nafte, rafinerija i tvornica nafte te njezina skladištenja i prijenosa —središnja tijela za zalihe kako su definirana u članku 2. točki (f) Direktive Vijeća 2009/119/EZ (4) (d) plin —poduzeća za opskrbu kako su definirana u članku 2. točki 8. Direktive 2009/73/EZ Europskog parlamenta i Vijeća (5) —operatori distribucijskog			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 energije Pojam *„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		

sustava kako su definirani u članku 2. točki 6. Direktive 2009/73/EZ — operatori transportnog sustava kako su definirani u članku 2. točki 4. Direktive 2009/73/EZ — operatori sustava skladišta plina kako su definirani u članku 2. točki 10. Direktive 2009/73/EZ — operatori terminala za UPP kako su definirani u članku 2. točki 12. Direktive 2009/73/EZ — poduzeća za prirodni plin kako su definirana u			opterećenju kod krajnjih kupaca u odnosu na njihove uobičajene ili trenutačne obrasce potrošnje električne energije kao odgovor na tržišne signale, uključujući vremenski ovisnu promjenu cijene električne energije ili novčane poticaje, ili kao odgovor na prihvat ponude krajnjeg kupca za prodaju smanjenja ili povećanja potražnje po cijeni na organiziranim tržištima, kako je definirano u članku 2. točki 4. Provedbene uredbe Komisije (EU) br. 1348/2014 od 17. prosinca 2014. o izvješćivanju o podacima i provedbi članka 8. stavaka 2. i 6. Uredbe (EU) br. 1227/2011 Europskog parlamenta i Vijeća o cjelovitosti i transparentnosti veleprodajnog tržišta energije (Tekst značajan za EGP) (SL L 363, 18. 12. 2014.), pojedinačno ili putem agregiranja. Pojam „*skladištenje energije*" u smislu 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		

		članku 2. točki 1. Direktive 2009/73/EZ			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 postrojenja za rafiniranje i obradu prirodnog plina					
	(e) vodik	— operatori proizvodnje, skladištenja i prijenosa vodika			- operatori mjesta za punjenje koji su o upravljanje i rad mjesta za punjenj krajnjim korisnicima pruža usluga ops ostalim u ime i za račun pružat mobilnosti		
2. Promet	(a) zračni promet	—zračni prijevoznici kako su definirani u članku 4. točki 3. Uredbe (EZ) br. 300/2008 koji se upotrebljavaju u komercijalne svrhe					
		—upravna tijela zračne luke kako su definirana u članku 2. točki 2. Direktive 2009/12/EZ		(centralizira b no 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		

Europskog parlamenta i Vijeća (6), zračne luke kako su definirane u članku 2. točki 1. te direktive, uključujući osnovne zračne luke navedene u odjeljku 2. Priloga II. Uredbi (EU) br. 1315/2013 Europskog parlamenta i Vijeća (7) te tijela koja upravljaju pomoćnim objektima u zračnim lukama — operatori kontrole upravljanja prometom koji pružaju usluge kontrole zračnog prometa (ATC) kako su			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			

	definirani u članku 2. točki 1. Uredbe (EZ) br. 549/2004 Europskog parlamenta i Vijeća (8) (b) željeznički promet — upravitelji infrastrukture kako su definirani u članku 3. točki 2. Direktive 2012/34/EU Europskog parlamenta i Vijeća (9) — željeznički prijevoznici kako su definirani u članku 3. točki 1. Direktive 2012/34/EU, među ostalim i operatori uslužnih objekata kako su definirani u članku 3. točki 12. te direktive			države članice obvezuju održavati minimalne zalihe sirove nafte i/ili naftnih derivata (SL L 265/9 od 9. 10. 2009.).		
			(d) plin	- opskrbljivači plinom, uključujući opskrbljivače u obvezi javne usluge Pojam *„opskrbljivač plinom“* u smislu 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 Zakona znači prodaja ili preprodaja plina kupcu, uključujući prodaju ili preprodaju UPP-a i SPP-a. Pojam *„opskrba plinom u obvezi javne usluge“* u smislu ovog Zakona znači opskrba plinom koja se u općem gospodarskom interesu obavlja po reguliranim uvjetima radi osiguravanja sigurnosti, redovitosti, kvalitete i cijene opskrbe kućanstava. Pojmovi *„opskrbljivač plinom“, „opskrbljivač plinom u obvezi javne usluge“, „opskrba plinom“* i *„opskrba*		

