HRVATSKI SABOR

P.Z.E. br. 320

KLASA: 022-03/18-01/48
URBROJ: 65-18-02

Zagreb, 22. ožujka 2018.

Hs**NP*022-03/18-01/48*65-18-02**Hs

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 operatora ključnih usluga i davatelja digitalnih usluga***, koji je predsjedniku Hrvatskoga sabora podnijela Vlada Republike Hrvatske, aktom od 22. ožujka 2018. 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 Damira Krstičevića, potpredsjednika Vlade Republike Hrvatske i ministra obrane, dr. sc. Davora Božinovića, ministra unutarnjih poslova, Tomislava Ivića i mr. sc. Zdravka Jakopa, državne tajnike u Ministarstvu obrane, doc. dr. sc. Roberta Kopala, Žarka Katića i Tereziju Gras, državne tajnike u Ministarstvu unutarnjih poslova, dr sc. Petra Mihatova, pomoćnika ministra obrane, dr. sc. Damira Truta, pomoćnika ministra unutarnjih poslova, te Maju Čavlović, predstojnicu Ureda Vijeća za nacionalnu sigurnost.

PREDSJEDNIK

Gordan Jandroković

P.Z.E. br. 320

VLADA REPUBLIKE HRVATSKE

Klasa: 022-03/17-01/182
Urbroj: 50301-29/09-18-6

Zagreb, 22. ožujka 2018.

Hs**NP*022-03/18-01/48*50-18-01**Hs

REPUBLIKA HRVATSKA
65 - HRVATSKI SABOR
ZAGREB, Trg Sv. Marka 6

Primljeno: 22-03-2018		
Klasifikacijska oznaka:	Org. jed.	
022-03/18-01/48	65	
Urudžbeni broj:	Pril.	Vrij.
50-18-01	1	CD

PREDSJEDNIKU HRVATSKOGA SABORA

Predmet: Prijedlog zakona o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga

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 i 69/17), Vlada Republike Hrvatske podnosi Prijedlog zakona o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga.

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 Damira Krstičevića, potpredsjednika Vlade Republike Hrvatske i ministra obrane, dr. sc. Davora Božinovića, ministra unutarnjih poslova, Tomislava Ivića i mr. sc. Zdravka Jakopa, državne tajnike u Ministarstvu obrane, doc. dr. sc. Roberta Kopala, Žarka Katića i Tereziju Gras, državne tajnike u Ministarstvu unutarnjih poslova, dr. sc. Petra Mihatova, pomoćnika ministra obrane, dr. sc. Damira Truta, pomoćnika ministra unutarnjih poslova, te Maju Čavlović, predstojnicu Ureda Vijeća za nacionalnu sigurnost.

PREDSJEDNIK

REPUBLIKA HRVATSKA 2 VLADA REPUBLIKE HRVATSKE ZAGREB

mr. sc. Andrej Plenković

VLADA REPUBLIKE HRVATSKE

PRIJEDLOG ZAKONA O KIBERNETIČKOJ SIGURNOSTI OPERATORA KLJUČNIH USLUGA I DAVATELJA DIGITALNIH USLUGA

Zagreb, ožujak 2018.

PRIJEDLOG ZAKONA O KIBERNETIČKOJ SIGURNOSTI OPERATORA KLJUČNIH USLUGA I DAVATELJA DIGITALNIH USLUGA

I. USTAVNA OSNOVA ZA DONOŠENJE ZAKONA

Ustavna osnova za donošenje ovog Zakona sadržana je u članku 2. stavku 4. podstavku 1. Ustava Republike Hrvatske (Narodne novine, br. 85/10 – pročišćeni tekst i 5/14 – Odluka Ustavnog suda Republike Hrvatske).

II. OCJENA STANJA, OSNOVNA PITANJA KOJA TREBA UREDITI ZAKONOM TE POSLJEDICE KOJE ĆE PROISTEĆI DONOŠENJEM ZAKONA

Donošenje predmetnog Zakona proizlazi iz obveza Republike Hrvatske (u daljnjem tekstu: RH) kao članice Europske unije (u daljnjem tekstu: EU) za prijenos Direktive o mjerama za visoku zajedničku razinu sigurnosti mrežnih i informacijskih sustava 2016/1148 donesene 6. srpnja 2016. (u daljnjem tekstu: NIS direktiva) u nacionalno zakonodavstvo.

NIS direktiva nastala je na temelju provedbe EU strategije kibernetičke sigurnosti donesene 7. veljače 2013. godine (Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, 7.2.2013, JOIN(2013)1 final). Tekst NIS direktive je tri godine usuglašavan između Vijeća, Komisije, Parlamenta EU i država članica, kako bi obuhvatio nužni minimalni opseg bitnih društvenih i gospodarskih sektora država članica koji je potreban za široku i ubrzanu inicijativu razvoja digitalnog gospodarstva EU. Time se uvode zajedničke mjere u svim državama članicama za postizanje visoke razine zaštite kibernetičke sigurnosti i koordinaciju postupanja niza potrebnih dionika na nacionalnim i sektorskim razinama država članica.

NIS direktiva je dio široke digitalne inicijative EU–a, kojom se svijest o nužnosti razvoja digitalnog gospodarstva širi kroz niz segmenata suvremenog društva, kroz aktualni proces stvaranja jedinstvenog digitalnog tržišta EU–a, zatim niz inicijativa za jačanje sigurnosne svijesti o kibernetičkom prostoru, kao i putem poticanja razvoja javno–privatnog partnerstva i elektroničkih usluga u državnoj upravi i gospodarstvu. Pritom NIS direktiva stvara primjerene okvire prevencije i zaštite društva od kibernetičkih ugroza zajedničkim pristupom svih država članica koje osiguravaju usklađene vertikalne sektorske pristupe u NIS direktivi, dok nova EU regulativa zaštite osobnih podataka (GDPR) sličan pristup osigurava horizontalnim funkcionalnim pristupom kroz sve segmente društva u cjelini.

Temeljni cilj NIS direktive je osigurati u svim državama članicama zajedničku razinu sigurnosti mrežnih i informacijskih sustava čije bi neispravno funkcioniranje uslijed sigurnosnih incidenata moglo imati snažne posljedice na društvo ili nacionalnu ekonomiju. Pritom NIS direktiva uvodi regulativne elemente koji omogućavaju trajno praćenje stanja automatiziranosti i digitalizacije utvrđenih sektora.

NIS direktiva utvrđuje obvezu država članica uvesti mjere za visoku razinu zaštite kibernetičke sigurnosti u sljedećim sektorima: energetika – električna energija, nafta, plin; prijevoz – zračni, željeznički, vodni, cestovni; bankarstvo; infrastrukture financijskog tržišta;

zdravstveni sektor; opskrba vodom za piće i njezina distribucija; digitalna infrastruktura – razmjena internetskog prometa, usluge naziva domena i kontrola vršne nacionalne domene.

Kako bi se osigurao temeljni cilj NIS direktive u svim državama članicama, kroz NIS direktivu je prepoznata i postavljena obveza državama članicama za donošenje nacionalne strategije kibernetičke sigurnosti.

Zahtjevi koji se postavljaju na nacionalne strategije država članica u ovom području prate se i analiziraju putem EU agencije ENISA, a Nacionalna strategija kibernetičke sigurnosti RH (Narodne novine, broj 108/15) prevedena je na engleski jezik te je raspoloživa, zajedno sa strategijama drugih država članica, na poveznici: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/strategies/croatian-cyber-security-strategy.

Hrvatska strategija kibernetičke sigurnosti zadovoljava potrebne zahtjeve koji se postavljaju NIS direktivom u odnosu na strateške nacionalne okvire za ostvarivanje ciljeva i zahtjeva u kibernetičkom prostoru kao virtualnoj dimenziji društva.

Na sličan način kao i EU strategija, koja je nadopunjena akcijskim planom i konkretnim zahtjevima koji proizlaze iz NIS direktive, i hrvatska strategija sadrži detaljan i strukturiran Akcijski plan za provedbu Nacionalne strategije kibernetičke sigurnosti, kao i uspostavljena strateška i operativna međuresorna nacionalna tijela za upravljanje provedbom strategije i rješavanje svih bitnih nacionalnih pitanja u području kibernetičke sigurnosti (Narodne novine, broj 61/16). Ovaj postojeći nacionalni okvir koji čine Nacionalna strategija kibernetičke sigurnosti s pripadajućim Akcijskim planom za njenu provedbu, Prijedlogom zakona proširuje se dodatnim zahtjevima, koji su usklađeni, kako s postojećim hrvatskim nacionalnim okvirom kibernetičke sigurnosti, tako i sa zahtjevima koji proizlaze iz potrebe transpozicije NIS direktive u RH kao državi članici EU-a. Na taj način postojeći nacionalni organizacijski okvir koji je sukladan s EU zahtjevima, povezuje sva potrebna nacionalna tijela odgovarajućih nadležnosti s EU formatima strateških, operativnih ili sektorskih tijela, u okviru potreba definiranih NIS direktivom. Nacionalnom strategijom kibernetičke sigurnosti u RH su prepoznate i potrebe za razmjenom podataka između različitih dionika Strategije, za koordiniranim upravljanjem u krizama, za međusektorskom razmjenom najbolje sigurnosne prakse te prepoznavanjem rizika povezanih s osjetljivim podacima i infrastrukturama, čija izloženost potencijalnim ugrozama u kibernetičkom prostoru raste iz dana u dan.

Nacionalna strategija kibernetičke sigurnosti u smislu opsega predstavlja okvir hrvatskog društva u cjelini, a specifično se određuje nizom ciljeva i mjera prema javnom, akademskom i gospodarskom sektoru, kao i prema sektoru građanstva u cjelini. Upravo stoga, Strategija je uspostavila međuresorne okvire upravljanja povezivanjem ključnih dionika Strategije u Nacionalno vijeće za kibernetičku sigurnost te povezivanjem čitavog niza dionika provedbe Strategije iz različitih sektora društva. Prijedlogom zakona nacionalna nadležna tijela na strateškoj i operativnoj razini, kao i drugi dionici provedbe Strategije, uključuju se u odgovarajuće organizacijske okvire i provode potrebne zahtjeve EU-a kroz NIS direktivu.

Nacionalna strategija kibernetičke sigurnosti prepoznala je i široku potrebu prilagodbe različitih obrazovnih i drugih edukacijskih programa povezanih s kibernetičkom sigurnošću i kibernetičkim prostorom, kao i usklađenu potrebu podizanja razine sigurnosne svijesti u svim društvenim sektorima te je ciljeve i mjere Akcijskog plana u ovom području usmjerila na sve postojeće razine hrvatskog obrazovnog sustava, kao i na specijalizirane sektorske edukativne

institucije. Prepoznate su i mogućnosti koje se otvaraju za RH u području digitalnog gospodarstva te je sadržaj Nacionalne strategije kibernetičke sigurnosti usko koordiniran sa Strategijom pametne specijalizacije (Narodne novine, broj 32/16), s povezanim aktivnostima Hrvatske gospodarske komore, kao i s mogućnostima korištenja EU CEF fonda (Connecting European Facilities), koji će u 2018. biti usko povezan s primjenom NIS direktive te se njenom transpozicijom za države članice i njihovo gospodarstvo otvaraju dodatne mogućnosti.

Nacionalna strategija kibernetičke sigurnosti i Akcijski plan za njenu provedbu utemeljeni su na metodologiji kojom su opći ciljevi Strategije razrađeni na posebne ciljeve svakog od odabranih područja i poveznica područja kibernetičke sigurnosti, a za svaki posebni cilj utvrđene su u Akcijskom planu mjere za koje su definirani vremenski rokovi, odgovorna tijela – nositelji i sunositelji, kao i potrebna metrika za mjerenje provedbe mjera Akcijskog plana. Izvješće o provedbi početnog ciklusa Akcijskog plana u 2016. raspoloživo je na poveznici:
http://www.uvns.hr/UserDocsImages/dokumenti/informacijska-sigurnost/Izvjesce%20o%20provedbi%20Akcijskog%20plana%20za%20provedbu%20NSKS%20u%202016.pdf,
kao i inicijalno izvješće o osnivanju međuresornih nacionalnih tijela za upravljanje strategijom:
http://www.uvns.hr/UserDocsImages/dokumenti/informacijska-sigurnost/InicijalnoIzvjesceVijecaVladiRH_13062017.pdf.

Ubrzani proces digitalizacije različitih industrijskih sektora prepoznat je u NIS direktivi kao potencijalna prijetnja, ukoliko nije praćen odgovarajućim sigurnosnim mjerama. Stoga se NIS direktiva usmjerava na uvođenje mjera za postizanje visoke razine kibernetičke sigurnosti u odabranim sektorima te zahtijeva od država članica da u tu svrhu prepoznaju sve ključne usluge koje pripadaju tim sektorima. Prepoznavanje ključnih usluga potrebno je provesti neovisno o trenutnom stanju digitalizacije pojedinih sektora, jer se njihova ovisnost o mrežnim i informacijskim sustavima može pojaviti u budućnosti.

Provedba odgovarajućih mjera prema NIS direktivi obvezna je samo za slučajeve kada ključna usluga operatora na tržištu ovisi o mrežnim i informacijskim sustavima, no, postupak prepoznavanja operatora ključnih usluga odnosno njihove ovisnosti o mrežnim i informacijskim sustavima potrebno je redovito provoditi i ažurirati popis takvih operatora.

Stoga, prvu skupinu obveznika zahtjeva iz NIS direktive čine operatori koji pružaju ključne usluge za društvo ili nacionalnu ekonomiju (Operators of Essential Services – OES), u okviru utvrđenih sedam NIS sektora koji su ranije navedeni.

Drugu skupinu obveznika primjene mjera utvrđenih NIS direktivom čine davatelji digitalnih usluga (Digital Service Providers – DSP).

Digitalne usluge definirane su u NIS direktivi kao: internetsko tržište, internetske tražilice i usluge računalstva u oblaku, koje su od primarne važnosti za jedinstveno digitalno tržište EU–a. Upravo stoga donesena je Provedbena uredba Komisije (EU) 2018/151 od 30. siječnja 2018. o utvrđivanju pravila za primjenu Direktive (EU) 2016/1148 Europskog parlamenta i Vijeća u odnosu na dodatne specifikacije elemenata koje pružatelji digitalnih usluga moraju uzeti u obzir u upravljanju rizicima kojima je izložena sigurnost njihovih mrežnih i informacijskih sustava i parametara za utvrđivanje ima li incident znatan učinak (SL

L 26/48, 31.1.2018.) – dalje u tekstu: Provedbena uredba Komisije, kojom se na jedinstven način detaljnije reguliraju obveze u odnosu na tri definirane vrste digitalnih usluga iz NIS direktive u svim državama članicama.

Budući da važećim propisima nisu već od ranije u RH uvedene obveze koje bi bile kompatibilne sa svim zahtjevima NIS direktive te bi njezino prenošenje u važeće propise zahtijevalo dopune i izmjene više zakonskih (sektorskih) propisa, izrađen je ovaj Prijedlog zakona, kojim se namjerava na jedinstveni način urediti navedena materija.

NIS direktiva, uz obvezu uvođenje tehničkih i organizacijskih mjera za upravljanje rizicima i mjera za sprečavanje i svođenje na najmanju moguću mjeru učinaka incidenata na sigurnost mrežnih i informacijskih sustava, uvodi i obvezu obavješćivanja o incidentima koji mogu imati znatan učinak na kontinuitet u pružanju usluga.

Iako su rizici u NIS direktivi usmjereni prvenstveno na mrežne i informacijske sustave koji su u potpori ključnih usluga u odabranim sektorima, odnosno digitalnim uslugama, incidenti, prema definiciji iz NIS direktive obuhvaćaju široki, opći opseg svih kategorija mogućih incidenata (kvarova, nesreća i napada), koji mogu imati negativni učinak na sigurnost mrežnih i informacijskih sustava korištenih u realizaciji ključnih usluga ili digitalnih usluga.

Kriteriji za određivanje incidenata koji imaju znatan učinak na davanje digitalnih usluga propisani su Provedbenom uredbom Komisije.

Kriteriji za određivanje incidenata koji imaju znatan učinak na pružanje ključnih usluga, sadržaj obavijesti o incidentima, kod operatora ključnih usluga i davatelja digitalnih usluga, način dostave obavijesti i druga pitanja bitna za postupanje s takvim obavijestima predlaže se urediti podzakonskim propisom. Stoga je Prijedlogom zakona, radi potpunog prijenosa NIS direktive u nacionalno zakonodavstvo, predviđeno donošenje podzakonskog akta, uredbe Vlade RH.

Države članice dužne su donijeti i objaviti zakone i druge propise koji su potrebni za usklađivanje s NIS direktivom do 9. svibnja 2018. te o tome odmah obavijestiti Europsku komisiju.

Također, države članice dužne su najkasnije do 9. studenoga 2018., a nakon toga svake dvije godine, Europskoj komisiji dostavljati podatke koji su potrebni kako bi se Komisiji omogućila procjena provedbe NIS direktive.

Prijedlogom zakona preuzimaju se obveze iz NIS direktive koje su u odgovornosti država članica te se na prikladan način povezuje nacionalno stanje RH u području kibernetičke sigurnosti te postojeće nadležnosti u svakom od NIS sektora u okviru RH te su stoga u Prijedlogu zakona primijenjeni prilagođeni kriteriji i pridružena primjerena nadležna tijela, kako bi se postigli željeni rezultati u odnosu na stvarno stanje koje postoji u predmetnim sektorima u RH.

Izričaj Prijedloga zakona obuhvaća svu potrebnu različitost javnih i privatnih subjekata koji su ili nadležna tijela, ili obveznici primjene ovog Zakona. Prijedlog zakona pri tome prati NIS direktivom zadanu metodologiju koja se primjenjuje na složeni postupak identifikacije operatora ključnih usluga u svim sektorima te uređuje sva bitna pitanja koja su

dana u nadležnost država članica. Istovremeno, Prijedlogom zakona se u slučaju davatelja digitalnih usluga prenose sve relevantne odredbe NIS direktive te se u provedbi referira na provedbeni propis Europske Komisije koji će se izravno primjenjivati na sve države članice. Prijedlogom zakona uvode se zahtjevi koji se postavljaju kao mjere za postizanje visoke razine kibernetičke sigurnosti operatora ključnih usluga i koji su usmjereni na osiguravanje kontinuiteta definiranih ključnih usluga u NIS direktivom zadanim sektorima u RH. U tu svrhu, Prijedlogom zakona obuhvaćene su tehničke i organizacijske mjere za upravljanje rizicima, kao i mjere za sprečavanje i ublažavanje učinaka incidenata, ali i obveza sustavnog obavješćivanja o incidentima i njihovog koordiniranog rješavanja na sektorskoj, nacionalnoj i EU razini. Predmetne mjere (za operatore ključnih usluga) i razrada obveze izvješćivanja o incidentima (za operatore ključnih usluga i davatelje digitalnih usluga) pobliže će se propisati ranije spomenutom uredbom Vlade RH odnosno provedbenim propisom Komisije (za davatelje digitalnih usluga).

Prijedlogom zakona u potpunosti se regulira sustav nadležnih tijela na nacionalnoj razini i njegovo povezivanje s nadležnim tijelima EU i država članica, kao i potrebna nacionalna koordinacija na sektorskim razinama. Pritom se određuju funkcionalnosti zahtijevane na EU razini od svih država članica, kao što su to Jedinstvena nacionalna kontaktna točka, CSIRT tijela i njihova sektorska nadležnost, odnosno nadležna sektorska tijela odgovorna za provedbu nadzora nad primjenom prenesenih obveza iz NIS direktive, koristeći pri tome u najvećoj mogućoj mjeri postojeće nadležnosti i funkcionalnosti središnjih državnih tijela i drugih tijela u RH.

Jedinstvena nacionalna kontaktna točka objedinjava niz funkcionalnosti koje upotpunjavaju ulogu koju predloženo tijelo već ima u RH vezano uz provedbu Nacionalne strategije kibernetičke sigurnosti, odnosno rad Nacionalnog vijeća za kibernetičku sigurnost, dok su CSIRT nadležnosti pridjeljenje postojećim tijelima koja imaju odgovarajuće sposobnosti u tom području djelovanja.

Izbor nadležnih sektorskih tijela prati postojeće nadležnosti središnjih državnih tijela u područjima koji obuhvaćaju zadane NIS sektore, proširujući u određenoj mjeri postojeće nadzorne ovlasti tih tijela na područje primjene ovog Zakona te se oslanjajući na već regulirane revizijske procese u sektorima u kojima postoji obveza revizije, uz prikladno redefiniranje revizijskog procesa u omjeru koji je potreban za potpuni prijenos obveza iz NIS direktive.

Kako bi se uskladili uvjeti u vrlo raznorodnim i regulativno različito uređenim sektorima po pitanju provedbe revizije odnosno njezine procjene u nadzornim postupcima, uvedena je i uloga tehničkog tijela za ocjenu sukladnosti, prvenstveno za slučajeve u kojima revizija nije obvezujuća za pružatelje odnosno davatelje usluga iz NIS direktive.

Pored sektora koji su kao obvezujući predviđeni već samom NIS direktivom kao područja u kojima države članice moraju uvesti nove obveze odnosno prilagoditi postojeće, Prijedlogom zakona se predlaže uključivanje još jednog sektora koji obuhvaća poslovne usluge za središnja državna tijela (e–Građani, kao i elektroničke poslovne aplikacije državne riznice ili centralnog obračuna plaća državnih službenika). Ovaj sektor nije zadan NIS direktivom, ali je prepoznat i kroz Nacionalnu strategiju kibernetičke sigurnosti (područje elektroničke uprave) kao visoko digitaliziran i vrlo osjetljiv zbog kumulacije velikih i različitih fondova podataka cjelokupnog stanovništva i/ili njegovih pojedinih segmenata u digitalnom obliku. Osim toga, u sklopu digitalne inicijative EU, u proceduri je i Prijedlog

uredbe Europskog parlamenta i Vijeća o uspostavi jedinstvenog digitalnog pristupnika kao izvora informacija koji će omogućiti pristup na prostoru cjelokupne EU prema elektroničkim uslugama državne administracije svih država članica, što će dodatno postaviti proširene zahtjeve prema postojećim elektroničkim uslugama hrvatske državne uprave.

Kako bi se ispunila temeljna svrha NIS direktive odnosno uspostavila sustavna koordinacija svih relevantnih dionika, kao i razvila svijest o mogućim ugrozama u kibernetičkom prostoru te prikladno upravljalo rizicima i razmjerno rizicima provodile mjere zaštite, prema NIS direktivi nužno je predvidjeti i odgovarajuće prekršajne odredbe kojima bi se obuhvatilo one subjekte koji ne postupaju u skladu sa zahtjevima Zakona.

Prekršajne odredbe i prikladno povezani nadzor vezuju se na postojeće nadzorne ovlasti u pojedinim sektorima koje imaju nadležna sektorska tijela, dok su sami prekršaji sustavno grupirani u tri razine prema ozbiljnosti prekršaja.

Prijedlogom zakona se na sustavan način koriste postojeći kapaciteti i potencijali prepoznati Nacionalnom strategijom kibernetičke sigurnosti i povezuju se sa zahtjevima koji proizlaze iz NIS direktive te se na sveobuhvatan i učinkovit način uključuju u postojeću strukturu nacionalnih međuresornih tijela, Nacionalnog vijeća za kibernetičku sigurnost i Operativno–tehničke koordinacije za kibernetičku sigurnost. Takav pristup zahtijeva usklađeno djelovanje svih tijela uključenih u procese uređene ovim Prijedlogom zakona, ali istovremeno omogućava međusobno komplementarno djelovanje različitih subjekata u širokom opsegu pokrivanja društvenih i gospodarskih sektora, čime se ostvaruje učinkovita uporaba svih resursa i ostvaruje sinergija djelovanja svih uključenih dionika.

To će omogućiti usklađeno i optimalno usmjeravanje proračunskih sredstava, korištenje EU fondova i za javni i za privatni sektor, kao i izbjegavanje neracionalnog multipliciranja kapaciteta ili neracionalnosti u pristupu opremanju radi razvoja novih sposobnosti koje već postoje u drugim tijelima. Važno je napomenuti da je u okviru provedbe NIS direktive planirano i korištenje sredstava iz EU fondova (npr. Connecting European Facilities – CEF), a slijedom iskustva i odobrenja hrvatskog projekta GrowCERT, koji je pokrenut 2017. i vrijedan 1 mil. EUR, uz sufinanciranje iz CEF fonda na razini 75% (nositelj CARNet – Nacionalni CERT). U 2018.g., prema najavi Europske komisije i nakon prijenosa NIS direktive u nacionalno zakonodavstvo, očekuje se mogućnost apliciranja i korištenja CEF fonda i za pravne osobe – sektorske operatore, putem nadležnih sektorskih tijela.

Kombiniranjem postojećih centraliziranih funkcionalnosti kibernetičke sigurnosti koje je Vlada RH uspostavila kroz Nacionalno vijeće za kibernetičku sigurnost i Prijedlogom zakona predloženim povezivanjem tijela nadležnih za sektore obuhvaćene Prijedlogom zakona, stvara se organizirani i upravljani sustav u kibernetičkom prostoru RH koji se direktno veže na puno širi sustav domovinske sigurnosti, odnosno kritičnih nacionalnih sektora i nacionalnog kriznog upravljanja, ostvarujući pri tome potrebnu sinergiju djelovanja između fizičke i virtualne dimenzije suvremenog društva.

Ovim Prijedlogom zakona osigurava se provedba obveza RH iz NIS direktive, osiguravaju se potrebne pretpostavke za trajno unaprjeđenje stanja kibernetičke sigurnosti u širokom opsegu društvenih i gospodarskih sektora koji su obuhvaćeni njegovom primjenom, ali se istovremeno potiče i razvoj RH u području digitalnog gospodarstva usklađenim pristupom između niza dionika iz javnog i privatnog sektora. Time se otvaraju mogućnosti za učinkovitiji zajednički pristup i sinergiju djelovanja državnog, akademskog i gospodarskog

sektora, prvenstveno u razvoju novih hrvatskih proizvoda i usluga sukladnih s jedinstvenim zahtjevima za cijelo područje Europske unije.

III. OCJENA I IZVORI SREDSTAVA POTREBNIH ZA PROVEDBU ZAKONA

Za provedbu ovog Zakona bit će potrebno osigurati određena dodatna sredstva u državnom proračunu Republike Hrvatske ovisno o: 1. stanju postojećih kapaciteta nadležnih tijela, 2. broju obveznika provedbe zahtjeva iz ovog Zakona te 3. realizaciji plana korištenja sredstava EU fondova osiguranih u svrhu provedbe NIS direktive u državama članicama.

PRIJEDLOG ZAKONA O KIBERNETIČKOJ SIGURNOSTI OPERATORA KLJUČNIH USLUGA I DAVATELJA DIGITALNIH USLUGA

DIO PRVI

OSNOVNE ODREDBE

Cilj i predmet

Članak 1.

(1) Ovim se Zakonom uređuju postupci i mjere za postizanje visoke zajedničke razine kibernetičke sigurnosti operatora ključnih usluga i davatelja digitalnih usluga, nadležnosti i ovlasti nadležnih sektorskih tijela, jedinstvene nacionalne kontaktne točke, tijela nadležnih za prevenciju i zaštitu od incidenata (dalje u tekstu: nadležni CSIRT) i tehničkog tijela za ocjenu sukladnosti, nadzor nad operatorima ključnih usluga i davateljima digitalnih usluga u provedbi ovog Zakona i prekršajne odredbe.

(2) Cilj je ovog Zakona osigurati provedbu mjera za postizanje visoke zajedničke razine kibernetičke sigurnosti u davanju usluga koje su od posebne važnosti za odvijanje ključnih društvenih i gospodarskih aktivnosti, uključujući funkcioniranje digitalnog tržišta.

(3) Sastavni su dio ovog Zakona:
a) Prilog I. – Popis ključnih usluga s kriterijima i pragovima za donošenje ocjene o važnosti negativnog učinka incidenta
b) Prilog II. – Popis digitalnih usluga
c) Prilog III. – Popis nadležnih tijela.

Usklađenost s propisima Europske unije

Članak 2.

Ovim Zakonom u hrvatsko zakonodavstvo preuzima se sljedeći akt Europske unije:
– Direktiva 2016/1148 Europskog parlamenta i Vijeća od 6. srpnja 2016. o mjerama za visoku zajedničku razinu sigurnosti mrežnih i informacijskih sustava širom Unije (SL L 194, 19.7.2016.).

Primjena

Članak 3.

(1) Ovaj Zakon primjenjuje se na operatore ključnih usluga, neovisno o tome jesu li u pitanju javni ili privatni subjekti, neovisno o državi njihova sjedišta, njihovoj veličini, ustroju i vlasništvu.

(2) Davatelji digitalnih usluga podliježu nadležnostima i ovlastima propisanim ovim Zakonom ako na teritoriju Republike Hrvatske imaju sjedište ili svog predstavnika te pod uvjetom da takav davatelj ne predstavlja mikro ili mali subjekt malog gospodarstva kako su

oni definirani zakonom kojim se uređuju osnove za primjenu poticajnih mjera gospodarske politike usmjerenih razvoju, restrukturiranju i tržišnom prilagođavanju malog gospodarstva.

Odnos propisa prema drugim propisima

Članak 4.

(1) Ako u provedbi ovog Zakona nastaju ili se koriste klasificirani podaci ili se obrađuju osobni podaci, na takve podatke primjenjuju se posebni propisi o njihovoj zaštiti.

(2) Primjena ovog Zakona ne utječe na prava potrošača, koja su uređena posebnim zakonom.

(3) Ako su za pojedini sektor s Popisa iz Priloga I. ovog Zakona posebnim zakonom propisane mjere koje po svom sadržaju i svrsi odgovaraju zahtjevima iz ovog Zakona, ili predstavljaju strože zahtjeve, na pružatelje ključnih usluga koji pripadaju tom sektoru primjenjuju se odgovarajuće odredbe tog posebnog zakona.

Pojmovi

Članak 5.

U smislu ovog Zakona pojedini pojmovi imaju sljedeće značenje:

1) *„kibernetička sigurnost“* – je sustav organizacijskih i tehničkih aktivnosti i mjera kojima se postiže autentičnost, povjerljivost, cjelovitost i dostupnost podataka, kao i mrežnih i informacijskih sustava u kibernetičkom prostoru
2) *„kibernetički prostor“* – je virtualni prostor unutar kojeg se odvija komunikacija izmedu mrežnih i informacijskih sustava te obuhvaća sve mrežne i informacijske sustave neovisno o tome jesu li povezani na Internet
3) *„mrežni i informacijski sustav“* – je (a) elektronička komunikacijska mreža kako je ona definirana zakonom kojim se uređuje područje elektroničkih komunikacija; (b) bilo koji uređaj ili grupa povezanih ili srodnih uređaja, od kojih jedan ili više njih programski izvršava automatsku obradu digitalnih podataka ili (c) digitalni podaci koji se pohranjuju, obraduju, dobivaju ili prenose elementima opisanim u točkama (a) i (b) u svrhu njihova rada, uporabe, zaštite i održavanja
4) *„sigurnost mrežnih i informacijskih sustava”* – je sposobnost mrežnih i informacijskih sustava da, na određenoj razini pouzdanosti, odolijevaju bilo kojoj radnji koja ugrožava dostupnost, autentičnost, cjelovitost ili povjerljivost, pohranjenih, prenesenih ili obrađenih podataka, ili srodnih usluga koje ti mrežni i informacijski sustavi nude ili kojima omogućuju pristup
5) *„nacionalna strategija kibernetičke sigurnosti”* – je okvir kojim se pružaju strateški ciljevi i prioriteti za kibernetičku sigurnost na nacionalnoj razini
6) *„nadležna tijela“* – su nadležna sektorska tijela, jedinstvena nacionalna kontaktna točka, nadležni CSIRT–ovi i tehnička tijela za ocjenu sukladnosti
7) *„operator ključnih usluga“* – je bilo koji javni ili privatni subjekt koji ispunjava kriterije iz članka 6. ovog Zakona
8) *„davatelj digitalnih usluga”*– je bilo koji privatni subjekt koji pruža neku digitalnu uslugu s Popisa iz Priloga II. ovog Zakona u Europskoj uniji
9) *“javni subjekti“* – su tijela državne uprave, druga državna tijela, jedinice lokalne i područne (regionalne) samouprave te pravne osobe koje imaju javne ovlasti ili obavljaju javnu službu

10) *„privatni subjekti“* – su fizičke i pravne osobe koje pružaju ili daju usluge,
11) *„sjedište“* – je stalno mjesto poslovanja gdje pružatelj odnosno davatelj usluga u neodređenom vremenskom razdoblju upravlja svojom djelatnošću
12) *„predstavnik“* – je bilo koja fizička ili pravna osoba sa sjedištem u Republici Hrvatskoj koju je davatelj digitalnih usluga koji nema sjedište u Europskoj uniji izričito imenovao da djeluje u njegovo ime i kojoj se nadležno sektorsko tijelo ili nadležni CSIRT mogu obratiti umjesto davatelju digitalnih usluga koji je obveznik primjene ovog Zakona
13) *„incident”* – je bilo koji događaj koji ima stvaran negativni učinak na sigurnost mrežnih i informacijskih sustava
14) *„rješavanje incidenta”* – su svi postupci koji podupiru otkrivanje, analizu i zaustavljanje incidenta te odgovor na njega
15) *„rizik”* – je bilo koja razumno prepoznatljiva okolnost ili događaj koji ima potencijalno negativni učinak na sigurnost mrežnih i informacijskih sustava
16) *„središte za razmjenu internetskog prometa (IXP)”* – je mrežni instrument koji omogućuje međusobno povezivanje više od dvaju neovisnih autonomnih sustava, prvenstveno u svrhu olakšavanja razmjene internetskog prometa; IXP pruža međusobno povezivanje samo za autonomne sustave; za IXP nije potrebno da internetski promet između bilo kojih dvaju autonomnih sustava sudionika prođe kroz bilo koji treći autonomni sustav, on takav promet ne mijenja i ne utječe na njega ni na koji drugi način
17) *„sustav naziva domena (DNS)”* – je hijerarhijsko raspoređeni sustav imenovanja na mreži koji odgovara na upite o nazivima domena
18) *„pružatelj DNS usluge”* – je javni ili privatni subjekt koji pruža DNS usluge na Internetu
19) *„registri naziva vršnih domena”* – su javni ili privatni subjekti koji upravljaju i rukuju registracijom naziva internetskih domena za određenu vršnu domenu (TLD)
20) *„internetsko tržište”* – je digitalna usluga koja potrošačima i/ili trgovcima, kako su oni definirani zakonom kojim se uređuje alternativno rješavanje potrošačkih sporova, omogućuje da na Internetu sklapaju kupoprodajne ugovore i ugovore o uslugama s trgovcima na mrežnoj stranici tog internetskog tržišta ili na mrežnoj stranici tog trgovca koji se služi računalnim uslugama koje pruža internetsko tržište
21) *„internetska tražilica”* – je digitalna usluga koja korisniku omogućuje da pretražuje u načelu sve internetske stranice ili internetske stranice na određenom jeziku na temelju upita o bilo kojoj temi u obliku ključne riječi, rečenice ili nekog drugog unosa, a rezultat su poveznice na kojima se mogu pronaći informacije koje su povezane sa zatraženim sadržajem
22) *„usluga računalstva u oblaku”* – je digitalna usluga kojom se pruža pristup nadogradivom i elastičnom skupu djeljivih računalnih resursa, usluga i aplikacija
23) *„država članica“* – država članica Europske unije
24) *“kvalificirani revizor“* – je fizička ili pravna osoba koja je za obavljanje poslova revizije sigurnosti mrežnih i informacijskih sustava akreditirana pri odgovarajućoj organizaciji za normizaciju, koja je izdala ili daje na korištenje norme koje su u okviru provedbe zahtjeva iz ovog Zakona primijenjene kod određenog operatora ključnih usluga ili davatelja digitalnih usluga
25) *„revizija sigurnosti mrežnih i informacijskih sustava“* – su postupci koje obavlja kvalificirani revizor radi ocjene usklađenosti uspostavljenih procesa upravljanja mrežnim i informacijskim sustavom i dokumentiranih sigurnosnih politika sa zahtjevima iz ovog Zakona
26) *„CSIRT“* – je kratica za Computer Security Incident Response Team, odnosno tijelo nadležno za prevenciju i zaštitu od incidenata, za koju se u Republici Hrvatskoj koristi i kratica CERT (Computer Emergency Response Team).

