



P.Z.E. br. 320

HRVATSKI SABOR

KLASA: 022-03/18-01/48

URBROJ: 65-18-08

Zagreb, 7. lipnja 2018.



Hs**NP*022-03/18-01/48*65-18-08**Hs

**ZASTUPNICAMA I ZASTUPNICIMA
HRVATSKOGA SABORA**

**PREDSJEDNICAMA I PREDSJEDNICIMA
RADNIH TIJELA**

Na temelju članaka 178. i 192. Poslovnika Hrvatskoga sabora u prilogu upućujem *Konačni prijedlog zakona o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga*, koji je predsjedniku Hrvatskoga sabora podnijela Vlada Republike Hrvatske, aktom od 7. lipnja 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: 50301-29/09-18-10

Zagreb, 7. lipnja 2018.



Hs**NP*022-03/18-01/48*50-18-07**Hs

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

Primljeno: 07-06-2018		
Klasifikacijska oznaka	Org. jed.	
022-03/18-01/48	65	
Uredbeni broj	Prij.	Vrij.
50-18-07	1	01

PREDSJEDNIKU HRVATSKOGA SABORA

Predmet: Konačni 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. u vezi sa člankom 190. Poslovnika Hrvatskoga sabora (Narodne novine, br. 81/13, 113/16, 69/17 i 29/18), Vlada Republike Hrvatske podnosi Konačni 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



dr. sc. Andrej Plenković

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

KONAČNI 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 (u daljnjem 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.

(1) Ovim Zakonom se u hrvatsko zakonodavstvo preuzima 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.).

(2) Ovim se Zakonom osigurava provedba Provedbene uredbe 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. – u daljnjem tekstu: Provedbena uredba Komisije).

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) 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 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 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, obrađuju, 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 prioriteta 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 (u daljnjem tekstu: subjekt) odredit će se operatorom ključnih usluga ako:

- a) subjekt pruža neku od ključnih usluga s Popisa iz Priloga I. ovog Zakona (u daljnjem tekstu: 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 donijeti 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 nacionalnom 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 (u daljnjem tekstu: Vlada).

(2) Mjere za postizanje visoke razine kibernetičke sigurnosti davatelja digitalnih usluga provode se sukladno Provedbenoj uredbi Komisije iz članka 2. stavka 2. ovog Zakona.

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 2. 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 pogodjenih 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 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 2. 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 Republici Hrvatskoj, 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 2. stavka 2. ovog Zakona i/ili odredbi ovog Zakona
- podnose optužne prijedloge.

(3) Nadležna sektorska tijela dužna su u aktima iz stavka 2. podstavka 1. i 2. ovog članka naznačiti 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 poslovnih usluga za državna tijela
- 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 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 preusmjerenjem, 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 godine dana od dana dostave obavijesti iz članka 10. ovog Zakona.

(2) Operatori ključnih usluga dužni su započeti s dostavom obavijesti iz članka 21. ovog Zakona u roku od 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 2. stavka 2. ovog Zakona u roku propisanom tom Uredbom.

(2) Davatelji digitalnih usluga dužni su započeti s dostavom obavijesti iz članka 21. ovog Zakona u roku od 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: <ul style="list-style-type: none"> ▪ 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

Sektor	Podsektor	Ključna usluga	Kriteriji za utvrđivanje važnosti negativnog učinka incidenta	Pragovi za utvrđivanje važnosti negativnog učinka incidenta
	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
		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

Sektor	Podsektor	Ključna usluga	Kriteriji za utvrđivanje važnosti negativnog učinka incidenta	Pragovi za utvrđivanje važnosti negativnog učinka incidenta
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 ima udio veći od 30% na ključnom aerodromu
		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

Sektor	Podsektor	Ključna usluga	Kriteriji za utvrđivanje važnosti negativnog učinka incidenta	Pragovi za utvrđivanje važnosti negativnog učinka incidenta
		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
			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

Sektor	Podsektor	Ključna usluga	Kriteriji za utvrđivanje važnosti negativnog učinka incidenta	Pragovi za utvrđivanje važnosti negativnog učinka incidenta
		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
	Vodni prijevoz	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

Sektor	Podsektor	Ključna usluga	Kriteriji za utvrđivanje važnosti negativnog učinka incidenta	Pragovi za utvrđivanje važnosti negativnog učinka incidenta		
	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		
			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		Usluge mjesta trgovanja	Bez iznimke	–

Sektor	Podsektor	Ključna usluga	Kriteriji za utvrđivanje važnosti negativnog učinka incidenta	Pragovi za utvrđivanje važnosti negativnog učinka incidenta
tržišta		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
			Zdravstvena VPN mreža HealthNet – bez iznimke	–
		Sekundarna zdravstvena zaštita	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

Sektor	Podsektor	Ključna usluga	Kriteriji za utvrđivanje važnosti negativnog učinka incidenta	Pragovi za utvrđivanje važnosti negativnog učinka incidenta
		Sigurnost hrane	Središnji informacijski sustav sanitarne inspekcije – bez iznimke	
		Zaštita od opasnih kemikalija	Broj sigurnosno-tehničkih listova pregledanih i uvrštenih u registar sigurnosno-tehničkih listova (STL) godišnje	9.000
		Zaštita od opasnih kemikalija	Broj opasnih kemikalija prikupljenih i uvrštenih u registar opasnih kemikalija proizvedenih ili uvezenih/unesenih na teritorij RH godišnje	3.500
		Distribucija i sigurnost lijekova i medicinskih proizvoda	Broj lijekova (uključujući cjepiva) stavljenih u promet u RH	3.000
		Distribucija i sigurnost lijekova i medicinskih proizvoda	Broj medicinskih proizvoda (različitih klasa rizika) stavljenih u promet u RH	250.000
		Distribucija i sigurnost lijekova i medicinskih proizvoda	Broj stanovnika / osiguranih osoba na broj distribucijskih centara	330.000

Sektor	Podsektor	Ključna usluga	Kriteriji za utvrđivanje važnosti negativnog učinka incidenta	Pragovi za utvrđivanje važnosti negativnog učinka incidenta
		Nadzor nad zdravstvenim stanjem stanovništva i ljudskim resursima u zdravstvu kroz vođenje javnozdravstvenih registara	Nacionalni javnozdravstveni informacijski sustav – bez iznimke	–
Opskrba vodom za piće i njezina distribucija		Opskrba krajnjih korisnika	Količina isporučene vode	10.000.000 m ³ /godišnje
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 članica	Veći od 15
Poslovne usluge za državna tijela		Usluge u sustavu e–Građani	Broj korisnika pojedine usluge	100.000
			Dostupnost usluge isključivo putem elektroničke usluge	Utvrđeno da ne postoji alternativni način korištenja usluge