(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 (10), ne uključujući pojedinačna plovila kojima upravljaju te kompanije — upravljačka tijela luka kako su definirane u članku 3. točki 1. Direktive 2005/65/EZ Europskog parlamenta i Vijeća (11), uključujući njihove luke			*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,		

	kako su definirane u članku 2. točki 11. Uredbe (EZ) br. 725/2004 te subjekti koji upravljaju postrojenjima i opremom u lukama — služba za nadzor i upravljanje pomorskim prometom (VTS) kako je definirana u članku 3. točki (o) Direktive 2002/59/EZ Europskog parlamenta i Vijeća (12) (d) cestovni promet — tijela nadležna za ceste kako su definirana u članku 2. točki 12. Delegirane uredbe Komisije (EU) 2015/962 (13) odgovorna za kontrolu			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		

	upravljanja prometom, osim javnih subjekata kojima upravljanje prometom ili rad inteligentnih prometnih sustava nisu ključni dio njihove opće djelatnosti — operatori inteligentnih prometnih sustava kako su definirani u članku 4. točki 1. Direktive 2010/40/EU Europskog parlamenta i Vijeća (14)			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.		
3.	Bankarstvo	kreditne institucije kako su definirane u članku 4. točki 1. Uredbe (EU) br. 575/2013 Europskog parlamenta i Vijeća (15)			- operatori sustava skladišta plina Pojam *„operator sustava skladišta plina“* u smislu ovog Zakona znači energetski subjekt koji obavlja energetsku djelatnost skladištenja		

4Infrastru . ktura financijsk og tržišta	— operatori mjestâ trgovanja kako su definirani u članku 4. točki 24. Direktive 2014/65/EU Europskog parlamenta i Vijeća (16) — središnje druge ugovorne strane (CCP-i) kako su definirane u članku 2. točki 1. Uredbe (EU) br. 648/2012 Europskog parlamenta i Vijeća (17)			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,		
5. Zdravlje	—pružatelji zdravstvene zaštite kako su definirani u članku 3. točki (g) Direktive 2011/24/EU Europskog					

parlamenta i Vijeća (18) — referentni laboratoriji EU-a iz članka 15. Uredbe (EU) 2022/2371 Europskog parlamenta i Vijeća (19) — subjekti koji obavljaju djelatnosti istraživanja i razvoja lijekova kako su definirani u članku 1. točki 2. Direktive 2001/83/EZ Europskog parlamenta i Vijeća (20) — subjekti koji proizvode osnovne farmaceutske proizvode i farmaceutske pripravke iz područja C			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. 300/2008 Europskog parlamenta i Vijeća od 11. ožujka 2008. o zajedničkim pravilima u području zaštite civilnog zračnog prometa i		

	odjeljka 21. NACE Rev. 2 — 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 (21)			stavljanju izvan snage Uredbe (EZ) br. 2320/2002 (Tekst značajan za EGP), koji se upotrebljavaju u komercijalne svrhe		
6. Voda za piće	dobavljači i distributeri vode namijenjene za			- 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 lukama Pojam *„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		

	ljudsku potrošnju kako je definirana u članku 2. točki 1. podtočki (a) Direktive (EU) 2020/2184 Europskog parlamenta i Vijeća (22), isključujući distributere kojima distribucija vode za ljudsku potrošnju nije ključni dio njihove općenite djelatnosti distribucije druge robe i proizvoda			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 (SL L 70, 14. 3. 2009.).		
7. Otpadne vode	poduzeća koja prikupljaju, odlažu ili pročišćavaju komunalne otpadne vode, otpadne vode iz kućanstva ili industrijske otpadne vode kako su definirane u			- 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,		

	članku 2. točkama od 1., 2., i 3. Direktive Vijeća 91/271/EEZ (23), ali isključujući poduzeća kojima prikupljanje, odlaganje ili pročišćavanje komunalnih otpadnih voda, otpadnih voda iz kućanstva ili industrijskih otpadnih voda nije ključni dio njihove općenite djelatnosti — pružatelji središta za razmjenu internetskog prometa — pružatelji usluga DNS-a, osim operatora korijenskih poslužitelja naziva — registri naziva vršnih domena			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.).		
8. Digitalna infrastruktura				- željeznički prijevoznici, među ostalim i operatori uslužnih objekata Pojam *„željeznički prijevoznik“* u smislu ovog Zakona znači svaka pravna osoba		