DIO DRUGI

OPERATORI KLJUČNIH USLUGA I DIGITALNE USLUGE

Određivanje operatora ključnih usluga

Članak 6.

Pojedini javni ili privatni subjekt (dalje u tekstu: subjekt) odredit će se operatorom ključnih usluga ako:

a) subjekt pruža neku od ključnih usluga s Popisa iz Priloga I. ovog Zakona (dalje: ključna usluga)
b) pružanje ključne usluge kod tog subjekta ovisi o mrežnim i informacijskim sustavima i
c) incident bi imao znatan negativan učinak na pružanje ključne usluge.

Identifikacijski postupak

Članak 7.

(1) Nadležna sektorska tijela provode postupak identifikacije operatora ključnih usluga po sektorima s Popisa iz Priloga I. ovog Zakona, u kojem:

a) izrađuju popise svih subjekata koji pružaju ključnu uslugu
b) provode izdvajanje subjekta ovisno o važnosti negativnog učinka koji bi incident imao na pružanje ključne usluge kod tog subjekta i
c) za sve izdvojene subjekte provode procjenu ovisnosti pružanja ključne usluge o mrežnim i informacijskim sustavima.

(2) Nadležno sektorsko tijelo dužno je postupak identifikacije operatora ključnih usluga provoditi redovito, sukladno tržišnim promjenama u sektoru, a najmanje jednom u dvije godine.

Određivanje važnosti negativnog učinka incidenta

Članak 8.

(1) Za određivanje važnosti negativnog učinka koji bi incident imao na pružanje ključne usluge uzimaju se u obzir sljedeći kriteriji:

- broj i vrsta korisnika kojima subjekt pruža uslugu
- postojanje ovisnosti drugih djelatnosti ili područja o pružanju usluge
- tržišni udio subjekta koji pruža uslugu
- zemljopisna raširenost subjekta u pružanju usluge
- mogući utjecaj incidenta, s obzirom na njegovu težinu i trajanje, na gospodarske i društvene aktivnosti te na javnu sigurnost
- važnosti poslovanja subjekta za održavanje dostatne razine ključne usluge, uzimajući u obzir i raspoloživost alternativnih sredstava za pružanje te usluge ili
- drugi sektorski kriteriji poput količine pružene usluge, udjela u pružanju usluge ili imovine subjekta.

(2) Kriteriji iz stavka 1. ovog članka, i kriterijski pragovi, ako su definirani, primjenjuju se u postupku identifikacije operatora ključnih usluga, prema njihovom razvrstavanju po ključnim uslugama kako je to predviđeno Popisom iz Priloga I. ovog Zakona.

(3) Ako subjekt koji pruža ključnu uslugu ispunjava kriterije prema Popisu iz Priloga I. ovog Zakona te dostiže kriterijski prag, kada je on Popisom definiran, daje se ocjena važnosti negativnog učinka incidenta na pružanje ključne usluge za tog subjekta te se subjekt izdvaja za provođenje procjene ovisnosti pružanja ključne usluge o mrežnim i informacijskim sustavima.

Procjena ovisnosti o mrežnom i informacijskom sustavu

Članak 9.

(1) Ako se utvrdi da subjekt iz članka 8. stavka 3. ovog Zakona koristi mrežni i informacijski sustav za potporu pružanju ključne usluge te da prekid rada ili neispravno funkcioniranje tog sustava može dovesti do prekida u pružanju usluge ili na drugi način negativno utjecati na kvalitetu i/ili obujam usluge, nadležno sektorsko tijelo donosi odluku o određivanju tog subjekta operatorom ključnih usluga.

(2) Iznimno od stavka 1. ovog članka, nadležno sektorsko tijelo može odnijeti odluku o određivanju subjekta operatorom ključne usluge neovisno o kriterijima s Popisa iz Priloga I. ovog Zakona, ako u postupku identifikacije utvrdi da subjekt pruža ključnu uslugu u dvije ili više država članica te da ovisnost o mrežnom i informacijskom sustavu subjekta u pružanju usluge može zbog toga imati negativan prekogranični učinak na kontinuitet u pružanju usluge.

(3) Nadležno sektorsko tijelo, radi utvrđivanja kritičnosti prekograničnog učinka iz stavka 2. ovog članka, u suradnji s jedinstvenom kontaktnom točkom provodi savjetovanja s nadležnim tijelom uključene države članice.

Obavijest o identifikaciji

Članak 10.

Nadležno sektorsko tijelo dostavlja identificiranom operatoru ključne usluge obavijest o odluci iz članka 9. ovog Zakona u roku od osam dana od dana njezina donošenja.

Dostava podataka za potrebe postupka identifikacije operatora ključne usluge

Članak 11.

(1) Svaki subjekt koji pruža neku od ključnih usluga dužan je nadležnom sektorskom tijelu, na njegov zahtjev, dostaviti podatke koji su mu potrebni za provođenje postupka identifikacije operatora ključnih usluga.

(2) U zahtjevu iz stavka 1. ovog članka obvezno se navodi svrha zahtjeva, naznaka podataka koji su tijelu potrebni i rok za dostavu podataka.

(3) Subjekti kod kojih nastupe promjene u odnosu na podatke dostavljene sukladno stavku 2. ovog članka, dužni su nadležnom sektorskom tijelu dostaviti obavijest o tim promjenama ako bi one mogle utjecati na određivanje statusa subjekta u postupku identifikacije operatora ključne usluge.

(4) Obavijesti iz stavka 3. ovog članka dostavljaju se u roku od sedam dana od dana nastanka ili uvođenja promjene.

Popis operatora ključnih usluga

Članak 12.

(1) Na temelju odluka iz članka 9. ovog Zakona nadležna sektorska tijela izrađuju, preispituju i ažuriraju Popise operatora ključnih usluga po sektorima s Popisa iz Priloga I. ovog Zakona.

(2) Nadležna sektorska tijela obavješćuju jedinstvenu nacionalnu kontaktnu točku o broju identificiranih operatora ključnih usluga u pojedinom sektoru, s naznakom njihove važnosti za sektor.

Digitalne usluge

Članak 13.

Digitalne usluge na čije se davatelje odnosi ovaj Zakon utvrđene su Popisom iz Priloga II. ovog Zakona.

DIO TREĆI

MJERE ZA POSTIZANJE VISOKE RAZINE KIBERNETIČKE SIGURNOSTI OPERATORA KLJUČNIH USLUGA I DAVATELJA DIGITALNIH USLUGA

Obveza provedbe mjera

Članak 14.

(1) Operatori ključnih usluga i davatelji digitalnih usluga dužni su, radi osiguranja kontinuiteta u obavljanju tih usluga, poduzimati mjere za postizanje visoke razine kibernetičke sigurnosti svojih usluga.

(2) Mjere iz stavka 1. ovog članka sastoje se minimalno od:
- tehničkih i organizacijskih mjera za upravljanje rizicima, uzimajući pri tome u obzir najnovija tehnička dostignuća koja se koriste u okviru najbolje sigurnosne prakse u području kibernetičke sigurnosti i
- mjera za sprečavanje i ublažavanje učinaka incidenata na sigurnost mrežnih i informacijskih sustava.

Mjere za upravljanje rizikom operatora ključnih usluga

Članak 15.

Operatori ključnih usluga dužni su poduzimati tehničke i organizacijske mjere za upravljanje rizicima koje moraju obuhvatiti mjere za:

- utvrđivanje rizika od incidenata
- sprječavanje, otkrivanje i rješavanje incidenata i
- ublažavanje učinka incidenata na najmanju moguću mjeru.

Mjere za upravljanje rizikom davatelja digitalnih usluga

Članak 16.

Davatelji digitalnih usluga dužni su prilikom poduzimanja tehničkih i organizacijskih mjera za upravljanje rizicima voditi računa osobito o:

- sigurnosti sustava i objekata
- rješavanju incidenata
- upravljanju kontinuitetom poslovanja
- praćenju, reviziji i testiranju
- sukladnosti s međunarodnim standardima.

Opseg primjene mjera

Članak 17.

(1) Operatori ključnih usluga dužni su mjere za postizanje visoke razine kibernetičke sigurnosti provoditi u odnosu na mrežni i informacijski sustav, ili njegov dio, za koji je u postupku identifikacije operatora ključne usluge utvrđeno da o njemu ovisi pružanje ključne usluge kod dotičnog subjekta.

(2) Davatelji digitalnih usluga dužni su mjere za postizanje visoke razine kibernetičke sigurnosti provoditi u odnosu na mrežni i informacijski sustav koji kod njih podržava digitalnu uslugu.

Primjena mjera prema procjeni rizika

Članak 18.

Operatori ključnih usluga i davatelji digitalnih usluga primjenjuju mjere za sprečavanje i ublažavanje učinaka incidenata razmjerno riziku kojemu je izložen njihov mrežni ili informacijski sustav.

Odgovornost za primjenu mjera

Članak 19.

Operatori ključnih usluga i davatelji digitalnih usluga dužni su provoditi mjere za postizanje visoke razine kibernetičke sigurnosti bez obzira na to upravljaju li i/ili održavaju svoje mrežne i informacijske sustave sami ili za to koriste vanjskog davatelja usluge.

Utvrđivanje mjera

Članak 20.

(1) Mjere za postizanje visoke razine kibernetičke sigurnosti operatora ključnih usluga i način njihove provedbe pobliže se propisuju uredbom koju donosi Vlada Republike Hrvatske (dalje u tekstu: Vlada).

(2) Mjere za postizanje visoke razine kibernetičke sigurnosti davatelja digitalnih usluga provode se sukladno Provedbenoj uredbi Komisije (EU) 2018/151 od 30. siječnja 2018. o utvrđivanju pravila za primjenu Direktive (EU) 2016/1148 Europskog parlamenta i Vijeća u odnosu na dodatne specifikacije elemenata koje pružatelji digitalnih usluga moraju uzeti u obzir u upravljanju rizicima kojima je izložena sigurnost njihovih mrežnih i informacijskih sustava i parametara za utvrđivanje ima li incident znatan učinak (SL L 26/48, 31.1.2018.).

DIO ČETVRTI

OBAVJEŠĆIVANJE O INCIDENTIMA

Obveza obavješćivanja

Članak 21.

(1) Operatori ključnih usluga i davatelji digitalnih usluga dužni su nadležni CSIRT, bez neopravdane odgode, obavješćivati o incidentima koji imaju znatan učinak na kontinuitet usluga koje pružaju.

(2) Ako je incident na mrežnom i informacijskom sustavu davatelja digitalne usluge imao znatan učinak na pružanje neke ključne usluge, operator ključne usluge dužan je o tom incidentu obavijestiti nadležni CSIRT.

(3) Obveza obavješćivanja iz ovog članka odnosi se na incidente na mrežnim i informacijskim sustavima iz članka 17. ovog Zakona.

Kriteriji za određivanje učinka incidenata

Članak 22.

(1) Kriteriji za određivanje incidenata koji imaju znatan učinak na pružanje ključnih usluga propisuju se uredbom Vlade iz članka 20. stavka 1. ovog Zakona.

(2) Kriteriji za određivanje incidenata koji imaju znatan učinak na davanje digitalnih usluga propisani su Provedbenom uredbom Komisije iz članka 20. stavka 2. ovog Zakona.

Obavijesti o incidentima

Članak 23.

Sadržaj obavijesti o incidentima iz članka 21. ovog Zakona, način dostave obavijesti i druga pitanja bitna za postupanje s takvim obavijestima uređuju se uredbom Vlade iz članka 20. stavka 1. ovog Zakona.

Informiranje javnosti o incidentu

Članak 24.

(1) Nadležni CSIRT može, po prethodno provedenom savjetovanju s operatorom ključne usluge i nadležnim sektorskim tijelom, obavijestiti javnost o pojedinačnim incidentima koji imaju znatan učinak na kontinuitet usluge koju operator pruža, ako je osviještenost javnosti nužna za sprečavanje širenja i jačanja učinka incidenta ili za rješavanje incidenta koji je u tijeku.

(2) Nadležni CSIRT te, prema potrebi, CSIRT–ovi drugih pogođenih država članica, mogu javnost obavijestiti o pojedinačnim incidentima koji imaju znatan učinak na kontinuitet pojedine digitalne usluge ili zatražiti od davatelja digitalnih usluga da to učini, ako je objavljivanje informacije o incidentu u javnome interesu, osobito ako je to potrebno radi sprečavanja širenja i jačanja učinka incidenta ili rješavanja incidenta koji je u tijeku.

DIO PETI

NADLEŽNA TIJELA

Nadležna sektorska tijela

Članak 25.

(1) Nadležna sektorska tijela utvrđena su Popisom iz Priloga III. ovog Zakona.

(2) Nadležna sektorska tijela obavljaju sljedeće poslove:
- provode postupke identifikacije operatora ključnih usluga sukladno ovome Zakonu
- obavljaju nadzor operatora ključnih usluga i davatelja digitalnih usluga u provedbi mjera za postizanje visoke razine kibernetičke sigurnosti i ispunjavanju drugih obveza iz ovog Zakona
- međusobno surađuju i razmjenjuju iskustva u provedbi ovog Zakona
- surađuju i razmjenjuju relevantne informacije s drugim nadležnim tijelima iz ovog Zakona
- surađuju i razmjenjuju relevantne informacije s tijelom za zaštitu osobnih podataka, kada su osobni podaci ugroženi zbog incidenta na mrežnom i informacijskom sustavu operatora ključne usluge odnosno davatelja digitalne usluge, odnosno s pravosudnim tijelima, kada je takav incident rezultat kriminalnih aktivnosti.

Nadzor

Članak 26.

(1) Nadzor nad operatorom ključnih usluga provodi se najmanje jednom svake dvije godine.

(2) Nadzor nad operatorom ključnih usluga provest će se i prije proteka roka iz stavka 1. ovog članka, ako nadležno sektorsko tijelo utvrdi ili zaprimi informacije koje ukazuju na to da operator ključne usluge ne izvršava svoje obveze iz ovog Zakona.

(3) Nadzor nad davateljem digitalnih usluga provodi se isključivo nakon što nadležno sektorsko tijelo zaprimi informacije koje ukazuju na to da davatelj digitalne usluge ne postupa sukladno Provedbenoj uredbi Komisije iz članka 20. stavka 2. ovog Zakona i/ili odredbama ovog Zakona.

(4) Nadležno sektorsko tijelo za davatelje digitalnih usluga provodi nadzor uz podršku nadležnog tehničkog tijela za ocjenu sukladnosti i nadležnog CSIRT-a.

Obveze operatora ključnih usluga i davatelja digitalnih usluga u okviru nadzora

Članak 27.

(1) Operatori ključnih usluga i davatelji digitalnih usluga dužni su u okviru nadzora nadležnom sektorskom tijelu, na njegov zahtjev, dostaviti:

- podatke potrebne za procjenu razine sigurnosti njihovih mrežnih i informacijskih sustava, uključujući dokumentirane sigurnosne politike i
- dokaze o učinkovitoj provedbi sigurnosnih mjera.

(2) Učinkovita provedba sigurnosnih mjera dokazuje se ili rezultatima revizije sigurnosti mrežnih i informacijskih sustava koju je obavio kvalificirani revizor ili ocjenom sukladnosti mrežnih i informacijskih sustava koju daje tehničko tijelo za ocjenu sukladnosti.

(3) U zahtjevu iz stavka 1. ovog članka obvezno se navodi svrha zahtjeva, naznaka podataka koji su nadležnom sektorskom tijelu potrebni za provođenje nadzora i rok za dostavu podataka.

(4) Operatori ključnih usluga i davatelji digitalnih usluga dužni su u okviru nadzora nadležnom sektorskom tijelu, na njegov zahtjev, omogućiti neposredan pristup svojim objektima i sustavima koji im služe za potporu u obavljanju ključnih odnosno digitalnih usluga.

(5) Nadležno sektorsko tijelo nadzor davatelja digitalne usluge, koji ima sjedište ili svog predstavnika u RH, a čiji se mrežni i informacijski sustavi nalaze u drugoj ili više država članica, može provoditi u suradnji s nadležnim tijelima tih država članica.

Predmet nadzora

Članak 28.

(1) U okviru nadzora, nadležna sektorska tijela nadziru pravilnost provedbe propisanih:
- mjera za postizanje visoke razine kibernetičke sigurnosti
- obveza vezanih uz obavješćivanje o incidentima i
- drugih postupanja prema zahtjevima nadležnih tijela koja se podnose sukladno ovom Zakonu ili propisu donesenom na temelju ovog Zakona.

(2) U provedbi nadzora, nadležna sektorska tijela:
- izdaju obvezujuću uputu operatoru ključnih usluga kada utvrde da on:
  a) ne provodi mjere za postizanje visoke razine kibernetičke sigurnosti i/ili da ne izvršava druge obveze iz ovog Zakona ili
  b) da postoje nedostaci u provedbi mjera odnosno izvršavanju obveza iz ovog Zakona
- izdaju naloge davatelju digitalnih usluga za otklanjanje svakog utvrđenog nepoštivanja provedbenog propisa Europske komisije iz članka 20. stavka 2. ovog Zakona i/ili odredbi ovog Zakona
- podnose optužne prijedloge.

(3) Nadležna sektorska tijela dužna su u aktima iz članka 2. podstavka 1. i 2. ovog članka naznačit rok za postupanje.

Obavljanje nadzora

Članak 29.

Nadzor obavljaju inspektori, nadzornici i supervizori, u skladu s nadležnostima koje proizlaze iz propisa o ustrojstvu i djelokrugu rada tih tijela te drugih propisa koji određuju njihovu nadležnost.

Jedinstvena nacionalna kontaktna točka

Članak 30.

Jedinstvena nacionalna kontaktna točka:
- dostavlja Europskoj komisiji podatke koji omogućavaju procjenu učinkovitosti provedbe mjera iz ovog Zakona i propisa donesenog na temelju ovog Zakona, sukladno zahtjevima utvrđenim propisom iz članka 2. ovog Zakona
- sudjeluje u radu Skupine za suradnju, koja je 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,
- jednom godišnje podnosi Skupini za suradnju sažeto izvješće o zaprimljenim obavijestima o incidentima, među ostalim o broju obavijesti i naravi incidenata o kojima ih se obavijestilo te o radnjama poduzetim u skladu s člankom 21. i člankom 32. stavkom 1. točkama 8., 10. i 11. ovog Zakona, osim za sektor usluga u sustavima državne informacijske infrastrukture

- na zahtjev nadležnog CSIRT–a, obavijesti o incidentima iz članka 21. ovog Zakona prosljeđuje jedinstvenim kontaktnim točkama drugih pogođenih država članica, osim za sektor poslovnih usluga za središnja državna tijela
- izrađuje smjernice o sadržaju obavijesti, načinu i rokovima informiranja jedinstvene nacionalne kontaktne točke o broju identificiranih operatora ključnih usluga i naznakama njihove važnosti te o obavijestima o incidentima
- vodi brigu o potrebi razvoja i usklađivanja nacionalne strategije kibernetičke sigurnosti s ciljevima ovog Zakona i zahtjevima Europske unije u području kibernetičke sigurnosti
- surađuje s drugim nadležnim tijelima iz ovog Zakona,
- kada je to potrebno, savjetuje se i surađuje s tijelom za zaštitu osobnih podataka i pravosudnim tijelima.

Članak 31.

Jedinstvena nacionalna kontaktna točka je Ured Vijeća za nacionalnu sigurnost.

Zadaće nadležnog CSIRT–a

Članak 32.

(1) Nadležni CSIRT na sektorskoj razini, prema popisu nadležnosti iz Priloga III. ovog Zakona, obavlja sljedeće poslove:

- prati incidente
- pruža rana upozorenja i najave te informira o rizicima i incidentima
- provodi dinamičku analizu rizika i incidenata te izrađuje pregled situacije u sektoru
- provodi redovite provjere ranjivosti mrežnih i informacijskih sustava operatora ključnih usluga odnosno davatelja digitalnih usluga
- prima obavijesti o incidentima
- na zahtjev operatora ključnih usluga odnosno davatelja digitalnih usluga analizira i odgovara na incidente
- ako to dopuštaju okolnosti, nakon primitka obavijesti o incidentu dostavlja operatoru ključnih usluga relevantne informacije u pogledu daljnjeg postupanja po njegovoj obavijesti, a osobito informacije koje bi mogle doprinijeti djelotvornom rješavanju incidenta
- donosi smjernice za ujednačavanje i unapređenje stanja provedbe obveze obavješćivanja o incidentima iz članka 21. ovog Zakona
- informira nadležno sektorsko tijelo o incidentima iz članka 21. ovog Zakona
- u suradnji s nadležnim sektorskim tijelom, određuje prekogranične utjecaje incidenata iz članka 21. ovog Zakona
- informira jedinstvenu nacionalnu kontaktnu točku o incidentima iz članka 21. ovog Zakona, sukladno njezinim smjernicama
- dostavlja jedinstvenoj nacionalnoj kontaktnoj točki podatke o glavnim elementima postupaka rješavanja incidenata koje provodi,
- obavješćuje nadležni CSIRT druge pogođene države članice ili više njih o incidentu iz članka 21. ovog Zakona na mrežnom i informacijskom sustavu operatora ključnih usluga ako incident ima znatan učinak na kontinuitet ključnih usluga u toj državi članici,
- obavješćuje nadležni CSIRT druge pogođene države članice ili više njih o incidentu iz članka 21. ovog Zakona na mrežnom i informacijskom sustavu pružatelja digitalnih usluga ako se incident odnosi na dvije ili više država članica

- surađuje s drugim CSIRT–ovima na nacionalnoj i međunarodnoj razini
- sudjeluje u Mreži CSIRT–ova na razini Europske unije koja je osnovana s ciljem razvoja povjerenja i pouzdanja među državama članicama te promicanju brze i učinkovite operativne suradnje
- promiče usvajanje i primjenu zajedničkih ili normiranih praksi za postupke rješavanja incidenata i rizika te planove za klasifikaciju incidenata, rizika i informacija.

(2) Operatori ključnih usluga i davatelji digitalnih usluga dužni su surađivati s nadležnim CSIRT–om i s njim razmjenjivati potrebne informacije u postupku rješavanja incidenata.

(3) Nadležni CSIRT u obavljanju svojih zadaća iz ovog Zakona ne može snositi odgovornost za štetu uzrokovanu incidentom na mrežnim i informacijskim sustavima operatora ključnih usluga i davatelja digitalnih usluga.

Osiguravanje uvjeta za obavljanje poslova nadležnog CSIRT–a

Članak 33.

Nadležni CSIRT je dužan:

- osigurati visoku razinu dostupnosti svojih usluga komuniciranja izbjegavanjem jedinstvenih točki prekida, uz raspoloživost sredstava za mogućnost dvosmjernog kontaktiranja te jasno određenim i poznatim komunikacijskim kanalima za njihove klijente i suradnike
- svoje prostore i informacijske sustave za potporu smjestiti na sigurne lokacije i
- osigurati kontinuitet rada na način da:
  a) je opremljen odgovarajućim sustavom za upravljanje zahtjevima i njihovim preusmjeravanjem, kako bi se olakšale primopredaje
  b) ima dovoljno zaposlenika kako bi se na odgovarajući način osigurala dostupnost u svako doba
  c) se oslanja na infrastrukturu čiji je kontinuitet osiguran te su im u tu svrhu dostupni redundantni sustavi i rezervni radni prostor.

Tehničko tijelo za ocjenu sukladnosti

Članak 34.

(1) Tehničko tijelo za ocjenu sukladnosti provodi periodičke provjere mjera iz članka 14. ovog Zakona poduzetih nad sigurnošću mrežnih i informacijskih sustava operatora ključnih usluga i davatelja digitalnih usluga, ako reviziju sigurnosti mrežnih i informacijskih sustava ne obavlja kvalificirani revizor.

(2) Tehnička tijela za ocjenu sukladnosti određena su Popisom s Priloga III. ovog Zakona.

Zahtjev za ocjenu sukladnosti

Članak 35.

(1) Tehničko tijelo za ocjenu sukladnosti provodi provjere iz članka 34. ovog Zakona na zahtjev nadležnog sektorskog tijela ili samog operatora ključnih usluga, odnosno davatelja digitalnih usluga.

(2) Nadležno sektorsko tijelo podnosi zahtjev iz stavka 1. ovog članka kada utvrdi da revizija sigurnosti mrežnih i informacijskih sustava kod pojedinog operatora ključne usluge odnosno davatelja digitalne usluge nije provedena ili da ju nije proveo kvalificirani revizor.

(3) Operator ključne usluge, odnosno davatelj digitalnih usluga može podnijeti zahtjev za ocjenu sukladnosti kada ne postoji obveza revizije subjekta prema posebnom propisu.

Dostava podataka u postupku ocjene sukladnosti

Članak 36.

(1) Operatori ključnih usluga i davatelji digitalnih usluga dužni su tehničkom tijelu za ocjenu sukladnosti, na njegov zahtjev, dostaviti podatke potrebne za procjenu razine sigurnosti njihovih mrežnih i informacijskih sustava te im omogućiti pristup svojim objektima i sustavima koji im služe za potporu u obavljanju ključnih odnosno digitalnih usluga.

(2) U zahtjevu iz stavka 1. ovog članka obvezno se navodi svrha zahtjeva, naznaka podataka koji su tijelu potrebni i rok za dostavu podataka.

Izvješće o ocjeni sukladnosti

Članak 37.

(1) Tehničko tijelo za ocjenu sukladnosti nakon provedene provjere iz članka 34. ovog Zakona izrađuje izvješće o provjeri mjera za postizanje visoke razine sigurnost mrežnih i informacijskih sustava, koje sadrži:

- ocjenu sukladnosti, ukoliko utvrdi da operator ključne usluge odnosno davatelj digitalne usluge učinkovito provodi mjere za postizanje visoke razine kibernetičke sigurnosti ili
- korektivne mjere za postizanje učinkovite provedbe mjera za postizanje visoke razine kibernetičke sigurnosti, s naznakom roka njihova izvršenja.

(2) Tehničko tijelo za ocjenu sukladnosti dostavlja izvješće iz stavka 1. ovog članka, bez odgode nadležnom sektorskom tijelu i operatoru ključnih usluga, odnosno davatelju digitalnih usluga.

Završno izvješće o ocjeni sukladnosti

Članak 38.

(1) Operator ključnih usluga, kao i davatelj digitalnih usluga, dužan je, u zadanom roku, provesti korektivne mjere i o tome, bez odlaganja, obavijestiti tehničko tijelo za ocjenu sukladnosti.

(2) Tehničko tijelo za ocjenu sukladnosti će po primitku obavijesti iz stavka 1. ovog članka, kao i u slučaju neprovođenja ili nepotpunog provođenja korektivnih mjera, izraditi završno izvješće o provedenoj provjeri iz članka 34. ovog Zakona koje će dostaviti nadležnom sektorskom tijelu radi provođenja nadzora.

Obavijest o onemogućavanju ili otežavanju provedbe ocjene sukladnosti

Članak 39.

Ako operator ključnih usluga i davatelj digitalnih usluga odbije omogućiti ili neopravdano odgađa ili otežava provedbu povjere iz članka 34. ovog Zakona, tehničko tijelo za ocjenu sukladnosti će o tome bez odgode izvijestiti nadležno sektorsko tijelo.

DIO ŠESTI

ZAŠTITA PODATAKA

Članak 40.

(1) Popisi operatora ključnih usluga, kao i svi drugi podaci koji nastaju u okviru provedbe ovog Zakona koriste se isključivo u svrhu izvršavanja zahtjeva iz ovog Zakona.

(2) Popis i podaci iz stavka 1. ovog članka predstavljaju informacije u odnosu na koje je moguće ograničiti pravo pristupa korisniku informacija, ovisno o rezultatima testa razmjernosti i javnog interesa koji se provodi prema odredbama posebnog zakona o pravu na pristup informacijama.

(3) Nadležna tijela dužna su pri razmjeni podataka iz stavka 1. ovog članka voditi računa o potrebi ograničavanja pristupa podacima kada je to potrebno u svrhu sprječavanja, otkrivanja, provođenja istraživanja i vođenja kaznenog postupka.

Članak 41.

Nadležna tijela iz ovog Zakona dužna su s podacima operatora ključnih usluga i davatelja digitalnih usluga postupati u skladu sa zahtjevima povjerljivosti, ako su oni utvrđeni posebnim propisima o zaštiti takvih podataka.

DIO SEDMI

PREKRŠAJNE ODREDBE

Članak 42.

(1) Novčanom kaznom u iznosu od 150.000,00 do 500.000,00 kuna kaznit će se za prekršaj pravna osoba – operator ključne usluge koji:

- ne postupi po obvezujućoj uputi nadležnog sektorskog tijela iz članka 28. stavka 2. podstavka 1. ovog Zakona
- odbije dostaviti ili neopravdano odgađa dostavljati obavijesti o incidentima iz članka 21. ovog Zakona.

(2) Novčanom kaznom u iznosu od 50.000,00 do 150.000,00 kuna kaznit će se za prekršaj iz stavka 1. ovog članka fizička osoba obrtnik ili osoba koja obavlja drugu samostalnu djelatnost.

(3) Novčanom kaznom u iznosu od 15.000,00 do 50.000,00 kuna kaznit će se za prekršaj iz stavka 1. ovog članka i odgovorna osoba u pravnoj osobi i odgovorna osoba u javnom subjektu.

Članak 43.

(1) Novčanom kaznom u iznosu od 150.000,00 do 500.000,00 kuna kaznit će se za prekršaj pravna osoba – davatelj digitalne usluge koji:

- ne postupi po danom nalogu nadležnog sektorskog tijela iz članka 28. stavka 2. podstavka 2. ovog Zakona
- odbije dostaviti ili neopravdano odgađa dostavljati obavijesti o incidentima iz članka 21. ovog Zakona.

(2) Novčanom kaznom u iznosu od 50.000,00 do 150.000,00 kuna kaznit će se za prekršaj iz stavka 1. ovog članka fizička osoba obrtnik ili osoba koja obavlja drugu samostalnu djelatnost.

(3) Novčanom kaznom u iznosu od 15.000,00 do 50.000,00 kuna kaznit će se za prekršaj iz stavka 1. ovog članka i odgovorna osoba u pravnoj osobi i odgovorna osoba u javnom subjektu.

Članak 44.

(1) Novčanom kaznom u iznosu od 50.000,00 do 100.000,00 kuna kaznit će se za prekršaj pravna osoba – operator ključne usluge i davatelj digitalne usluge koji:

- odbije postupiti ili neopravdano ne postupi po zahtjevu iz članka 27. ovog Zakona
- odbije omogućiti ili neopravdano odgađa ili otežava postupanje tehničkog tijela za ocjenu sukladnosti po zahtjevu iz članka 35. stavka 2. ovog Zakona.

(2) Novčanom kaznom u iznosu od 20.000,00 do 50.000,00 kaznit će se za prekršaj iz stavka 1. ovog članka fizička osoba obrtnik ili osoba koja obavlja drugu samostalnu djelatnost.

(3) Novčanom kaznom u iznosu od 10.000,00 do 25.000,00 kuna kaznit će se za prekršaj iz stavka 1. ovog članka i odgovorna osoba u pravnoj osobi i odgovorna osoba u javnom subjektu.

Članak 45.

(1) Novčanom kaznom u iznosu od 15.000,00 do 50.000,00 kuna kaznit će se za prekršaj pravna osoba – subjekt koji pruža neku od ključnih usluga koji:

- ne postupi po zahtjevu nadležnog sektorskog tijela za dostavu podataka iz članka 11. stavka 1. ovog Zakona
- ne dostavlja obavijesti o promjenama u roku iz članka 11. stavka 4. ovog Zakona.

(2) Novčanom kaznom u iznosu od 5.000,00 do 25.000,00 kuna kaznit će se za prekršaj iz stavka 1. ovog članka fizička osoba obrtnik ili osoba koja obavlja drugu samostalnu djelatnost.

(3) Novčanom kaznom u iznosu od 2.000,00 do 20.000,00 kuna kaznit će se za prekršaj iz stavka 1. ovog članka i odgovorna osoba u pravnoj osobi i odgovorna osoba u javnom subjektu.

DIO OSMI

PRIJELAZNE I ZAVRŠNE ODREDBE

Članak 46.

Vlada će Uredbu iz članka 20. stavka 1. ovog Zakona donijeti u roku od 30 dana od dana stupanja na snagu ovog Zakona.

Članak 47.

(1) Nadležna sektorska tijela dužna su postupak identifikacije operatora ključnih usluga provesti u roku od 90 dana od dana stupanja na snagu ovog Zakona.

(2) Nadležna sektorska tijela dužna su jedinstvenoj nacionalnoj kontaktnoj točki dostaviti obavijesti iz članka 12. stavka 2. ovog Zakona u roku od 120 dana od dana stupanja na snagu ovog Zakona.

Članak 48.

(1) Operatori ključnih usluga dužni su provesti mjere za osiguravanje visoke razine kibernetičke sigurnosti u roku od 12 mjeseci od dana dostave obavijesti iz članka 10. ovog Zakona.

(2) Operatori ključnih usluga dužni su započeti s dostavom obavijesti iz članka 21. ovog Zakona 30 dana od dana dostave obavijesti iz članka 10. ovog Zakona.

Članak 49.

(1) Davatelji digitalnih usluga dužni su se uskladiti sa zahtjevima Provedbene uredbe Komisije iz članka 20. stavka 2. ovog Zakona u roku propisanom tom Uredbom.