Sektor	Podsektor	Ključna usluga	Kriteriji za utvrđivanje važnosti negativnog učinka incidenta	Pragovi za utvrđivanje važnosti negativnog učinka incidenta
		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 ključnih usluga	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
Poslovne usluge za 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**

Davatelji digitalnih usluga	Nadležno sektorsko tijelo	CSIRT	Tehničko tijelo za ocjenu sukladnosti
	tijelo državne uprave nadležno za gospodarstvo	Nacionalni CERT	Zavod za sigurnost informacijskih sustava

*Napomena: Nadležni CSIRT za sektor Poslovne usluge za državna tijela za sve usluge je Zavod za sigurnost informacijskih sustava, osim za područje koje je u djelokrugu tijela državne uprave 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 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.

OBRAZLOŽENJE

I. RAZLOZI ZBOG KOJIH SE ZAKON DONOSI

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 ubranu inicijativu razvoja digitalnog gospodarstva EU. Time se uvode zajedničke mjere u svim državama članicama za postizanje visoke razine kibernetičke sigurnosti i koordinaciju postupanja niza potrebnih dionika na nacionalnim i sektorskim razinama država članica i EU-a.

Sadržaj svih pitanja koja se ovim Zakonom rješavaju predstavlja i prirodni slijed niza nacionalnih aktivnosti započetih Nacionalnim programom informacijske sigurnosti iz 2005. (<https://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2005-04-110.pdf>), kao i slijednim zakonodavnim promjenama i donošenjem Zakona o informacijskoj sigurnosti (Narodne novine, broj 79/07). Već tada je u RH prepoznata potreba i propisane su osnovne CERT sposobnosti koje se trebaju razviti u RH, kroz uspostavu Zavoda za sigurnost informacijskih sustava (<https://www.zsis.hr/>), sa zadaćama koje su, između ostalog vezane za koordinaciju prevencije i odgovora na računalne ugroze sigurnosti informacijskih sustava u okviru državnog sektora, te kroz uspostavu Nacionalnog CERT-a (<https://www.cert.hr/>), u okviru Hrvatske akademske i istraživačke mreže (CARNET), sa zadaćama vezanim za prevenciju i zaštitu od računalnih ugroza sigurnosti svih javnih informacijskih sustava u Republici Hrvatskoj. Upravo ove dvije institucije, deset godina nakon ustrojavanja njihovih temeljnih CERT-ovskih sposobnosti, u predmetnom Zakonu predstavljaju CSIRT¹ tijela sa sličnim zadaćama prevencije i odgovora na računalne ugroze sigurnosti informacijskih sustava. Predmetnim Zakonom provodi se daljnje uređenje područja prevencije i zaštite od računalnih ugroza sigurnosti kroz usmjeravanje mjera na Zakonom utvrđene sektore ključnih usluga i davatelja digitalnih usluga kako ih propisuje EU², te na dodatni sektor ključnih usluga od interesa za RH³. Pri tome se

¹ CSIRT je kratica za Computer Security Incident Response Team, odnosno tijelo nadležno za prevenciju i zaštitu od incidenata, za koju se u RH koristi i kratica istog značenja CERT (Computer Emergency Response Team).

² NIS direktiva utvrđuje obvezu država članica uvesti mjere za visoku razinu zaštite kibernetičke sigurnosti u sljedećim sektorima ključnih usluga: 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. NIS direktiva također utvrđuje obvezu za davatelje digitalnih usluga na razini jedinstvenog digitalnog tržišta EU u području usluga: internetsko tržište, internetske tražilice i usluge računalstva u oblaku.

³ RH u okviru Zakona uvodi dodatni sektor: poslovne usluge za državna tijela, koji se sastoji od dva podsektora: usluge u sustavu e–Građani, poslovne usluge za korisnike državnog proračuna.

provodi uravnoteženje obveza i odgovornosti korisnika informacijskih sustava s jedne strane, te načina obavješćivanja i međusobne pomoći u rješavanju incidenata na sektorskoj, nacionalnoj i EU razini, s druge strane.

S predmetnim Zakonom povezan je i niz drugih inicijativa u RH, koje su mu prethodile u prijašnjim godinama, primjerice procjena ključnih ugroza u telekomunikacijskom sustavu RH provedena 2010. godine u koordinaciji Ureda Vijeća za nacionalnu sigurnost (UVNS), koja je rezultirala nizom mjera, od kojih je jedna provedena u koordinaciji sa Sveučilišnim računskim centrom Sveučilišta u Zagrebu (Srce), s ciljem uspostavljanja organizacijskih i sigurnosnih mjera za razmjenu internetskog prometa između davatelja internetskih usluga u RH (Croatian Internet Exchange – CIX, <http://www.srce.unizg.hr/croatian-internet-exchange-cix>), a što danas predstavlja jedan od zahtjeva NIS direktive za sve države članice EU.

Primjer postignuća RH na razvoju sposobnosti u području kibernetičke sigurnosti u prošlom razdoblju predstavlja i suradnja Hrvatske regulatorne agencije za mrežne djelatnosti (HAKOM) i Nacionalnog CERT-a, provedena 2012. godine pod okriljem UVNS-a, koja je rezultirala izradom Pravilnika o načinu i rokovima provedbe mjera zaštite sigurnosti i cjelovitosti mreža i usluga⁴ (Narodne novine, broj 109/12, 33/13, 126/13 i 67/16). Time su u RH uvedene obveze provedbe sigurnosnih mjera za operatore javnih komunikacijskih mreža u RH, u obliku minimalnih sigurnosnih mjera u skladu s međunarodnom normom ISO 27001, kao i koordinacija rješavanja sigurnosnih incidenata između operatora i Nacionalnog CERT-a. Važno je uočiti da za razliku od ovog primjera u kojem se primarno adresira kriterij raspoloživosti infrastrukture davatelja javnih komunikacijskih mreža u RH, predmetnim Zakonom se uvode širi zahtjevi i adresira se sva tri temeljna sigurnosna kriterija (povjerljivost, cjelovitost i raspoloživost), uključujući i svojstvo autentičnosti digitalnih vjerodajnica, za mrežne i informacijske sustave kojima se upravlja ključnim i digitalnim uslugama koje su u opsegu Zakona.