	— 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			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.		
9.	Upravljanje uslugama IKT-a (B2B)	— pružatelji upravljanih usluga — pružatelji upravljanih sigurnosnih usluga		(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		

10. Javna uprava 11. Svemir	— subjekti središnje državne uprave kako ih je definirala država članica u skladu s nacionalnim pravom — subjekti javne uprave na regionalnoj razini kako ih je definirala država članica u skladu s nacionalnim pravom 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			članku 2. točki 11. Uredbe (EZ) br. 725/2004, te subjekti koji upravljaju postrojenjima i opremom u lukama Pojam *„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.).		

komunikacijskih mreža (1) 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., str. 125.). (2) Uredba (EU) 2019/943 Europskog parlamenta i Vijeća od 5. lipnja 2019. o unutarnjem tržištu električne energije (SL L 158, 14.6.2019., str. 54.). (3) Direktiva (EU) 2018/2001 Europskog parlamenta i Vijeća od 11. prosinca 2018. o promicanju uporabe energije iz obnovljivih izvora (SL L 328, 21.12.2018., str. 82.). (4) Direktiva Vijeća 2009/119/EZ od 14. rujna 2009. o obvezi država članica da održavaju minimalne zalihe sirove nafte i/ili naftnih derivata (SL L 265, 9.10.2009., str. 9.). (5) Direktiva 2009/73/EZ Europskog parlamenta i Vijeća od 13. srpnja 2009. o zajedničkim pravilima za unutarnje tržište prirodnog plina i stavljanju izvan			- 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		
		(cestovni d promet)	- tijela nadležna za ceste kako su definirana u članku 2. točki 12. Delegirane uredbe Komisije (EU) 2015/962 od 18. prosinca 2014. o dopuni Direktive 2010/40/EU Europskog parlamenta i Vijeća u pogledu pružanja usluga prometnih informacija u cijeloj Europskoj uniji u realnom vremenu (Tekst značajan za EGP), odgovorna za kontrolu upravljanja prometom, osim javnih subjekata kojima upravljanje prometom ili rad inteligentnih prometnih sustava nisu ključni dio njihove opće djelatnosti Prema članku 2. točki 12. Delegirane uredbe Komisije (EU) 2015/962 pojam *„tijelo nadležno za ceste”* znači svako		

snage Direktive 2003/55/EZ (SL L 211, 14.8.2009., str. 94.). (6) Direktiva 2009/12/EZ Europskog parlamenta i Vijeća od 11. ožujka 2009. o naknadama zračnih luka (SL L 70, 14.3.2009., str. 11.). (7) Uredba (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 (SL L 348, 20.12.2013., str. 1.). (8) Uredba (EZ) br. 549/2004 Europskog parlamenta i Vijeća od 10. ožujka 2004. o utvrđivanju okvira za stvaranje jedinstvenog europskog neba (Okvirna uredba) (SL L 96, 31.3.2004., str. 1.). (9) Direktiva 2012/34/EU Europskog parlamenta i Vijeća od 21. studenoga 2012. o uspostavi jedinstvenog Europskog željezničkog prostora (SL L 343, 14.12.2012., str. 32.). (10) Uredba (EZ) br. 725/2004 Europskog parlamenta i Vijeća od 31. ožujka 2004. o jačanju sigurnosne zaštite brodova i luka (SL L 129, 29.4.2004., str. 6.).			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		

(11) Direktiva 2005/65/EZ Europskog parlamenta i Vijeća od 26. listopada 2005. o jačanju sigurnosne zaštite luka (SL L 310, 25.11.2005., str. 28.). (12) 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 (SL L 208, 5.8.2002., str. 10.). (13) Delegirana uredba Komisije (EU) 2015/962 od 18. prosinca 2014. o dopuni Direktive 2010/40/EU Europskog parlamenta i Vijeća u pogledu pružanja usluga prometnih informacija u cijeloj Europskoj uniji u realnom vremenu (SL L 157, 23.6.2015., str. 21.). (14) Direktiva 2010/40/EU Europskog parlamenta i Vijeća od 7. srpnja 2010. o okviru za uvođenje inteligentnih prometnih sustava u cestovnom prometu i za veze s ostalim vrstama prijevoza (SL L 207, 6.8.2010., str. 1.). (15) Uredba (EU) br. 575/2013 Europskog parlamenta i Vijeća od 26. lipnja 2013. o bonitetnim zahtjevima za kreditne institucije i o izmjeni Uredbe			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).		