(2) Davatelji digitalnih usluga dužni su započeti s dostavom obavijesti iz članka 21. ovog Zakona 120 dana od dana stupanja na snagu ovog Zakona.

Članak 50.

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

Prilog I.

Popis ključnih usluga s kriterijima i pragovima za utvrđivanje važnosti negativnog učinka incidenta:

Sektor	Podsektor	Ključna usluga	Kriteriji za utvrđivanje važnosti negativnog učinka incidenta	Pragovi za utvrđivanje važnosti negativnog učinka incidenta
Energetika	Električna energija	**Proizvodnja električne energije**	Instalirana snaga proizvodnog postrojenja	300 MW
		Prijenos električne energije	Bez iznimke	–
		Distribucija električne energije	Prekid napajanja	Više od 100.000 obračunskih mjernih mjesta
			Ovisnosti drugih djelatnosti ili područja o pružanju usluge	Distribucija za: ▪ bolnice ▪ zračne luke i kontrole leta ▪ objekte banaka s podatkovnim centrima ▪ policijske uprave ▪ vojne lokacije ▪ aktivna vodocrpilišta i centre upravljanja ▪ objekte operatora telekomunikacijskog sustava ▪ objekte tijela sigurnosno–obavještajnog sustava, ▪ objekte profesionalnih vatrogasnih postrojbi, ▪ objekte Državne uprave za zaštitu i spašavanje (Služba 112) ili ▪ objekte određene nacionalnom kritičnom infrastrukturom
	Nafta	**Transport nafte naftovodima**	Bez iznimke	–

Sektor	Podsektor	Ključna usluga	Kriteriji za utvrđivanje važnosti negativnog učinka incidenta	Pragovi za utvrđivanje važnosti negativnog učinka incidenta
		Proizvodnja nafte	Proizvedeno nafte pojedinog naftnog polja u tonama godišnje	50.000 t/god
		Proizvodnja naftnih derivata	Proizvedeno naftnih derivata pojedine rafinerije u tonama godišnje	Motorni benzini: 200.000 t/god Dizelsko gorivo: 200.000 t/god Plinska ulja: 100.000 t/god
		Skladištenje nafte i naftnih derivata	Ukupni skladišni kapacitet nafte pojedinog terminala u m^3	1.000.000 m^3
			Ukupni skladišni kapacitet naftnih derivata pojedinog skladišta (na istoj lokaciji) u m^3	60.000 m^3
	Plin	**Distribucija plina**	Broj krajnjih kupaca priključen na distribucijski sustav	Više od 100.000 obračunskih mjernih mjesta.
		Transport plina	Bez iznimke	
		Skladištenje plina	Potrošnja plina u RH, u kWh	25% potrošnje plina u RH u prethodnoj godini
		Prihvat i otprema UPP–a	Kapacitet uplinjavanja UPP u m^3/h	Više od 500.000 m^3/h
		Proizvodnja prirodnog plina	Godišnja proizvodnja plina predana u transportni sustav na pojedinom ulazu, u kWh	1.000.000 kWh
Prijevoz	Zračni promet	**Zračni prijevoz putnika i tereta**	Udio putnika pojedinog zračnog prijevoznika na bilo kojem nacionalnom aerodromu koji ima promet putnika veći od 2.000.000 godišnje (ključni aerodrom)	Zračni prijevoznik koji imao udio veći od 30% na ključnom aerodromu

Sektor	Podsektor	Ključna usluga	Kriteriji za utvrđivanje važnosti negativnog učinka incidenta	Pragovi za utvrđivanje važnosti negativnog učinka incidenta
		Upravljanje infrastrukturom zračne luke, uključujući upravljanje pomoćnim objektima zračne luke	Ukupni godišnji promet putnika pojedine zračne luke	Više od 2.000.000 putnika
		Kontrola zračnog prometa	Otvorenost područja letnih informacija Zagreb (FIR Zagreb) – bez iznimke	–
			Broj operacija na godišnjem nivou	Ukupno 500.000 operacija za FIR Zagreb
	Željeznički promet	**Upravljanje i održavanje željezničke infrastrukture, uključujući upravljanje prometom i prometno–upravljačkim i signalno–sigurnosnim podsustavom**	Upravitelj željezničke infrastrukture za javni prijevoz – bez iznimke	
		Usluge prijevoza robe i/ili putnika željeznicom	Broj voznih jedinica (vlakova)	20 dnevno
		Upravljanje uslužnim objektima i pružanje usluga u uslužnim objektima	Broj voznih jedinica (vlakova)	20 dnevno
		Pružanje dodatnih usluga koje su nužne za pružanje usluga prijevoza robe ili putnika željeznicom	Broj voznih jedinica (vlakova)	20 dnevno
	Vodni prijevoz	**Nadzor kretanja brodova (VTS usluga)**	Godišnji broj dolazaka brodova iz međunarodne plovidbe	najmanje 4.000

Sektor	Podsektor	Ključna usluga	Kriteriji za utvrđivanje važnosti negativnog učinka incidenta	Pragovi za utvrđivanje važnosti negativnog učinka incidenta
			Godišnji broj putovanja brodova u domaćem prometu, uključujući obalni linijski promet	najmanje 200.000
		Obavljanje poslova pomorske radijske službe	Godišnji broj dolazaka brodova iz međunarodne plovidbe	najmanje 4.000
			Godišnji broj putovanja brodova u domaćem prometu, uključujući obalni linijski promet	najmanje 200.000
		Održavanje objekata sigurnosti plovidbe	Bez iznimke	–
		Prijevoz putnika u međunarodnom i/ili domaćem prometu	Broj putnika godišnje	1.000.000
	Vodni prijevoz	**Ukrcaj i iskrcaj tereta u lukama u međunarodnom i domaćem prometu**	Količina tereta godišnje u tonama	2.500.000
		Prijevoz putnika, tereta i vozila u unutarnjim morskim vodama i teritorijalnom moru Republike Hrvatske koji se obavlja na unaprijed utvrđenim linijama prema javno objavljenim uvjetima reda plovidbe i cjenikom usluga	Broj korisnika	15% ukupno prevezenih putnika i/ili vozila godišnje
			Tržišni udio	Minimalno 15% tržišnog udjela

Sektor	Podsektor	Ključna usluga	Kriteriji za utvrđivanje važnosti negativnog učinka incidenta	Pragovi za utvrđivanje važnosti negativnog učinka incidenta
		Praćenje i lociranje plovila u unutarnjoj plovidbi	Broj plovila na unutarnjim plovnim putovima u Republici Hrvatskoj tijekom godine	100
		Obavijesti brodarstvu u unutarnjoj plovidbi	Broj izdanih obavijesti brodarstvu tijekom godine	100
		Pristup elektroničkim navigacijskim kartama u unutarnjoj plovidbi	Pokrivenost unutarnjih vodnih putova u Republici Hrvatskoj	Pokrivenost 500 riječnih km
		Baza podataka o trupu plovila u unutarnjoj plovidbi	Broj plovila unesenih u bazu podataka tijekom godine	50
		Međunarodno elektroničko izvještavanje u unutarnjoj plovidbi	Broj ERI poruka upućenih prema RIS centrima dnevno	50
	Cestovni prijevoz	**Javni prijevoz putnika**	Broj voznih jedinica	100
			Broj putnika godišnje	5.000.000
		Korištenje cestovne infrastrukture	Upravitelj ceste na TEN–T mreži – bez iznimke	–
			Broj vozila na glavnoj cesti koja vodi do središta naseljenog mjesta većeg od 35.000 stanovnika	20.000 PGDP (prosječni godišnji dnevni promet)
			Zemljopisna raširenost korištenja usluga	Teritorij cijele države ili grada većeg od 35.000 stanovnika
		Upravljanje prometnim tokovima ili informiranje vozača (ITS)	Uspostavljen centar za kontrolu i upravljanje prometom 24/7 – bez iznimke	
			Uspostavljen centar za informiranje vozača o stanju u prometu 24/7– bez iznimke	
			Broj prometnih svjetala (semafora) u sustavu	100

Sektor	Podsektor	Ključna usluga	Kriteriji za utvrđivanje važnosti negativnog učinka incidenta	Pragovi za utvrđivanje važnosti negativnog učinka incidenta
			Zemljopisna raširenost korištenja usluga	Teritorij cijele države ili grada većeg od 35.000 stanovnika
Bankarstvo		**Platne usluge**	Globalno sistemski važne kreditne institucije i ostale sistemski važne kreditne institucije	–
Infrastrukture financijskog tržišta		**Usluge mjesta trgovanja**	Bez iznimke	–
		Usluge središnjih drugih ugovornih strana (CCP)	Bez iznimke	–
Zdravstveni sektor		**Primarna zdravstvena zaštita**	Centralni zdravstveni informacijski sustav Hrvatske – bez iznimke	–
			Pokrivenost pružatelja primarne zdravstvene zaštite odobrenim programskim rješenjem	40%
			Broj intervencija u izvanbolničkoj djelatnosti hitne medicine po županijama godišnje	70.000
			Broj zdravstvenih djelatnika zaposlenih u domu zdravlja	500
		Sekundarna zdravstvena zaštita	Zdravstvena VPN mreža HealthNet – bez iznimke	–
			Pokrivenost pružatelja sekundarne zdravstvene zaštite odobrenim programskim rješenjem	40%
			Broj obavljenih zdravstvenih postupaka, pregleda ili pretraga godišnje	1.000.000
			Broj zdravstvenih djelatnika zaposlenih u općoj bolnici	800

Sektor	Podsektor	Ključna usluga	Kriteriji za utvrđivanje važnosti negativnog učinka incidenta	Pragovi za utvrđivanje važnosti negativnog učinka incidenta
		Tercijarna zdravstvena zaštita	Broj postelja u stacionarnim djelatnostima kliničkog bolničkog centra	900
			Broj postelja u stacionarnim djelatnostima kliničke bolnice	300
			Broj postelja u stacionarnim djelatnostima klinike	80
		Transfuzijska medicina i transplantacija organa	Broj prikupljenih doza pune krvi godišnje	100.000
			Broj donora organa na milijun stanovnika godišnje	30
			Broj transplantacijskih zahvata na milijun stanovnika godišnje	80
		Zdravstveno osiguranje i prekogranična zdravstvena zaštita	Broj osiguranih osoba u obveznom zdravstvenom osiguranju (OZO)	4.000.000
			Broj osiguranih osoba u dopunskom zdravstvenom osiguranju (DZO)	2.000.000
			Broj upita za provjerom statusa obveznog i dopunskog zdravstvenog osiguranja dnevno	100.000
			Broj izdanih Europskih kartica zdravstvenog osiguranja (EKZO) godišnje	100.000
		Sigurnost hrane	Središnji informacijski sustav sanitarne inspekcije – bez iznimke	

Sektor	Podsektor	Ključna usluga	Kriteriji za utvrđivanje važnosti negativnog učinka incidenta	Pragovi za utvrđivanje važnosti negativnog učinka incidenta
		Zaštita od opasnih kemikalija	Broj sigurnosno–tehničkih listova pregledanih i uvrštenih u registar sigurnosno–tehničkih listova (STL) godišnje	9.000
			Broj opasnih kemikalija prikupljenih i uvrštenih u registar opasnih kemikalija proizvedenih ili uvezenih/unesenih na teritorij RH godišnje	400
		Distribucija i sigurnost lijekova i medicinskih proizvoda	Broj lijekova (uključujući cjepiva) stavljenih u promet u RH	3.000
			Broj medicinskih proizvoda (različitih klasa rizika) stavljenih u promet u RH	250.000
			Broj stanovnika / osiguranih osoba na broj distribucijskih centara	330.000
		Nadzor nad zaraznim bolestima te skladištenjem i distribucijom cjepiva	Nacionalni javnozdravstveni informacijski sustav – bez iznimke	–
			Procijepljenost stanovništva RH godišnje	80%
Opskrba vodom za piće i njezina distribucija		**Opskrba krajnjih korisnika**	Broj korisnika	20.000 priključaka kućanstava
Digitalna infrastruktura		**DNS usluga za .hr TLD**	Bez iznimke	–
		Registar naziva domena za .hr TLD	Bez iznimke	–

Sektor	Podsektor	Ključna usluga	Kriteriji za utvrđivanje važnosti negativnog učinka incidenta	Pragovi za utvrđivanje važnosti negativnog učinka incidenta
		Sustav za registriranje i administriranje sekundarne domene	Subjekt koji pruža ključnu uslugu, ima registriranu domenu preko registara i prepoznao je ovisnost svoje usluge o DNS sustavu.	–
			Broj registriranih domena	20 % od ukupnog broja registriranih domena (unutar .hr i com.hr)
		Usluga IXP	Broj spojenih autonomnih sustava	Veći od 15
Poslovne usluge za središnja državna tijela		**Usluge u sustavu e–Građani**	Broj jedinstvenih korisnika pojedine usluge	100.000
			Dostupnost usluge isključivo putem elektroničke usluge	Utvrđeno da ne postoji alternativni način korištenja usluge
		Poslovne usluge za korisnike državnog proračuna	Broj institucija koje nisu sektorski povezane	10

Prilog II.

Popis digitalnih usluga

1. Internetsko tržište
2. Internetska tražilica
3. Usluge računalstva u oblaku

Prilog III.

Popis nadležnih tijela

Jedinstvena nacionalna kontaktna točka – Ured Vijeća za nacionalnu sigurnost

Sektor	Nadležno sektorsko tijelo	CSIRT	Tehničko tijelo za ocjenu sukladnosti
Energetika	tijelo državne uprave nadležno za energetiku	Zavod za sigurnost informacijskih sustava	Zavod za sigurnost informacijskih sustava
Prijevoz	tijelo državne uprave nadležno za promet	Zavod za sigurnost informacijskih sustava	Zavod za sigurnost informacijskih sustava
Bankarstvo	Hrvatska narodna banka	Nacionalni CERT	–
Infrastrukture financijskog tržišta	Hrvatska agencija za nadzor financijskih usluga	Nacionalni CERT	–
Zdravstveni sektor	tijelo državne uprave nadležno za zdravstvo	Zavod za sigurnost informacijskih sustava	Zavod za sigurnost informacijskih sustava
Opskrba vodom za piće i njezina distribucija	tijelo državne uprave nadležno za vodno gospodarstvo	Zavod za sigurnost informacijskih sustava	Zavod za sigurnost informacijskih sustava
Digitalna infrastruktura	Središnji državni ured za razvoj digitalnog društva	Nacionalni CERT	Hrvatska akademska i istraživačka mreža – CARNet
Davatelji digitalnih usluga	tijelo državne uprave nadležno za gospodarstvo	Nacionalni CERT	Zavod za sigurnost informacijskih sustava
Poslovne usluge za središnja državna tijela	Središnji državni ured za razvoj digitalnog društva	Zavod za sigurnost informacijskih sustava ili Nacionalni CERT*	Zavod za sigurnost informacijskih sustava ili Nacionalni CERT**

*Napomena: Nadležni CSIRT za sektor Poslovne usluge za središnja državna tijela za sve usluge je Zavod za sigurnost informacijskih sustava, osim za područje koje je u djelokrugu središnjeg državnog tijela nadležnog za znanost i obrazovanje, Sveučilišnog računskog centra (SRCE) ili CARNeta, za koje je nadležni CSIRT Nacionalni CERT.

**Napomena: Tehničko tijelo za ocjenu sukladnosti za sektor Poslovne usluge za središnja državna tijela za sve usluge je Zavod za sigurnost informacijskih sustava, osim za područje koje je u djelokrugu središnjeg državnog tijela nadležnog za znanost i obrazovanje, Sveučilišnog računskog centra (SRCE) ili Hrvatske akademske i istraživačke mreže – CARNeta, za koje je tehničko tijelo za ocjenu sukladnosti Hrvatska akademska i istraživačka mreža – CARNet.

O B R A Z L O Ž E N J E

Člankom 1. utvrđuju se cilj i predmet ovog Zakona te se propisuje da se njime uređuju postupci i mjere za postizanje visoke zajedničke razine kibernetičke sigurnosti operatora ključnih usluga i davatelja digitalnih usluga, nadležnosti i ovlasti nadležnih sektorskih tijela, jedinstvene nacionalne kontaktne točke, tijela nadležnih za prevenciju i zaštitu od incidenata i tehničkog tijela za ocjenu sukladnosti, nadzor nad operatorima ključnih usluga i davateljima digitalnih usluga u provedbi Zakona te prekršajne odredbe. Ovim se člankom utvrđuju i prilozi, koji su sastavni dio Zakona, koji definiraju popis ključnih usluga s kriterijima i pragovima za donošenje ocjene o važnosti negativnog učinka incidenta, popis digitalnih usluga te popis nadležnih tijela.

Člankom 2. utvrđuje se da se Zakonom u pravni poredak RH prenosi Direktiva 2016/1148 Europskog parlamenta i Vijeća od 6. srpnja 2016. o mjerama za visoku zajedničku razinu sigurnosti mrežnih i informacijskih sustava širom Unije (SL L 194, 19.7.2016.) – u daljnjem tekstu: Direktiva 2016/1148.

Člankom 3. utvrđuje se primjena ovog Zakona na operatore ključnih usluga, neovisno o tome jesu li u pitanju javni ili privatni subjekti, neovisno o državi njihova sjedišta, njihovoj veličini, ustroju i vlasništvu, kao i na davatelje digitalnih usluga ako oni na teritoriju RH imaju sjedište ili svog predstavnika te pod uvjetom da takav davatelj ne predstavlja mikro ili mali subjekt malog gospodarstva kako su definirani Zakonom o poticanju razvoja malog gospodarstva.

Člankom 4. uređuje se odnos ovog Zakona prema drugim propisima, odnosno propisuje se primjena posebnih propisa ako u provedbi ovog Zakona nastaju ili se koriste klasificirani podaci ili se obrađuju osobni podaci. Primjena ovog Zakona ne utječe na prava potrošača, koja su uređena posebnim zakonom. Ako su posebnim zakonom propisane mjere za pojedini sektor s Popisa iz Priloga I. ovog Zakona koje po svom sadržaju i svrsi odgovaraju zahtjevima iz ovog Zakona, ili predstavljaju strože zahtjeve, na pružatelje ključnih usluga koji pripadaju tom sektoru, primjenjuju se odgovarajuće odredbe tog posebnog zakona.

Člankom 5. utvrđuju se značenja pojedinih pojmova u smislu ovog Zakona i to: kibernetička sigurnost, kibernetički prostor, mrežni i informacijski sustav, sigurnost mrežnih i informacijskih sustava, nacionalna strategija kibernetičke sigurnosti, nadležna tijela, operator ključnih usluga, davatelj digitalnih usluga, sjedište, javni subjekti, privatni subjekti, fizičke osobe, pravne osobe, predstavnik, incident, rješavanje incidenta, rizik, središte za razmjenu internetskog prometa (IXP), sustav naziva domena (DNS), pružatelj DNS usluge, registri naziva vršnih domena, internetsko tržište, internetska tražilica, usluga računalstva u oblaku, država članica, kvalificirani revizor, revizija sigurnosti mrežnih i informacijskih sustava te CSIRT.

Člankom 6. propisuju se uvjeti za određivanje operatora ključnih usluga koji pružaju neku od ključnih usluga odnosno usluga s Popisa iz Priloga I. Zakona.

Člankom 7. uređuje se postupak identifikacije operatora ključnih usluga po sektorima.

Člankom 8. utvrđuje se primjena kriterija u postupku identifikacije operatora ključnih usluga koje je potrebno uzeti u obzir prilikom određivanja važnosti negativnog učinka koji bi incident imao na pružanje ključne usluge, donošenje ocjene važnosti negativnog učinka incidenta na pružanje ključne usluge za tog subjekta te izdvajanje tog subjekta za provođenje procjene ovisnosti pružanja ključne usluge o mrežnim i informacijskim sustavima.

Člankom 9. propisuje se provođenje procjene ovisnosti o mrežnom i informacijskom sustavu, odnosno donošenje odluke nadležnog sektorskog tijela o određivanju subjekta operatorom ključnih usluga ako se utvrdi da izdvojeni subjekt koji pruža ključnu uslugu koristi mrežni i informacijski sustav za potporu pružanju ključne usluge, a prekid rada ili neispravno funkcioniranje tog sustava može dovesti do prekida u pružanju usluge ili na drugi način negativno utjecati na kvalitetu i/ili obujam usluge. Ovim člankom propisuje se i obveza uvažavanja prekograničnog utjecaja incidenta kao dodatnog kriterija u postupku identifikacije subjekta operatorom ključnih usluga, ako se utvrdi da subjekt pruža ključnu uslugu u dvije ili više država članica.

Člankom 10. propisuje se obveza izvješćivanja operatora ključne usluge o odluci nadležnog sektorskog tijela o identificiranju pojedinog subjekta operatorom ključne usluge, s rokom obavješćivanja od osam dana od dana donošenja odluke.

Člankom 11. propisuje se obveza dostave podataka koji su potrebni nadležnom sektorskom tijelu za provođenje postupka identifikacije operatora ključnih usluga te sadržaj zahtjeva za dostavom podataka. Propisuje se i obveza obavješćivanja nadležnog sektorskog tijela o promjenama koje su kod subjekta naknadno nastupile ako bi one mogle utjecati na određivanje statusa subjekta u postupku identifikacije operatora ključne usluge.

Člankom 12. propisuje se obveza izrade i redovitog ažuriranja popisa operatora ključnih usluga te izvješćivanja jedinstvene nacionalne kontaktne točku o broju identificiranih operatora ključnih usluga u pojedinom sektoru, s naznakom njihove važnosti za sektor.

Člankom 13. utvrđuju da se digitalne usluge, na čije se davatelje digitalnih usluga primjenjuje ovaj Zakon utvrđuju Popisom iz Priloga II. Zakona.

Člankom 14. propisuje se obveza primjene mjera za postizanje visoke razine kibernetičke sigurnosti usluga, njihova svrha i minimalni opseg.

Člankom 15. propisuje se opseg mjera za upravljanje rizikom operatora ključnih usluga. .

Člankom 16. utvrđuje se opseg primjene mjera za upravljanje rizikom davatelja digitalnih usluga.

Člankom 17. propisuje se predmet obveze primjene mjera za postizanje visoke razine kibernetičke sigurnosti – mrežni i informacijski sustav, ili njegov dio, za koji je u postupku identifikacije operatora ključne usluge utvrđeno da o njemu ovisi pružanje ključne usluge kod dotičnog subjekta odnosno mrežni i informacijski sustav koji podržava digitalnu uslugu.

Člankom 18. propisuje se operatorima ključnih usluga i davateljima digitalnih usluga obveza primjene mjera za sprječavanje i ublažavanje učinaka incidenata razmjerno riziku kojemu je izložen njihov mrežni ili informacijski sustav.

Člankom 19. utvrđuje se operatorima ključnih usluga i davateljima digitalnih usluga obveza primjene mjera za postizanje visoke razine kibernetičke sigurnosti bez obzira na to upravljaju li i/ili održavaju svoje mrežne i informacijske sustave sami ili za to koriste vanjskog davatelja usluge.

Člankom 20. propisuje se obveza donošenja mjera za postizanje visoke razine kibernetičke sigurnosti operatora ključnih usluga i način njihove provedbe uredbom koju donosi Vlada RH. Utvrđuje se davateljima digitalnih usluga obveza primjene mjera za postizanje visoke razine kibernetičke sigurnosti sukladno Provedbenoj uredbi Komisije (EU) 2018/151 od 30. siječnja 2018. o utvrđivanju pravila za primjenu Direktive (EU) 2016/1148 Europskog parlamenta i Vijeća u odnosu na dodatne specifikacije elemenata koje pružatelji digitalnih usluga moraju uzeti u obzir u upravljanju rizicima kojima je izložena sigurnost njihovih mrežnih i informacijskih sustava i parametara za utvrđivanje ima li incident znatan učinak (SL L 26/48, 31.1.2018.) – dalje u tekstu: Provedbena uredba Komisije.

Člankom 21. utvrđuje se obveza operatorima ključnih usluga i davateljima digitalnih usluga da, bez neopravdane odgode, obavješćuju nadležni CSIRT o incidentima koji imaju znatan učinak na kontinuitet pružanja ključne usluge i podržavanje digitalne usluge. Obavijest o incidentu na mrežnom i informacijskom sustavu davatelja digitalne usluge koji ima znatan učinak na pružanje neke ključne usluge, operator ključne usluge dužan je dostaviti u svoj nadležni CSIRT.

Člankom 22. utvrđuje se da će se kriteriji za određivanje incidenata koji imaju znatan učinak na pružanje ključnih usluga propisati uredbom koju donosi Vlada RH, a kriteriji za određivanje incidenata koji imaju znatan učinak na davanje digitalnih usluga uređeni su Provedbenom uredbom Komisije.

Člankom 23. utvrđuje se da će se sadržaj obavijesti o incidentima na mrežnim i informacijskim sustavima koji imaju znatan učinak na kontinuitet usluga koje pružaju, način dostave obavijesti i druga pitanja bitna za postupanje s takvim obavijestima urediti uredbom koju donosi Vlada RH.

Člankom 24. utvrđuje se mogućnost, po prethodno provedenom savjetovanju s operatorom ključne usluge i nadležnim sektorskim tijelom, da nadležni CSIRT obavijesti javnost o pojedinačnim incidentima koji imaju znatan učinak na kontinuitet usluge koju operator pruža, ako je osviještenost javnosti nužna za sprečavanje širenja i jačanja incidenta ili za rješavanje incidenta koji je u tijeku. Ovim se člankom uređuje i mogućnost da nadležni CSIRT ili CSIRT-ovi drugih pogođenih država članica, prema potrebi i ako je objavljivanje informacije o incidentu u javnome interesu, a osobito ako je to potrebno radi sprečavanja širenja i jačanja incidenta ili rješavanja incidenta koji je u tijeku, obavijeste javnost o pojedinačnim incidentima koji imaju znatan učinak na kontinuitet pojedine digitalne usluge ili može zatražiti od davatelja digitalnih usluga da to učini.

Člankom 25. utvrđuju se nadležna sektorska tijela Popisom iz Priloga III. Zakona (za sektor energetike, prijevoza, bankarstva, infrastrukture financijskog tržišta, zdravstveni sektor, sektor opskrbe vodom za piće i njezinu distribuciju, digitalnu infrastrukturu, davatelje digitalnih usluga, usluge digitalnog društva) te njihove zadaće: provođenje postupaka identifikacije operatora ključnih usluga, obavljanje nadzora operatora ključnih usluga i davatelja digitalnih usluga u provedbi ovog Zakona, međusobne suradnje i razmjene iskustva, suradnje i razmjene relevantnih informacija s drugim nadležnim tijelima te suradnju i razmjenu relevantnih informacija s tijelom za zaštitu osobnih podataka, kada su osobni podaci ugroženi zbog incidenta na mrežnom i informacijskom sustavu operatora ključne usluge odnosno davatelja digitalne usluge, odnosno s pravosudnim tijelima, kada je takav incident rezultat kriminalnih aktivnosti.

Člankom 26. propisuje se da se nadzor nad operatorom ključnih usluga provodi najmanje jednom svake dvije godine te da se može provesti i prije isteka tog roka ako nadležno sektorsko tijelo utvrdi ili zaprimi informacije koje ukazuju na to da operator ključne usluge ne izvršava svoje obveze iz ovog Zakona. Nadzor nad davateljem digitalnih usluga provodi se isključivo nakon što nadležno sektorsko tijelo zaprimi informacije koje ukazuju na to da davatelj digitalne usluge ne postupa sukladno Provedbenoj uredbi Komisije.

Člankom 27. propisuje se obveza operatorima ključnih usluga i davateljima digitalnih usluga, u okviru nadzora, dostavljati nadležnom sektorskom tijelu podatke potrebne za procjenu razine sigurnosti njihovih mrežnih i informacijskih sustava, uključujući dokumentirane sigurnosne politike i dokaze o učinkovitoj provedbi sigurnosnih mjera. Podaci se dostavljaju na zahtjev nadležnog sektorskog tijela koji mora sadržavati naznačenu svrhu zahtjeva, naznaku podataka koji se traže, a koji su nadležnom sektorskom tijelu potrebni za provođenje nadzora, s rokom za dostavu podataka. U okviru nadzora, operatori ključnih usluga i davatelji digitalnih usluga dužni su nadležnom sektorskom tijelu, na njegov zahtjev, omogućiti i neposredan pristup svojim objektima i sustavima koji im služe za potporu u obavljanju ključnih odnosno digitalnih usluga. Nadalje se utvrđuje da se učinkovita provedba sigurnosnih mjera dokazuje ili rezultatima revizije sigurnosti mrežnih i informacijskih sustava koju provodi kvalificirani revizor ili ocjenom sukladnosti mrežnih i informacijskih sustava koju daje tehničko tijelo za ocjenu sukladnosti primijenjenih mjera.

Člankom 28. utvrđuje se da je predmet nadzora pravilnost provedbe propisanih mjera za postizanje visoke razine kibernetičke sigurnosti, obveza vezanih uz obavješćivanje o incidentima i drugih postupanja prema zahtjevima nadležnih tijela. U provedbi nadzora, nadležna sektorska tijela: 1. izdaju obvezujuću uputu operatoru ključnih usluga kada utvrde da se ne provode mjere za postizanje visoke razine kibernetičke sigurnosti i/ili da se ne izvršavaju obveze s naznakom roka postupanja te kada postoje nedostaci u provedbi mjera i izvršavanju obveza, 2. izdaju naloge davatelju digitalnih usluga za otklanjanje svakog utvrđenog nepoštivanja provedbenog propisa Europske komisije donesenog temeljem Direktive 2016/1148i/ili odredbi ovog Zakona te 3. podnose optužne prijedloge.

Člankom 29. propisuje se da nadzor provode inspektori, nadzornici i supervizori u skladu s nadležnostima koje proizlaze iz propisa o ustrojstvu i djelokrugu rada tih tijela te drugih propisa koji određuju njihovu nadležnost.

Člankom 30. utvrđuju se obveze i odgovornosti jedinstvene nacionalne kontaktne točke, koja u obavljanju svojih zadaća: dostavlja Europskoj komisiji podatke koji omogućavaju procjenu učinkovitosti provedbe mjera iz ovog Zakona i propisa donesenog na temelju ovog Zakona, a prema zahtjevima Direktive 2016/1148; sudjeluje u radu Skupine za suradnju, koja je 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; podnosi Skupini za suradnju sažeto izvješće o zaprimljenim obavijestima o incidentima, na zahtjev nadležnog CSIRT–a, obavijesti o incidentima na mrežnim i informacijskim sustavima koji imaju znatan učinak na kontinuitet usluga koje se pružaju, prosljeđuje jedinstvenim kontaktna točkama drugih pogođenih država članica, osim za sektor usluga u sustavima državne informacijske infrastrukture; izrađuje smjernice o sadržaju obavijesti, načinu i rokovima informiranja jedinstvene nacionalne kontaktne točke o broju identificiranih operatora ključnih usluga i naznakama njihove važnosti te o obavijestima o incidentima; vodi brigu o potrebi razvoja i usklađivanja nacionalne strategije kibernetičke sigurnosti s ciljevima ovog Zakona i zahtjevima EU u području kibernetičke sigurnosti; surađuje s drugim nadležnim tijelima iz ovog Zakona te, kada je to potrebno, savjetuje se i surađuje s tijelom za zaštitu osobnih podataka i pravosudnim tijelima.

Člankom 31. utvrđuje se da je jedinstvena nacionalna kontaktna točka Ured Vijeća za nacionalnu sigurnost.

Člankom 32. propisuju se zadaće nadležnog CSIRT–a, odnosno da nadležni CSIRT na sektorskoj razini prati incidente, pruža rana upozorenja i najave te informira o rizicima i incidentima; provodi dinamičku analizu rizika i incidenata te izrađuje pregled situacije u sektoru; provodi redovite provjere ranjivosti mrežnih i informacijskih sustava operatora ključne usluge odnosno davatelja digitalne usluge iz svoje nadležnosti; prima obavijesti o incidentima; na zahtjev operatora ključne usluge odnosno davatelja digitalne usluge analizira i odgovara na incidente; ako to dopuštaju okolnosti, nakon primitka obavijesti o incidentu dostavlja operatoru ključnih usluga relevantne informacije u pogledu daljnjeg postupanja po njegovoj obavijesti, a osobito informacije koje bi mogle doprinijeti djelotvornom rješavanju incidenta; donosi smjernice o provedbi obveze obavješćivanja o incidentima; informira nadležno sektorsko tijelo o incidentima; u suradnji s nadležnim sektorskim tijelom, određuje prekogranične utjecaje incidenata, i informira jedinstvenu nacionalnu kontaktna točku o incidentima, kao i glavnim elementima postupaka koja primjenjuje u rješavanju incidenata; obavješćuje nadležni CSIRT druge pogođene države članice ili više njih o incidentu na mrežnom i informacijskom sustavu operatora ključnih usluga ako incident ima znatan učinak na kontinuitet ključnih usluga u toj državi članici; obavješćuje nadležni CSIRT druge pogođene države članice ili više njih o incidentu na mrežnom i informacijskom sustavu pružatelja digitalnih usluga ako se incident odnosi na dvije ili više država članica; surađuje s drugim CSIRT–ovima na nacionalnoj i međunarodnoj razini te u Mreži CSIRT–ova na razini EU koja je osnovana s ciljem razvoja povjerenja i pouzdanja među državama članicama te promicanju brze i učinkovite operativne suradnje; promiče usvajanje i primjenu zajedničkih ili normiranih praksi za postupke rješavanja incidenata i rizika te planove za klasifikaciju incidenata, rizika i informacija. Utvrđuje se operatorima ključnih usluga i davateljima digitalnih usluga obveza suradnje i razmjene potrebnih informacija s nadležnim CSIRT–om u postupku rješavanja incidenata, u okviru čijeg rješavanja

nadležni CSIRT ne snosi odgovornost za štetu uzrokovanu incidentom na mrežnim i informacijskim sustavima operatora ključnih usluga i davatelja digitalnih usluga.

Člankom 33. utvrđuje se da je nadležni CSIRT dužan osigurati visoku razinu dostupnosti svojih usluga komuniciranja izbjegavanjem jedinstvenih točki prekida, uz raspoloživost sredstava za mogućnost dvosmjernog kontaktiranja te jasno određenim i poznatim komunikacijskim kanalima za njihove klijente i suradnike; smještaj svojih prostora i informacijskih sustava za potporu na sigurnim lokacijama i osigurati kontinuitet rada kroz opremljenost odgovarajućim sustavom za upravljanje zahtjevima i njihovim preusmjeravanjem, kako bi se olakšale primopredaje; kroz dovoljan broj zaposlenika na odgovarajući način osigurati dostupnost u svako doba te oslanjanje na infrastrukturu čiji je kontinuitet osiguran te su im u tu svrhu dostupni redundantni sustavi i rezervni radni prostor. Utvrđuje se i izuzeće za nadležne CSIRT–ove od ograničavajućih odredbi drugih propisa koje utječu na mogućnost novih zapošljavanja ili druga pitanja bitna za osiguranje uvjeta utvrđenih za rad nadležnih CSIRT–ova.