Jedno od postignuća iz ovog prethodnog razdoblja RH predstavlja i sustav SRU@HR – Nacionalni sustav ranog upozoravanja na sigurnosne ugroze na Internetu, koji je u koordinaciji s UVNS-om uspostavio CARNET-ov Nacionalni CERT 2011. godine (<https://www.cert.hr/sru/>) i koji široj javnosti u RH danas omogućava uvid u stanje kibernetičkog prostora u RH i globalno.

NIS direktiva dio je široke aktualne digitalne inicijative EU–a, kojom se svijest o nužnosti razvoja digitalnog gospodarstva širi kroz niz segmenata suvremenog društva, počevši od procesa stvaranja jedinstvenog digitalnog tržišta EU–a, preko niza inicijativa za jačanje sigurnosne svijesti građanstva o kibernetičkom prostoru, do poticanja razvoja javno–privatnog partnerstva i elektroničkih usluga u državnoj upravi i gospodarstvu. Pri tome NIS direktiva stvara primjerene okvire prevencije i zaštite društva od kibernetičkih ugroza zajedničkim pristupom svih država članica koje osiguravaju usklađene vertikalne sektorske pristupe u nacionalnom okruženju, dok nova EU regulativa zaštite osobnih podataka (GDPR) sličan pristup osigurava horizontalnim funkcionalnim pristupom kroz sve segmente društva u cjelini. Potrebno je uočiti da se aktualna problematika zlouporabe osobnih podataka u kibernetičkom prostoru primarno

⁴ Neslužbeni pročišćeni tekst: <https://www.hakom.hr/UserDocsImages/2016/propisi/VL-KU-PR-INTS-Pravilnik%20o%20sigurnosti-neslu%C5%BEbeni%20pro%C4%8Di%C5%A1%C4%87eni%20tekst.pdf>

adresira kroz GDPR regulativu, dok NIS direktiva primarno adresira problem sigurnosti infrastrukture koja služi za ključne i digitalne usluge društva i gospodarstva.

Sustavno povezivanje niza aktivnosti i inicijativa u RH koje su provedene u razdoblju od 2005. do 2014. godine, provedeno je tijekom izrade Nacionalne strategije kibernetičke sigurnosti, koja je zajedno s detaljnim Akcijskim planom provedbe donesena 2015. godine (Narodne novine, broj 108/15). Pristup uveden u RH u Nacionalnoj strategiji kibernetičke sigurnosti, iako dovršen prije objave NIS direktive, u potpunosti je sukladan sa zahtjevima NIS direktive. Tako je Nacionalnom strategijom RH uvedeno i jedno od pet nacionalnih područja kibernetičke sigurnosti: kritična komunikacijska i informacijska infrastruktura i upravljanje kibernetičkim krizama, koje u potpunosti pretpostavlja provedbu mjera iz predmetnog Zakona, te će provedba Zakona u najvećoj mogućoj mjeri predstavljati i istovremenu provedbu mjera Nacionalne strategije kibernetičke sigurnosti RH u spomenutom području. Nadalje, kako bi se omogućilo učinkovito praćenje provedbe Nacionalne strategije kibernetičke sigurnosti, ali i osiguralo potrebnu međuresornu povezanost nadležnih institucija državnog i javnog sektora, 2016. godine uspostavljena su strateška i operativna međuresorna nacionalna tijela za upravljanje provedbom Nacionalne strategije kibernetičke sigurnosti i rješavanje svih bitnih nacionalnih pitanja u području kibernetičke sigurnosti (Narodne novine, broj 61/16).

Nacionalno vijeće za kibernetičku sigurnost⁵ (dalje: Vijeće) konstituirano je 16. ožujka 2017. godine, slijedom Rješenja o imenovanju predsjednika, zamjenika predsjednika, članova i zamjenika članova Nacionalnog vijeća za kibernetičku sigurnost, koje je donijela Vlada Republike Hrvatske na sjednici održanoj 16. veljače 2017. godine. Po imenovanju predstavnika u Vijeću, uslijedilo je imenovanje predstavnika tijela u Operativno-tehničkoj koordinaciji za kibernetičku sigurnost (dalje: Koordinacija), koja 23. ožujka 2017. započinje sa svojim radom. Konstituiranjem Vijeća i Koordinacije otvoren je put za punu provedbu mjera Akcijskog plana i ostvarenje ciljeva Nacionalne strategije kibernetičke sigurnosti u RH.

Vijeće predstavlja stratešku međuresorno tijelo sastavljeno od predstavnika 18 institucija s ciljem uspostave i upravljanja svim potrebnim horizontalnim inicijativama u području kibernetičke sigurnosti RH, kako u državnom sektoru, tako i međusektorski, odnosno u društvu u cjelini. Rad Vijeća koordinira UVNS. Koordinacija predstavlja međuresorno operativno tijelo sastavljeno od predstavnika 8 institucija s odgovarajućim operativnim nadležnostima i resursima, putem kojeg se žele učinkovitije koordinirati i provoditi potrebne aktivnosti prevencije i reakcije na ugroze kibernetičke sigurnosti, primarno u smislu komplementarnog pristupa u prevenciji i rješavanju sigurnosnih incidenata, a time i usklađenog razvoja nacionalnih sposobnosti u kibernetičkom prostoru. Rad Koordinacije koordinira Ministarstvo unutarnjih poslova (MUP), a usmjerava Vijeće.

UVNS na svojoj mrežnoj stranici redovito objavljuje godišnja izvješća o provedbi Akcijskog plana za provedbu Nacionalne strategije kibernetičke sigurnosti na kraju drugog

⁵ http://www.uvns.hr/UserDocsImages/dokumenti/informacijska-sigurnost/InicijalnoIzvjescjeVijecaVladiRH_13062017.pdf

kvartala tekuće godine za prošlu godinu⁶. Također, u Godišnjem izvješću o radu Nacionalnog vijeća za kibernetičku sigurnost i Operativno-tehničke koordinacije za kibernetičku sigurnost za 2017. godinu, objavljenom 12. travnja 2018. godine na mrežnoj stranici UVNS-a⁷, daje se i osvrt na stanje kibernetičkog prostora u 2017. godini.