(EU) br. 648/2012 (SL L 176, 27.6.2013., str. 1.). (16) 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 (SL L 173, 12.6.2014., str. 349.). (17) Uredba (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., str. 1.). (18) Direktiva 2011/24/EU Europskog parlamenta i Vijeća od 9. ožujka 2011. o primjeni prava pacijenata u prekograničnoj zdravstvenoj skrbi (SL L 88, 4.4.2011., str. 45.). (19) Uredba 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 (SL L 314, 6.12.2022., str. 26.). (20) Direktiva 2001/83/EZ Europskog parlamenta i Vijeća od 6. studenoga 2001. o zakoniku Zajednice o lijekovima			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		

za humanu primjenu (SL L 311, 28.11.2001., str. 67.). (21) Uredba (EU) 2022/123 Europskog parlamenta od 25. siječnja 2022. i Vijeća o pojačanoj ulozi Europske agencije za lijekove u pripravnosti za krizne situacije i upravljanju njima u području lijekova i medicinskih proizvoda (SL L 20, 31.1.2022., str. 1). (22) Direktiva (EU) 2020/2184 Europskog parlamenta i Vijeća od 16. prosinca 2020. o kvaliteti vode namijenjene za ljudsku potrošnju (SL L 435, 23.12.2020., str. 1.). (23) Direktiva Vijeća 91/271/EEZ od 21. svibnja 1991. o pročišćavanju komunalnih otpadnih voda (SL L 135, 30.5.1991., str. 40.).			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 proizvoda Pojam *„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 djelatnosti Pojam *„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 3. 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		
	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		
			- tijela jedinica 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 I. dorađen prema danom prijedlogu.

18.8.2023.:
U pitanju je pozivanje na relevantne direktive EU povezano s definiranjem slijedećih pojmova: *„poduzeće za prirodni plin“, „upravno tijelo zračne luke“, „zračna luka“ „služba za nadzor i upravljanje pomorskim prometom (VTS)“* i *„pružatelj zdravstvene zaštite“.*

Budući da nije pronađeno da nacionalni transpozicijski propisi sadrže (da su prenijeli) definiciju predmetnih pojmova, prilikom pripreme teksta Priloga I. vezano uz citirane pojmove zatraženo je resorna Ministarstva (putem njihovih predstavnika u Radnoj skupini zaduženoj za NIS2

	transpoziciju), potvrdu je li tome tako, odnosno ako nije, zamoljeni su unijeti odgovarajuću definiciju pojma i pozivanje na relevantnu odredbu nacionalnog propisa. **„poduzeće za prirodni plin" - odgovor MGOR-a:** ***„Definicija predmetnog pojma nije prenesena tim izričajem već je definiran pojam Energetski subjekt, čl. 3. st. 8. Zakonu o tržištu plina koji u svom članku 4. st. 1. obuhvaća sve predmetne djelatnosti."*** **„upravno tijelo zračne luke", „zračna luka" „služba za nadzor i upravljanje pomorskim prometom (VTS)" – odgovor MMPI-a:** ***„U prilogu I, potvrđujemo da definicije pojmova „upravno tijelo zračne luke", „zračna luka" i „služba za nadzor i upravljanje pomorskim prometom (VTS)" nisu u potpunosti prenesene u nacionalnim propisima te je stoga opravdano koristiti definicije iz mjerodavnih direktiva."*** **„pružatelj zdravstvene zaštite – odgovor MZ-a:** ***„Nastavno na Prilog I. u kojem je definiran pojam „pružatelja zdravstvene zaštite", obavještavamo kako se planira prema Nacrtu Pravilnika o Nacionalnom registru pružatelja zdravstvene zaštite, u svom članku 2. točki 2. definirati pojam pružatelja zdravstvene zaštite:*** ***2) pružatelj zdravstvene zaštite je fizička i/ili pravna osoba u zdravstvu (nositelj privatne prakse, zdravstvena ustanova i trgovačko društvo za obavljanje zdravstvene djelatnosti) koja poduzima odgovarajuće mjere i aktivnosti te pruža zdravstvene usluge za očuvanje i unapređenje zdravlja, sprečavanje bolesti,***		