Člankom 34. propisuje se da, ako reviziju sigurnosti mrežnih i informacijskih sustava ne provodi kvalificirani revizor, tada tehničko tijelo za ocjenu sukladnosti provodi periodičke provjere tehničkih i organizacijskih mjera za upravljanje rizicima, uzimajući pri tome u obzir najbolje prakse u području kibernetičke sigurnosti te mjera za sprečavanje i ublažavanje učinaka incidenata na sigurnost mrežnih i informacijskih sustava, poduzetih nad sigurnošću mrežnih i informacijskih sustava operatora ključnih usluga i davatelja digitalnih usluga. Popisom iz Priloga III. utvrđuje se da su tehnička tijela za ocjenu sukladnosti primijenjenih mjera Zavod za sigurnost informacijskih sustava i Hrvatska akademska i istraživačka mreža – CARNet.

Člankom 35. propisuje se da provjeru tehničkih i organizacijskih mjera za upravljanje rizicima i mjera za sprečavanja i ublažavanje učinaka incidenata na sigurnost mrežnih i informacijskih sustava, provodi tehničko tijelo za ocjenu sukladnosti na zahtjev nadležnog sektorskog tijela ili samog operatora ključnih usluga, odnosno davatelja digitalnih usluga. Zahtjev podnosi nadležno sektorsko tijelo kada utvrdi da revizija sigurnosti mrežnih i informacijskih sustava kod pojedinog operatora ključne usluge odnosno davatelja digitalne usluge nije provedena ili ju nije proveo kvalificirani revizor. Zahtjev za ocjenu sukladnosti može podnijeti i sam operator ključne usluge, odnosno davatelj digitalnih usluga kada po posebnom propisu ne postoji obveza revizije subjekta.

Člankom 36. propisuje se da su operatori ključnih usluga i davatelji digitalnih usluga, na zahtjev tehničkog tijela za ocjenu sukladnosti, u kojem se mora naznačiti svrha zahtjeva i potrebni podaci s rokom dostave, u obvezi dostaviti mu podatke potrebne za procjenu razine sigurnosti njihovih mrežnih i informacijskih sustava te mu omogućiti pristup svojim objektima i sustavima koji im služe za potporu u obavljanju ključnih odnosno digitalnih usluga.

Člankom 37. propisuje se da tehničko tijelo za ocjenu sukladnosti, nakon provjere tehničkih i organizacijskih mjera za upravljanje rizicima te mjera za sprečavanje i ublažavanje učinaka incidenata na sigurnost mrežnih i informacijskih sustava, izrađuje izvješće, koje sadrži ocjenu sukladnosti provedenih mjera, odnosno korektivne mjere s naznakom roka izvršenja ukoliko utvrdi da operator ključne usluge odnosno davatelj digitalne usluge mjere ne provodi učinkovito,

i dostavlja ga nadležnom sektorskom tijelu i operatoru ključnih usluga odnosno davatelju digitalnih usluga.

Člankom 38. utvrđuje se operatorima ključnih usluga i davateljima digitalnih usluga obveza primjene korektivnih mjera u zadanim rokovima, o čijoj primjeni moraju obavijestiti tehničko tijelo za ocjenu sukladnosti, koje, po prijemu obavijesti i u slučaju djelomičnog ili potpunog neprovođenja mjera, izrađuje završno izvješće i dostavlja nadležnom sektorskom tijelu radi provođenja nadzora.

Člankom 39. propisuje se da je tehničko tijelo za ocjenu sukladnosti dužno izvijestiti nadležno sektorsko tijelo, ako operator ključne usluge i davatelj digitalne usluge ne omogući ili neopravdano odgađa i otežava provedbu provjere tehničkih i organizacijskih mjera za upravljanje rizicima i mjera za sprečavanje i ublažavanje učinaka incidenata na sigurnost mrežnih i informacijskih sustava.

Člankom 40. propisuje se da se popisi identificiranih operatora ključnih usluga i svi drugi podaci koji nastaju u okviru provedbe Zakona o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga koriste samo za potrebe izvršenja Zakona, da pri razmjeni tih podataka potrebno voditi računa o ograničenju pristupa podacima ako je to potrebno u svrhu sprječavanja, otkrivanja, provođenja istraživanja i vođenja kaznenog postupka. Također, propisuje se kako ti podaci predstavljaju informacije u odnosu na koje je moguće ograničiti pravo pristupa korisniku informacija, ovisno o rezultatima testa razmjernosti i javnog interesa koji se provodi prema odredbama posebnog zakona o pravu na pristup informacijama.

Člankom 41. propisuje se nadležnim tijelima iz ovog Zakona dužnost postupanja s podacima operatora ključnih usluga i davatelja digitalnih usluga u skladu sa zahtjevima povjerljivosti, ako su oni utvrđeni posebnim propisima o zaštiti takvih podataka.

Člancima 42., 43., 44. i 45. propisuju se prekršajne odredbe.

Člankom 46. propisuje se da će mjere za postizanje visoke razine kibernetičke sigurnosti operatora ključnih usluga i način njihove provedbe donijeti uredbom koju donosi Vlada RH u roku od 30 dana od dana stupanja na snagu ovog Zakona.

Člankom 47. propisuje se da su nadležna sektorska tijela dužna postupak identifikacije operatora ključnih usluga provesti u roku od 90 dana od dana stupanja na snagu ovog Zakona te obavijest o broju identificiranih operatora ključnih usluga u pojedinom sektoru, s naznakom njihove važnosti za sektor, dostaviti jedinstvenoj nacionalnoj kontaktnoj točki u roku od 120 dana od dana stupanja na snagu ovog Zakona.

Člankom 48. propisuje se da su identificirani operatori ključnih usluga dužni provesti mjere za osiguranje visoke razine kibernetičke sigurnosti u roku od 12 mjeseci od dana dostave obavijesti o odluci nadležnog sektorskog tijela o određivanju subjekta operatorom ključnih usluga te da su dužni započeti s dostavom obavijesti o incidentima na mrežnim i informacijskim sustavima koji imaju znatan učinak na kontinuitet usluga koje pružaju 30 dana od dana dostave obavijesti o odluci nadležnog sektorskog tijela o određivanju subjekta operatorom ključnih usluga.

Člankom 49. propisuje se da su davatelji digitalnih usluga obvezni uskladiti se sa zahtjevima Provedbene uredbe Komisije.

Člankom 50. propisuje se da ovaj Zakon stupa na snagu osmoga dana od dana objave u Narodnim novinama.

Prilogom I. utvrđuju se, popisom u tabličnom pregledu, ključne usluge prema sektorima i podsektorima na koje se primjenjuje ovaj Zakon, s kriterijima i pragovima za utvrdivanje važnosti negativnog učinka incidenta, izraženi u različitim (mjernim) jedinicama (npr. MW, tonama, broju korisnika, m^3, postocima i sl.) u ovisnosti od sektora kojem pripadaju. Popis ključnih usluga koristi se za identificiranje operatora ključnih usluga.

Prilogom II. utvrđuju se, popisom, digitalne usluge na čije davatelje se primjenjuje ovaj Zakon.

Prilogom III. utvrđuju se nadležna tijela: jedinstvena nacionalna kontaktna točka – Ured Vijeća za nacionalnu sigurnost nadležna sektorska tijela za sektore energetike – središnje državno tijelo nadležno za energetiku, prijevoza – središnje državno tijelo nadležno za promet, bankarstva – Hrvatska narodna banka, infrastrukture financijskog tržišta – Hrvatska agencija za nadzor financijskih usluga, zdravstveni sektor – središnje državno tijelo nadležno za zdravstvo, sektor opskrbe vodom za piće i njezinu distribuciju – središnje državno tijelo nadležno za vodno gospodarstvo, digitalne infrastrukture – Središnji državni ured za razvoj digitalnog društva, digitalne usluge – središnje državno tijelo nadležno za gospodarstvo te poslovne usluge za središnja državna tijela – Središnji državni ured za razvoj digitalnog društva, nadležni CSIRT–ovi – Zavod za sigurnost informacijskih sustava ili Nacionalni CERT i nadležna tehnička tijela za ocjenu sukladnosti – Zavod za sigurnost informacijskih sustava ili Hrvatska akademska i istraživačka mreža – CARNet.

PRILOG – IZVJEŠĆE O PROVEDENOM SAVJETOVANJU SA ZAINTERESIRANOM JAVNOŠĆU

OBRAZAC IZVJEŠĆA O PROVEDENOM SAVJETOVANJU SA ZAINTERESIRANOM JAVNOŠĆU	
Naslov dokumenta	Izvješće o provedenom savjetovanju sa zainteresiranom javnošću o Nacrt prijedloga zakona o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga, s konačnim prijedlogom zakona
Stvaratelj dokumenta, tijelo koje provodi savjetovanje	Ured Vijeća za nacionalnu sigurnost
Svrha dokumenta	Izvješće o provedenom savjetovanju
Datum dokumenta	14.02.2018.
Verzija dokumenta	I.
Vrsta dokumenta	Izvješće
Naziv nacrta zakona, drugog propisa ili akta	Nacrt prijedloga zakona o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga, s konačnim prijedlogom zakona
Jedinstvena oznaka iz Plana donošenja zakona, drugih propisa i akata objavljenog na internetskim stranicama Vlade	121.
Naziv tijela nadležnog za izradu nacrta	Ured Vijeća za nacionalnu sigurnost
Koji su predstavnici zainteresirane javnosti bili uključeni u postupak izrade odnosno u rad stručne radne skupine za izradu nacrta?	-
Je li nacrt bio objavljen na internetskim stranicama ili na drugi odgovarajući način?	Da, na portalu e-savjetovanje, u razdoblju od 12.01.2018. do 10.02.2018., 30 dana.
Ako jest, kada je nacrt objavljen, na kojoj internetskoj stranici i koliko je vremena ostavljeno za savjetovanje?	
Ako nije, zašto?	
Koji su predstavnici zainteresirane javnosti dostavili svoja očitovanja?	Fizička osoba
ANALIZA DOSTAVLJENIH PRIMJEDBI	Dani opći komentari i prijedlozi u odnosu na dijelove Nacrta prijedloga Zakona o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga koji se odnose na davatelje digitalnih usluga. Obrazloženje o prihvaćanju/neprihvaćanju istih nalazi se u Obrascu „Analiza dostavljenih primjedbi" koji je objavljen na portalu
Primjedbe koje su prihvaćene	
Primjedbe koje nisu prihvaćene i obrazloženje razloga za	

neprihvaćanje	esavjetovanja.gov.hr.
Troškovi provedenog savjetovanja	Nije bilo troškova.

Izvješće o provedenom savjetovanju - Savjetovanje o Nacrtu prijedloga zakona o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga s konačnim prijedlogom zakona

Korisnik/Sekcija/Komentar	Odgovor
Mladen Milavić **NACRT PRIJEDLOG ZAKONA O KIBERNETIČKOJ SIGURNOSTI OPERATORA KLJUČNIH USLUGA I DAVATELJA DIGITALNIH USLUGA, S KONAČNIM PRIJEDLOGOM ZAKONA** Opći komentar i prijedlozi: Poštovani, U svezi novog Zakona o kibernetičkoj sigurnosti u nastavku slijede komentari i prijedlozi. Mišljenje je kako bi se postojeći prijedlog ovog zakona morao još malo raspraviti s obrirom na nedavnu odluku EK, gdje je EK poduzela još jedan važan korak u vezi s poboljšanjem kibernetičke sigurnosti. Sve države članice će morati transponirati do 9. svibnja Direktivu o sigurnosti mrežnih i informacijskih sustava (NIS Directive), Komisija je donijela provedbenu Uredbu (implementing regulation) o digitalnim pružateljima usluga (npr. cloud computing usluge, online tržišta i tražilice). Predlažemo da se s obzirom na novu provedbenu Uredbu, napravi dodatno usuglašavanje s trendovima u kibernetičkoj sigurnosti, jer vjeujemo kako postoji potreba za dodatnim usklađenjem. Pri ovom, predlažemo da se kontaktiraju najbolje svjetske tvrtke i razmijene najbolje svjetske prakse u domeni kibernetičke sigurnosti. Naši komentari su usredotočeni na pet prioritetnih pitanja vezanih uz davatelje digitalnih usluga (Digital Service Providers – DSP): 1) režim "light-touch" i "one-stop shop" pristup reguliranju DSP-ova; 2) potreba da bilo koji predloženi režim novčanih kazni biti razmjeran i odražavati dogovoreni "light-touch" pristup; 3) definicija "usluge računalstva u oblaku"; 4) uloga nacionalnog nadležnog tijela za DSP i 5) prijedlog prijelaznog razdoblja u primjeni zakona; kao i povratne informacije o obvezama za DSP, kao što su sigurnosne osnove i prijavljivanje incidenta. "Light-touch" režim i One-Stop Shop U postupku usvjanja NIS direktive dogovoreno je kako DSP-ovi ne bi trebali biti podložni istim obvezama ili razinama kontrole kao operatori koji pružaju ključne usluge za društvo ili nacionalnu ekonomiju (Operators of Essential Services - OES), u energetici, transportu i drugim kritičnim sektorima. S obzirom na "prirodu njihovih usluga i operacija", europski su zakonodavci prihvatili samo DSP-ove u okviru NIS direktive, s razumijevanjem da će DSP-ovi biti podložni "light-touch" režimu. "One-stop shop", koji osigurava da DSP-ovi podliježu jedino nadležnosti regulatora unutar EU gdje DSP ima stalno mjesto poslovanja odnosno gdje davatelj usluga u neodređenom vremenskom razdoblju upravlja svojom djelatnošću kao što je to navedeno u članku 5. stavku 13. prijedloga. Navedeno predstavlja kritički element "light-touch" pristupa. To je osobito važno jer DSP-ovi obično nude svoje usluge u mnogim ili svim državama članicama. Od ključne je važnosti da se Hrvatska pridržava načela "one-stop shop". DSP-ovi koji	**Djelomično prihvaćen** Provedbena uredba Europske komisije od 30.01.2018. (SL L 26/48, 31.1.2018.) predstavlja provedbeni akt NIS direktive (DIREKTIVA (EU) 2016/1148 EUROPSKOG PARLAMENTA I VIJEĆA od 6. srpnja 2016.) s kojom je potpuno usklađena te ju dodatno razrađuje u elementima istaknutim u naslovu (masno): „PROVEDBENA UREDBA KOMISIJE (EU) 2018/151 od 30. siječnja 2018. o utvrđivanju pravila za primjenu Direktive (EU) 2016/1148 Europskog parlamenta i Vijeća u odnosu na dodatne specifikacije elemenata koje pružatelji digitalnih usluga moraju uzeti u obzir u upravljanju rizicima kojima je izložena sigurnost njihovih mrežnih i informacijskih sustava i parametara za utvrđivanje ima li incident znatan učinak. Za razliku od NIS direktive koja predstavlja obvezu transpozicije u nacionalno zakonodavstvo svake države članice EU, Provedbena uredba se direktno primjenjuje na sve države članice u dijelu koji propisuje odgovornosti DSP-ova sa sjedištem u zemlji članici. Prema tome, u ovom dijelu odgovornosti DSP-ova nema mogućnosti dodatnog usklađivanja na razini države članice već se izravno primjenjuje Provedbena uredba od 30. siječnja 2018., nastavno na NIS direktivu. Provedbena uredba EK bila je prije donošenja na javnoj raspravi u organizaciji EK (https://ec.europa.eu/info/law/better-regulation/initiatives/ares-2017-4460501_en) te su u razdoblju od 13. rujna do 11. listopada 2017. zaprimljene i obrađene primjedbe i prijedlozi različitih subjekata koji su iskazali interes pa i globalnih kompanija. 1) "light-touch" pristup predstavlja razliku između DSP-ova i OES-ova u smislu odgovornosti za provedbu procjene rizika i primjene mjera, pri čemu DSP-ovi to procjenjuju sami na bazi pravila EK u NIS direktivi i Provedbenoj uredbi EK, dok u slučaju OES-a pravila donose države članice nacionalnim transpozicijskim aktima za prijenos NIS direktive. Druga razlika je odgovornost za obavješćivanje o incidentima u okviru koje su DSP-ovi odgovorni provoditi izvješćivanje prema parametrima značajnih incidenata utvrđenih spomenutom Provedbenom uredbom EK, a OES-ovi će obvezu obavještavanja izvršavati prema parametrima utvrđenim nacionalnim transpozicijskim aktima. Dodatno, DSP-ovi su izuzeti od obveza iz NIS direktive u slučaju kada zadovoljavaju uvjet za mikro i male subjekte malog gospodarstva (do 50 zaposlenih, godišnji promet do 10 milijuna EUR). "One-stop shop" se odnosi na utvrđivanje primjene obveza DSP-ova sukladno sjedištu DSP-a u jednoj državi članici EU i bez obzira na mogućnost davanja specificiranih vrsta digitalnih usluga na tržištu cijele EU. Pri tome se nadležna tijela država članica u kojima DSP daje usluge moraju koordinirati s nadležnim tijelima države u kojoj DSP ima sjedište (npr CSIRT-ovi), a nadležna tijela u kojima DSP ima sjedište dužna su

imaju svoje glavno sjedište u EU, ali koji također pružaju usluge u Hrvatskoj, ne bi se trebali suočiti sa zahtjevima za dvostrukim izvješćivanjem (npr. prema DSP regulatoru zemlje sa stalnim mjestom poslovanja i nadležnom nacionalnom regulatoru) ili dvostrukim novčanim kaznama. Pozivamo da se u donošenju ovog zakona imaju na umu ovi problemi kako bi se izbjeglo kažnjavanje DSP-a jednostavno zbog osnivanja u Hrvatskoj. Prekršajne odredbe U sedmom dijelu naznačeno je da bi novčane kazne za OES operatore u kontekstu implementacije NIS direktive trebale biti u skladu s DSP-ovima. Niža razina potencijalnih novčanih kazni za DSP-ove bila bi više u skladu s usporedivim zakonima EU i Velikoj Britaniji, kao što su iste u području zdravlja i sigurnosti i odgovornosti za proizvode, te u skladu s planovima ostalih država članica u implementaciji NIS direktive. Ukratko, prijedlog da se DSP-ovi podvrgnu sličnim razinama kazni neproporcionalno je u usporedbi s drugim zakonima. Prijedlog da se DSP-ovi podvrgnu istoj razini kazni kao i OES operatore također ne uzima u obzir dogovoreni "light-touch" režim. Iako je NIS direktiva prepustila državama članicama da utvrde pravila o kaznama, bilo bi u suprotnosti s NIS direktivom podvrgnuti DSP-ove na istu razinu kazni kao i OES operatore. To bi se trebalo mijenjati kako bi se osigurala jedna razina novčanih kazni za OES operatore i još jedna, mnogo smanjenu razinu novčanih kazni za DSP-ove. Definicija " usluge računalstva u oblaku " i opseg pokrivenih DSP-ova Prijedlog iz članka 5., stavka 24. definicije "usluge računalstva u oblaku" je preširok jer ne razlikuje različite razine kritičnosti povezane s različitim vrstama usluga računalstva u oblaku. U skladu s priznatim, slobodno dostupnim međunarodnim standardima, obveze za usluge računalstva u oblaku trebale bi se primjenjivati samo na najkritičnije usluge na koje se druge tvrtke oslanjaju, a to su javne IaaS usluge računalstva u oblaku. Jedan od načina da se pruži najveća jasnoća razmatranja kritičnosti usluge računalstva u oblaku temelji se na vrsti usluge (servis, platforma ili infrastruktura) i modela implementacije oblaka (privatni, zajednički, hibridni ili javni) kao što je definirano u ISO17788:2014. Ovaj pristup bi također bio u skladu s zahtjevom iz NIS direktive za države članice EU I Veliku Britaniju da potiču usklađenost ili sukladnost s određenim i priznatim standardima. Vrsta infrastrukturne usluge, često se naziva Infrastructure-as-a-Service (IaaS), ima značajan utjecaj na razmatranje kritičnosti u tim okolnostima. Kao što je objašnjeno u odjeljku 10.2.1 "Service capabilities functional component" (ISO 17789:2014), vrsta usluge servisa (tj. Software-as-a-Service ili SaaS) može se implementirati pomoću platforme (npr. Platform-as-a-Service ili PaaS) koji zauzvrat može biti implementiran pomoću infrastrukture (IaaS). Sučelja između tih sukcesivnih slojeva potrebnih za pokretanje i upravljanje usluga računalstva u oblaku znače da IaaS incident može imati veću kritičnost nego PaaS ili SaaS. Nadalje, javne usluge računalstva u oblaku potencijalno su dostupne svakom klijentu. Javni će oblak imati veću kritičnost od privatnog oblaka, kao što je objašnjeno u odjeljku ISO 17789:2014, poglavlje 8.5.12.4 "Implications of cloud deployment models". Ograničavanje obveza za usluge računalstva u oblaku za javne računalne usluge IaaS također bi bilo u skladu s poštivati obveze DSP-ova propisane aktima EK. U tom smislu nema dvostrukog postupanja prema DSP-ova ni po kojoj osnovi već su nadležna tijela koja postupaju uvijek ona iz države članice u kojoj je sjedište DSP-a i sam DSP je odgovoran koordinirati svoje sigurnosne mjere i obavješćivanje o incidentima prema nadležnim tijelima države članice u kojoj ima sjedište. Hrvatska je dužna osigurati nadležna tijela za DSP-ove koji imaju ili će imati sjedište u RH, kao i za potrebe koordinacije s nadležnim tijelima u drugim državama EU-a u kojima je sjedište DSP-a koji pruža usluge hrvatskim građanima. Pri tome je odgovornost za procjenjivanje potpadaju li pod obveze NIS direktive, na samim DSP-ovima, kao i za provedbu sigurnosnih mjera i obavješćivanje o značajnim incidentima u odgovornosti DSP-a. Nadležna tijela za DSP-ove moraju biti definirana u svim državama članicama kako bi mogla postupati u slučaju zahtjeva DSP-a koji je sam prepoznao da je obveznik NIS direktive, ili u slučaju incidenta sa znatnim učinkom koji je nastao zbog DSP-ovog izbjegavanja obveza u provedbi NIS direktive (i spomenute Provedbene uredbe EK). U svim slučajevima to su nadležna tijela države članice u kojoj DSP ima sjedište. "Light-touch" režim za DSP-ove nije u vezi s iznosima kazni zbog neprovođenja obveza, već isključivo s načelom primjerene pažnje za korisnike svojih usluga i to se odnosi kako na OES-ove tako i na DSP-ove. Predložene kazne su simetrične za OES i DSP pravne osobe i usklađene su s iznosima predviđenim u RH za ovakve postupke. Naravno, te kazne su primjenjive za sve identificirane OES-ove te DSP-ove sa sjedištem u RH. S obzirom da DSP može predstavljati dio infrastrukture OES operatora, a broj korisnika i geografska pokrivenost uslugama su bitno veći u slučaju DSP-ova, nema razloga za njihov povlašteni tretman u slučaju izbjegavanja provedbe obveza iz NIS direktive. Ograničenja primjene hrvatskog zakona na DSP-ove jasno su utvrđena u čl.3., st.2., Nacrta, a primjena ranije spomenute Provedbene uredbe EK na DSP-ove kako je gore pojašnjeno predviđena je člankom 15. stavkom 2. i člankom 22. stavkom 2. Nacrta. Definicija digitalne usluge „računalstvo u oblaku" prenesena je u cijelosti iz NIS direktive te ju nije moguće mijenjati na razini država članica već ju države članice moraju transponirati u nacionalno zakonodavstvo. Tri NIS direktivom odabrane digitalne usluge (prema procjeni EK i suglasnosti država članica u okviru postupka donošenja NIS direktive), predstavljaju ključne usluge na razini jedinstvenog digitalnog tržišta EU-a, dok kritičnost pojedinih načina implementacije infrastrukture i usluga DSP-ova, koje daju na EU tržištu, procjenjuju sami DSP-ovi. Pri tome su DSP-ovi dužni birati način provedbe sigurnosnih mjera i relevantne međunarodne ili EU norme koje će koristiti. Primjerice, parametri po kojima DSP mora utvrđivati je li učinak nekog incidenta znatan, u potpunosti su zadani čl.3. Provedbene uredbe EK. Obveza obavješćivanja o incidentu se primjenjuje samo kada DSP ima pristup podacima za procjenu utjecaja incidenta prema zadanim parametrima. Članak 27. stavak 4. Nacrta bit će izmijenjen i nadopunjen, uvažavajući posebno članak 17. stavak 3. NIS direktive. Nacrtom se predviđa davanje novih nadležnosti tijelima u RH koje su u određenoj mjeri i do sada obavljale slične poslove ili su sektorski nadležna za gospodarska područja obuhvaćena NIS direktivom. U tom smislu sva tijela posjeduju inicijalnu spremnost za obavljanje traženih poslova, a kroz rokove

tekstom i ciljem NIS direktive. Nasuprot tome, uključivanje privatnih i hibridnih oblaka u opsegu bi bio u suprotnosti s pristupom NIS direktive navedenima u čl. 16 (4), jer DSP često neće biti svjestan incidenata koji utječu na pojedine organizacije koje realiziraju (koriste) usluge privatnog ili hibridnog oblaka i nakon toga neće imati dovoljno podataka za izvješćivanje. Proširivanje opsega za uključivanje svih poslovnih SaaS usluga ponuđenih u Hrvatskoj učinilo bi provedbu neizvedivom i vjerojatno neučinkovitom jer bi nadležno tijelo trebalo raditi kroz veliku količinu "šumova" u sustavu, što može lako smanjiti fokusiranje na najvažnije incidente koji utječu na kritičnu infrastrukturu / platformske usluge - na kojima se zatim izvode SaaS usluge. Obveze operatora ključnih usluga i davatelja digitalnih usluga u okviru nadzora U ovom dijelu (članak 27. (4) govori se kako su operatori ključnih usluga (OES) i davatelji digitalnih usluga (DSP) dužni u okviru nadzora nadležnom sektorskom tijelu, na njegov zahtjev, omogućiti neposredan pristup svojim objektima i sustavima koji im služe za potporu u obavljanju ključnih odnosno digitalnih usluga. Obzirom na poslovni model pružatelj usluga računalstva u oblaku ovakva odredba neće biti provediva jer u stvarnosti nije moguće omogućiti pristup mreži podatkovnih centara (izravni pristup), osobito objekata i sustava. Naš je prijedlog da se navedeno treba regulirati / upravljati kroz postojeće revizije ili neki drugi model kako bi se omogućilo nesmetano obavljanje ovih usluga na jedinstvenom tržištu EU. Hrvatsko nacionalno nadležno tijelo za davatelje digitalnih usluga Napominjemo da sadašnji prijedlog transpozicije predviđa da je nacionalni CERT nacionalno nadležno tijelo (NCA). Pozdravljamo ovu odredbu, jer svaka nacionalna agencija mora imati potrebnu tehničku stručnost, fizičku infrastrukturu i odgovarajuće resurse koji su posebno važni za mrežnu i informacijsku sigurnost. Osim toga, od ključne je važnosti da svaki obvezni režim obavijesti o incidentima ne utječe negativno na postojeće, dobrovoljne prakse za razmjenu informacija koje se danas odvijaju između industrije i vlade. Dobrovoljna razmjena informacija najčešće se temelji na povjerljivim odnosima uspostavljenim tijekom određenog vremenskog razdoblja. Sukladno tome, hrvatska vlada bi trebala osigurati: (1) da nacionalnom CERT-u daju odgovarajuće resurse, infrastrukturu i stručnost; i (2) da industrija dobiva pojašnjenja o predviđenom odnosu između tradicionalnih dionika u području mrežne i informacijske sigurnosti u Hrvatskoj kako bi se osigurali odgovarajući vatrozidovi između postojećeg dobrovoljnog dijeljenja informacija na temelju povjerenja i obaveznog izvješćivanja o incidentu. Svaki nedostatak jasne razdvojenosti između tih procesa može imati neželjene posljedice s potencijalno štetnim posljedicama na sposobnost očuvanja postojeće povjerljive mreže. Prijelazno razdoblje S obzirom na prilično kasnu fazu u kojoj Hrvatska sada prenosi NIS direktivu i odgađanje donošenja provedbenih akata, predlažemo produženje prijelaznog razdoblja (do kraja 2019.) tijekom kojeg bi tvrtke trebale imati koristi od određene fleksibilnosti u smislu primjene. Takvo prijelazno razdoblje bit će ključno kako bi se tvrtkama dala dovoljno vremena za prilagodbu i pripremu za usklađivanje s tim novim zahtjevima.

provedbe Nacrta bit će potrebno daljnje oblikovanje poslovnih procesa i infrastrukture u svim nadležnim tijelima i identificiranim operatorima ključnih usluga, a za što će im biti na raspolaganju i mogućnosti korištenja nepovratnih EU financijskih sredstava kako je pojašnjeno u obrazloženju Nacrta. Detaljnija razrada sustava obavješćivanja na nacionalnoj razini i u odnosu na EU razinu planira se u okviru podzakonskog akta ovog Nacrta, Uredbi Vlade RH, koja je u izradi i planira se njeno stupanje na snagu ubrzo nakon stupanja na snagu predmetnog Zakona. Prijelazno razdoblje za provedbu mjera za identificirane OES-e je utvrđeno u roku od 12 mjeseci od identifikacije OES-a, koja se provodi u roku od 90 dana od donošenja Zakona planiranog za svibanj 2018. U tom smislu ovaj rok se za identificirane OES-ove i očekuje u 4. kvartalu 2019. Što se tiče obaveza o izvješćivanju, definiran je rok od 120 dana od stupanja na snagu Zakona, a isti će u velikoj mjeri služiti lakšoj provedbi sigurnosnih mjera kod operatora ključnih usluga i koordinaciji nadležnih tijela te uigravanju cijelog sustava tijekom 4. kvartala 2018. i u 2019. godini. Rok za obavješćivanje i nakon stupanja na snagu primjenjiv je samo za identificirane nacionalne OES-ove, a za DSP-ove sa sjedištem u RH (i koji ne predstavljaju mikro i mali subjekt malog gospodarstva), koji procjene da zadovoljavaju kriterije iz NIS direktive i Provedbene uredbe EK, taj rok je prema tim aktima teče od 10. svibnja 2018. Prijelazni rokovi u Nacrtu su odabrani na sličan način u svim državama članicama i prate NIS direktivu, a proces transpozicije u RH je u okvirima prosječne dinamike kakva je u transpoziciji NIS direktive u državama članicama, s tim da se Nacrtom u odnosu na DSP-ove njegovim člankom 48. ponovno upućuje na Provedbenu uredbu EK (budući da se ona izravno primjenjuje u svim državama članicama).

IZJAVA O USKLAĐENOSTI PRIJEDLOGA PROPISA S PRAVNOM STEČEVINOM EUROPSKE UNIJE

1. Naziv prijedloga propisa

Zakon o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga

2. Stručni nositelj izrade prijedloga propisa

URED VIJEĆA ZA NACIONALNU SIGURNOST

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 2018. godinu.
Rok: I. kvartal 2018.

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) 2016/1148 Europskog parlamenta i Vijeća od 6. srpnja 2016. o mjerama za visoku zajedničku razinu sigurnosti mrežnih i informacijskih sustava širom Unije (SL L 194, 19.7.2016.)

32016L1148

- Članci 1., 14., 16., 19., 20., i 25. bit će preuzeto: Uredba o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga (09.04.2018)
- Članci 1. i 7. preuzeto: ODLUKA O DONOŠENJU NACIONALNE STRATEGIJE KIBERNETIČKE SIGURNOSTI I AKCIJSKOG PLANA ZA PROVEDBU NACIONALNE STRATEGIJE KIBERNETIČKE SIGURNOSTI (NN 108/15)
- Članak 7. preuzeto: Odluka o osnivanju Nacionalnog vijeća za kibernetičku sigurnost i Operativno-tehničke koordinacije za kibernetičku sigurnost (NN 61/16)

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

Maja Čavlović

PREDSTOJNICA

14. 2. 2018.

(potpis) (datum i pečat)

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

mr. sc. Marija Pejčinović Burić

POTPREDSJEDNICA VLADE I MINISTRICA

19. veljače 2018.