II. PITANJA KOJA SE ZAKONOM RJEŠAVAJU

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 za uvođenje mjera 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 prevedena je na engleski jezik te je raspoloživa, zajedno sa strategijama drugih država članica, na mrežnoj poveznici ENISA-e⁸.

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. Ovaj postojeći nacionalni okvir koji čine Nacionalna strategija kibernetičke sigurnosti s pripadajućim Akcijskim planom za njenu provedbu, predmetnim Zakonom proširuje se 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

⁶ Izvješće o provedbi Akcijskog plana za 2016. godinu:

<http://www.uvns.hr/UserDocsImages/dokumenti/informacijska-sigurnost/Izvjesce%20o%20provedbi%20Akcijskog%20plana%20za%20provedbu%20NSKS%20u%202016.pdf>

⁷ http://www.uvns.hr/UserDocsImages/dokumenti/informacijska-sigurnost/GI2017_NVKS_VRH_12042018.pdf

⁸ <https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ness-map/strategies/croatian-cyber-security-strategy>

odgovarajućih nadležnosti s EU formatima strateških, operativnih ili sektorskih nadležnih 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. Predmetnim Zakonom nacionalna nadležna tijela na strateškoj i operativnoj razini, kao i drugi dionici provedbe Strategije, uključuju se u odgovarajuće organizacijske okvire i, uz postojeće nacionalne nadležnosti, provode potrebne i sukladne 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. Najveći dio mjera Akcijskog plana razrađen je upravo u svrhu poboljšanja obrazovnog sustava i to u svim njenim segmentima, od formalnog obrazovanja po svim razinama, preko specijalističkih stručnih obrazovnih akademija poput pravosudne, policijske i vojne, do sustava cjeloživotnog obrazovanja. Određeni pomaci postignuti su u segmentima specijalističkih stručnih akademija i cjeloživotnog obrazovanja, dok se u formalnim obrazovnim programima isto očekuje kroz uspostavu i provedbu nacionalnog obrazovnog kurikuluma za koji su u području kibernetičke sigurnosti spomenutim dokumentima Strategije i Akcijskog plana postavljani zahtjevi.

Nacionalnom strategijom kibernetičke sigurnosti 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 razdoblju od svibnja do studenog 2018. biti raspoloživ za tijela i operatore nacionalno nadležne za primjenu NIS direktive.

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 mrežnoj

poveznici UVNS-a⁹, kao i inicijalno izvješće o osnivanju međuresornih nacionalnih tijela za upravljanje strategijom¹⁰.

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 i u narednim godinama kroz razvoj sektorske tehnologije. Važno je napomenuti da je provedba odgovarajućih mjera prema NIS direktivi obvezna 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 trajno ažurirati popis takvih operatora.

Prvu skupinu obveznika zahtijeva iz predmetnog Zakona čine operatori koji pružaju ključne usluge za društvo ili nacionalnu ekonomiju (Operators of Essential Services – OES), u okviru utvrđenih sedam NIS sektora i jednog nacionalnog sektora, odnosno ukupno 8 sektora sa 14 podsektora. Sektori ključnih usluga u odgovornosti su država članica EU.

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 pri 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.) – u daljnjem 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 sukladne sa svim zahtjevima NIS direktive te bi njezino prenošenje u važeće propise zahtijevalo dopune i izmjene više zakonskih (sektorskih) propisa, izrađen je predmetni Zakon, kojim se namjerava na jedinstveni način urediti navedena materija, uzevši pri tome u obzir nacionalne potrebe RH i predmetne EU zahtjeve.

Predmetni Zakon, uz obvezu uvođenje tehničkih i organizacijskih mjera za upravljanje rizicima i mjera za sprečavanje i svodenje na najmanju moguću mjeru učinaka incidenata na

⁹ <http://www.uvns.hr/UserDocsImages/dokumenti/informacijska-sigurnost/Izvjescje%20o%20provedbi%20Akcijuskog%20plana%20za%20provedbu%20NSKS%20u%202016.pdf>

¹⁰ http://www.uvns.hr/UserDocsImages/dokumenti/informacijska-sigurnost/InicijalnoIzvjescjeVijecaVladiRH_13062017.pdf

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 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 predmetnog Zakona. Stoga je predmetnim Zakonom, predviđeno donošenje podzakonskog akta, uredbe Vlade RH. Kriteriji za određivanje incidenata koji imaju znatan učinak na davanje digitalnih usluga propisani su spomenutom Provedbenom uredbom Komisije.

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, a prvo izvješće o provedbi identifikacije ključnih operatora u RH i statistici incidenata, UVNS, kao nadležna nacionalna jedinstvena kontaktna točka, podnosi Europskoj komisiji najkasnije do 9. studenog 2018. godine. Sve države članice dužne su nakon 9. studenoga 2018., svake dvije godine, Europskoj komisiji dostavljati podatke koji su potrebni kako bi se Komisiji omogućila procjena nacionalne provedbe NIS direktive.

Predmetnim Zakonom preuzimaju se obveze iz NIS direktive koje su u odgovornosti država članica te se na prikladan način povezuju u nacionalnu organizaciju RH u području kibernetičke sigurnosti i s postojećim nadležnostima tijela u svakom od sektora ključnih usluga u RH. Stoga su u predmetnom Zakonu primijenjeni prilagođeni kriteriji i pridružena primjerena nadležna tijela, kako bi se postigli željeni rezultati u odnosu na stvarno stanje koje postoji u predmetnim sektorima i na nacionalnoj razini u RH.

Izričaj Prijedloga zakona obuhvaća svu potrebnu različitost javnih i privatnih subjekata koji su ili nadležna tijela, ili obveznici primjene ovog Zakona. Predmetni Zakon 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, predmetnim Zakonom 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 pa i na RH u ovom području.

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 ključnim sektorima u RH. U tu svrhu, predmetnim Zakonom 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).