	rano otkrivanje bolesti, pravodobno liječenje te zdravstvenu njegu i rehabilitaciju. ***Također, pojam „pružatelj zdravstvene zaštite“ definiran je člankom 3. točkom (g) Direktive 2011/24/EU Europskog parlamenta i Vijeća od 9. ožujka 2011. o primjeni prava pacijenata u prekograničnoj zdravstvenoj skrbi, kako ste i naveli.*** ***Predložena definicija pojma u Prilogu I. proširuje krug osoba i na „ili bilo koji subjekt“ koji zakonito pruža zdravstvenu zaštitu na državnom području države članice.*** ***Stoga, unatoč neuobičajenosti, a s obzirom da nemamo u važećem propisu definiran ovaj pojam, zdravstvenom ili negdje drugdje, potvrđujemo da se u Nacrtu zakona o kibernetičkoj sigurnosti zadrži pojam kako je predloženo.“*** **Uvažavajući odgovor MMPI-a vezano uz pojmove iz njihove nadležnosti, da se definicija „energetskog subjekta“ odnosi na sve energetske djelatnosti (npr. i na transport i skladištenje plin), te da spomenuti Pravilnik o Nacionalnom registru pružatelja zdravstvene zaštite za sada još nije donesen, u Prilogu I. predlaže se primijeniti model definiranja gore navedenih pojmova kako je to već sadržano u Nacrtu zakona.** **vraćeno na provjeru s dopunom u tekstu Priloga I. - točka 9. dopunjena na način da su dodani subjekti koji greškom nisu bili navedeni (pružatelji upravljanih sigurnosnih usluga).**		

<table>
<tr>
<td>PRILOG II.

DRUGI KRITIČNI SEKTORI

Sektor Podsektor Vrsta subjekta

1. Poštanske i kurirske usluge pružatelji poštanskih usluga kako su definirani u članku 2. točki 1.a Direktive 97/67/EZ, uključujući pružatelje kurirskih usluga

2. Gospodarenje otpadom poduzeća koja se bave gospodarenjem otpadom kako je definirano u članku 3. točki 9. Direktive 2008/98/EZ Europskog parlamenta i Vijeća (1), isključujući poduzeća kojima</td>
<td>PRILOG II.

DRUGI KRITIČNI SEKTORI

<table>
<tr><th>Sektor</th><th>Podsektor</th><th>Vrsta subjekta</th></tr>
<tr><td>1. Poštanske i kurirske usluge</td><td></td><td>- davatelji poštanskih usluga

Pojam „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</td></tr>
</table>
</td>
<td>U potpunosti preuzeto</td>
<td></td>
</tr>
</table>

3.	Izrada, proizvodnja i distribucija kemikalija	gospodarenje otpadom nije glavna gospodarska djelatnost poduzeća koja se bave izradom tvari te distribucijom tvari ili mješavina kako su definirana u članku 3. točkama 9. i 14. Uredbe (EZ) br. 1907/2006 Europskog parlamenta i Vijeća (2) i poduzeća koja se bave proizvodnjom proizvoda kako su definirana u članku 3. točki 3. te uredbe, iz tvari ili mješavina			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.).		

4.	Proizvodnja, prerada i distribucija hrane		poduzeća za poslovanje s hranom kako su definirana u članku 3. točki 2. Uredbe (EZ) br. 178/2002 Europskog parlamenta i Vijeća (3) koja se bave veleprodajom te industrijskom proizvodnjom i preradom			- pružatelji kurirskih usluga		
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 (4) i subjekti koji	2.	Gospodarenje otpadom		- subjekti koji se bave gospodarenjem otpadom, isključujući subjekte kojima gospodarenje otpadom nije glavna gospodarska djelatnost Pojam *„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.		

		proizvode in vitro dijagnostičke medicinske proizvode kako su definirani u članku 2. točki 2. Uredbe (EU) 2017/746 Europskog parlamenta i Vijeća (5), osim subjekata koji proizvode medicinske proizvode navedene u Prilogu I. točki 5. petoj alineji ove Direktive.			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		
(b)	proizvodnja računalate elektroničkih i optičkih proizvoda	poduzeća koja obavljaju bilo koju od gospodarskih djelatnosti iz područja C odjeljka 26. NACE Rev. 2					