(potpis) (datum i pečat)

USPOREDNI PRIKAZ PODUDARANJA ODREDBI PROPISA EUROPSKE UNIJE S PRIJEDLOGOM PROPISA

1. **Naziv propisa Europske unije**
   Direktiva (EU) 2016/1148 Europskog parlamenta i Vijeća od 6. srpnja 2016. o mjerama za visoku zajedničku razinu sigurnosti mrežnih i informacijskih sustava širom Unije

2. **Naziv prijedloga propisa**
   Zakon o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga

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**	**Obrazloženje (ako sadržaj odredbe propisa Europske unije nije preuzet ili je djelomično preuzet u odredbu prijedloga propisa)**

		preuzetu odredbu prijedloga propisa?	
POGLAVLJE I. OPĆE ODREDBE Članak 1. Predmet i područje primjene 1. Ovom Direktivom utvrđuju se mjere s ciljem postizanja visoke zajedničke razine sigurnosti mrežnih i informacijskih sustava unutar Unije kako bi se poboljšalo funkcioniranje unutarnjeg tržišta. 2. U tu svrhu, ovom Direktivom: (a)utvrđuje se obveza za sve države članice da donesu nacionalnu strategiju za sigurnost mrežnih i informacijskih sustava; (b)stvara se skupina za suradnju u svrhu podupiranja i olakšavanja strateške suradnje i razmjene informacija među državama članicama i razvijanja	*Cilj i predmet* *Članak 1.* (1) Ovim se Zakonom uređuju postupci i mjere za postizanje visoke zajedničke razine kibernetičke sigurnosti operatora ključnih usluga i davatelja digitalnih usluga, nadležnosti i ovlasti nadležnih sektorskih tijela, jedinstvene nacionalne kontaktne točke, tijela nadležnih za prevenciju i zaštitu od incidenata (dalje u tekstu: nadležni CSIRT) i tehničkog tijela za ocjenu sukladnosti, nadzor nad operatorima ključnih usluga i davateljima digitalnih usluga u provedbi ovog Zakona i prekršajne odredbe. (2) Cilj je ovog Zakona osigurati provedbu mjera za postizanje visoke zajedničke razine kibernetičke sigurnosti u davanju usluga koje su od posebne važnosti za odvijanje ključnih društvenih i gospodarskih aktivnosti, uključujući funkcioniranje digitalnog tržišta.	U potpunosti preuzeto	
	Jedinstvena nacionalna kontaktna točka *Članak 30.* Jedinstvena nacionalna kontaktna točka:	U potpunosti preuzeto	

međusobnog povjerenja i pouzdanja; (c)stvara se mreža timova za odgovor na računalne sigurnosne incidente („mreža CSIRT-ova") kako bi se doprinijelo razvoju pouzdanja i povjerenja među državama članicama i promicalo brzu i učinkovitu operativnu suradnju; (d)utvrđuju se zahtjevi za sigurnost i obavješćivanje za operatore ključnih usluga i za pružatelje digitalnih usluga; (e)utvrđuju se obveze za države članice da imenuju nacionalna nadležna tijela, jedinstvene kontaktne točke i CSIRT-ove čije su zadaće vezane uz sigurnost mrežnih i informacijskih sustava. 3. Zahtjevi za sigurnost i obavješćivanje iz ove Direktive ne primjenjuju se na poduzeća na koje se primjenjuju zahtjevi iz članaka 13.a i 13.b Direktive 2002/21/EZ ni na pružatelje usluga povjerenja na koje se primjenjuju zahtjevi iz	– vodi brigu o potrebi razvoja i usklađivanja nacionalne strategije kibernetičke sigurnosti s ciljevima ovog Zakona i zahtjevima Europske unije u području kibernetičke sigurnosti		
	Jedinstvena nacionalna kontaktna točka *Članak 30.* Jedinstvena nacionalna kontaktna točka: – sudjeluje u radu Skupine za suradnju, koja je 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,	U potpunosti preuzeto	
	Zadaće nadležnog CSIRT-a *Članak 32.* (1) Nadležni CSIRT na sektorskoj razini, prema popisu nadležnosti iz Priloga III. ovog Zakona, obavlja sljedeće poslove: – sudjeluje u Mreži CSIRT-ova na razini Europske unije koja je osnovana s ciljem razvoja povjerenja i pouzdanja među državama članicama te promicanju brze i učinkovite operativne suradnje	U potpunosti preuzeto	

članka 19. Uredbe (EU) br. 910/2014. 4. Ova Direktiva primjenjuje se ne dovodeći u pitanje Direktivu Vijeća 2008/114/EZ (14) i direktive 2011/93/EU (15) i 2013/40/EU (16) Europskog parlamenta i Vijeća. 5. Ne dovodeći u pitanje članak 346. UFEU-a, informacije koje se smatraju povjerljivima u skladu s pravilima Unije i nacionalnim pravilima, kao što su pravila o poslovnoj tajni, Komisiji i drugim relevantnim tijelima, ustupaju se samo u slučaju kad je takva razmjena nužna za primjenu ove Direktive. Razmijenjene informacije ograničuju se na ono što je relevantno i mora biti razmjerna svrsi takve razmjene. Pri takvoj razmjeni informacija čuva se povjerljivost tih informacija te se štite sigurnost i komercijalni interesi operatora ključnih usluga i pružatelja digitalnih usluga. 6. Ovom Direktivom ne dovode se u pitanje mjere koje države članice poduzimaju za zaštitu svojih temeljnih državnih funkcija, posebno za zaštitu nacionalne sigurnosti, što uključuje mjere za	*Utvrđivanje mjera* *Članak 20.* (1) Mjere za postizanje visoke razine kibernetičke sigurnosti operatora ključnih usluga i način njihove provedbe pobliže se propisuju uredbom koju donosi Vlada. (2) Mjere za postizanje visoke razine kibernetičke sigurnosti davatelja digitalnih usluga provode se sukladno Provedbenoj uredbi Komisije (EU) 2018/151 od 30. siječnja 2018. o utvrđivanju pravila za primjenu Direktive (EU) 2016/1148 Europskog parlamenta i Vijeća u odnosu na dodatne specifikacije elemenata koje pružatelji digitalnih usluga moraju uzeti u obzir u upravljanju rizicima kojima je izložena sigurnost njihovih mrežnih i informacijskih sustava i parametara za utvrđivanje ima li incident znatan učinak (SL L 26/48, 31.1.2018.).	Djelomično preuzeto	Bit će preuzeto u: Uredba o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga (09.04.2018)
	Obveza obavješćivanja *Članak 21.* (1) Operatori ključnih usluga i davatelji digitalnih usluga dužni su nadležni CSIRT, bez neopravdane odgode, obavješćivati o incidentima koji imaju znatan učinak na kontinuitet usluga koje pružaju. (2) Ako je incident na mrežnom i informacijskom sustavu davatelja digitalne usluge imao znatan učinak na pružanje neke ključne usluge, operator ključne usluge dužan je o tom incidentu obavijestiti nadležni CSIRT. (3) Obveza obavješćivanja iz ovog članka odnosi se na incidente na mrežnim i informacijskim sustavima iz članka 17. ovog Zakona. *Kriteriji za određivanje učinka incidenata* *Članak 22.*	Djelomično preuzeto	Bit će preuzeto u: Uredba o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga (09.04.2018)

<table>
<tr>
<td>zaštitu informacija za čije otkrivanje države članice smatraju da bi bilo suprotno osnovnim interesima njihove sigurnosti, te za održavanje zakona i reda, posebno za to da se dopuste istraga, otkrivanje i kažnjavanje kaznenih djela.

7. Ako se pravnim aktom Unije za pojedini sektor od operatora ključnih usluga ili pružatelja digitalnih usluga zahtijeva da osiguraju ili sigurnost svojih mrežnih i informacijskih sustava ili da obavijeste o incidentima, pod uvjetom da su takvi zahtjevi po učinku barem jednaki obvezama utvrđenima u ovoj Direktivi, primjenjuju se te odredbe iz tog pravnog akta Unije za pojedini sektor.</td>
<td>(1) Kriteriji za određivanje incidenata koji imaju znatan učinak na pružanje ključnih usluga propisuju se uredbom Vlade iz članka 20. stavka 1. ovog Zakona.

(2) Kriteriji za određivanje incidenata koji imaju znatan učinak na davanje digitalnih usluga propisani su Provedbenom uredbom Komisije iz članka 20. stavka 2. ovog Zakona.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Prilog III.

Popis nadležnih tijela

Jedinstvena nacionalna kontaktna točka - Ured Vijeća za nacionalnu sigurnost
<table>
<tr><th>Sektor</th><th>Nadležno sektorsko tijelo</th><th>CSIRT</th><th>Tehničko tijelo za ocjenu sukladnosti</th></tr>
<tr><td>Energetika</td><td>središnje državno tijelo nadležno za energetiku</td><td>Zavod za sigurnost informacijskih sustava</td><td>Zavod za sigurnost informacijskih sustava</td></tr>
<tr><td>Prijevoz</td><td>središnje državno tijelo nadležno za promet</td><td>Zavod za sigurnost informacijskih sustava</td><td>Zavod za sigurnost informacijskih sustava</td></tr>
<tr><td>Bankarstvo</td><td>Hrvatska narodna banka</td><td>Nacionalni CERT</td><td>-</td></tr>
<tr><td>Infrastrukture financijskog tržišta</td><td>Hrvatska agencija za nadzor financijskih usluga</td><td>Nacionalni CERT</td><td>-</td></tr>
</table></td>
<td>U potpunosti preuzeto</td>
<td></td>
</tr>
</table>

Zdravstveni sektor	središnje državno tijelo nadležno za zdravstvo	Zavod za sigurnost informacijskih sustava	Zavod za sigurnost informacijskih sustava
Opskrba vodom za piće i njezina distribucija	središnje državno tijelo nadležno za vodno gospodarstvo	Zavod za sigurnost informacijskih sustava	Zavod za sigurnost informacijskih sustava
Digitalna infrastruktura	središnje državno tijelo nadležno za znanost i obrazovanje	Nacionalni CERT	Hrvatska akademska i istraživačka mreža - CARNet
Davatelji digitalnih usluga	središnje državno tijelo nadležno za gospodarstvo	Nacionalni CERT	Zavod za sigurnost informacijskih sustava
Usluge u sustavima državne informacijske infrastrukture	Središnji državni ured za razvoj digitalnog društva	Zavod za sigurnost informacijskih sustava ili Nacionalni CERT*	Zavod za sigurnost informacijskih sustava ili Nacionalni CERT**

*Napomena: Nadležni CSIRT za sektor Usluge u sustavima državne informacijske infrastrukture za sve usluge je Zavod za sigurnost informacijskih sustava, osim za područje koje je u djelokrugu središnjeg državnog tijela nadležnog za znanost i obrazovanje, Sveučilišnog računskog centra (SRCE) ili CARNeta, za koje je nadležni CSIRT Nacionalni CERT.

**Napomena: Tehničko tijelo za ocjenu sukladnosti za sektor Usluge u sustavima državne informacijske infrastrukture za sve usluge je Zavod

	za sigurnost informacijskih sustava, osim za područje koje je u djelokrugu središnjeg državnog tijela nadležnog za znanost i obrazovanje, Sveučilišnog računskog centra (SRCE) ili Hrvatske akademske i istraživačke mreže – CARNeta, za koje je tehničko tijelo za ocjenu sukladnosti Hrvatska akademska i istraživačka mreža – CARNet.		
	Primjena *Članak 3.* (1) Ovaj Zakon primjenjuje se na operatore ključnih usluga, neovisno o tome jesu li u pitanju javni ili privatni subjekti, neovisno o državi njihova sjedišta, njihovoj veličini, ustroju i vlasništvu. (2) Davatelji digitalnih usluga podliježu nadležnostima i ovlastima propisanim ovim Zakonom ako na teritoriju Republike Hrvatske imaju sjedište ili svog predstavnika te pod uvjetom da takav davatelj ne predstavlja mikro ili mali subjekt malog gospodarstva kako su oni definirani Zakonom o poticanju razvoja malog gospodarstva („Narodne novine“, broj: 29/02., 63/07., 53/12., 56/13. i 121/16.).	U potpunosti preuzeto	
	ZAŠTITA PODATAKA Članak 40. (1) Popisi operatora ključnih usluga, kao i svi drugi podaci koji nastaju u okviru provedbe ovog Zakona koriste se isključivo u svrhu izvršavanja zahtjeva iz ovog Zakona. (2) Nadležna tijela dužna su pri razmjeni podataka iz stavka 1. ovog članka voditi računa o potrebi ograničavanja pristupa podacima kada je	U potpunosti preuzeto	

	to potrebno u svrhu sprječavanja, otkrivanja, provođenja istraživanja i vođenja kaznenog postupka. (3) Podaci iz stavka 1. ovog članka predstavljaju informacije u odnosu na koje je moguće ograničiti pravo pristupa korisniku informacija, ovisno o rezultatima testa razmjernosti i javnog interesa koji se provodi prema odredbama posebnog zakona o pravu na pristup informacijama. Članak 41. Nadležna tijela iz ovog Zakona dužna su s podacima operatora ključnih usluga i davatelja digitalnih usluga postupati u skladu sa zahtjevima povjerljivosti, ako su oni utvrđeni posebnim propisima o zaštiti takvih podataka.		
	Odnos propisa prema drugim propisima *Članak 4.* (1) Ako u provedbi ovog Zakona nastaju ili se koriste klasificirani podaci ili se obrađuju osobni podaci, na takve podatke primjenjuju se posebni propisi o njihovoj zaštiti. (2) Primjena ovog Zakona ne utječe na prava potrošača, koja su uređena posebnim zakonom. (3) Ako su za pojedini sektor s Popisa iz Priloga I. ovog Zakona posebnim zakonom propisane mjere koje po svom sadržaju i svrsi odgovaraju zahtjevima iz ovog Zakona, ili predstavljaju strože zahtjeve, na pružatelje ključnih usluga koji pripadaju tom sektoru primjenjuju se odgovarajuće odredbe tog posebnog zakona.	U potpunosti preuzeto	

	Vezano uz čl. 1 (1) (a) Dikretive (a) utvrđuje se obveza za sve države članice da donesu nacionalnu strategiju za sigurnost mrežnih i informacijskih sustava;	Djelomično preuzeto	Preuzeto u: ODLUKA O DONOŠENJU NACIONALNE STRATEGIJE KIBERNETIČKE SIGURNOSTI I AKCIJSKOG PLANA ZA PROVEDBU NACIONALNE STRATEGIJE KIBERNETIČKE SIGURNOSTI (NN 108/15) članak/članci 3., 5.2., 6.4, 7., 1.,
Članak 2. Obrada osobnih podataka 1. Obrada osobnih podataka na temelju ove Direktive provodi se u skladu s Direktivom 95/46/EZ. 2. Obrada osobnih podataka koju prema ovoj Direktivi provode institucije i tijela Unije provodi se u skladu s Uredbom (EZ) br. 45/2001.	*Odnos propisa prema drugim propisima* *Članak 4.* (1) Ako u provedbi ovoga Zakona nastaju ili se koriste klasificirani podaci ili se obrađuju osobni podaci, na takve podatke primjenjuju se posebni propisi o njihovoj zaštiti.	U potpunosti preuzeto	

Članak 3. Minimalno usklađivanje Ne dovodeći u pitanje članak 16. stavak 10. i obveze država članica u skladu s pravom Unije, države članice mogu donijeti ili zadržati odredbe čiji je cilj postizanje više razine sigurnosti mrežnih i informacijskih sustava.		Nije potrebno preuzimanje	Predmetnom odredbom Direktive propisana je mogućnost uvođenja strožih zahtjeva nacionalnim propisima te kao takva ne zahtijeva izravno prenošenje same odredbe u tekst predmetnog Nacrta zakona.
Članak 4. Definicije Za potrebe ove Direktive primjenjuju se sljedeće definicije: 1.„mrežni i informacijski sustav" znači: (a)elektronička komunikacijska mreža u smislu članka 2. točke (a) Direktive 2002/21/EZ; (b)bilo koji uređaj ili grupa 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	*Pojmovi* *Članak 5.* U smislu ovog Zakona pojedini pojmovi imaju sljedeće značenje: 1) *„kibernetička sigurnost"* – je sustav organizacijskih i tehničkih aktivnosti i mjera kojima se postiže autentičnost, povjerljivost, cjelovitost i dostupnost podataka, kao i mrežnih i informacijskih sustava u kibernetičkom prostoru 2) *„kibernetički prostor"* – je virtualni prostor unutar kojeg se odvija komunikacija između mrežnih i informacijskih sustava te obuhvaća sve mrežne i informacijske sustave neovisno o tome jesu li povezani na Internet 3) *„mrežni i informacijski sustav"* – je (a) elektronička komunikacijska mreža kako je ona definirana Zakonom o elektroničkim komunikacijama („Narodne novine", broj: 73/08., 90/11., 133/12., 80/13., 71/14. i 72/17.); (b) bilo koji uređaj ili grupa 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 opisanim u točkama (a) i (b) u svrhu njihova rada, uporabe, zaštite i održavanja	U potpunosti preuzeto	

opisanim 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 odolijevaju, na određenoj razini pouzdanosti, bilo kojoj radnji koja ugrožava dostupnost, autentičnost, cjelovitost ili povjerljivost pohranjenih ili prenesenih ili obrađenih podataka ili srodnih usluga koje ti mrežni i informacijski sustavi nude ili kojima omogućuju pristup; 3.„nacionalna strategija za sigurnost mrežnih i informacijskih sustava" znači okvir kojim se pružaju strateški ciljevi i prioriteti za sigurnost mrežnih i informacijskih sustava na nacionalnoj razini; 4.„operator ključne usluge" znači javni ili privatni subjekt tipa navedenog u Prilogu II., koji ispunjava kriterije utvrđene u članku 5. stavku 2.; 5.„digitalna usluga" znači usluga u smislu članka 1. stavka 1. točke (b) Direktive (EU) 2015/1535 Europskog parlamenta i Vijeća (17) tipa navedenog na popisu u Prilogu III.;	4) *„sigurnost mrežnih i informacijskih sustava"* – je sposobnost mrežnih i informacijskih sustava da, na određenoj razini pouzdanosti, odolijevaju bilo kojoj radnji koja ugrožava dostupnost, autentičnost, cjelovitost ili povjerljivost, pohranjenih, prenesenih ili obrađenih podataka, ili srodnih usluga koje ti mrežni i informacijski sustavi nude ili kojima omogućuju pristup 5) *„nacionalna strategija kibernetičke sigurnosti"* – je okvir kojim se pružaju strateški ciljevi i prioriteti za kibernetičku sigurnost na nacionalnoj razini 6) *„nadležna tijela"* – su nadležna sektorska tijela, jedinstvena nacionalna kontaktna točka, nadležni CSIRT-ovi i tehnička tijela za ocjenu sukladnosti 7) *„operator ključnih usluga"* – je bilo koji javni ili privatni subjekt koji ispunjava kriterije iz članka 6. ovog Zakona 8) *„davatelj digitalnih usluga"*- je bilo koji privatni subjekt koji pruža neku digitalnu uslugu s Popisa iz Priloga II. ovog Zakona 9) *"javni subjekti"* - su tijela državne uprave, druga državna tijela, jedinice lokalne i područne (regionalne) samouprave te pravne osobe koje imaju javne ovlasti ili obavljaju javnu službu 10) *„privatni subjekti"* – su fizičke i pravne osobe koje pružaju ili daju usluge, 11) *„fizička osoba"* - je osoba obrtnika ili osoba koja obavlja drugu samostalnu djelatnost 12) *„pravna osoba"* – je svaka pravna osoba, neovisno o njezinoj veličini, ustroju i vlasništvu 13) *„sjedište"* – je stalno mjesto poslovanja gdje pružatelj odnosno davatelj usluga u neodređenom vremenskom razdoblju upravlja svojom djelatnošću 14) *„predstavnik"* – je bilo koja fizička ili pravna osoba sa sjedištem u Republici Hrvatskoj koju je davatelj digitalnih usluga koji nema sjedište u Europskoj uniji izričito imenovao da djeluje u njegovo ime i kojoj se nadležno sektorsko tijelo ili nadležni CSIRT mogu obratiti umjesto davatelju digitalnih usluga koji je obveznik primjene ovog Zakona		

6.„pružatelj digitalnih usluga" znači bilo koja pravna osoba koja pruža neku digitalnu uslugu; 7.„incident" znači bilo koji događaj koji ima stvaran negativni učinak na sigurnost mrežnih i informacijskih sustava; 8.„rješavanje incidenta" znači svi postupci koji podupiru otkrivanje, analizu i zaustavljanje incidenta te odgovor na njega; 9.„rizik" znači bilo koja razumno prepoznatljiva okolnost ili događaj koji ima potencijalan negativni učinak na sigurnost mrežnih i informacijskih sustava; 10.„predstavnik" znači bilo koja fizička ili pravna osoba s poslovnim nastanom u Uniji koju je pružatelj digitalnih usluga koji nema poslovni nastan u Uniji izričito imenovao da djeluje u njegovo ime i kojoj se nacionalno nadležno tijelo ili CSIRT mogu obratiti umjesto tom pružatelju digitalnih usluga u pogledu obveza tog pružatelja digitalnih usluga iz ove Direktive; 11.„norma" znači norma u smislu članka 2. točke 1. Uredbe (EU) br. 1025/2012; 12.„specifikacija" znači tehnička specifikacija u smislu članka 2.	15) *„incident"* – je bilo koji događaj koji ima stvaran negativni učinak na sigurnost mrežnih i informacijskih sustava 16) *„rješavanje incidenta"* – su svi postupci koji podupiru otkrivanje, analizu i zaustavljanje incidenta te odgovor na njega 17) *„rizik"* – je bilo koja razumno prepoznatljiva okolnost ili događaj koji ima potencijalno negativni učinak na sigurnost mrežnih i informacijskih sustava 18) *„središte za razmjenu internetskog prometa (IXP)"* – je mrežni instrument koji omogućuje međusobno povezivanje više od dvaju neovisnih autonomnih sustava, prvenstveno u svrhu olakšavanja razmjene internetskog prometa; IXP pruža međusobno povezivanje samo za autonomne sustave; za IXP nije potrebno da internetski promet između bilo kojih dvaju autonomnih sustava sudionika prođe kroz bilo koji treći autonomni sustav, on takav promet ne mijenja i ne utječe na njega ni na koji drugi način 19) *„sustav naziva domena (DNS)"* – je hijerarhijsko raspoređeni sustav imenovanja na mreži koji odgovara na upite o nazivima domena 20) *„pružatelj DNS usluge"* – je javni ili privatni subjekt koji pruža DNS usluge na Internetu 21) *„registri naziva vršnih domena"* – su javni ili privatni subjekti koji upravljaju i rukuju registracijom naziva internetskih domena za određenu vršnu domenu (TLD) 22) *„internetsko tržište"* – je digitalna usluga koja potrošačima i/ili trgovcima, kako su oni definirani Zakonom o alternativnom rješavanju potrošačkih sporova („Narodne novine", broj: 121/16.), omogućuje da na Internetu sklapaju kupoprodajne ugovore i ugovore o uslugama s trgovcima na mrežnoj stranici tog internetskog tržišta ili na mrežnoj stranici tog trgovca koji se služi računalnim uslugama koje pruža internetsko tržište 23) *„internetska tražilica"* – je digitalna usluga koja korisniku omogućuje da pretražuje u načelu sve internetske stranice ili internetske stranice na određenom jeziku na temelju upita o bilo kojoj temi u obliku ključne riječi, rečenice ili nekog drugog unosa,		

točke 4. Uredbe (EU) br. 1025/2012; 13.„središte za razmjenu internetskog prometa (IXP)" znači mrežni instrument koji omogućuje međusobno povezivanje više od dvaju neovisnih autonomnih sustava, prvenstveno u svrhu olakšavanja razmjene internetskog prometa; IXP pruža međusobno povezivanje samo za autonomne sustave; za IXP nije potrebno da internetski promet između bilo kojih dvaju autonomnih sustava sudionika prođe kroz bilo koji treći autonomni sustav, on takav promet ne mijenja i ne utječe na njega ni na koji drugi način; 14.„sustav naziva domena (DNS)" znači hijerarhijsko raspoređeni sustav imenovanja na mreži koji šalje upite o nazivima domena; 15.„pružatelj DNS usluge" znači subjekt koji pruža DNS usluge na internetu; 16.„registri naziva vršnih domena" znači subjekt koji upravlja i rukuje registracijom naziva internetskih domena za određenu vršnu domenu (TLD); 17.„internetsko tržište" znači digitalna usluga koja potrošačima i/ili trgovcima, kako su utvrđeni	a rezultat su poveznice na kojima se mogu pronaći informacije koje su povezane sa zatraženim sadržajem 24) *„usluga računalstva u oblaku"* – je digitalna usluga kojom se pruža pristup nadogradivom i elastičnom skupu djeljivih računalnih resursa, usluga i aplikacija 25) *„država članica"* – država članica Europske unije 26) *"kvalificirani revizor"* – je fizička ili pravna osoba koja je za obavljanje poslova revizije sigurnosti mrežnih i informacijskih sustava akreditirana pri odgovarajućoj organizaciji za normizaciju, koja je izdala ili daje na korištenje norme koje su u okviru provedbe zahtjeva iz ovog Zakona primijenjene kod određenog operatora ključnih usluga ili davatelja digitalnih usluga 27) *„revizija sigurnosti mrežnih i informacijskih sustava"* – su postupci koje obavlja kvalificirani revizor radi ocjene usklađenosti uspostavljenih procesa upravljanja mrežnim i informacijskim sustavom i dokumentiranih sigurnosnih politika sa zahtjevima iz ovog Zakona 28) *„CSIRT"* – je kratica za Computer Security Incident Response Team, odnosno tijelo nadležno za prevenciju i zaštitu od incidenata, za koju se u Republici Hrvatskoj koristi i kratica CERT (Computer Emergency Response Team).		

u članku 4. stavku 1. točki (a) odnosno točki (b) Direktive 2013/11/EU Europskog parlamenta i Vijeća (18), omogućuje da na internetu sklapaju kupoprodajne ugovore i ugovore o uslugama s trgovcima na mrežnoj stranici tog internetskog tržišta ili na mrežnoj stranici tog trgovca koji se služi računalnim uslugama koje pruža internetsko tržište; 18. „internetska tražilica" znači digitalna usluga koja korisniku omogućuje da vrši pretraživanja u načelu svih internetskih stranica ili internetskih stranica na određenom jeziku na temelju upita o bilo kojoj temi koji je u obliku ključne riječi, rečenice ili nekog drugog unosa, a rezultat su poveznice na kojima se mogu pronaći informacije koje su povezane sa zatraženim sadržajem; 19. „usluga računalstva u oblaku" znači digitalna usluga kojom se pruža pristup nadogradivom i elastičnom skupu djeljivih računalnih resursa.			

Članak 5. Identifikacija operatora ključnih usluga 1. Do 9. studenoga 2018. za svaki sektor i podsektor iz Priloga II. države članice identificiraju operatore ključnih usluga s poslovnim nastanom na njihovom državnom području. 2. Kriteriji za identifikaciju operatora ključnih usluga iz članka 4. točke 4. jesu sljedeći: (a)subjekt pruža uslugu koja je ključna za održavanje ključnih društvenih i/ili ekonomskih djelatnosti; (b)pružanje takve usluge ovisi o mrežnim i informacijskim sustavima; i (c)incident bi imao znatan negativan učinak na pružanje te usluge. 3. Za potrebe stavka 1. svaka država članica sastavlja popis usluga iz stavka 2. točke (a). 4. Za potrebe stavka 1. ako subjekt pruža uslugu kako je navedeno u	*Cilj i predmet* *Članak 1.* (3) Sastavni su dio ovog Zakona: a) Prilog I. - Popis ključnih usluga s kriterijima i pragovima za donošenje ocjene o važnosti negativnog učinka incidenta	U potpunosti preuzeto	
	Primjena *Članak 3.* (1) Ovaj Zakon primjenjuje se na operatore ključnih usluga, neovisno o tome jesu li u pitanju javni ili privatni subjekti, neovisno o državi njihova sjedišta, njihovoj veličini, ustroju i vlasništvu.	U potpunosti preuzeto	
	Određivanje operatora ključnih usluga *Članak 6.* Pojedini javni ili privatni subjekt (dalje u tekstu: subjekt) odredit će se operatorom ključnih usluga ako: a) subjekt pruža neku od ključnih usluga s Popisa iz Priloga I. ovog Zakona (dalje: ključna usluga), b) pružanje ključne usluge kod tog subjekta ovisi o mrežnim i informacijskim sustavima i c) incident bi imao znatan negativan učinak na pružanje ključne usluge.	U potpunosti preuzeto	

stavku 2. točki (a) u dvije ili više država članica, te države članice uključuju se u međusobna savjetovanja. Savjetovanja se održavaju prije nego što bude donesena odluka o identificiranju. 5. Države članice redovito, a najmanje svake dvije godine nakon 9. svibnja 2018., preispituju i, prema potrebi, ažuriraju popis identificiranih operatora ključnih usluga. 6. Uloga skupine za suradnju u skladu sa zadaćama iz članka 11. jest podupirati države članice u zauzimanju dosljednog pristupa u postupku identifikacije operatora ključnih usluga. 7. Za potrebe preispitivanja iz članka 23. i najkasnije 9. studenoga 2018., a nakon toga svake dvije godine, države članice Komisiji dostavljaju podatke koji su potrebni kako bi se Komisiji omogućila procjena provedbe ove Direktive, posebno dosljednosti u pristupu država članica pri identifikaciji	*Identifikacijski postupak* *Članak 7.* (1) Nadležna sektorska tijela provode postupak identifikacije operatora ključnih usluga po sektorima s Popisa iz Priloga I. ovog Zakona, u kojem: a) izrađuju popise svih subjekata koji pružaju ključnu uslugu, b) provode izdvajanje subjekta ovisno o važnosti negativnog učinka koji bi incident imao na pružanje ključne usluge kod tog subjekta i c) za sve izdvojene subjekte provode procjenu ovisnosti pružanja ključne usluge o mrežnim i informacijskim sustavima. (2) Nadležno sektorsko tijelo dužno je postupak identifikacije operatora ključnih usluga provoditi redovito, sukladno tržišnim promjenama u sektoru, a najmanje jednom u dvije godine.	U potpunosti preuzeto	
	Popis operatora ključnih usluga *Članak 12.* (1) Na temelju odluka iz članka 9. ovog Zakona nadležna sektorska tijela izrađuju, preispituju i ažuriraju Popise operatora ključnih usluga po sektorima s Popisa iz Priloga I. ovog Zakona. (2) Nadležna sektorska tijela obavješćuju jedinstvenu nacionalnu kontaktnu točku o broju identificiranih operatora ključnih usluga u pojedinom sektoru, s naznakom njihove važnosti za sektor.	U potpunosti preuzeto	

operatora ključnih usluga. Ti podaci obuhvaćaju barem: (a)nacionalne mjere kojima se omogućuje identifikacija operatora ključnih usluga; (b) popis usluga iz stavka 3.; (c)broj operatora ključnih usluga identificiranih za svaki sektor iz Priloga II. te oznaku njihove važnosti u odnosu na taj sektor; (d)pragove, ako postoje, za određivanje odgovarajuće razine opskrbe prema broju korisnika koji se oslanjaju na tu uslugu kako je navedeno u članku 6. stavku 1. točki (a) ili u skladu s važnošću tog određenog operatora ključnih usluga kako je navedeno u članku 6. stavku 1. točki (f). Kako bi se doprinijelo tome da dostavljeni podaci budu usporedivi, Komisija, uzimajući u najvećoj mogućoj mjeri u obzir mišljenje ENISA-e, može donijeti odgovarajuće tehničke smjernice u pogledu parametara za informacije navedene u ovom stavku.	*Jedinstvena nacionalna kontaktna točka* *Članak 30.* Jedinstvena nacionalna kontaktna točka: – dostavlja Europskoj komisiji podatke koji omogućavaju procjenu učinkovitosti provedbe mjera iz ovog Zakona i propisa donesenog na temelju ovog Zakona, sukladno zahtjevima utvrđenim propisom iz članka 2. ovog Zakona – sudjeluje u radu Skupine za suradnju, koja je osnovana u svrhu podupiranja i olakšavanja strateške suradnje i – izrađuje smjernice o sadržaju obavijesti, načinu i rokovima informiranja jedinstvene nacionalne kontaktne točke o broju identificiranih operatora ključnih usluga i naznakama njihove važnosti te o obavijestima o incidentima ***Procjena ovisnosti o mrežnom i informacijskom sustavu*** *Članak 9.* (3) Nadležno sektorsko tijelo, radi utvrđivanja kritičnosti prekograničnog učinka iz stavka 2. ovog članka, u suradnji s jedinstvenom kontaktnom točkom provodi savjetovanja s nadležnim tijelom uključene države članice. ***Zadaće nadležnog CSIRT-a*** *Članak 32.* (1) Nadležni CSIRT na sektorskoj razini, prema popisu nadležnosti iz Priloga III. ovog Zakona, obavlja sljedeće poslove: • u suradnji s nadležnim sektorskim tijelom, određuje prekogranične utjecaje incidenata iz članka 21. ovog Zakona	U potpunosti preuzeto	

	Članak 46. (1) Nadležna sektorska tijela dužna su postupak identifikacije operatora ključnih usluga provesti u roku od 90 dana od dana stupanja na snagu ovog Zakona. (2) Nadležna sektorska tijela dužna su jedinstvenoj nacionalnoj kontaktnoj točki dostaviti obavijesti iz članka 12. stavka 2. ovog Zakona u roku od 120 dana od dana stupanja na snagu ovog Zakona.	U potpunosti preuzeto	
Članak 6. Znatan negativan učinak 1. Pri utvrđivanju važnosti negativnog učinka iz točke (c) članka 5. stavka 2., države članice uzimaju u obzir barem sljedeće međusektorske čimbenike: (a)broj korisnika koji se oslanjaju na usluge koje taj subjekt pruža; (b)ovisnost drugih sektora iz Priloga II. o uslugama koje dotični subjekt pruža;	***Određivanje važnosti negativnog učinka incidenta*** *Članak 8.* (1) Za određivanje važnosti negativnog učinka koji bi incident imao na pružanje ključne usluge uzimaju se u obzir sljedeći kriteriji: – broj i vrsta korisnika kojima subjekt pruža uslugu, – postojanje ovisnosti drugih djelatnosti ili područja o pružanju usluge, – tržišni udio subjekta koji pruža uslugu, – zemljopisna raširenost subjekta u pružanju usluge, – mogući utjecaj incidenta, s obzirom na njegovu težinu i trajanje, na gospodarske i društvene aktivnosti te na javnu sigurnost,	U potpunosti preuzeto	

(c)mogući utjecaj incidenata, u pogledu njihova stupnja i trajanja, na gospodarske i društvene aktivnosti te na javnu sigurnost; (d) tržišni udio tog subjekta; (e)zemljopisnu raširenost u smislu područja na koje bi incident mogao utjecati; (f)važnost subjekta za održavanje dostatne razine usluge, uzimajući u obzir raspoloživost alternativnih sredstava za pružanje te usluge. 2. Kako bi se utvrdilo bi li incident imao znatan negativan učinak, države članice također, prema potrebi, u obzir uzimaju čimbenike specifične za pojedini sektor.	– važnosti poslovanja subjekta za održavanje dostatne razine ključne usluge, uzimajući u obzir i raspoloživost alternativnih sredstava za pružanje te usluge ili – drugi sektorski kriteriji poput količine pružene usluge, udjela u pružanju usluge ili imovine subjekta. (2) Kriteriji iz stavka 1. ovog članka, i kriterijski pragovi, ako su definirani, primjenjuju se u postupku identifikacije operatora ključnih usluga, prema njihovom razvrstavanju po ključnim uslugama kako je to predviđeno Popisom iz Priloga I. ovog Zakona. (3) Ako subjekt koji pruža ključnu uslugu ispunjava kriterije prema Popisu iz Priloga I. ovog Zakona te dostiže kriterijski prag, kada je on Popisom definiran, daje se ocjena važnosti negativnog učinka incidenta na pružanje ključne usluge za tog subjekta te se subjekt izdvaja za provođenje procjene ovisnosti pružanja ključne usluge o mrežnim i informacijskim sustavima.		
POGLAVLJE II. NACIONALNI OKVIRI ZA SIGURNOST MREŽNIH I INFORMACIJSKIH SUSTAVA Članak 7. Nacionalna strategija za sigurnost mrežnih i informacijskih sustava 1. Svaka država članica donosi nacionalnu strategiju za sigurnost mrežnih i informacijskih sustava, kojom se određuju strateški ciljevi te	*Jedinstvena nacionalna kontaktna točka* *Članak 30.* Jedinstvena nacionalna kontaktna točka: – vodi brigu o potrebi razvoja i usklađivanja nacionalne strategije kibernetičke sigurnosti s ciljevima ovog Zakona i zahtjevima Europske unije u području kibernetičke sigurnosti	Djelomično preuzeto	Preuzeto u: ODLUKA O DONOŠENJU NACIONALNE STRATEGIJE KIBERNETIČKE SIGURNOSTI I AKCIJSKOG PLANA ZA PROVEDBU NACIONALNE STRATEGIJE KIBERNETIČKE SIGURNOSTI (NN 108/15) članak/članci POGLAVLJE 3. NACIONALNE STRATEGIJE KIBERNETIČKE

primjerena politika i regulatorne mjere s ciljem postizanja i održavanja visoke razine sigurnosti mrežnih i informacijskih sustava te koja obuhvaća barem sektore iz Priloga II. i usluge navedene u Prilogu III. Nacionalna strategija za sigurnost mrežnih i informacijskih sustava posebno se bavi sljedećim pitanjima: (a)ciljevima i prioritetima nacionalnih strategija za sigurnost mrežnih i informacijskih sustava; (b)upravljačkim okvirom za postizanje ciljeva i prioriteta nacionalne strategije za sigurnost mrežnih i informacijskih sustava, među ostalim ulogama i odgovornostima vladinih tijela i drugih relevantnih sudionika; (c)određivanjem mjera u vezi s pripravnošću, odgovorom i ponovnom uspostavom, uključujući mehanizme suradnje između javnog i privatnog sektora; (d)određivanjem programâ edukacije, podizanja razine svijesti i osposobljavanja povezanih sa strategijom sigurnosti mrežnih i informacijskih sustava;			SIGURNOSTI - OPĆI CILJEVI STRATEGIJE POGLAVLJE 4. NACIONALNE STRATEGIJE KIBERNETIČKE SIGURNOSTI - SEKTORI DRUŠTVA I OBLICI SURADNJE DIONIKA KIBERNETIČKE SIGURNOSTI POGLAVLJE 5.2 Kritična komunikacijska i informacijska infrastruktura i upravljanje kibernetičkim krizama (D) POGLAVLJE 6.4. NACIONALNE STRATEGIJE KIBERNETIČKE SIGURNOSTI - Obrazovanje, istraživanje, razvoj i jačanje svijesti o sigurnosti u kibernetičkom prostoru (I) POGLAVLJE 7. NACIONALNE STRATEGIJE KIBERNETIČKE SIGURNOSTI - PROVEDBA STRATEGIJE POGLAVLJE 1. AKCIJSKOG PLANA ZA PROVEDBU NACIONALNE

(e)određivanjem istraživačkih i razvojnih planova u pogledu strategije za sigurnost mrežnih i informacijskih sustava; (f)planom za procjenu rizika s ciljem prepoznavanja rizika; (g)popisom različitih sudionika u provedbi nacionalne strategije za sigurnost mrežnih i informacijskih sustava. 2. Države članice mogu zatražiti podršku ENISA-e u razvijanju nacionalnih strategija za sigurnost mrežnih i informacijskih sustava. 3. Države članice priopćuju svoje nacionalne strategije za sigurnost mrežnih i informacijskih sustava Komisiji u roku od tri mjeseca od njihova donošenja. Pritom države članice mogu isključiti elemente strategije koji su povezani s nacionalnom sigurnosti.			STRATEGIJE KIBERNETIČKE SIGURNOSTI - UVOD POGLAVLJE 2. PODRUČJA I POVEZNICE PODRUČJA KIBERNETIČKE SIGURNOSTI - D. Kritična komunikacijska i informacijska infrastruktura i upravljanje krizama; I. Obrazovanje, istraživanje, razvoj i jačanje svijesti o sigurnosti u kibernetičkom prostoru DODATAK AKCIJSKOM PLANU ZA PROVEDBU NACIONALNE STRATEGIJE KIBERNETIČKE SIGURNOSTI - KRATICE Nacionalna strategija kibernetičke sigurnosti RH prevedena je na engleski jezik te je raspoloživa, zajedno sa strategijama drugih država članica, na poveznici: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/strategies/croatian-cyber-security-strategy.