Predmetnim Zakonom 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: jedinstvena nacionalna kontaktna točka, CSIRT tijela i njihova sektorska nadležnost, odnosno nadležna sektorska tijela odgovorna za provedbu nadzora nad primjenom prenesenih obveza u ključnim sektorima, 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 UVNS kao predloženo tijelo već ima u RH, vezano uz provedbu Nacionalne strategije kibernetičke sigurnosti, odnosno rad Nacionalnog vijeća za kibernetičku sigurnost, dok su CSIRT nadležnosti dodijeljene postojećim tijelima koja već deset godina razvijaju odgovarajuće sposobnosti u tom području djelovanja. Izbor nadležnih sektorskih tijela prati postojeće nadležnosti središnjih državnih tijela RH u područjima koji obuhvaćaju utvrđene sektore ključnih usluga, 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 RH po pitanju provedbe revizije odnosno njezine procjene u nadzornim postupcima, uvedena je i uloga tehničkog tijela za ocjenu sukladnosti, prvenstveno za slučajeve sektora u kojima revizija nije obvezujuća za pružatelje odnosno davatelje ključnih usluga iz predmetnog Zakona.

Pored sektora koji su kao obvezujući predviđeni samom NIS direktivom kao područja u kojima države članice moraju uvesti nove obveze odnosno prilagoditi postojeće, predmetnim zakonom se uključuje još jedan sektor koji obuhvaća poslovne usluge za 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 predmetnog Zakona, odnosno uspostavila sustavna koordinacija svih relevantnih dionika, razvila svijest o mogućim ugrozama u kibernetičkom prostoru te prikladno upravljalo rizicima i razmjerno rizicima provodile mjere zaštite, 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.

Predmetnim Zakonom se na sustavan način koriste postojeći kapaciteti i potencijali prepoznati Nacionalnom strategijom kibernetičke sigurnosti RH 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 predmetnim Zakonom, ali istovremeno omogućava međusobno komplementarno djelovanje različitih subjekata u širokom opsegu pokrivanja društvenih i gospodarskih sektora, čime se ostvaruje učinkovita uporaba svih nacionalnih 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 nepotrebnog multipliciranja kapaciteta ili neracionalnosti u pristupu opremanju radi razvoja novih sposobnosti koje su već realizirane 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 prije odobrenog hrvatskog projekta GrowCERT, koji je pokrenut 2017. i vrijedan milijun EUR-a, uz sufinanciranje iz CEF fonda na razini 75% (nositelj CARNET – Nacionalni CERT). U 2018. godini, Europska komisija u svibnju otvara mogućnost apliciranja i korištenja CEF fonda i za pravne osobe – sektorske operatore, putem nadležnih sektorskih tijela i uz uvjet prethodne nacionalne transpozicije NIS direktive.

Kombiniranjem postojećih centraliziranih međuresornih funkcionalnosti kibernetičke sigurnosti koje je Vlada RH uspostavila kroz Nacionalno vijeće za kibernetičku sigurnost i predmetnim Zakonom predloženim povezivanjem tijela nadležnih za sektore ključnih usluga obuhvaćene Zakonom, nastavlja se nacionalna razrada već uspostavljene organizacije i upravljanja sigurnošću u kibernetičkom prostoru RH i njeno povezivanje s EU razinom. Istovremeno ova organizacija i sustav upravljanja direktno se veže na puno širi nacionalni sustav domovinske sigurnosti, odnosno kritičnih nacionalnih sektora i nacionalnog kriznog upravljanja, ostvarujući pri tome potrebnu sinergiju djelovanja između fizičke i virtualne dimenzije našeg društva.

Zaključno se može reći da se predmetnim Zakonom osigurava provedba obveza RH iz NIS direktive te se istovremeno osiguravaju i sve potrebne pretpostavke za daljnje unaprjeđenje stanja kibernetičke sigurnosti u širokom opsegu društvenih i gospodarskih sektora koji su obuhvaćeni. Istovremeno se potiče i razvoj RH u području digitalnog gospodarstva, usklađenim pristupom između niza dionika iz javnog i privatnog sektora koji se omogućava kroz provedbu Zakona. 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 sigurnosnim zahtjevima za cijelo područje Europske unije.

III. OBRAZLOŽENJE ODREDBI PREDLOŽENOG ZAKONA

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 2016/114 i osigurava provedba Provedbene uredbe 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. – u daljnjem tekstu: Provedbena uredba Komisije).

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. 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, 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. propisuje 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 obavješćivanja 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.

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 održavanje 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, poslovne usluge za državna tijela te davatelje digitalnih usluga) 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 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 2016/1148 i/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 nacionalnim kontaktnim točkama drugih pogodnih država članica, osim za sektor poslovnih usluga za 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 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 kontaktnu 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.

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 ovog Zakona koriste samo za potrebe izvršenja Zakona te da 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. Također, propisuje se da je 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.

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 u roku od 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 utvrđivanje

važnosti negativnog učinka incidenta, izraženi u različitim (mjernim) jedinicama (npr. MW, tonama, broju korisnika, m³, 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 –tijelo državne uprave nadležno za energetiku, prijevoza – tijelo državne uprave nadležno za promet, bankarstva – Hrvatska narodna banka, infrastrukture financijskog tržišta – Hrvatska agencija za nadzor financijskih usluga, zdravstveni sektor –tijelo državne uprave nadležno za zdravstvo, sektor opskrbe vodom za piće i njezinu distribuciju –tijelo državne uprave nadležno za vodno gospodarstvo, digitalne infrastrukture – Središnji državni ured za razvoj digitalnog društva, digitalne usluge –tijelo državne uprave nadležno za gospodarstvo te poslovne usluge za 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.

IV. OCJENA SREDSTAVA ZA PROVEDBU ZAKONA

Za provedbu ovog Zakona bit će potrebno osigurati dodatna sredstva u Državnom proračunu Republike Hrvatske u razdoblju 2018.-2020. u ukupnom iznosu od 3.949.114,00 kn i to za zaposlene i njihove materijalne rashode u Središnjem državnom uredu za razvoj digitalnog društva u ukupnom iznosu od 1.566.614,00 kn, a za zaposlene i njihove materijalne rashode te IT usluge za potrebe CARNET-a u ukupnom iznosu od 2.382.500,00 kn. Potrebna sredstva osigurat će se u 2018., 2019. i 2020. preraspodjelom sredstava unutar limita ukupnih rashoda navedenih nadležnih tijela. Ostala nadležna tijela iz Zakona za provedbu zadaća iz svoje nadležnosti koristit će postojeće kapacitete i redovna proračunska sredstva osigurana u Državnom proračunu na razdjelima tih tijela. Vezano za stanje postojećih kapaciteta nadležnih tijela, potrebno je napomenuti da određena nadležna tijela iz predmetnog Zakona, već niz godina razvijaju potrebne kapacitete kroz aktivnosti opisane u poglavlju *I. Razlozi zbog kojih se Zakon donosi*. Stoga, već postoje redovne proračunske pozicije koje se razvijaju iz godine u godinu. Dodatno, sinergija djelovanja različitih tijela postignuta je boljom međusobnom koordinacijom rada različitih tijela kroz uspostavljeno Nacionalno vijeće za kibernetičku sigurnost. Time se omogućava puno bolje usmjeravanje predviđenih sredstava za rad pojedinog tijela, primjerice kroz usklađivanje sličnih aktivnosti javnih promocija sigurnosti na Internetu koje se mogu tematski uskladiti i učinkovitije realizirati kroz međusobnu koordinaciju različitih nositelja kao što su tijela u sektoru javnih komunikacija, sektoru bankarstva ili u javnoj sigurnosti.