(c)	proizvodnja električne opreme	poduzeća koja obavljaju bilo koju od gospodarskih djelatnosti iz područja C odjeljka 27. NACE Rev. 2			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.		
(d)	proizvodnja strojeva i uređaja, d. n.	poduzeća koja obavljaju bilo koju od gospodarskih djelatnosti iz područja C odjeljka 28. NACE Rev. 2					
(e)	proizvodnja motornih vozila, prikolica i poluprikolica	poduzeća koja obavljaju bilo koju od gospodarskih djelatnosti iz područja C odjeljka 29. NACE Rev. 2					
(f)	proizvodnja ostale opreme za prijevoz	poduzeća koja obavljaju bilo koju od gospodarskih djelatnosti iz područja C					

	odjeljka 30. NACE Rev. 2					
6. Pružatelji digitalnih usluga	—pružatelji internetskih tržišta —pružatelji internetskih tražilica —pružatelji platforma za usluge društvenih mreža					
7 Istraživanje	Istraživačke organizacije					
				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 (EU) 2008/98/EZ Europskog parlamenta i Vijeća od 19. studenoga 2008. o otpadu i stavljanju izvan snage određenih direktiva (Tekst značajan za EGP) (SL L 312, 22. 11. 2008.).		
		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		

---

(1) 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., str. 3.).

(2) Uredba (EZ) br. 1907/2006 Europskog parlamenta i Vijeća od 18. prosinca 2006. o registraciji, evaluaciji, autorizaciji i ograničavanju kemikalija (REACH), o osnivanju Europske agencije za kemikalije i 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 te Direktiva Komisije

91/155/EEZ, 93/67/EEZ, 93/105/EZ i 2000/21/EZ (SL L 396, 30.12.2006., str. 1.). (3) Uredba (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 (SL L 31, 1.2.2002., str. 1.). (4) Uredba (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 (SL L 117, 5.5.2017., str. 1.). (5) Uredba (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 (SL L 117, 5.5.2017., str. 176.).				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	(proizvodnja medicinskih) proizvoda i in vitro dijagnostički		- 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		

			h medicinskih proizvoda	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		

Člankom 2. stavkom 5. točkom b) NIS2 direktive propisano je da države članice mogu predvidjeti da se ova Direktiva primjenjuje na obrazovne ustanove, posebno ako provode ključne istraživačke aktivnosti. Također, napominje se da, neovisno o citiranoj odredbi NIS2 direktive, nije zabranjeno na nacionalnoj razini donijeti odluku o širem području primjene zahtjeva koji proizlaze iz NIS2 direktive odnosno transpozicijskim zakonom propisati kako se isti primjenjuje i na druge sektore odnosno vrste subjekata koji nisu izrijekom obuhvaćeni ili izuzeti od područja primjene NIS2 direktive.
Budući da se predmetnim Nacrtom prijedloga zakona predviđa mogućnost uključivanja i subjekata iz sustava obrazovanja u krug obveznika njegove primjene i to kao važnih subjekata (članak 13. Nacrta), slijedno je u Prilog II. Nacrta dodan sektor „sustav obrazovanja“ (kao i odgovarajuća definicija pojma u članku 6. Nacrta – točka 55.).
Prilog II. se ne referira na Direktivu 2022/2557. Direktiva 2022/2557 navodi se u odredbama NIS2 direktive koje se odnose na „subjekte utvrđene kao kritične subjekte na temelju Direktive (EU) 2022/2557“ (npr. članak 2. stavak 3. i članak 3. stavak 1. točka f) NIS2 direktive), o čemu je prilikom izrade predmetnog Nacrta vođeno računa, vodeći pri preuzimanju tih odredbi računa o tome da se problematika Direktive 2022/2557 nacionalno uređuje propisima o kritičnoj infrastrukturi (npr. vidi članak 9. stavak 1. podstavak 4. Nacrta prijedloga zakona).