	Članak 31. Jedinstvena nacionalna kontaktna točka je Ured Vijeća za nacionalnu sigurnost.	Djelomično preuzeto	Preuzeto u: Odluka o osnivanju Nacionalnog vijeća za kibernetičku sigurnost i Operativno-tehničke koordinacije za kibernetičku sigurnost (NN 61/16) članak/članci II. Zadaće Nacionalnog vijeća su: – sustavno pratiti i koordinirati provedbu Nacionalne strategije kibernetičke sigurnosti (u daljnjem tekstu: Strategija) te raspravljati o svim pitanjima od važnosti za kibernetičku sigurnost – predlagati mjere za unaprjeđenje provođenja Strategije i Akcijskog plana za provedbu Strategije (u daljnjem tekstu: Akcijski plan) – predlagati organiziranje nacionalnih vježbi iz područja kibernetičke sigurnosti, – izrađivati preporuke, mišljenja, izvješća i smjernice u vezi s provedbom Strategije i Akcijskog plana – predlagati izmjene i dopune Strategije i Akcijskog plana odnosno donošenje nove Strategije i akcijskih planova, u skladu s novim potrebama

			– razmatrati pitanja bitna za upravljanje u kibernetičkim krizama i predlagati mjere za veću učinkovitost – razmatrati izvješća o stanju kibernetičke sigurnosti koja mu dostavlja Operativno-tehnička koordinacija – izrađivati periodične procjene o stanju kibernetičke sigurnosti – utvrđivati planove postupanja u kibernetičkim krizama te – izrađivati programe i planove aktivnosti Operativno-tehničke koordinacije i usmjeravati njezin rad. IV. Članovi Nacionalnog vijeća su: – predstavnik Ureda Vijeća za nacionalnu sigurnost, predsjednik – predstavnik Ministarstva unutarnjih poslova, član – predstavnik Ministarstva vanjskih i europskih poslova, član – predstavnik Ministarstva uprave, član – predstavnik Ministarstva gospodarstva, član

			– predstavnik Ministarstva znanosti, obrazovanja i sporta, član – predstavnik Ministarstva obrane, član – predstavnik Ministarstva pravosuđa, član – predstavnik Sigurnosno-obavještajne agencije, član – predstavnik Zavoda za sigurnost informacijskih sustava, član – predstavnik Operativno-tehničkog centra za nadzor telekomunikacija, član – predstavnik Državne uprave za zaštitu i spašavanje, član predstavnik Hrvatske akademske i istraživačke mreže – CARNet-a, Nacionalnog CERT-a, član – predstavnik Hrvatske regulatorne agencije za mrežne djelatnosti, član – predstavnik Hrvatske narodne banke, član – predstavnik Agencije za zaštitu osobnih podataka, član.

Članak 8. Nacionalna nadležna tijela i jedinstvene kontaktne točke 1. Svaka država članica imenuje jedno ili više nacionalnih nadležnih tijela za sigurnost mrežnih i informacijskih sustava („nadležno tijelo") koja obuhvaćaju barem sektore iz Priloga II. i usluge iz Priloga III. Države članice mogu tu ulogu dodijeliti postojećem tijelu ili tijelima. 2. Nadležna tijela nadgledaju primjenu ove Direktive na nacionalnoj razini. 3. Svaka država određuje nacionalnu jedinstvenu kontaktnu točku za sigurnost mrežnih i informacijskih sustava („jedinstvena kontaktna točka"). Države članice mogu tu ulogu dodijeliti postojećem tijelu. Ako država članica odredi samo jedno nadležno tijelo, to nadležno tijelo također je i jedinstvena kontaktna točka. 4. Jedinstvena kontaktna točka izvršava funkciju povezivanja s ciljem osiguravanja prekogranične suradnje tijela države članice s relevantnim tijelima u drugim	*Cilj i predmet* *Članak 1.* (1) Ovim se Zakonom uređuju postupci i mjere za postizanje visoke zajedničke razine kibernetičke sigurnosti operatora ključnih usluga i davatelja digitalnih usluga, nadležnosti i ovlasti nadležnih sektorskih tijela, jedinstvene nacionalne kontaktne točke, tijela nadležnih za prevenciju i zaštitu od incidenata (dalje u tekstu: nadležni CSIRT) i tehničkog tijela za ocjenu sukladnosti, nadzor nad operatorima ključnih usluga i davateljima digitalnih usluga u provedbi ovog Zakona i prekršajne odredbe. (3) Sastavni su dio ovog Zakona: c) Prilog III. - Popis nadležnih tijela.	U potpunosti preuzeto	
	Nadležna sektorska tijela *Članak 25.* (1) Nadležna sektorska tijela utvrđena su Popisom iz Priloga III. ovog Zakona. (2) Nadležna sektorska tijela obavljaju sljedeće poslove: – provode postupke identifikacije operatora ključnih usluga sukladno ovome Zakonu – obavljaju nadzor operatora ključnih usluga i davatelja digitalnih usluga u provedbi mjera za postizanje visoke razine kibernetičke sigurnosti i ispunjavanju drugih obveza iz ovog Zakona – međusobno surađuju i razmjenjuju iskustva u provedbi ovog Zakona – surađuju i razmjenjuju relevantne informacije s drugim nadležnim tijelima iz ovog Zakona – surađuju i razmjenjuju relevantne informacije s tijelom za zaštitu osobnih podataka, kada su osobni podaci ugroženi zbog	U potpunosti preuzeto	

državama članicama te sa skupinom za suradnju iz članka 11. i mrežom CSIRT-ova iz članka 12. 5. Države članice osiguravaju da nadležna tijela i jedinstvene kontaktne točke imaju odgovarajuće resurse za učinkovitu i djelotvornu provedbu zadaća koje su im dodijeljene te da tako ispune ciljeve ove Direktive. Države članice osiguravaju učinkovitu, djelotvornu i sigurnu suradnju imenovanih predstavnika u skupini za suradnju. 6. Nadležna tijela i jedinstvena kontaktna točka, kad god je to prikladno i u skladu s nacionalnim pravom, savjetuju se s relevantnim nacionalnim tijelima za izvršavanje zakonodavstva i nacionalnim tijelima za zaštitu podataka te s njima surađuju. 7. Svaka država članica bez odgode obavješćuje Komisiju o imenovanju nadležnog tijela i jedinstvene kontaktne točke te njihovim zadaćama i svim naknadnim promjenama. Svaka država članica objavljuje imenovanje nadležnog tijela i jedinstvene kontaktne točke.	incidenta na mrežnom i informacijskom sustavu operatora ključne usluge odnosno davatelja digitalne usluge, odnosno s pravosudnim tijelima, kada je takav incident rezultat kriminalnih aktivnosti.		
	Jedinstvena nacionalna kontaktna točka *Članak 30.* Jedinstvena nacionalna kontaktna točka: – dostavlja Europskoj komisiji podatke koji omogućavaju procjenu učinkovitosti provedbe mjera iz ovog Zakona i propisa donesenog na temelju ovog Zakona, sukladno zahtjevima utvrđenim propisom iz članka 2. ovog Zakona – sudjeluje u radu Skupine za suradnju, koja je 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, – jednom godišnje podnosi Skupini za suradnju sažeto izvješće o zaprimljenim obavijestima o incidentima, među ostalim o broju obavijesti i naravi incidenata o kojima ih se obavijestilo te o radnjama poduzetim u skladu s člankom 21. i člankom 32. stavkom 1. točkama 8., 10. i 11. ovog Zakona, osim za sektor usluga u sustavima državne informacijske infrastrukture – na zahtjev nadležnog CSIRT-a, obavijesti o incidentima iz članka 21. ovog Zakona prosljeđuje jedinstvenim kontaktnim točkama drugih pogođenih država članica, osim za sektor usluga u sustavima državne informacijske infrastrukture – izrađuje smjernice o sadržaju obavijesti, načinu i rokovima informiranja jedinstvene nacionalne kontaktne točke o broju	U potpunosti preuzeto	

<table>
<tr>
<td>Komisija objavljuje popis određenih jedinstvenih kontaktnih točaka.</td>
<td>identificiranih operatora ključnih usluga i naznakama njihove važnosti te o obavijestima o incidentima
– vodi brigu o potrebi razvoja i usklađivanja nacionalne strategije kibernetičke sigurnosti s ciljevima ovog Zakona i zahtjevima Europske unije u području kibernetičke sigurnosti
– surađuje s drugim nadležnim tijelima iz ovog Zakona,
– kada je to potrebno, savjetuje se i surađuje s tijelom za zaštitu osobnih podataka i pravosudnim tijelima.

Članak 31.

Jedinstvena nacionalna kontaktna točka je Ured Vijeća za nacionalnu sigurnost.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Prilog III.

Popis nadležnih tijela

Jedinstvena nacionalna kontaktna točka - Ured Vijeća za nacionalnu sigurnost
<table>
<tr><th>Sektor</th><th>Nadležno sektorsko tijelo</th><th>CSIRT</th><th>Tehničko tijelo za ocjenu sukladnosti</th></tr>
<tr><td>Energetika</td><td>središnje državno tijelo nadležno za energetiku</td><td>Zavod za sigurnost informacijskih sustava</td><td>Zavod za sigurnost informacijskih sustava</td></tr>
<tr><td>Prijevoz</td><td>središnje državno tijelo nadležno za promet</td><td>Zavod za sigurnost informacijskih sustava</td><td>Zavod za sigurnost informacijskih sustava</td></tr>
</table>
</td>
<td>U potpunosti preuzeto</td>
<td></td>
</tr>
</table>

Bankarstvo	Hrvatska narodna banka	Nacionalni CERT	-
Infrastrukture financijskog tržišta	Hrvatska agencija za nadzor financijskih usluga	Nacionalni CERT	-
Zdravstveni sektor	središnje državno tijelo nadležno za zdravstvo	Zavod za sigurnost informacijskih sustava	Zavod za sigurnost informacijskih sustava
Opskrba vodom za piće i njezina distribucija	središnje državno tijelo nadležno za vodno gospodarstvo	Zavod za sigurnost informacijskih sustava	Zavod za sigurnost informacijskih sustava
Digitalna infrastruktura	središnje državno tijelo nadležno za znanost i obrazovanje	Nacionalni CERT	Hrvatska akademska i istraživačka mreža - CARNet
Davatelji digitalnih usluga	središnje državno tijelo nadležno za gospodarstvo	Nacionalni CERT	Zavod za sigurnost informacijskih sustava
Usluge u sustavima državne informacijske infrastrukture	Središnji državni ured za razvoj digitalnog društva	Zavod za sigurnost informacijskih sustava ili Nacionalni CERT*	Zavod za sigurnost informacijskih sustava ili Nacionalni CERT**

	*Napomena: Nadležni CSIRT za sektor Usluge u sustavima državne informacijske infrastrukture za sve usluge je Zavod za sigurnost informacijskih sustava, osim za područje koje je u djelokrugu središnjeg državnog tijela nadležnog za znanost i obrazovanje, Sveučilišnog računskog centra (SRCE) ili CARNeta, za koje je nadležni CSIRT Nacionalni CERT. **Napomena: Tehničko tijelo za ocjenu sukladnosti za sektor Usluge u sustavima državne informacijske infrastrukture za sve usluge je Zavod za sigurnost informacijskih sustava, osim za područje koje je u djelokrugu središnjeg državnog tijela nadležnog za znanost i obrazovanje, Sveučilišnog računskog centra (SRCE) ili Hrvatske akademske i istraživačke mreže – CARNeta, za koje je tehničko tijelo za ocjenu sukladnosti Hrvatska akademska i istraživačka mreža – CARNet.		
Članak 9. Timovi za odgovor na računalne sigurnosne incidente (CSIRT-ovi) 1. Svaka država članica imenuje jedan ili više CSIRT-ova koji udovoljavaju zahtjevima iz točke 1. Priloga I. i koji obuhvaćaju barem sektore iz Priloga II. i usluge iz Priloga III., odgovornih za rješavanje rizika i incidenata u skladu s točno propisanim	*Cilj i predmet* *Članak 1.* (1) Ovim se Zakonom uređuju postupci i mjere za postizanje visoke zajedničke razine kibernetičke sigurnosti operatora ključnih usluga i davatelja digitalnih usluga, nadležnosti i ovlasti nadležnih sektorskih tijela, jedinstvene nacionalne kontaktne točke, tijela nadležnih za prevenciju i zaštitu od incidenata (dalje u tekstu: nadležni CSIRT) i tehničkog tijela za ocjenu sukladnosti, nadzor nad operatorima ključnih usluga i davateljima digitalnih usluga u provedbi ovog Zakona i prekršajne odredbe. (3) Sastavni su dio ovog Zakona: c) Prilog III. - Popis nadležnih tijela.	U potpunosti preuzeto	

postupkom. CSIRT se može osnovati unutar nadležnog tijela. 2. Države članice imenovanim CSIRT-ovima osiguravaju odgovarajuće resurse za učinkovito izvršavanje zadaća iz Priloga I. točke 2. Države članice osiguravaju učinkovitu, djelotvornu i sigurnu suradnju svojih CSIRT-ova u mreži CSIRT-ova iz članka 12. 3. Države članice osiguravaju da CSIRT-ovi imaju pristup prikladnoj, sigurnoj i otpornoj infrastrukturi za komunikaciju i informiranje na nacionalnoj razini. 4. Države članice obavješćuju Komisiju o mandatu i glavnim elementima postupka za rješavanje incidenata svojih CSIRT-ova. 5. Države članice mogu zatražiti podršku ENISA-e u razvijanju nacionalnih CSIRT-ova.	*Zadaće nadležnog CSIRT-a* *Članak 32.* (1) Nadležni CSIRT na sektorskoj razini, prema popisu nadležnosti iz Priloga III. ovog Zakona, obavlja sljedeće poslove: – prati incidente – pruža rana upozorenja i najave te informira o rizicima i incidentima – provodi dinamičku analizu rizika i incidenata te izrađuje pregled situacije u sektoru – provodi redovite provjere ranjivosti mrežnih i informacijskih sustava operatora ključnih usluga odnosno davatelja digitalnih usluga – prima obavijesti o incidentima – na zahtjev operatora ključnih usluga odnosno davatelja digitalnih usluga analizira i odgovara na incidente – ako to dopuštaju okolnosti, nakon primitka obavijesti o incidentu dostavlja operatoru ključnih usluga relevantne informacije u pogledu daljnjeg postupanja po njegovoj obavijesti, a osobito informacije koje bi mogle doprinijeti djelotvornom rješavanju incidenta – donosi smjernice o provedbi obveze obavješćivanja o incidentima iz članka 21. ovog Zakona – informira nadležno sektorsko tijelo o incidentima iz članka 21. ovog Zakona	U potpunosti preuzeto	

	– u suradnji s nadležnim sektorskim tijelom, određuje prekogranične utjecaje incidenata iz članka 21. ovog Zakona – informira jedinstvenu nacionalnu kontaktnu točku o incidentima iz članka 21. ovog Zakona, sukladno njezinim smjernicama – dostavlja jedinstvenoj nacionalnoj kontaktnoj točki podatke o glavnim elementima postupaka rješavanja incidenata koje provodi, – obavješćuje nadležni CSIRT druge pogođene države članice ili više njih o incidentu iz članka 21. ovog Zakona na mrežnom i informacijskom sustavu operatora ključnih usluga ako incident ima znatan učinak na kontinuitet ključnih usluga u toj državi članici, – obavješćuje nadležni CSIRT druge pogođene države članice ili više njih o incidentu iz članka 21. ovog Zakona na mrežnom i informacijskom sustavu pružatelja digitalnih usluga ako se incident odnosi na dvije ili više država članica – surađuje s drugim CSIRT-ovima na nacionalnoj i međunarodnoj razini – sudjeluje u Mreži CSIRT-ova na razini Europske unije koja je osnovana s ciljem razvoja povjerenja i pouzdanja među državama članicama te promicanju brze i učinkovite operativne suradnje – promiče usvajanje i primjenu zajedničkih ili normiranih praksi za postupke rješavanja incidenata i rizika te planove za klasifikaciju incidenata, rizika i informacija.		

	(2) Operatori ključnih usluga i davatelji digitalnih usluga dužni su surađivati s nadležnim CSIRT-om i s njim razmjenjivati potrebne informacije u postupku rješavanja incidenata. (3) Nadležni CSIRT u obavljanju svojih zadaća iz ovog Zakona ne može snositi odgovornost za štetu uzrokovanu incidentom na mrežnim i informacijskim sustavima operatora ključnih usluga i davatelja digitalnih usluga.		
	Osiguravanje uvjeta za obavljanje poslova nadležnog CSIRT-a *Članak 33.* (1) Nadležni CSIRT je dužan: – osigurati visoku razinu dostupnosti svojih usluga komuniciranja izbjegavanjem jedinstvenih točki prekida, uz raspoloživost sredstava za mogućnost dvosmjernog kontaktiranja te jasno određenim i poznatim komunikacijskim kanalima za njihove klijente i suradnike – svoje prostore i informacijske sustave za potporu smjestiti na sigurne lokacije i – osigurati kontinuitet rada na način da: a) je opremljen odgovarajućim sustavom za upravljanje zahtjevima i njihovim preusmjeravanjem, kako bi se olakšale primopredaje b) ima dovoljno zaposlenika kako bi se na odgovarajući način osigurala dostupnost u svako doba	U potpunosti preuzeto	

c) se oslanja na infrastrukturu čiji je kontinuitet osiguran te su im u tu svrhu dostupni redundantni sustavi i rezervni radni prostor.

(2) Radi osiguranja uvjeta iz stavka 1. ovog članka, na nadležne CSIRT-ove neće se primjenjivati ograničavajuće odredbe drugih propisa koje utječu na mogućnost novih zapošljavanja ili druga pitanja bitna za osiguranje tih uvjeta.

Prilog III.

Popis nadležnih tijela

Jedinstvena nacionalna kontaktna točka - Ured Vijeća za nacionalnu sigurnost

Sektor	**Nadležno sektorsko tijelo**	**CSIRT**	**Tehničko tijelo za ocjenu sukladnosti**
Energetika	središnje državno tijelo nadležno za energetiku	Zavod za sigurnost informacijskih sustava	Zavod za sigurnost informacijskih sustava
Prijevoz	središnje državno tijelo nadležno za promet	Zavod za sigurnost informacijskih sustava	Zavod za sigurnost informacijskih sustava
Bankarstvo	Hrvatska narodna banka	Nacionalni CERT	-
Infrastrukture financijskog tržišta	Hrvatska agencija za nadzor	Nacionalni CERT	-

U potpunosti preuzeto

	financijskih usluga		
Zdravstveni sektor	središnje državno tijelo nadležno za zdravstvo	Zavod za sigurnost informacijskih sustava	Zavod za sigurnost informacijskih sustava
Opskrba vodom za piće i njezina distribucija	središnje državno tijelo nadležno za vodno gospodarstvo	Zavod za sigurnost informacijskih sustava	Zavod za sigurnost informacijskih sustava
Digitalna infrastruktura	središnje državno tijelo nadležno za znanost i obrazovanje	Nacionalni CERT	Hrvatska akademska i istraživačka mreža - CARNet
Davatelji digitalnih usluga	središnje državno tijelo nadležno za gospodarstvo	Nacionalni CERT	Zavod za sigurnost informacijskih sustava
Usluge u sustavima državne informacijske infrastrukture	Središnji državni ured za razvoj digitalnog društva	Zavod za sigurnost informacijskih sustava ili Nacionalni CERT*	Zavod za sigurnost informacijskih sustava ili Nacionalni CERT**

*Napomena: Nadležni CSIRT za sektor Usluge u sustavima državne informacijske infrastrukture za sve usluge je Zavod za sigurnost informacijskih sustava, osim za područje koje je u djelokrugu središnjeg državnog tijela nadležnog za znanost i obrazovanje, Sveučilišnog računskog centra (SRCE) ili CARNeta, za koje je nadležni CSIRT Nacionalni CERT.

	**Napomena: Tehničko tijelo za ocjenu sukladnosti za sektor Usluge u sustavima državne informacijske infrastrukture za sve usluge je Zavod za sigurnost informacijskih sustava, osim za područje koje je u djelokrugu središnjeg državnog tijela nadležnog za znanost i obrazovanje, Sveučilišnog računskog centra (SRCE) ili Hrvatske akademske i istraživačke mreže – CARNeta, za koje je tehničko tijelo za ocjenu sukladnosti Hrvatska akademska i istraživačka mreža – CARNet.		
Članak 10. Suradnja na nacionalnoj razini 1. Ako su odvojeni, nadležno tijelo, jedinstvena kontaktna točka i CSIRT-ovi iste države članice surađuju u pogledu ispunjavanja obveza propisanih u ovoj Direktivi. 2. Države članice osiguravaju da bilo nadležna tijela ili CSIRT-ovi primaju obavijesti o incidentima podnesene u skladu s ovom Direktivom. Ako država članica odluči da CSIRT-ovi ne primaju obavijesti, CSIRT-ovima se, u onoj mjeri u kojoj je to potrebno za ispunjavanje njihovih zadaća, omogućuje pristup podacima o incidentima o kojima su obavijestili operatori ključnih usluga u skladu s člankom 14. stavcima 3. i 5. ili	*Nadležna sektorska tijela* *Članak 25.* (2) Nadležna sektorska tijela obavljaju sljedeće poslove: – surađuju i razmjenjuju relevantne informacije s drugim nadležnim tijelima iz ovog Zakona ***Jedinstvena nacionalna kontaktna točka*** *Članak 30.* Jedinstvena nacionalna kontaktna točka: – surađuje s drugim nadležnim tijelima iz ovog Zakona,	U potpunosti preuzeto	
	Obveza obavješćivanja *Članak 21.* (1) Operatori ključnih usluga i davatelji digitalnih usluga dužni su nadležni CSIRT, bez neopravdane odgode, obavješćivati o incidentima koji imaju znatan učinak na kontinuitet usluga koje pružaju. (2) Ako je incident na mrežnom i informacijskom sustavu davatelja digitalne usluge imao znatan učinak na pružanje neke ključne usluge, operator ključne usluge dužan je o tom incidentu obavijestiti nadležni CSIRT.	U potpunosti preuzeto	

pružatelji digitalnih usluga, u skladu s člankom 16. stavcima 3. i 6. 3. Države članice osiguravaju da nadležna tijela ili CSIRT-ovi informiraju jedinstvene kontaktne točke o obavijestima o incidentima koje su im dostavljene u skladu s ovom Direktivom. Do 9. kolovoza 2018., a nakon toga svake godine, jedinstvena kontaktna točka podnosi skupini za suradnju sažeto izvješće o zaprimljenim obavijestima, među ostalim o broju obavijesti i naravi incidenata o kojima ih se obavijestilo te o radnjama poduzetim u skladu s člankom 14. stavcima 3. i 5. te člankom 16. stavcima 3. i 6.	(3) Obveza obavješćivanja iz ovog članka odnosi se na incidente na mrežnim i informacijskim sustavima iz članka 17. ovog Zakona.		
	Zadaće nadležnog CSIRT-a *Članak 32.* (1) Nadležni CSIRT na sektorskoj razini, prema popisu nadležnosti iz Priloga III. ovog Zakona, obavlja sljedeće poslove: – prima obavijesti o incidentima – informira nadležno sektorsko tijelo o incidentima iz članka 21. ovog Zakona – u suradnji s nadležnim sektorskim tijelom, određuje prekogranične utjecaje incidenata iz članka 21. ovog Zakona – informira jedinstvenu nacionalnu kontaktnu točku o incidentima iz članka 21. ovog Zakona, sukladno njezinim smjernicama – dostavlja jedinstvenoj nacionalnoj kontaktnoj točki podatke o glavnim elementima postupaka rješavanja incidenata koje provodi,	U potpunosti preuzeto	

	Jedinstvena nacionalna kontaktna točka *Članak 30.* Jedinstvena nacionalna kontaktna točka: – jednom godišnje podnosi Skupini za suradnju sažeto izvješće o zaprimljenim obavijestima o incidentima, među ostalim o broju obavijesti i naravi incidenata o kojima ih se obavijestilo te o radnjama poduzetim u skladu s člankom 21. i člankom 32. stavkom 1. točkama 8., 10. i 11. ovog Zakona, osim za sektor usluga u sustavima državne informacijske infrastrukture	U potpunosti preuzeto	
POGLAVLJE III. SURADNJA Članak 11. Skupina za suradnju 1. U svrhu podupiranja i olakšavanja strateške suradnje i razmjene informacija među državama članicama te razvijanja povjerenja i pouzdanja s ciljem postizanja visoke zajedničke razine sigurnosti mrežnih i informacijskih sustava u Uniji, uspostavlja se skupina za suradnju. Skupina za suradnju izvršava svoje zadaće na temelju dvogodišnjih programa rada iz stavka 3. drugog podstavka.		Nije potrebno preuzimanje	U pitanju 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.

2. Skupina za suradnju sastoji se od predstavnika država članica, Komisije i ENISA-e. Skupina za suradnju može, prema potrebi, pozvati predstavnike relevantnih zainteresiranih strana da sudjeluju u njezinu radu. Komisija osigurava tajništvo. 3. Zadaće su skupine za suradnju: (a)pružanje strateških smjernica za aktivnosti mreže CSIRT-ova osnovane prema članku 12.; (b)razmjena najbolje prakse o razmjeni informacija povezanih s obavijestima o incidentima iz članka 14. stavaka 3. i 5. i članka 16. stavaka 3. i 6.; (c)razmjena najbolje prakse među državama članicama i, u suradnji s ENISA-om, pomaganje državama članicama u izgradnji kapaciteta za sigurnost mrežnih i informacijskih sustava; (d)rasprava o sposobnostima i pripravnosti država članica te, na dobrovoljnoj osnovi, obavljanje procjene nacionalnih strategija za sigurnost mrežnih i informacijskih sustava i učinkovitosti CSIRT-ova te utvrđivanje najbolje prakse;			

(e)razmjena informacija i najbolje prakse u pogledu podizanja svijesti i osposobljavanja; (f)razmjena informacija i najbolje prakse u pogledu istraživanja i razvoja u vezi sa sigurnošću mrežnih i informacijskih sustava; (g)prema potrebi, razmjena iskustava o pitanjima povezanima sa sigurnošću mrežnih i informacijskih sustava u relevantnim institucijama, tijelima, uredima i agencijama Unije; (h)rasprava o normama i specifikacijama iz članka 19. s predstavnicima relevantnih europskih organizacija za normizaciju; (i)prikupljanje informacija o najboljoj praksi u pogledu rizika i incidenata; (j)provjera, na godišnjoj osnovi, sažetih izvješća iz članka 10. stavka 3. drugog podstavka; (k)rasprava o radu obavljenom u pogledu vježbi koje se odnose na sigurnost mrežnih i informacijskih sustava, programa za obrazovanje i osposobljavanja, uključujući rad ENISA-e; (l)uz pomoć ENISA-e, razmjena najbolje prakse u pogledu identifikacije operatora ključnih			

usluga od strane država članica, među ostalim u pogledu prekograničnih ovisnosti u odnosu na rizike i incidente; (m)rasprava o modalitetima za slanje obavijesti o incidentima iz članka 14. i 16. Do 9. veljače 2018., a nakon toga svake dvije godine, skupina za suradnju sastavlja program rada u pogledu mjera koje treba poduzeti za provedbu svojih ciljeva i zadaća, a koje moraju biti u skladu s ciljevima ove Direktive. 4. Za potrebe preispitivanja iz članka 23. i najkasnije 9. kolovoza 2018., a nakon toga svakih godinu i pol, skupina za suradnju priprema izvješće o procjeni stečenog iskustva u pogledu strateške suradnje iz ovoga članka. 5. Komisija donosi 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 22. stavka 2. Za potrebe prvog podstavka Komisija dostavlja prvi nacrt			

provedbenog akta odboru iz članka 22. stavka 1. do 9. veljače 2017.			
Članak 12. Mreža CSIRT-ova 1. S ciljem doprinosa razvoju povjerenja i pouzdanja među državama članicama te promicanju brze i učinkovite operativne suradnje osniva se mreža nacionalnih CSIRT-ova. 2. Mreža CSIRT-ova sastoji se od predstavnikâ CSIRT-ova iz država članica i iz CERT-EU-a. Komisija u mreži CSIRT-ova sudjeluje kao promatrač. ENISA osigurava tajništvo i aktivno podržava suradnju među CSIRT-ovima. 3. Zadaće su mreže CSIRT-ova: (a)razmjena informacija o uslugama CSIRT-ova te njihovim aktivnostima i sposobnostima za suradnju; (b)na zahtjev predstavnika CSIRT-a iz države članice na koju bi		Nije potrebno preuzimanje	U pitanju 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.

incident mogao utjecati, razmjenjivanje informacija koje nisu komercijalno osjetljive naravi, a odnose se na taj incident i s njime povezane rizike, te rasprava o tim informacijama; međutim, CSIRT svake države članice može odbiti davanje doprinosa takvoj raspravi ako postoji rizik da se u pitanje dovede istraga o incidentu; (c)razmjena i stavljanje na raspolaganje na dobrovoljnoj osnovi informacija o pojedinačnim incidentima koje nisu povjerljive; (d)na zahtjev predstavnika CSIRT-a države članice, razmatranje, a ako je to moguće, i određivanje koordiniranog odgovora na incident koji je utvrđen u području za koje je nadležna ista ta država članica; (e)pružanje podrške državama članicama u rješavanju prekograničnih incidenata na temelju dobrovoljne uzajamne pomoći; (f)rasprava o daljnjim oblicima operativne suradnje te njihovo istraživanje i utvrđivanje, među ostalim u odnosu na: i.kategorije rizika i incidenata;			

ii. rana upozorenja; iii. uzajamnu pomoć; iv.načela i načine koordinacije, kada države članice odgovaraju na prekogranične rizike i incidente; (g)obavješćivanje skupine za suradnju o svojim aktivnostima i daljnjim oblicima operativne suradnje razmotrenima u skladu s točkom (f) te traženje smjernica u tom pogledu; (h)rasprava o poukama stečenima u vježbama koje se odnose na sigurnost mrežnih i informacijskih sustava, među ostalim i onima koje organizira ENISA; (i)na zahtjev pojedinačnog CSIRT-a, rasprava o sposobnostima i pripravnosti tog CSIRT-a; (j)izdavanje smjernica radi olakšavanja konvergencije operativnih praksi s ciljem primjene odredaba ovoga članka u pogledu operativne suradnje. 4. Za potrebe preispitivanja iz članka 23. i najkasnije 9. kolovoza 2018., a nakon toga svakih godinu i pol, mreža CSIRT-ova priprema izvješće o procjeni stečenog iskustva u pogledu operativne suradnje iz ovoga članka, među ostalim			

zaključke i preporuke. To se izvješće dostavlja i skupini za suradnju. 5. Mreža CSIRT-ova utvrđuje vlastiti poslovnik.			
Članak 13. Međunarodna suradnja Unija u skladu s člankom 218. UFEU-a može sklapati međunarodne sporazume s trećim državama ili međunarodnim organizacijama kojima im se dopušta i organizira sudjelovanje u nekim aktivnostima skupine za suradnju. Takvi sporazumi uzimaju u obzir potrebu da se osigura primjerena zaštita podataka.		Nije potrebno preuzimanje	Odredba se odnosi na nadležne EU institucije.
POGLAVLJE IV. SIGURNOST MREŽNIH I INFORMACIJSKIH SUSTAVA OPERATORA KLJUČNIH USLUGA Članak 14.	*Obveza provedbe mjera* *Članak 14.* (1) Operatori ključnih usluga i davatelji digitalnih usluga dužni su, radi osiguranja kontinuiteta u obavljanju tih usluga, poduzimati mjere za postizanje visoke razine kibernetičke sigurnosti svojih usluga. (2) Mjere iz stavka 1. ovog članka sastoje se minimalno od: – tehničkih i organizacijskih mjera za upravljanje rizicima, uzimajući pri tome u obzir najnovija tehnička dostignuća koja	U potpunosti preuzeto	