Broj obveznika provedbe zahtjeva u području sektora ključnih usluga procijenit će se kroz Zakonom propisani postupak identifikacije u roku od 90 dana od stupanja na snagu predmetnog Zakona. Potrebno je napomenuti da unatoč novim odredbama ovog Zakona svi operatori koji danas koriste mrežne i informacijske sustave za upravljanje ključnim uslugama, koriste i odgovarajuće sigurnosne mjere temeljene na procjeni rizika poslovanja. Za mnoge od

hrvatskih operatora neće biti velikih promjena, kao što je u poglavlju I. napomenuto za slučaj u RH davno uredenog središta za razmjenu internetskog prometa (CIX). Zakonom se samo formaliziraju sigurnosni uvjeti koji će potvrditi dobru praksu nekih operatora i vjerojatno popraviti postojeću praksu kod drugih operatora, a svim operatorima će olakšati slučajeve rješavanja sigurnosnih incidenata koji postaju sve češći i pružiti im potrebne instrumente rješavanja na nacionalnoj i EU razini. Ono što je najvažnije, jest da će se Zakonom u narednom razdoblju povećane digitalizacije hrvatskog gospodarstva osigurati ujednačen pristup za sve nove operatore i sve nove digitalizirane usluge u opsegu Zakona.

Vežano za korištenje sredstava EU fondova osiguranih u svrhu provedbe NIS direktive u državama članicama, prvi natječaj za sredstva direktno namijenjena za provedbu ovog Zakona iz spomenutog CEF fonda raspisan je u svibnju i otvoren do studenog 2018. te je na raspolaganju nadležnim tijelima i identificiranim operatorima ključnih usluga (CEF-TC-2018-3: Cyber Security). U pitanju je ukupan iznos osiguranih sredstava za ovu svrhu od 9.000.000,00 eura. Projekti usmjereni na jačanje kapaciteta nadležnih CSIRT-ovi mogu biti financirati iznosom do 1.000.000,00 eura, za prilagodbu operatora ključnih usluga i davatelja digitalnih usluga obvezama iz NIS direktive moguće je, po pojedinačnom projektu, povući EU sredstva u iznosu od 150.000,00 eura, a za potrebe jačanja kapaciteta nadležnih sektorskih tijela i jedinstvene nacionalne kontaktne točke iznos od 100.000,00 eura.

Indirektno su dostupna sredstva i iz drugih EU fondova koja će u prvom redu ovisiti o daljnjem horizontalnom povezivanju sektora društva i osobito o uspješnosti programa javno-privatnog partnerstva u RH.

V. RAZLIKE IZMEĐU RJEŠENJA KOJA SE PREDLAŽU KONAČNIM PRIJEDLOGOM ZAKONA U ODNOSU NA RJEŠENJA IZ PRIJEDLOGA ZAKONA I RAZLOZI ZBOG KOJIH SU TE RAZLIKE NASTALE

U odnosu na tekst Prijedloga zakona koji je bio u prvom čitanju i koji je prihvaćen u Hrvatskome saboru, u Konačnom prijedlogu zakona nastale su određene razlike kao rezultat uvažavanja prijedloga i primjedbi iznijetih između prvog i drugog čitanja. Sve upućene primjedbe i prijedlozi su pomno razmotreni te su prihvaćene sljedeće primjedbe:

Odbor za zakonodavstvo Hrvatskoga sabora uputio je primjedbe i prijedloge nomotehničke naravi koje su sve prihvaćene na sljedeći način:

- u člancima 1., 6. i 20. – kod skraćivanja pojmova naznačeno je „u daljnjem tekstu“
- u članku 2. – doraden je izričaj odredbe na način da je sve povezano u jednu rečenicu, s obzirom da se radi o jednom propisu Europske unije
- u članku 4. – brisan je stavak 2. koji je ocijenjen suvišnim zbog cjelovitosti i jedinstva pravnog sustava, jer ako pojedine odredbe nekog propisa utječu na odredbe nekog drugog propisa tada se propisuju iznimke
- u članku 26. – u stavku 1. brisana je riječ: “najmanje“ s obzirom na izričaj stavka 2.
- u članku 27. – u stavku 5. naveden je puni naziv Republike Hrvatske s obzirom da naziv prethodno u normativnom dijelu Prijedloga nije bio skraćen

– u članku 48. – u stavku 1. ujednačeno je pisanje rokova („u roku godine dana“).

Također, ispravljene su pojedine uočene greške u pisanju (primjerice, u članku 28. stavku 3. riječ „članka“ zamijenjena je riječju „stavka“).

U okviru pripreme Nacrta konačnog prijedloga zakona dodatno je, temeljem prijedloga tijela, unesena dopuna i određene izmjene teksta u Konačnog prijedloga zakona.

Na prijedlog Ministarstva uprave u članak 2. unesen je novi stavak 2. koji glasi:

“Ovim se Zakonom osigurava provedba Provedbene uredbe 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. – u daljnjem tekstu: Provedbena uredba Komisije).”.

Na prijedlog Ministarstva zaštite okoliša i energetike izmijenjen je kriterij, i kriterijski prag, za utvrđivanje važnosti negativnog učinka incidenta u Popisu iz Priloga I. Zakona, temeljem kojih kriterija i pragova se, uz ostale opće kriterije, određuju operatori ključnih usluga za sektor „Opskrbe vodom za piće“. Kriteriji „Broj korisnika“ i kriterijski prag „20.000 priključaka kućanstava“ izmijenjeni su na način da glase „Količina isporučene vode“ - 10.000.000 m³/godišnje”.