PRILOG III. KORELACIJSKA TABLICA Direktiva (EU) 2016/1148 — Ova Direktiva članak 1. stavak 1. — članak 1. stavak 1. članak 1. stavak 2. — članak 1. stavak 2. članak 1. stavak 3. — - članak 1. stavak 4. — članak 2. stavak 12. članak 1. stavak 5. — članak 2. stavak 13. članak 1. stavak 6. — članak 2. stavci 6. i 11. članak 1. stavak 7. — članak 4. članak 2. — članak 2. stavak 14. članak 3. — članak 5. članak 4. — članak 6. članak 5. — - članak 6. — - članak 7. stavak 1. — članak 7. stavci 1. i 2. članak 7. stavak 2. — članak 7. stavak 4. članak 7. stavak 3. — članak 7. stavak 3. članak 8. stavci od 1. do 5. — članak 8. stavci od 1. do 5. članak 8. stavak 6. — članak 13. stavak 4. članak 8. stavak 7. — članak 8. stavak 6. članak 9. stavci 1., 2. i 3. — članak 10. stavci 1., 2. i 3. članak 9. stavak 4. — članak 10. stavak 9. članak 9. stavak 5. — članak 10. stavak 10.		Nije potrebno preuzimanje	Nije potrebno preuzimanje.

članak 10. stavak 1., stavak 2. i stavak 3. prvi podstavak	članak 13. stavci 1., 2. i 3.			
članak 10. stavak 3. drugi podstavak	članak 23. stavak 9.			
članak 11. stavak 1.	članak 14. stavci 1. i 2.			
članak 11. stavak 2.	članak 14. stavak 3.			
članak 11. stavak 3.	članak 14. stavak 4. prvi podstavak točke od (a) do (q) i točka (s) i stavak 7.			
članak 11. stavak 4.	članak 14. stavak 4. prvi podstavak točka (r) i drugi podstavak			
članak 11. stavak 5.	članak 14. stavak 8.			
članak 12. stavci od 1. do 5.	članak 15. stavci od 1. do 5.			
članak 13.	članak 17.			
članak 14. stavci 1. i 2.	članak 21. stavci od 1. do 4.			
članak 14. stavak 3.	članak 23. stavak 1.			
članak 14. stavak 4.	članak 23. stavak 3.			
članak 14. stavak 5.	članak 23. stavci 5., 6. i 8.			
članak 14. stavak 6.	članak 23. stavak 7.			
članak 14. stavak 7.	članak 23. stavak 11.			
članak 15. stavak 1.	članak 31. stavak 1.			
članak 15. stavak 2. prvi podstavak točka (a)	članak 32. stavak 2. točka (e)			

članak 15. stavak 2. prvi podstavak točka (b)	članak 32. stavak 2. točka (g)			
članak 15. stavak 2. drugi podstavak	članak 32. stavak 3.			
članak 15. stavak 3.	članak 32. stavak 4. točka (b)			
članak 15. stavak 4.	članak 31. stavak 3.			
članak 16. stavci 1. i 2.	članak 21. stavci od 1. do 4.			
članak 16. stavak 3.	članak 23. stavak 1.			
članak 16. stavak 4.	članak 23. stavak 3.			
članak 16. stavak 5.	-			
članak 16. stavak 6.	članak 23. stavak 6.			
članak 16. stavak 7.	članak 23. stavak 7.			
članak 16. stavci 8. i 9.	članak 21. stavak 5. i članak 23. stavak 11.			
članak 16. stavak 10.	-			
članak 16. stavak 11.	članak 2. stavci 1., 2. i 3.			
članak 17. stavak 1.	članak 33. stavak 1.			
članak 17. stavak 2. točka (a)	članak 32. stavak 2. točka (e)			
članak 17. stavak 2. točka (b)	članak 32. stavak 4. točka (b)			
članak 17. stavak 3.	članak 37. stavak 1. točke (a) i (b)			
članak 18. stavak 1.	članak 26. stavak 1. točka (b) i stavak 2.			
članak 18. stavak 2.	članak 26. stavak 3.			
članak 18. stavak 3.	članak 26. stavak 4.			
članak 19.	članak 25.			

članak 20. članak 21. članak 22. članak 23. članak 24. članak 25. članak 26. članak 27. Prilog I. točka 1. Prilog I. točka 2. podtočka (a) podtočke od i. do iv. Prilog I. točka 2. podtočka (a) podtočka v. Prilog I. točka 2. podtočka (b) Prilog I. točka 2. podtočka (c) podtočke i. i ii. Prilog II. Prilog III. točke 1. i 2. Prilog III. točka 3.	članak 30. članak 36. članak 39. članak 40. - članak 41. članak 45. članak 46. članak 11. stavak 1. članak 11. stavak 2. točke od (a) do (d) članak 11. stavak 2. točka (f) članak 11. stavak 4. članak 11. stavak 5. točka (a) Prilog I. Prilog II. točka 6. Prilog I. točka 8.			