Sigurnosni zahtjevi i obavješćivanje o incidentima 1. Države članice osiguravaju da operatori ključnih usluga poduzimaju odgovarajuće i razmjerne tehničke i organizacijske mjere za upravljanje rizicima kojima su izloženi mrežni i informacijski sustavi kojima se služe u svojem poslovanju. Uzimajući u obzir najnovija dostignuća tim se mjerama osigurava razina sigurnosti mrežnih i informacijskih sustava primjerena riziku kojem su izložene. 2. Države članice osiguravaju da operatori ključnih usluga poduzimaju odgovarajuće mjere za sprečavanje i svođenje na najmanju moguću mjeru učinaka incidenata koji utječu na sigurnost mrežnih i informacijskih sustava koji se koriste za pružanje takvih ključnih usluga s ciljem osiguravanja kontinuiteta tih usluga.	se koriste u okviru najbolje sigurnosne prakse u području kibernetičke sigurnosti i – mjera za sprečavanje i ublažavanje učinaka incidenata na sigurnost mrežnih i informacijskih sustava.		
	Mjere za upravljanje rizikom operatora ključnih usluga *Članak 15.* Operatori ključnih usluga dužni su poduzimati tehničke i organizacijske mjere za upravljanje rizicima koje moraju obuhvatiti mjere za: – utvrđivanje rizika od incidenata – sprječavanje, otkrivanje i rješavanje incidenata i – ublažavanje učinka incidenata na najmanju moguću mjeru.	U potpunosti preuzeto	
	Opseg primjene mjera *Članak 17.* (1) Operatori ključnih usluga dužni su mjere za postizanje visoke razine kibernetičke sigurnosti provoditi u odnosu na mrežni i informacijski sustav, ili njegov dio, za koji je u postupku identifikacije operatora ključne usluge utvrđeno da o njemu ovisi pružanje ključne usluge kod dotičnog subjekta.	U potpunosti preuzeto	

3. Države članice osiguravaju da operatori ključnih usluga bez neopravdane odgode obavješćuju nadležno tijelo ili CSIRT o incidentima koji imaju znatan učinak na kontinuitet ključnih usluga koje pružaju. Obavijesti sadržavaju informacije nadležnom tijelu ili CSIRT-u omogućuju da odredi sve prekogranične učinke incidenta. Strana koja šalje obavijest ne podliježe zbog toga povećanoj odgovornosti. 4. Kako bi se odredila važnost učinka nekog incidenta, osobito se uzimaju u obzir sljedeći parametri: (a)broj korisnika pogođenih prekidom osnovnih usluga; (b) trajanje incidenta; (c)zemljopisna raširenost u smislu područja na koje bi incident mogao utjecati. 5. Na temelju informacija koje dostavlja operator ključnih usluga u svojem obavješćivanju, nadležno tijelo ili CSIRT obavješćuju drugu pogođenu državu članicu ili više njih ako incident ima znatan učinak na kontinuitet ključnih usluga u toj državi članici. Pritom nadležno tijelo ili CSIRT, u skladu s pravom Unije	*Primjena mjera prema procjeni rizika* *Članak 18.* Operatori ključnih usluga i davatelji digitalnih usluga primjenjuju mjere za sprečavanje i ublažavanje učinaka incidenata razmjerno riziku kojemu je izložen njihov mrežni ili informacijski sustav.	U potpunosti preuzeto	
	Odgovornost za primjenu mjera *Članak 19.* Operatori ključnih usluga i davatelji digitalnih usluga dužni su provoditi mjere za postizanje visoke razine kibernetičke sigurnosti bez obzira na to upravljaju li i/ili održavaju svoje mrežne i informacijske sustave sami ili za to koriste vanjskog davatelja usluge.	U potpunosti preuzeto	
	Utvrđivanje mjera *Članak 20.* (1) Mjere za postizanje visoke razine kibernetičke sigurnosti operatora ključnih usluga i način njihove provedbe pobliže se propisuju uredbom koju donosi Vlada.	Djelomično preuzeto	Bit će preuzeto u: Uredba o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga (09.04.2018)
	Obveza obavješćivanja *Članak 21.* (1) Operatori ključnih usluga i davatelji digitalnih usluga dužni su nadležni CSIRT, bez neopravdane odgode, obavješćivati o incidentima koji imaju znatan učinak na kontinuitet usluga koje pružaju. (2) Ako je incident na mrežnom i informacijskom sustavu davatelja digitalne usluge imao znatan učinak na pružanje neke ključne usluge,	U potpunosti preuzeto	

ili nacionalnim zakonodavstvom u skladu s pravom Unije, čuvaju sigurnost i komercijalne interese operatora ključnih usluga, kao i povjerljivost informacija koje je dostavio u svojem obavješćivanju. Ako to dopuste okolnosti, nadležno tijelo ili CSIRT dostavljaju operatoru ključnih usluga koji je obavijest poslao relevantne informacije u pogledu daljnjeg postupanja po njegovoj obavijesti, primjerice informacije koje bi mogle doprinijeti djelotvornom rješavanju incidenta. Na zahtjev nadležnog tijela ili CSIRT-a jedinstvena kontaktna točka obavijesti iz prvog podstavka prosljeđuje jedinstvenim kontaktnim točkama drugih pogođenih država članica. 6. Nakon savjetovanja s operatorom ključnih usluga koji je obavijest poslao, nadležno tijelo ili CSIRT mogu obavijestiti javnost o pojedinačnim incidentima ako je osviještenost javnosti nužna za sprečavanje incidenta ili rješavanje incidenta koji je u tijeku.	operator ključne usluge dužan je o tom incidentu obavijestiti nadležni CSIRT. (3) Obveza obavješćivanja iz ovog članka odnosi se na incidente na mrežnim i informacijskim sustavima iz članka 17. ovog Zakona.		
	Kriteriji za određivanje učinka incidenata *Članak 22.* (1) Kriteriji za određivanje incidenata koji imaju znatan učinak na pružanje ključnih usluga propisuju se uredbom Vlade iz članka 20. stavka 1. ovog Zakona.	Djelomično preuzeto	Bit će preuzeto u: Uredba o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga (09.04.2018)
	Obavijesti o incidentima *Članak 23.* Sadržaj obavijesti o incidentima iz članka 21. ovog Zakona, način dostave obavijesti i druga pitanja bitna za postupanje s takvim obavijestima uređuju se uredbom Vlade iz članka 20. stavka 1. ovog Zakona.	Djelomično preuzeto	Bit će preuzeto u: Uredba o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga (09.04.2018)
	Zadaće nadležnog CSIRT-a *Članak 32.* (1) Nadležni CSIRT na sektorskoj razini, prema popisu nadležnosti iz Priloga III. ovog Zakona, obavlja sljedeće poslove: – ako to dopuštaju okolnosti, nakon primitka obavijesti o incidentu dostavlja operatoru ključnih usluga relevantne	U potpunosti preuzeto	

7. Nadležna tijela koja djeluju zajedno sa skupinom za suradnju mogu izraditi i donijeti smjernice u pogledu okolnosti u kojima su operatori ključnih usluga dužni obavijestiti o incidentu, među ostalim i o parametrima za određivanje važnosti učinka incidenta iz stavka 4.	informacije u pogledu daljnjeg postupanja po njegovoj obavijesti, a osobito informacije koje bi mogle doprinijeti djelotvornom rješavanju incidenta – donosi smjernice o provedbi obveze obavješćivanja o incidentima iz članka 21. ovog Zakona – informira nadležno sektorsko tijelo o incidentima iz članka 21. ovog Zakona – u suradnji s nadležnim sektorskim tijelom, određuje prekogranične utjecaje incidenata iz članka 21. ovog Zakona – informira jedinstvenu nacionalnu kontaktnu točku o incidentima iz članka 21. ovog Zakona, sukladno njezinim smjernicama – dostavlja jedinstvenoj nacionalnoj kontaktnoj točki podatke o glavnim elementima postupaka rješavanja incidenata koje provodi, – obavješćuje nadležni CSIRT druge pogođene države članice ili više njih o incidentu iz članka 21. ovog Zakona na mrežnom i informacijskom sustavu operatora ključnih usluga ako incident ima znatan učinak na kontinuitet ključnih usluga u toj državi članici,		

	Jedinstvena nacionalna kontaktna točka *Članak 30.* Jedinstvena nacionalna kontaktna točka: – na zahtjev nadležnog CSIRT-a, obavijesti o incidentima iz članka 21. ovog Zakona prosljeđuje jedinstvenim kontaktnim točkama drugih pogođenih država članica, osim za sektor usluga u sustavima državne informacijske infrastrukture	U potpunosti preuzeto	
	Informiranje javnosti o incidentu *Članak 24.* (1) Nadležni CSIRT može, po prethodno provedenom savjetovanju s operatorom ključne usluge i nadležnim sektorskim tijelom, obavijestiti javnost o pojedinačnim incidentima koji imaju znatan učinak na kontinuitet usluge koju operator pruža, ako je osviještenost javnosti nužna za sprečavanje širenja i jačanja incidenta ili za rješavanje incidenta koji je u tijeku.	U potpunosti preuzeto	
	Članak 41. Nadležna tijela iz ovog Zakona dužna su s podacima operatora ključnih usluga i davatelja digitalnih usluga postupati u skladu sa zahtjevima povjerljivosti, ako su oni utvrđeni posebnim propisima o zaštiti takvih podataka.	U potpunosti preuzeto	

Članak 15. Provedba i izvršavanje 1. Države članice osiguravaju da nadležna tijela imaju potrebne ovlasti i sredstva za procjenu ispunjavaju li operatori ključnih usluga svoje obveze iz članka 14. te učinke toga na sigurnost mrežnih i informacijskih sustava. 2. Države članice osiguravaju da nadležno tijelo ima ovlasti i sredstva da od operatora ključnih uloga zatraži dostavu:	*Nadležna sektorska tijela* *Članak 25.* (2) Nadležna sektorska tijela obavljaju sljedeće poslove: – obavljaju nadzor operatora ključnih usluga i davatelja digitalnih usluga u provedbi mjera za postizanje visoke razine kibernetičke sigurnosti i ispunjavanju drugih obveza iz ovog Zakona – surađuju i razmjenjuju relevantne informacije s tijelom za zaštitu osobnih podataka, kada su osobni podaci ugroženi zbog incidenta na mrežnom i informacijskom sustavu operatora ključne usluge odnosno davatelja digitalne usluge, odnosno s pravosudnim tijelima, kada je takav incident rezultat kriminalnih aktivnosti.	U potpunosti preuzeto	
(a)informacija potrebnih za procjenu sigurnosti njihovih mrežnih i informacijskih sustava, među ostalim dokumentirane sigurnosne politike; (b)dokaza o učinkovitoj provedbi sigurnosnih politika, primjerice rezultata revizije sigurnosti koju su obavili nadležno tijelo ili kvalificirani revizor te, u slučaju da je obavlja kvalificirani revizor,	*Nadzor* *Članak 26.* (1) Nadzor nad operatorom ključnih usluga provodi se najmanje jednom svake dvije godine. (2) Nadzor nad operatorom ključnih usluga provest će se i prije proteka roka iz stavka 1. ovog članka, ako nadležno sektorsko tijelo utvrdi ili zaprimi informacije koje ukazuju na to da operator ključne usluge ne izvršava svoje obveze iz ovog Zakona.	U potpunosti preuzeto	

stavljanje tih rezultata, zajedno s dokazima na kojima se temelje, na raspolaganje nadležnom tijelu. Prilikom traženja takvih informacija ili dokaza nadležno tijelo navodi svrhu zahtjeva i određuje koje su informacije potrebne. 3. Nakon procjene informacija ili rezultata revizije sigurnosti iz stavka 2., nadležno tijelo može izdavati obvezujuće upute operatorima ključnih usluga s ciljem ispravljanja utvrđenih nedostataka. 4. Nadležna tijela blisko surađuju s tijelima za zaštitu podataka u rješavanju incidenata koji za posljedicu imaju ugrožavanja osobnih podataka.	*Obveze operatora ključnih usluga i davatelja digitalnih usluga u okviru nadzora* *Članak 27.* (1) Operatori ključnih usluga i davatelji digitalnih usluga dužni su u okviru nadzora nadležnom sektorskom tijelu, na njegov zahtjev, dostaviti: – podatke potrebne za procjenu razine sigurnosti njihovih mrežnih i informacijskih sustava, uključujući dokumentirane sigurnosne politike i – dokaze o učinkovitoj provedbi sigurnosnih mjera. (2) Učinkovita provedba sigurnosnih mjera dokazuje se ili rezultatima revizije sigurnosti mrežnih i informacijskih sustava koju je obavio kvalificirani revizor ili ocjenom sukladnosti mrežnih i informacijskih sustava koju daje tehničko tijelo za ocjenu sukladnosti. (3) U zahtjevu iz stavka 1. ovog članka obvezno se navodi svrha zahtjeva, naznaka podataka koji su nadležnom sektorskom tijelu potrebni za provođenje nadzora i rok za dostavu podataka. (4) Operatori ključnih usluga i davatelji digitalnih usluga dužni su u okviru nadzora nadležnom sektorskom tijelu, na njegov zahtjev, omogućiti neposredan pristup svojim objektima i sustavima koji im služe za potporu u obavljanju ključnih odnosno digitalnih usluga.	U potpunosti preuzeto	
	Predmet nadzora *Članak 28.* (1) U okviru nadzora, nadležna sektorska tijela nadziru pravilnost provedbe propisanih: – mjera za postizanje visoke razine kibernetičke sigurnosti – obveza vezanih uz obavješćivanje o incidentima i	U potpunosti preuzeto	

	– drugih postupanja prema zahtjevima nadležnih tijela koja se podnose sukladno ovom Zakonu ili propisu donesenom na temelju ovog Zakona. (2) U provedbi nadzora, nadležna sektorska tijela: – izdaju obvezujuću uputu operatoru ključnih usluga kada utvrde da on: a) ne provodi mjere za postizanje visoke razine kibernetičke sigurnosti i/ili da ne izvršava druge obveze iz ovog Zakona ili b) da postoje nedostaci u provedbi mjera odnosno izvršavanju obveza iz ovog Zakona – izdaju naloge davatelju digitalnih usluga za otklanjanje svakog utvrđenog nepoštivanja provedbenog propisa Europske komisije iz članka 20. stavka 2. ovog Zakona i/ili odredbi ovog Zakona – podnose optužne prijedloge. (3) Nadležna sektorska tijela dužna su u aktima iz članka 2. podstavka 1. i 2. ovog članka naznačit rok za postupanje.		
	Obavljanje nadzora *Članak 29.* Nadzor nad provođenjem ovog Zakona i propisa donesenog na temelju ovog Zakona obavljaju inspektori, nadzornici i supervizori, u skladu s nadležnostima koje proizlaze iz propisa o ustrojstvu i djelokrugu rada tih tijela te drugih propisa koji određuju njihovu nadležnost.	U potpunosti preuzeto	

POGLAVLJE V. SIGURNOST MREŽNIH I INFORMACIJSKIH SUSTAVA PRUŽATELJA DIGITALNIH USLUGA Članak 16. Sigurnosni zahtjevi i obavješćivanje o incidentima 1. Države članice osiguravaju da pružatelji digitalnih usluga poduzimaju odgovarajuće i razmjerne tehničke i organizacijske mjere za upravljanje rizicima kojima su izloženi mrežni i informacijski sustavi kojima se u Uniji služe u okviru pružanja usluga iz Priloga III. Uzimajući u obzir najnovija dostignuća tim se mjerama osigurava razina sigurnosti mrežnih i informacijskih sustava primjerena riziku kojem su izloženi te uz	*Obveza provedbe mjera* *Članak 14.* (1) Operatori ključnih usluga i davatelji digitalnih usluga dužni su, radi osiguranja kontinuiteta u obavljanju tih usluga, poduzimati mjere za postizanje visoke razine kibernetičke sigurnosti svojih usluga. (2) Mjere iz stavka 1. ovog članka sastoje se minimalno od: – tehničkih i organizacijskih mjera za upravljanje rizicima, uzimajući pri tome u obzir najnovija tehnička dostignuća koja se koriste u okviru najbolje sigurnosne prakse u području kibernetičke sigurnosti i – mjera za sprečavanje i ublažavanje učinaka incidenata na sigurnost mrežnih i informacijskih sustava.	U potpunosti preuzeto	
	Mjere za upravljanje rizikom davatelja digitalnih usluga *Članak 16.* Davatelji digitalnih usluga dužni su prilikom poduzimanja tehničkih i organizacijskih mjera za upravljanje rizicima voditi računa osobito o: – sigurnosti sustava i objekata – rješavanju incidenata – upravljanju kontinuitetom poslovanja – praćenju, reviziji i testiranju – sukladnosti s međunarodnim standardima.	U potpunosti preuzeto	

vođenje računa o sljedećim elementima: (a) sigurnosti sustava i objekata; (b) rješavanju incidenata; (c)upravljanju kontinuitetom poslovanja; (d) praćenju, reviziji i testiranju; (e)sukladnosti s međunarodnim standardima. 2. Države članice osiguravaju da pružatelji digitalnih usluga poduzimaju mjere za sprečavanje i svođenje na najmanju moguću mjeru učinaka incidenata koji utječu na sigurnost njihovih mrežnih i informacijskih sustava na usluge iz Priloga III. koje se pružaju u Uniji, s ciljem osiguravanja kontinuiteta tih usluga. 3. Države članice osiguravaju da pružatelji digitalnih usluga bez nepotrebne odgode obavijeste nadležno tijelo ili CSIRT o svakom incidentu koji ima znatan učinak na pružanje neke od usluga iz Priloga III. koju oni nude unutar Unije. Obavijesti sadržavaju informacije s pomoću kojih nadležno tijelo ili CSIRT mogu odrediti važnost svakog prekograničnog učinka. Strana koja	*Pojmovi* *Članak 5.* U smislu ovog Zakona pojedini pojmovi imaju sljedeće značenje: 1) *„davatelj digitalnih usluga"*- je bilo koji privatni subjekt koji pruža neku digitalnu uslugu s Popisa iz Priloga II. ovog Zakona **Prilog II.** **Popis digitalnih usluga** 1. Internetsko tržište 2. Internetska tražilica 3. Usluge računalstva u oblaku	U potpunosti preuzeto	
	Obveza obavješćivanja *Članak 21.* (1) Operatori ključnih usluga i davatelji digitalnih usluga dužni su nadležni CSIRT, bez neopravdane odgode, obavješćivati o incidentima koji imaju znatan učinak na kontinuitet usluga koje pružaju. (2) Ako je incident na mrežnom i informacijskom sustavu davatelja digitalne usluge imao znatan učinak na pružanje neke ključne usluge, operator ključne usluge dužan je o tom incidentu obavijestiti nadležni CSIRT. (3) Obveza obavješćivanja iz ovog članka odnosi se na incidente na mrežnim i informacijskim sustavima iz članka 17. ovog Zakona.	U potpunosti preuzeto	

šalje obavijest ne podliježe zbog toga povećanoj odgovornosti. 4. Radi utvrđivanja je li učinak incidenta znatan, u obzir se osobito uzimaju sljedeći parametri: (a)broj korisnika na koje incident utječe, osobito ako je riječ o korisnicima koji se na te usluge oslanjaju za pružanje vlastitih usluga; (b) trajanje incidenta; (c)zemljopisna raširenost u smislu područja na koje bi incident mogao utjecati; (d)opseg poremećaja u funkcioniranju usluge; (e)opseg utjecaja na gospodarsko i društveno djelovanje. Obveza obavješćivanja o incidentu primjenjuje se samo ako pružatelj digitalnih usluga ima pristup informacijama potrebnima za	*Obavijesti o incidentima* *Članak 23.* Sadržaj obavijesti o incidentima iz članka 21. ovog Zakona, način dostave obavijesti i druga pitanja bitna za postupanje s takvim obavijestima uređuju se uredbom Vlade iz članka 20. stavka 1. ovog Zakona.	Djelomično preuzeto	Bit će preuzeto u: Uredba o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga (09.04.2018)
	Kriteriji za određivanje učinka incidenata *Članak 22.* (2) Kriteriji za određivanje incidenata koji imaju znatan učinak na davanje digitalnih usluga propisani su Provedbenom uredbom Komisije iz članka 20. stavka 2. ovog Zakona.	Nije potrebno preuzimanje	Uređeno Provedbenom uredbom Komisije (EU) 2018/151 od 30. siječnja 2018. o utvrđivanju pravila za primjenu Direktive (EU) 2016/1148 Europskog parlamenta i Vijeća u odnosu na dodatne specifikacije elemenata koje pružatelji digitalnih usluga moraju uzeti u obzir u upravljanju rizicima kojima je izložena sigurnost njihovih mrežnih i informacijskih sustava i parametara za utvrđivanje ima li incident znatan učinak (SL L 26/48, 31.1.2018.)

procjenu učinka incidenta spram kriterija iz prvog podstavka. 5. Ako se operator ključnih usluga oslanja na trećeg pružatelja digitalnih usluga za pružanje usluge koja je neophodna za održavanje ključnih društvenih i gospodarskih aktivnosti, taj operator ključnih usluga obavijestit će o svakom znatnom učinku na kontinuitet ključnih usluga koji je prouzročen incidentom koji utječe na tog pružatelja digitalnih usluga. 6. Nadležno tijelo ili CSIRT prema potrebi obavješćuju ostale pogođene države članice, a osobito ako se incident iz stavka 3. odnosi na dvije ili više država članica. Pritom nadležna tijela, CSIRT-ovi i jedinstvene kontaktne točke, u skladu s pravom Unije ili nacionalnim zakonodavstvom u skladu s pravom Unije, čuvaju sigurnost i komercijalne interese pružatelja digitalnih usluga te povjerljivost dostavljenih informacija. 7. Nakon savjetovanja s dotičnim pružateljem digitalnih usluga, nadležno tijelo ili CSIRT te, prema potrebi, tijela ili CSIRT-ovi drugih pogođenih država članica, mogu	*Zadaće nadležnog CSIRT-a* *Članak 32.* (1) Nadležni CSIRT na sektorskoj razini, prema popisu nadležnosti iz Priloga III. ovog Zakona, obavlja sljedeće poslove: – informira nadležno sektorsko tijelo o incidentima iz članka 21. ovog Zakona – u suradnji s nadležnim sektorskim tijelom, određuje prekogranične utjecaje incidenata iz članka 21. ovog Zakona – informira jedinstvenu nacionalnu kontaktnu točku o incidentima iz članka 21. ovog Zakona, sukladno njezinim smjernicama – dostavlja jedinstvenoj nacionalnoj kontaktnoj točki podatke o glavnim elementima postupaka rješavanja incidenata koje provodi, – obavješćuje nadležni CSIRT druge pogođene države članice ili više njih o incidentu iz članka 21. ovog Zakona na mrežnom i informacijskom sustavu pružatelja digitalnih usluga ako se incident odnosi na dvije ili više država članica	U potpunosti preuzeto	
	Jedinstvena nacionalna kontaktna točka *Članak 30.* Jedinstvena nacionalna kontaktna točka: – na zahtjev nadležnog CSIRT-a, obavijesti o incidentima iz članka 21. ovog Zakona prosljeđuje jedinstvenim kontaktnim točkama drugih pogođenih država članica, osim za sektor usluga u sustavima državne informacijske infrastrukture	U potpunosti preuzeto	

javnost obavijestiti o pojedinačnim incidentima ili zatražiti od pružatelja digitalnih usluga da to učini ako je javnost potrebno obavijestiti s ciljem sprečavanja incidenta ili rješavanja incidenta koji je u tijeku ili ako je objavljivanje incidenta zbog nekog drugog razloga u javnome interesu. 8. Komisija donosi provedbene akte radi dodatnog utvrđivanja elemenata iz stavka 1. te parametara navedenih u stavku 4. ovog članka. Ti se provedbeni akti donose do 9. kolovoza 2017. u skladu s postupkom ispitivanja iz članka 22. stavka 2. 9. Komisija može donijeti provedbene akte kojima se utvrđuju oblici i postupci primjenljivi na zahtjeve za obavješćivanje. Ti se provedbeni akti donose u skladu s postupkom ispitivanja iz članka 22. stavka 2. 10. Ne dovodeći u pitanje članak 1. stavak 6., države članice ne nameću nikakve dodatne sigurnosne zahtjeve			
	Informiranje javnosti o incidentu *Članak 24.* (2) Nadležni CSIRT te, prema potrebi, CSIRT-ovi drugih pogođenih država članica, mogu javnost obavijestiti o pojedinačnim incidentima koji imaju znatan učinak na kontinuitet pojedine digitalne usluge ili zatražiti od davatelja digitalnih usluga da to učini, ako je objavljivanje informacije o incidentu u javnome interesu, osobito ako je to potrebno radi sprečavanja širenja i jačanja incidenta ili rješavanja incidenta koji je u tijeku.	U potpunosti preuzeto	
	Članak 41. Nadležna tijela iz ovog Zakona dužna su s podacima operatora ključnih usluga i davatelja digitalnih usluga postupati u skladu sa zahtjevima povjerljivosti, ako su oni utvrđeni posebnim propisima o zaštiti takvih podataka.	U potpunosti preuzeto	

ni zahtjeve za obavješćivanje pružateljima digitalnih usluga. 11. Poglavlje V. ne primjenjuje se na mikropoduzeća i mala poduzeća kako su definirana u Preporuci Komisije 2003/361/EZ (19).	*Primjena* *Članak 3.* (2) Davatelji digitalnih usluga podliježu nadležnostima i ovlastima propisanim ovim Zakonom ako na teritoriju Republike Hrvatske imaju sjedište ili svog predstavnika te pod uvjetom da takav davatelj ne predstavlja mikro ili mali subjekt malog gospodarstva kako su oni definirani Zakonom o poticanju razvoja malog gospodarstva („Narodne novine", broj: 29/02., 63/07., 53/12., 56/13. i 121/16.).	U potpunosti preuzeto	
Članak 17. Provedba i izvršavanje 1. Države članice osiguravaju da nadležna tijela, ako je potrebno, poduzmu ex post nadzorne mjere kada dobiju dokaze da pružatelj digitalnih usluga ne ispunjava zahtjeve utvrđene u članku 16. Takve dokaze može dostaviti nadležno tijelo druge države članice u kojoj se pruža usluga. 2. Za potrebe stavka 1. nadležna tijela imaju potrebne ovlasti i sredstva da mogu od pružatelja digitalnih usluga tražiti: (a)dostavu informacija potrebnih za procjenu sigurnosti njihovih mrežnih i informacijskih sustava,	*Nadležna sektorska tijela* *Članak 25.* (2) Nadležna sektorska tijela obavljaju sljedeće poslove: – provode postupke identifikacije operatora ključnih usluga sukladno ovome Zakonu – obavljaju nadzor operatora ključnih usluga i davatelja digitalnih usluga u provedbi mjera za postizanje visoke razine kibernetičke sigurnosti i ispunjavanju drugih obveza iz ovog Zakona – međusobno surađuju i razmjenjuju iskustva u provedbi ovog Zakona – surađuju i razmjenjuju relevantne informacije s drugim nadležnim tijelima iz ovog Zakona – surađuju i razmjenjuju relevantne informacije s tijelom za zaštitu osobnih podataka, kada su osobni podaci ugroženi zbog incidenta na mrežnom i informacijskom sustavu operatora ključne usluge odnosno davatelja digitalne usluge, odnosno s pravosudnim tijelima, kada je takav incident rezultat kriminalnih aktivnosti.	U potpunosti preuzeto	

među ostalim dokumentirane sigurnosne politike; (b)otklanjanje svakog nepoštovanja zahtjeva utvrđenih u članku 16. 3. Ako pružatelj digitalnih usluga ima glavni poslovni nastan ili predstavnika u jednoj državi članici, ali se njegovi mrežni i informacijski sustavi nalaze u jednoj ili više država članica, nadležno tijelo države članice u kojoj se nalazi njegov glavni poslovni nastan ili predstavnik te nadležna tijela tih drugih država članica surađuju i međusobno si pomažu prema potrebi. Takva pomoć i suradnja mogu obuhvaćati razmjenu informacija između dotičnih nadležnih tijela i zahtjeve za poduzimanjem nadzornih mjera iz stavka 2.	*Nadzor* *Članak 26.* (3) Nadzor nad davateljem digitalnih usluga provodi se isključivo nakon što nadležno sektorsko tijelo zaprimi informacije koje ukazuju na to da davatelj digitalne usluge ne postupa sukladno Provedbenoj uredbi Komisije iz članka 20. stavka 2. ovog Zakona i/ili odredbama ovog Zakona.	U potpunosti preuzeto	
	Obveze operatora ključnih usluga i davatelja digitalnih usluga u okviru nadzora *Članak 27.* (1) Operatori ključnih usluga i davatelji digitalnih usluga dužni su u okviru nadzora nadležnom sektorskom tijelu, na njegov zahtjev, dostaviti: – podatke potrebne za procjenu razine sigurnosti njihovih mrežnih i informacijskih sustava, uključujući dokumentirane sigurnosne politike i – dokaze o učinkovitoj provedbi sigurnosnih mjera. (2) Učinkovita provedba sigurnosnih mjera dokazuje se ili rezultatima revizije sigurnosti mrežnih i informacijskih sustava koju je obavio kvalificirani revizor ili ocjenom sukladnosti mrežnih i informacijskih sustava koju daje tehničko tijelo za ocjenu sukladnosti. (3) U zahtjevu iz stavka 1. ovog članka obvezno se navodi svrha zahtjeva, naznaka podataka koji su nadležnom sektorskom tijelu potrebni za provođenje nadzora i rok za dostavu podataka. (4) Operatori ključnih usluga i davatelji digitalnih usluga dužni su u okviru nadzora nadležnom sektorskom tijelu, na njegov zahtjev, omogućiti neposredan pristup svojim objektima i sustavima koji im služe za potporu u obavljanju ključnih odnosno digitalnih usluga.	U potpunosti preuzeto	

	Predmet nadzora *Članak 28.* (1) U okviru nadzora, nadležna sektorska tijela nadziru pravilnost provedbe propisanih: – mjera za postizanje visoke razine kibernetičke sigurnosti – obveza vezanih uz obavješćivanje o incidentima i – drugih postupanja prema zahtjevima nadležnih tijela koja se podnose sukladno ovom Zakonu ili propisu donesenom na temelju ovog Zakona. (2) U provedbi nadzora, nadležna sektorska tijela: – izdaju naloge davatelju digitalnih usluga za otklanjanje svakog utvrđenog nepoštivanja provedbenog propisa Europske komisije iz članka 20. stavka 2. ovog Zakona i/ili odredbi ovog Zakona – podnose optužne prijedloge. (3) Nadležna sektorska tijela dužna su u aktima iz članka 2. podstavka 1. i 2. ovog članka naznačit rok za postupanje.	U potpunosti preuzeto	

Članak 18. Nadležnost i teritorijalnost 1. Za potrebe ove Direktive smatra se da pružatelj digitalnih usluga pripada nadležnosti države članice u kojoj ima glavni poslovni nastan. Smatra se da pružatelj digitalnih usluga ima glavni poslovni nastan u onoj državi članici u kojoj ima sjedište. 2. Pružatelj digitalnih usluga koji nema nastan u Uniji, ali nudi usluge u Uniji kako je navedeno u Prilogu III., imenuje svojeg predstavnika u Uniji. Predstavnik ima sjedište u jednoj od država članica u kojima pružatelj nudi svoje usluge. Smatra se da pružatelj digitalnih usluga pripada nadležnosti one države članice u kojoj njegov predstavnik ima poslovni nastan. 3. Imenovanje predstavnika od strane pružatelja digitalnih usluga ne	*Primjena* *Članak 3.* (2) Davatelji digitalnih usluga podliježu nadležnostima i ovlastima propisanim ovim Zakonom ako na teritoriju Republike Hrvatske imaju sjedište ili svog predstavnika te pod uvjetom da takav davatelj ne predstavlja mikro ili mali subjekt malog gospodarstva kako su oni definirani Zakonom o poticanju razvoja malog gospodarstva („Narodne novine“, broj: 29/02., 63/07., 53/12., 56/13. i 121/16.).	U potpunosti preuzeto	
	Pojmovi *Članak 5.* U smislu ovog Zakona pojedini pojmovi imaju sljedeće značenje: 8) *„davatelj digitalnih usluga”* - je bilo koji privatni subjekt koji pruža neku digitalnu uslugu s Popisa iz Priloga II. ovog Zakona 14) *„predstavnik“* – je bilo koja fizička ili pravna osoba sa sjedištem u Republici Hrvatskoj koju je davatelj digitalnih usluga koji nema sjedište u Europskoj uniji izričito imenovao da djeluje u njegovo ime i kojoj se nadležno sektorsko tijelo ili nadležni CSIRT mogu obratiti umjesto davatelju digitalnih usluga koji je obveznik primjene ovog Zakona	U potpunosti preuzeto	

dovodi u pitanje pravne postupke koji bi se mogli pokrenuti protiv samog pružatelja digitalnih usluga.	**Prilog II.** **Popis digitalnih usluga** 1. Internetsko tržište 2. Internetska tražilica 3. Usluge računalstva u oblaku	U potpunosti preuzeto	
POGLAVLJE VI. NORMIZACIJA I OBAVJEŠĆIVANJE NA DOBROVOLJNOJ OSNOVI Članak 19. Normizacija 1. Države članice, s ciljem promicanja konvergentne provedbe članka 14. stavaka 1. i 2. te članka 16. stavaka 1. i 2., bez nametanja ili diskriminacije određene vrste tehnologije, potiču primjenu europskih ili međunarodno priznatih normi i specifikacija relevantnih za sigurnost mrežnih i informacijskih sustava. 2. ENISA u suradnji s državama članicama izrađuje savjete i smjernice u pogledu tehničkih područja koja treba razmotriti u odnosu na stavak 1. te u odnosu na		Nije preuzeto	Bit će preuzeto u: Uredba o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga (09.04.2018)

postojeće norme, uključujući nacionalne norme država članica, kojima bi se ta područja mogla obuhvatiti.			
Članak 20. Obavješćivanje na dobrovoljnoj osnovi 1. Ne dovodeći u pitanje članak 3. subjekti koji nisu identificirani kao operatori ključnih usluga i nisu pružatelji digitalnih usluga obavješćuju na dobrovoljnoj osnovi o incidentima koji imaju znatan učinak na kontinuitet usluga koje pružaju. 2. Pri obradi obavijesti države članice djeluju u skladu s postupkom utvrđenim u članku 14. Države članice obradi obveznih obavijesti mogu dati prednost pred obradom obavijesti na dobrovoljnoj osnovi. Obavijesti na dobrovoljnoj osnovi obrađuju se samo ako takva obrada ne predstavlja nerazmjerno ili nepotrebno opterećenje za države članice o kojima je riječ.		Nije preuzeto	Bit će preuzeto u: Uredba o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga (09.04.2018)

Subjektu koji je obavijest podnio dobrovoljno ne nameću se zbog tog obavješćivanja nikakve obveze kojima ne bi podlijegao da nije podnio tu obavijest.			
POGLAVLJE VII. ZAVRŠNE ODREDBE Članak 21. Sankcije Države članice utvrđuju pravila o sankcijama koje se primjenjuju na kršenja nacionalnih odredaba 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 9. svibnja 2018. obavješćuju Komisiju o tim pravilima i mjerama te je bez odgode obavješćuju o svim naknadnim izmjenama koje na njih utječu.	**PREKRŠAJNE ODREDBE** Članak 42. (1) Novčanom kaznom u iznosu od 150.000,00 do 500.000,00 kuna kaznit će se za prekršaj pravna osoba koja: – ne postupi po obvezujućoj uputi nadležnog sektorskog tijela iz članka 28. stavka 2. podstavka 1. ovog Zakona odnosno danom nalogu nadležnog sektorskog tijela iz članka 28. stavka 2. podstavka 2. ovog Zakona – odbije dostaviti ili neopravdano odgađa dostavljati obavijesti o incidentima iz članka 21. ovog Zakona. (2) Novčanom kaznom u iznosu od 50.000,00 do 150.000,00 kuna kaznit će se za prekršaj iz stavka 1. ovog članka fizička osoba. (3) Novčanom kaznom u iznosu od 15.000,00 do 50.000,00 kuna kaznit će se za prekršaj iz stavka 1. ovog članka odgovorna osoba u pravnoj osobi i odgovorna osoba u javnom subjektu. Članak 43. (1) Novčanom kaznom u iznosu od 50.000,00 do 100.000,00 kuna kaznit će se za prekršaj pravna osoba koja: – ne postupi sukladno članku 27. ovog Zakona	U potpunosti preuzeto	

	– odbije omogućiti ili neopravdano odgađa ili otežava provedbu povjere iz članka 34. ovog Zakona. (2) Novčanom kaznom u iznosu od 20.000,00 do 50.000,00 kaznit će se za prekršaj iz stavka 1. ovog članka fizička osoba. (3) Novčanom kaznom u iznosu od 10.000,00 do 25.000,00 kuna kaznit će se za prekršaj iz stavka 1. ovog članka odgovorna osoba u pravnoj osobi i odgovorna osoba u javnom subjektu. Članak 44. (1) Novčanom kaznom u iznosu od 15.000,00 do 50.000,00 kuna kaznit će se za prekršaj pravna osoba koja: – ne postupi po zahtjevu nadležnog sektorskog tijela za dostavu podataka iz članka 11. stavka 1. ovog Zakona – ne dostavlja obavijesti o promjenama u roku iz članka 11. stavka 4. ovog Zakona. (2) Novčanom kaznom u iznosu od 5.000,00 do 25.000,00 kuna kaznit će se za prekršaj iz stavka 1. ovog članka fizička osoba. (3) Novčanom kaznom u iznosu od 2.000,00 do 20.000,00 kuna kaznit će se za prekršaj iz stavka 1. ovog članka odgovorna osoba u pravnoj osobi i odgovorna osoba u javnom subjektu.		