Na prijedlog Ministarstva zdravstva izmijenjen je kriterijski prag za ključnu uslugu „Zaštita od opasnih kemikalija“, na način da isti umjesto „400“ glasi „3.500“. Također, izmijenjen je naziv ključne usluge „Nadzor nad zaraznim bolestima te skladištenjem i distribucijom cjepiva“ na način da ista glasi „Nadzor nad zdravstvenim stanjem stanovništva i ljudskim resursima u zdravstvu kroz vođenje javnozdravstvenih registara“ te je u odnosu na istu uslugu brisan kriterij i kriterijski prag koji su glasili „Procijepljenost stanovništva RH godišnje – 80%”.

VI. PRIJEDLOZI, PRIMJEDBE I MIŠLJENJA DANI NA PRIJEDLOG ZAKONA KOJE PREDLAGATELJ NIJE PRIHVATIO TE RAZLOZI NEPRIHVATANJA

Sve upućene primjedbe, prijedlozi i mišljenja su razmotreni, a nisu prihvaćeni:

- primjedba o potrebi širenja primjene ovog Zakona na pitanja zaštite osobnih podataka od neovlaštenog korištenja.

Predmetni Zakon usmjeren je na jačanje otpornosti mrežnih i informacijskih sustava o kojima ovisi pružanje ključnih usluga ili davanje digitalnih usluga, te se njime, s ciljem sprečavanja, ublažavanja i rješavanja incidenata na tim sustavima (uzrokovanih ne samo napadima, već i kvarovima, ljudskim pogreškama ili prirodnim fenomenima), uvodi obveza

provedbe sigurnosnih mjera i obavješćivanja o incidentima sa znatnim učinkom na pružanje usluge (uslijed kojih je došlo do prekida ili znatnog poremećaja u pružanju usluge).

Područje zaštite osobnih podataka regulirano je posebnim propisima. S tim u svezi, napominje se kako je EU je 6. travnja 2016. prihvatila veliku reformu svojeg okvira za zaštitu osobnih podataka donošenjem paketa reformi, koji se, između ostalog, sastoji od Opće uredbe o zaštiti podataka, koja će se izravno primjenjivati u državama članicama od 25. svibnja 2018. Slijedom toga, predmetnim Zakonom, a kako je to apostrofirano i u članku 2. i članku 15. stavku 4. NIS direktive, određeno je da ako se u provedbi ovog Zakona obrađuju osobni podaci, na takve podatke primjenjuju posebni propisi o njihovoj zaštiti (članak 4. stavak 1. Zakona). Također, regulirano je pitanje suradnje i razmjene informacija nadležnih tijela iz Zakona 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 i s pravosudnim tijelima, kada je takav incident rezultat kriminalnih aktivnosti (članak 25. stavak 2. podstavak 5. i članak 30. podstavak 7. Zakona).



1. Naziv prijedloga propisa

Zakon o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga (II. čitanje)

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: II. 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., 1., 14., 14., 14., 16., 19., 20., 25., 25., 25., 25. i 25. bit će preuzeto: Uredba o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga (18.06.2018)
- 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

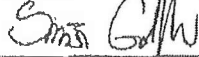
5. Prilog: tablice usporednih prikaza za propise kojima se preuzimaju odredbe sekundarnih izvora prava Europske unije u zakonodavstvo Republike Hrvatske

Da.

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

Siniša Gudlin

POMOĆNIK PREDSTOJNICE I EU KOORDINATOR



(potpis)

15-05-2018

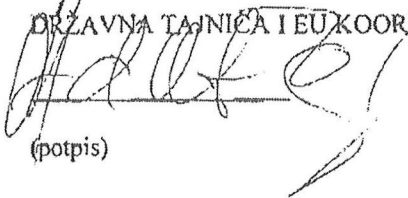
(datum i pečat)



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

Andreja Metelko-Zgombić

DRŽAVNA TAJNICA I EU KOORDINATORICA



(potpis)



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 (II. čitanje)

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)

		preuzet u odredbu u prijedloga propisa?		
<p>POGLAVLJE I.</p> <p>OPĆE ODREDBE</p> <p>Članak 1.</p> <p>Predmet i područje primjene</p> <p>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.</p> <p>2. U tu svrhu, ovom Direktivom:</p> <p>(a) utvrđuje se obveza za sve države članice da donesu nacionalnu strategiju za sigurnost mrežnih i informacijskih sustava;</p> <p>(b) stvara se skupina za suradnju u svrhu podupiranja i olakšavanja strateške suradnje i razmjene informacija među državama članicama i razvijanja</p>	<p><i>Cilj i predmet</i></p> <p><i>Članak 1.</i></p> <p>(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 (u daljnjem 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.</p> <p>(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.</p>	U potpuno sti preuzet o		
	<p><i>Jedinstvena nacionalna kontaktna točka</i></p> <p><i>Članak 30.</i></p> <p>Jedinstvena nacionalna kontaktna točka:</p> <p>– vodi brigu o potrebi razvoja i usklađivanja nacionalne strategije kibernetičke sigurnosti s ciljevima ovog Zakona i zahtjevima Europske unije u području kibernetičke sigurnosti</p>	U potpuno sti preuzet o		

<p>međusobnog povjerenja i pouzdanja;</p> <p>(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;</p>			
<p>(d) utvrđuju se zahtjevi za sigurnost i obavješćivanje za operatore ključnih usluga i za pružatelje digitalnih usluga;</p> <p>(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.</p>	<p style="text-align: center;">Jedinstvena nacionalna kontaktna točka</p> <p style="text-align: center;"><i>Članak 30.</i></p> <p>Jedinstvena nacionalna kontaktna točka:</p> <p>– 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,</p>	<p>U potpuno sti preuzet o</p>	
<p>3. Zahtjevi za sigurnost i obavješćivanje iz ove Direktive ne primjenjuju se na poduzeća na koje se primjenjuju zahtjevi iz članka 13.a i 13.b Direktive 2002/21/EZ ni na pružatelje usluga povjerenja na koje se primjenjuju zahtjevi iz</p>	<p style="text-align: center;">Zadaće nadležnog CSIRT-a</p> <p style="text-align: center;"><i>Članak 32.</i></p> <p>(1) Nadležni CSIRT na sektorskoj razini, prema popisu nadležnosti iz Priloga III. ovog Zakona, obavlja sljedeće poslove:</p> <p>– 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</p>	<p>U potpuno sti preuzet o</p>	