Članak 22. Postupak odbora 1. Komisiji pomaže Odbor za sigurnost mrežnih i informacijskih sustava. Navedeni odbor je odbor u smislu Uredbe (EU) br. 182/2011. 2. Pri upućivanju na ovaj stavak primjenjuje se članak 5. Uredbe (EU) br. 182/2011.		Nije potrebno preuzimanje	U pitanju odredba Direktive koja se provodi na razini nadležnih EU institucija.
Članak 23. Preispitivanje 1. Do 9. svibnja 2019. Komisija podnosi Europskom parlamentu i Vijeću izvješće s procjenom dosljednosti u pristupu država članica pri identifikaciji operatora ključnih usluga. 2. Komisija periodično preispituje funkcioniranje ove Direktive te podnosi izvješće Europskom parlamentu i Vijeću. U tu svrhu te s ciljem 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. Pri		Nije potrebno preuzimanje	U pitanju odredba Direktive koja se provodi od strane nadležnih EU institucija.

preispitivanju Komisija također procjenjuje popise iz priloga II. i III. te dosljednost u identifikaciji operatora ključnih usluga i usluga u sektorima iz Priloga II. Prvo se izvješće dostavlja do 9. svibnja 2021.			
Članak 24. Prijelazne mjere 1. Ne dovodeći u pitanje članak 25. te s ciljem da se državama članicama pruže dodatne mogućnosti za odgovarajuću suradnju tijekom razdoblja za prenošenje, skupina za suradnju i mreža CSIRT-ova počinju obavljati svoje zadaće utvrđene u članku 11. stavku 3. odnosno članku 12. stavku 3. najkasnije do 9. veljače 2017. 2. U razdoblju od 9. veljače 2017. do 9. studenoga 2018., a u svrhu podupiranja država članica u zauzimanju dosljednog pristupa u pogledu postupka identifikacije operatora ključnih usluga, skupina za suradnju raspravlja o postupku te sadržaju i vrsti nacionalnih mjera za omogućivanje identifikacije operatora ključnih usluga unutar određenog sektora u skladu s	*Jedinstvena nacionalna kontaktna točka* *Članak 30.* Jedinstvena nacionalna kontaktna točka: – sudjeluje u radu Skupine za suradnju, koja je 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,	U potpunosti preuzeto	
	Zadaće nadležnog CSIRT-a *Članak 32.* (1) Nadležni CSIRT na sektorskoj razini, prema popisu nadležnosti iz Priloga III. ovog Zakona, obavlja sljedeće poslove: – sudjeluje u Mreži CSIRT-ova na razini Europske unije koja je osnovana s ciljem razvoja povjerenja i pouzdanja među državama članicama te promicanju brze i učinkovite operativne suradnje	U potpunosti preuzeto	

kriterijima određenim u člancima 5. i 6. Skupina za suradnju, na zahtjev države članice, raspravlja i o konkretnim nacrtima nacionalnih mjera te države članice za omogućivanje identifikacije operatora ključnih usluga u određenom sektoru u skladu s kriterijima određenima u člancima 5. i 6. 3. Do 9. veljače 2017., a za potrebe ovog članka države članice osiguravaju odgovarajuću zastupljenost u skupini za suradnju i mreži CSIRT-ova.			
Članak 25. Prenošenje 1. Države članice do 9. svibnja 2018. donose i objavljuju zakone i druge propise koji su potrebni radi usklađivanja s ovom Direktivom. One o tome odmah obavješćuju Komisiju. One primjenjuju te mjere od 10. svibnja 2018. Kada države članice donose te mjere, one sadržavaju upućivanje na ovu Direktivu ili se na nju upućuje	*Usklađenost s propisima Europske unije* *Članak 2.* Ovim zakonom u hrvatsko zakonodavstvo preuzima se sljedeći akt Europske unije: - Direktiva 2016/1148 Europskog parlamenta i Vijeća od 6. srpnja 2016. o mjerama za visoku zajedničku razinu sigurnosti mrežnih i informacijskih sustava širom Unije (SL L 194, 19.7.2016.).	Djelomično preuzeto	Bit će preuzeto u: Uredba o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga (09.04.2018)

prilikom njihove službene objave. Načine tog upućivanja određuju države članice. 2. Države članice Komisiji dostavljaju tekst glavnih odredaba nacionalnog prava koje donesu u području na koje se odnosi ova Direktiva.	*Utvrđivanje mjera* *Članak 20.* (1) Mjere za postizanje visoke razine kibernetičke sigurnosti operatora ključnih usluga i način njihove provedbe pobliže se propisuju uredbom koju donosi Vlada. (2) Mjere za postizanje visoke razine kibernetičke sigurnosti davatelja digitalnih usluga provode se sukladno Provedbenoj uredbi Komisije (EU) 2018/151 od 30. siječnja 2018. o utvrđivanju pravila za primjenu Direktive (EU) 2016/1148 Europskog parlamenta i Vijeća u odnosu na dodatne specifikacije elemenata koje pružatelji digitalnih usluga moraju uzeti u obzir u upravljanju rizicima kojima je izložena sigurnost njihovih mrežnih i informacijskih sustava i parametara za utvrđivanje ima li incident znatan učinak (SL L 26/48, 31.1.2018.).	Djelomično preuzeto	Bit će preuzeto u: Uredba o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga (09.04.2018)
	Kriteriji za određivanje učinka incidenata *Članak 22.* (1) Kriteriji za određivanje incidenata koji imaju znatan učinak na pružanje ključnih usluga propisuju se uredbom Vlade iz članka 20. stavka 1. ovog Zakona. (2) Kriteriji za određivanje incidenata koji imaju znatan učinak na davanje digitalnih usluga propisani su Provedbenom uredbom Komisije iz članka 20. stavka 2. ovog Zakona.	Djelomično preuzeto	Bit će preuzeto u: Uredba o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga (09.04.2018)

	Obavijesti o incidentima *Članak 23.* Sadržaj obavijesti o incidentima iz članka 21. ovog Zakona, način dostave obavijesti i druga pitanja bitna za postupanje s takvim obavijestima uređuju se uredbom Vlade iz članka 20. stavka 1. ovog Zakona.	Djelomično preuzeto	Bit će preuzeto u: Uredba o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga (09.04.2018)
	Članak 45. Vlada će Uredbu iz članka 20. stavka 1. ovog Zakona donijeti u roku od 30 dana od dana stupanja na snagu ovog Zakona.	Djelomično preuzeto	Bit će preuzeto u: Uredba o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga (09.04.2018)
Članak 26. Stupanje na snagu Ova Direktiva stupa na snagu dvadesetog dana od dana objave u Službenom listu Europske unije.		Nije potrebno preuzimanje	U pitanju odredba Direktive koja utvrđuje njezino stupanja na snagu.
Članak 27. Adresati Ova je Direktiva upućena državama članicama.		Nije potrebno preuzimanje	U pitanju odredba Direktive koja utvrđuje adresate na koje se Direktiva odnosi.

PRILOG I. ZAHTJEVI U POGLEDU TIMOVA ZA ODGOVOR NA RAČUNALNE SIGURNOSNE INCIDENTE (CSIRT-ovi) I NJIHOVE ZADAĆE Zahtjevi u pogledu CSIRT-ova i njihove zadaće propisno su i jasno definirani i poduprti nacionalnom politikom i/ili zakonodavstvom. Oni obuhvaćaju sljedeće: 1.Zahtjevi u pogledu CSIRT-ova: (a)CSIRT-ovi osiguravaju visoku razinu dostupnosti svojih usluga komuniciranja izbjegavanjem jedinstvenih točki prekida te u svakom trenutku raspolažu s nekoliko sredstava za mogućnost dvosmjernog kontaktiranja. Nadalje, komunikacijski kanali jasno su određeni i dobro poznati klijentima i suradnicima. (b)Prostori CSIRT-ova i informacijski sustavi za potporu smješteni su na sigurnim lokacijama. (c)Kontinuitet rada:	*Zadaće nadležnog CSIRT-a* *Članak 32.* (1) Nadležni CSIRT na sektorskoj razini, prema popisu nadležnosti iz Priloga III. ovog Zakona, obavlja sljedeće poslove: – prati incidente – pruža rana upozorenja i najave te informira o rizicima i incidentima – provodi dinamičku analizu rizika i incidenata te izrađuje pregled situacije u sektoru – provodi redovite provjere ranjivosti mrežnih i informacijskih sustava operatora ključnih usluga odnosno davatelja digitalnih usluga – prima obavijesti o incidentima – na zahtjev operatora ključnih usluga odnosno davatelja digitalnih usluga analizira i odgovara na incidente – ako to dopuštaju okolnosti, nakon primitka obavijesti o incidentu dostavlja operatoru ključnih usluga relevantne informacije u pogledu daljnjeg postupanja po njegovoj obavijesti, a osobito informacije koje bi mogle doprinijeti djelotvornom rješavanju incidenta – donosi smjernice o provedbi obveze obavješćivanja o incidentima iz članka 21. ovog Zakona – informira nadležno sektorsko tijelo o incidentima iz članka 21. ovog Zakona	U potpunosti preuzeto	

i.CSIRT-ovi su opremljeni odgovarajućim sustavom za upravljanje zahtjevima i njihovim preusmjeravanjem, kako bi se olakšale primopredaje. ii.CSIRT-ovi imaju dovoljno zaposlenika kako bi se osigurala dostupnost u svako doba. iii.CSIRT-ovi se oslanjaju na infrastrukturu čiji je kontinuitet osiguran. U tu svrhu dostupni su redundantni sustavi i rezervni radni prostor. (d)CSIRT-ovi imaju mogućnost da, ako to žele, sudjeluju u međunarodnim mrežama za suradnju. 2.Zadaće CSIRT-ova: (a)Zadaće CSIRT-ova obuhvaćaju barem: i.praćenje incidenata na nacionalnoj razini; ii.pružanje ranih upozorenja i najava te informiranje relevantnih dionika o rizicima i incidentima; iii. odgovaranje na incidente;	– u suradnji s nadležnim sektorskim tijelom, određuje prekogranične utjecaje incidenata iz članka 21. ovog Zakona – informira jedinstvenu nacionalnu kontaktnu točku o incidentima iz članka 21. ovog Zakona, sukladno njezinim smjernicama – dostavlja jedinstvenoj nacionalnoj kontaktnoj točki podatke o glavnim elementima postupaka rješavanja incidenata koje provodi, – obavješćuje nadležni CSIRT druge pogođene države članice ili više njih o incidentu iz članka 21. ovog Zakona na mrežnom i informacijskom sustavu operatora ključnih usluga ako incident ima znatan učinak na kontinuitet ključnih usluga u toj državi članici, – obavješćuje nadležni CSIRT druge pogođene države članice ili više njih o incidentu iz članka 21. ovog Zakona na mrežnom i informacijskom sustavu pružatelja digitalnih usluga ako se incident odnosi na dvije ili više država članica – surađuje s drugim CSIRT-ovima na nacionalnoj i međunarodnoj razini – sudjeluje u Mreži CSIRT-ova na razini Europske unije koja je osnovana s ciljem razvoja povjerenja i pouzdanja među državama članicama te promicanju brze i učinkovite operativne suradnje – promiče usvajanje i primjenu zajedničkih ili normiranih praksi za postupke rješavanja incidenata i rizika te planove za klasifikaciju incidenata, rizika i informacija.		

iv.pružanje dinamičke analize rizika i incidenata te pregleda situacije; v.sudjelovanje u mreži CSIRT-ova. (b)CSIRT-ovi uspostavljaju suradnju s privatnim sektorom. (c)CSIRT-ovi s ciljem olakšavanja suradnje promiču usvajanje i primjenu zajedničkih ili normiranih praksi za: i.postupke rješavanja incidenata i rizika; ii.planove za klasifikaciju incidenata, rizika i informacija.	(2) Operatori ključnih usluga i davatelji digitalnih usluga dužni su surađivati s nadležnim CSIRT-om i s njim razmjenjivati potrebne informacije u postupku rješavanja incidenata. (3) Nadležni CSIRT u obavljanju svojih zadaća iz ovog Zakona ne može snositi odgovornost za štetu uzrokovanu incidentom na mrežnim i informacijskim sustavima operatora ključnih usluga i davatelja digitalnih usluga.		
	Osiguravanje uvjeta za obavljanje poslova nadležnog CSIRT-a *Članak 33.* (1) Nadležni CSIRT je dužan: – osigurati visoku razinu dostupnosti svojih usluga komuniciranja izbjegavanjem jedinstvenih točki prekida, uz raspoloživost sredstava za mogućnost dvosmjernog kontaktiranja te jasno određenim i poznatim komunikacijskim kanalima za njihove klijente i suradnike – svoje prostore i informacijske sustave za potporu smjestiti na sigurne lokacije i – osigurati kontinuitet rada na način da: a) je opremljen odgovarajućim sustavom za upravljanje zahtjevima i njihovim preusmjeravanjem, kako bi se olakšale primopredaje b) ima dovoljno zaposlenika kako bi se na odgovarajući način osigurala dostupnost u svako doba	U potpunosti preuzeto	

	c) se oslanja na infrastrukturu čiji je kontinuitet osiguran te su im u tu svrhu dostupni redundantni sustavi i rezervni radni prostor. (2) Radi osiguranja uvjeta iz stavka 1. ovog članka, na nadležne CSIRT-ove neće se primjenjivati ograničavajuće odredbe drugih propisa koje utječu na mogućnost novih zapošljavanja ili druga pitanja bitna za osiguranje tih uvjeta.		
PRILOG II. VRSTE SUBJEKATA ZA POTREBE ČLANKA 4. TOČKE 4. Sektor Podsektor Vrsta subjekta 1 Energetika (a) električna energija —elektroenergetsko poduzeće kako je definirano u članku 2. točki 35. Direktive 2009/72/EZ Europskog parlamenta i Vijeća (1), koje obavlja funkciju „opskrbe" kako je definirana u	*Cilj i predmet* *Članak 1.* (3) Sastavni su dio ovog Zakona: a) Prilog I. - Popis ključnih usluga s kriterijima i pragovima za donošenje ocjene o važnosti negativnog učinka incidenta	U potpunosti preuzeto	
	Prilog I. **Popis ključnih usluga s kriterijima i pragovima za utvrđivanje važnosti negativnog učinka incidenta:**	U potpunosti preuzeto	

članku 2. točki 19. te Direktive —operatori distribucijskog sustava kako su definirani u članku 2. točki 6. Direktive 2009 /72/EZ —operatori prijenosnog sustava kako su definirani u članku 2. točki 4. Direktive 2009 /72/EZ (b) nafta —operatori naftovoda —operatori proizvodnje nafte, rafinerija i tvornicâ nafte te njezina skladištenja i prijenosa (c) plin —poduzeća za opskrbu kako su definirana člankom 2. točkom 8.	<table><tr><th>Sektor</th><th>Podsektor</th><th>Ključna usluga</th><th>Kriteriji za utvrđivanje važnosti negativnog učinka incidenta</th><th>Pragovi za utvrđivanje važnosti negativnog učinka incidenta</th></tr><tr><td rowspan="3">Energetika</td><td rowspan="3">Električna energija</td><td>Proizvodnja električne energije</td><td>Instalirana snaga proizvodnog postrojenja</td><td>300 MW</td></tr><tr><td>Prijenos električne energije</td><td>Bez iznimke</td><td>-</td></tr><tr><td>Distribucija električne energije</td><td>Prekid napajanja</td><td>Više od 100.000 obračunskih mjernih mjesta</td></tr></table>						

Direktive 2009/73/EZ Europskog parlamenta i Vijeća (2) —operatori distribucijskog 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				Ovisnosti drugih djelatnosti ili područja o pružanju usluge	Distribucija za: § bolnice § zračne luke i kontrole leta § objekte banaka s podatkovnim centrima § policijske uprave § aktivne vojne objekte § aktivna vodocrpilišta i centre upravljanja § objekte operatora telekomunikacijskog sustava § objekte tijela sigurnosno-obavještajnog sustava, § objekte profesionalnih vatrogasnih postrojbi, § objekte Državne uprave za zaštitu i spašavanje		

		članku 2. točki 12. Direktive 2009/73/EZ —poduzeća za prirodni plin kako su definirana u članku 2. točki 1. Direktive 2009/73/EZ —operatori postrojenja za rafiniranje i obradu prirodnog plina				(Služba 112) ili § objekte određene nacionalnom kritičnom infrastrukturom .		
2. Prijevoz	(a) zračni promet	—zračni prijevoznici kako su definirani u članku 3. točki 4. Uredbe (EZ) br. 300/2008 Europskog parlamenta i Vijeća (3) —upravno tijelo zračne luke kako je definirano u članku 2.	Nafta	**Transport nafte naftovodima**	Bez iznimke	-		
				Proizvodnja nafte	Proizvedeno nafte pojedinog naftnog polja u tonama godišnje	50.000 t/god		
				Proizvodnja naftnih derivata	Proizvedeno naftnih derivata pojedine rafinerije u tonama godišnje	Motorni benzini: 200.000 t/god Dizelsko gorivo: 200.000 t/god Plinska ulja: 100.000 t/god		

točki 2. Direktive 2009/12/EZ Europskog parlamenta i Vijeća (4), zračna luka kako je definirana u članku 2. točki 1. te Direktive, među ostalim i glavne zračne luke s popisa u 2. odjeljku Priloga II. Uredbi (EU) br. 1315/2013 Europskog parlamenta i Vijeća (5) te tijela koja upravljaju pomoćnim objektima u zračnim lukama —operatori kontrole upravljanja prometom koji pružaju			**Skladištenje nafte i naftnih derivata**	Ukupni skladišni kapacitet nafte pojedinog terminala u m3	1.000.000 m3		
				Ukupni skladišni kapacitet naftnih derivata pojedinog skladišta (na istoj lokaciji) u m3	60.000 m3		
		Plin	**Distribucija plina**	Broj krajnjih kupaca priključen na distribucijski sustav	Više od 100.000 obračunskih mjernih mjesta.		
			Transport plina	Bez iznimke			
			Skladištenje plina	Potrošnja plina u RH, u kWh	25% potrošnje plina u RH u prethodnoj godini		
			Prihvat i otprema UPP-a	Kapacitet uplinjavanja UPP u m3/h	Više od 500.000 m3/h		

(željezn b ički) prijevo z	usluge kontrole zračnog prometa (ATC) kako su definirane u članku 2. točki 1. Uredbe (EZ) br. 549/2004 Europskog parlamenta i Vijeća (6) —upravitelji infrastrukture kako su definirani u članku 3. točki 2. Direktive 2012/34/EU Europskog parlamenta i Vijeća (7) —željeznički prijevoznici kako su definirani u članku 3. točki 1. Direktive 2012/34/EU, među ostalim i operatori			**Proizvodnja prirodnog plina**	Godišnja proizvodnja plina predana u transportni sustav na pojedinom ulazu, u kWh	1.000.000 kWh		
		Prijevoz	Zračni promet	**Zračni prijevoz putnika i tereta**	Udio putnika pojedinog zračnog prijevoznika na bilo kojem nacionalnom aerodromu koji ima promet putnika veći od 2.000.000 godišnje (ključni aerodrom)	Zračni prijevoznik koji imao udio veći od 30% na ključnom aerodromu		

	uslužnih objekata kako su definirani u članku 3. točki 12. Direktive 2012/34/EU			**Upravljanje infrastrukturom zračne luke, uključujući i upravljanje pomoćnim objektima zračne luke**	Ukupni godišnji promet putnika pojedine zračne luke	Više od 2.000.000 putnika		
(c vodni) prijevoz	—kompanije za prijevoz putnika unutarnjim plovnim putovima, morem i duž obale te kompanije za prijevoz tereta unutarnjim plovnim putovima, morem i duž obale kako su definirane u Prilogu I. Uredbi (EZ) br. 725/2004 Europskog parlamenta i Vijeća (8), ne uključujući pojedinačna plovila kojima			**Kontrola zračnog prometa**	Otvorenost područja letnih informacija Zagreb (FIR Zagreb) – bez iznimke	-		
					Broj operacija na godišnjem nivou	Ukupno 500.000 operacija za FIR Zagreb		

upravljaju te kopmanije —upravljačka tijela luka kako su definirana u članku 3. točki 1. Direktive 2005/65/EZ Europskog parlamenta i Vijeća (9), 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 —služba za nadzor i upravljanje pomorskim prometom kako je definirana u članku 3.		Željeznički promet	**Upravljanje i održavanje željezničke infrastrukture, uključujući upravljanje prometom i prometno-upravljačkim i signalno-sigurnosnim podsustavom**	Upravitelj željezničke infrastrukture za javni prijevoz – bez iznimke			
			Usluge prijevoza robe i/ili putnika željeznicom	Broj voznih jedinica (vlakova)	20 dnevno		

		točki (o) Direktive 2002/59/EZ Europskog parlamenta i Vijeća (10)						
	(d)	cestovni prijevoz	—tijela nadležna za ceste kako su definirana u članku 2. točki 12. Delegirane uredbe Komisije (EU) 2015/962 (11) odgovorna za upravljanje prometom —operatori inteligentnih prometnih sustava kako su definirani u članku 4. točki 1. Direktive 2010/40/EU Europskog parlamenta i Vijeća (12)		**Upravljanje uslužnim objektima i pružanje usluga u uslužnim objektima**	Broj voznih jedinica (vlakova)	20 dnevno		
				Pružanje dodatnih usluga koje su nužne za pružanje usluga prijevoza robe ili putnika željeznicom	Broj voznih jedinica (vlakova)	20 dnevno		
			Vodni prijevoz	**Nadzor kretanja brodova (VTS usluga)**	Godišnji broj dolazaka brodova iz međunarodne plovidbe	najmanje 4.000		
3	Bankarstvo	kreditne institucije kako						

4Infrastru . kture financijs kog tržišta	su definirane člankom 4. točkom 1. Uredbe (EU) br. 575/2013 Europskog parlamenta i Vijeća (13) —operatori mjestâ trgovanja kako su definirana u članku 4. točki 24. Direktive 2014/65/EU Europskog parlamenta i Vijeća (14) —središnje druge ugovorne strane (CCP) kako su definirane u članku 2. točki 1. Uredbe (EU) br. 648/2012 Europskog parlamenta i Vijeća (15)				Godišnji broj putovanja brodova u domaćem prometu, uključujući obalni linijski promet	najmanje 200.000		
				Obavljanje poslova pomorske radijske službe	Godišnji broj dolazaka brodova iz međunarodne plovidbe	najmanje 4.000		
					Godišnji broj putovanja brodova u domaćem prometu, uključujući obalni linijski promet	najmanje 200.000		
				Održavanje objekata sigurnosti plovidbe	Bez iznimke	-		

5.	Zdravstveni sektor	uređenje zdravstvene zaštite (uključujući bolnice i privatne klinike)	pružatelji zdravstvene zaštite kako su definirani u članku 3. točki (g) Direktive 2011/24/EU Europskog parlamenta i Vijeća (16)			**Prijevoz putnika u međunarodnom i/ili domaćem prometu**	Broj putnika godišnje	1.000.000	
6.	Opskrba vodom za piće i njezina distribucija		dobavljači i distributeri vode namijenjene za ljudsku potrošnju kako je definirana u članku 2. stavku 1. točki (a) Direktive Vijeća 98/83/EZ (17), ali isključujući distributere kojima distribucija vode za ljudsku potrošnju čini samo dio njihove općenite aktivnosti distribucije druge robe i proizvoda koji se ne smatraju		Vodni prijevoz	**Ukrcaj i iskrcaj tereta u lukama u međunarodnom i domaćem prometu**	Količina tereta godišnje u tonama	2.500.000	
						Prijevoz putnika, tereta i vozila u	Broj korisnika	15% ukupno prevezenih putnika i/ili vozila godišnje	

7Digitalna . infrastru ktura	ključnim uslugama — IXP-ovi —pružatelj DNS usluga —registri naziva TLD-ova			**unutarnji m morskim vodama i teritorijaln om moru Republike Hrvatske koji se obavlja na unaprijed utvrđenim linijama prema javno objavljeni m uvjetima reda plovidbe i cjenikom usluga**	Tržišni udio	Minimalno 15% tržišnog udjela		
				Praćenje i lociranje plovila u unutarnjoj plovidbi	Broj plovila na unutarnjim plovnim putovima u Republici Hrvatskoj tijekom godine	100		

(1) Direktiva 2009/72/EZ Europskog parlamenta i Vijeća od 13. srpnja 2009. o zajedničkim pravilima za unutarnje tržište električne energije i stavljanju izvan snage Direktive 2003/54/EZ (SL L 211, 14.8.2009., str. 55.).

(2) 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 (SL L 211, 14.8.2009., str. 94.).

(3) Uredba (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 (SL L 97, 9.4.2008., str. 72.).

(4) Direktiva 2009/12/EZ Europskog parlamenta i Vijeća od

11. ožujka 2009. o naknadama zračnih luka (SL L 70, 14.3.2009., str. 11.). (5) 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.). (6) 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.). (7) 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.). (8) 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.). (9) Direktiva 2005/65/EZ Europskog parlamenta i Vijeća od 26. listopada 2005. o jačanju							

		Obavijesti brodarstvu u unutarnjoj plovidbi	Broj izdanih obavijesti brodarstvu tijekom godine	100
		Pristup elektroničkim navigacijskim kartama u unutarnjoj plovidbi	Pokrivenost unutarnjih vodnih putova u Republici Hrvatskoj	Pokrivenost 500 riječnih km
		Baza podataka o trupu plovila u unutarnjoj plovidbi	Broj plovila unesenih u bazu podataka tijekom godine	50
		Međunarodno elektroničko izvještavanje u unutarnjoj plovidbi	Broj ERI poruka upućenih prema RIS centrima dnevno	50
	Cestovni		Broj voznih jedinica	100

sigurnosne zaštite luka (SL L 310, 25.11.2005, str. 28.). (10) 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.). (11) 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.). (12) 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.). (13) Uredba (EU) br. 575/2013 Europskog parlamenta i Vijeća od 26. lipnja 2013. o bonitetnim zahtjevima za kreditne institucije i investicijska društva i o izmjeni		prijevoz	**Javni prijevoz putnika**	Broj putnika godišnje	5.000.000		
			Korištenje cestovne infrastrukture	Upravitelj ceste na TEN-T mreži – bez iznimke	-		
				Broj vozila na glavnoj cesti koja vodi do središta naseljenog mjesta većeg od 35.000 stanovnika	20.000 PGDP (prosječni godišnji dnevni promet)		
				Zemljopisna raširenost korištenja usluga	Teritorij cijele države ili grada većeg od 35.000 stanovnika		
			Upravljanje prometnim tokovima ili informiran	Uspostavljen centar za kontrolu i upravljanje prometom 24/7 – bez iznimke			

Uredbe (EU) br. 648/2012 (SL L 176, 27.6.2013., str. 1.). (14) 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.). (15) 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.). (16) 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.). (17) Direktiva Vijeća 98/83/EZ od 3. studenoga 1998. o kvaliteti vode namijenjene za ljudsku potrošnju (SL L 330, 5.12.1998., str. 32.).			**je vozača (ITS)**	Uspostavljen centar za informiranje vozača o stanju u prometu 24/7- bez iznimke			
				Broj prometnih svjetala (semafora) u sustavu	100		
				Zemljopisna raširenost korištenja usluga	Teritorij cijele države ili grada većeg od 35.000 stanovnika		
	Bankarstvo		**Platne usluge**	Sistemski važne kreditne institucije – bez iznimke	-		
	Infrastrukture financijs		**Usluge mjesta trgovanja**	Bez iznimke	-		

	kog tržišta		**Usluge središnjih drugih ugovornih strana (CCP)**	Bez iznimke	-		
	Zdravstveni sektor		**Primarna zdravstvena zaštita – informacijski sustav**	Broj propisanih recepata za lijekove godišnje	50.000.000		
				Broj posjeta ordinacijama opće obiteljske medicine godišnje	35.000.000		
				Pokrivenost ustanova primarne zdravstvene zaštite pojedinim odobrenim programskim rješenjem	50%		

		Sekundarna zdravstvena zaštita	Broj upućivanja na specijalističke preglede godišnje	5.000.000	
			Broj obavljenih zdravstvenih postupaka, pregleda ili pretraga godišnje	1.000.000	
		Tercijarna zdravstvena zaštita	Broj postelja u stacionarnim djelatnostima kliničkih bolničkih centara (KBC)	1.000	
			Broj postelja u stacionarnim djelatnostima kliničkih bolnica (KB)	340	

				Broj postelja u stacionarnim djelatnostima klinika	100		
			Transfuzijska medicina i transplantacija organa	Broj prikupljenih doza pune krvi godišnje	100.000		
				Broj donora organa na milijun stanovnika godišnje	30		
				Broj transplantacijskih zahvata na milijun stanovnika godišnje	80		
			Zdravstveno osiguranje i prekogranična	Broj osiguranih osoba u obveznom zdravstvenom osiguranju (OZO)	4.000.000		

			zdravstvena zaštita	Broj osiguranih osoba u dopunskom zdravstvenom osiguranju (DZO)	2.000.000		
				Broj upita za provjerom statusa obveznog i dopunskog zdravstvenog osiguranja dnevno	100.000		
				Broj izdanih Europskih kartica zdravstvenog osiguranja (EKZO) godišnje	100.000		
			Sigurnost hrane	Bez iznimke	-		

			Zaštita od opasnih kemikalija	Broj sigurnosno-tehničkih listova pregledanih i uvrštenih u registar sigurnosno-tehničkih listova (STL) godišnje	9.000		
				Broj opasnih kemikalija prikupljenih i uvrštenih u registar opasnih kemikalija proizvedenih ili uvezenih/unesenih na teritorij RH godišnje	400		
			Distribucija i sigurnost lijekova i medicinski	Broj lijekova (uključujući cjepiva) stavljenih u promet u RH	3.000		

			h proizvoda	Broj medicinskih proizvoda (različitih klasa rizika) stavljenih u promet u RH	250.000		
				Broj stanovnika / osiguranih osoba na broj distribucijskih centara	330.000		
				Broj distribucijskih centara na broj veledrogerija	3		
			Cijepljenje i zarazne bolesti	Obuhvat primovakcinacijom u RH godišnje	90% ukupnog stanovništva RH		
				Ukupna vrijednost godišnje zalihe cjepiva u RH	15.000.000 kn		

	Opskrba vodom za piće i njezina distribucija		**Opskrba krajnjih korisnika**	Broj korisnika	20.000 priključaka kućanstava		
	Digitalna infrastruktura		**DNS usluga za .hr TLD**	Bez iznimke	-		
			Registar naziva domena za .hr TLD	Bez iznimke	-		
			Sustav za registriranje i administriranje sekundarne domene	Subjekt koji pruža ključnu uslugu, ima registriranu domenu preko registara i prepoznao je ovisnost svoje usluge o DNS sustavu.	-		
				Broj registriranih domena	20 % od ukupnog broja registriranih domena (unutar .hr i com.hr)		

			Usluga IXP	Broj spojenih autonomnih sustava	Veći od 15		
	Usluge u sustavima državne informacijske infrastrukture		**Usluge u sustavu e-Građani**	Broj jedinstvenih korisnika pojedine usluge	100.000,00		
				Dostupnost usluge isključivo putem elektroničke usluge	Utvrđeno da ne postoji alternativni način korištenja usluge		
			Poslovne usluge za korisnike državnog proračuna	Bez iznimke			
PRILOG III. VRSTE DIGITALNIH USLUGA ZA POTREBE ČLANKA 4. TOČKE 5. 1. Internetsko tržište 2. Internetska tražilica	*Cilj i predmet* *Članak 1.* (3) Sastavni su dio ovog Zakona: b) Prilog II. - Popis digitalnih usluga					U potpunosti preuzeto	

3. Usluge računalstva u oblaku	**Prilog II.** **Popis digitalnih usluga** 1. Internetsko tržište 2. Internetska tražilica 3. Usluge računalstva u oblaku	U potpunosti preuzeto	