<p>članka 19. Uredbe (EU) br. 910/2014.</p> <p>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.</p> <p>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.</p> <p>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 zaštitu informacija za čije otkrivanje</p>	<p style="text-align: center;">Utvrdjivanje mjera</p> <p style="text-align: center;"><i>Članak 20.</i></p> <p>(1) Mjere za postizanje visoke razine kibernetičke sigurnosti operatora ključnih usluga i način njihove provedbe pobliže se propisuju uredbom koju donosi Vlada Republike Hrvatske (u daljnjem tekstu: Vlada).</p> <p>(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.).</p>	<p>Djelomično preuzet</p> <p>o</p>	<p>Bit će preuzeto u: Uredba o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga (18.06.2018)</p>
<p>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 zaštitu informacija za čije otkrivanje</p>	<p style="text-align: center;">Obveza obavješćivanja</p> <p style="text-align: center;"><i>Članak 21.</i></p> <p>(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.</p> <p>(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.</p> <p>(3) Obveza obavješćivanja iz ovog članka odnosi se na incidente na mrežnim i informacijskim sustavima iz članka 17. ovog Zakona.</p> <p style="text-align: center;">Kriteriji za određivanje učinka incidenata</p> <p style="text-align: center;"><i>Članak 22.</i></p>	<p>Djelomično preuzet</p> <p>o</p>	<p>Bit će preuzeto u: Uredba o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga (18.06.2018)</p>

<p>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.</p>	<p>(1) Kriteriji za određivanje incidenata koji imaju znatan učinak na pružanje ključnih usluga propisuju se uredbom Vlade iz članka 20. stavka 1. ovog Zakona.</p> <p>(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.</p>		
<p>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.</p>	<p style="text-align: center;"><i>Primjena</i></p> <p style="text-align: center;"><i>Članak 3.</i></p> <p>(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.</p> <p>(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.</p>	<p>U potpuno sti preuzet o</p>	
	<p style="text-align: center;">ZAŠTITA PODATAKA</p> <p style="text-align: center;"><i>Članak 40.</i></p> <p>(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.</p> <p>(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</p>	<p>U potpuno sti preuzet o</p>	

	<p>koji se provodi prema odredbama posebnog zakona o pravu na pristup informacijama.</p> <p>(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.</p> <p style="text-align: center;">Članak 41.</p> <p>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.</p>		
	<p><i>Odnos propisa prema drugim propisima</i></p> <p style="text-align: center;">Članak 4.</p> <p>(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.</p> <p>(2) 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.</p>	<p>U potpuno sti preuzet o</p>	

	<p>Vežano uz čl. 1 (1) (a) Direktive (a) utvrđuje se obveza za sve države članice da donesu nacionalnu strategiju za sigurnost mrežnih i informacijskih sustava;</p>	<p>Djelomično preuzeto</p>	<p>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.,</p>												
<p>Prilog III.</p> <p>Popis nadležnih tijela</p> <p>Jedinstvena nacionalna kontaktna točka – Ured Vijeća za nacionalnu sigurnost</p>		<p>U potpunosti preuzeto</p>													
<table border="1"> <thead> <tr> <th data-bbox="560 981 806 1093">Sektor ključnih usluga</th> <th data-bbox="806 981 1019 1093">Nadležno sektorsko tijelo</th> <th data-bbox="1019 981 1254 1093">CSIRT</th> <th data-bbox="1254 981 1500 1093">Tehničko tijelo za ocjenu sukladnosti</th> </tr> </thead> <tbody> <tr> <td data-bbox="560 1093 806 1244">Energetika</td> <td data-bbox="806 1093 1019 1244">tijelo državne uprave nadležno za energetiku</td> <td data-bbox="1019 1093 1254 1244">Zavod za sigurnost informacijskih sustava</td> <td data-bbox="1254 1093 1500 1244">Zavod za sigurnost informacijskih sustava</td> </tr> <tr> <td data-bbox="560 1244 806 1399">Prijevoz</td> <td data-bbox="806 1244 1019 1399">tijelo državne uprave nadležno za promet</td> <td data-bbox="1019 1244 1254 1399">Zavod za sigurnost informacijskih sustava</td> <td data-bbox="1254 1244 1500 1399">Zavod za sigurnost informacijskih sustava</td> </tr> </tbody> </table>	Sektor ključnih usluga	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			
Sektor ključnih usluga	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			
	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**			
	Davatelji digitalnih usluga	Nadležno sektorsko tijelo	CSIRT	Tehničko tijelo za ocjenu sukladnosti			
		tijelo državne uprave	Nacionalni CERT	Zavod za sigurnost			

		nadležno za gospodarstvo		informativskih sustava		
<p>Članak 2.</p> <p>Obrada osobnih podataka</p> <p>1. Obrada osobnih podataka na temelju ove Direktive provodi se u skladu s Direktivom 95/46/EZ.</p> <p>2. Obrada osobnih podataka koju prema ovoj Direktivi provode institucije i tijela Unije provodi se u skladu s Uredbom (EZ) br. 45/2001.</p>	<p><i>Odnos propisa prema drugim propisima</i></p> <p><i>Članak 4.</i></p> <p>(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.</p>			<p>U potpuno sti preuzet o</p>		

<p>Članak 3.</p> <p>Minimalno usklađivanje</p> <p>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.</p>		<p>Nije potrebn o preuzim anje</p>	<p>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.</p>
<p>Članak 4.</p> <p>Definicije</p> <p>Za potrebe ove Direktive primjenjuju se sljedeće definicije:</p> <p>1. „mrežni i informacijski sustav” znači:</p> <p>(a) elektronička komunikacijska mreža u smislu članka 2. točke (a) Direktive 2002/21/EZ;</p> <p>(b) bilo koji uređaj ili grupa povezanih ili srodnih uređaja, od kojih jedan ili više njih programski izvršava automatsku obradu digitalnih podataka; ili</p> <p>(c) digitalni podaci koji se pohranjuju, obrađuju, dobivaju ili prenose elementima</p>	<p style="text-align: center;">Pojmovi</p> <p style="text-align: center;">Članak 5.</p> <p>U smislu ovog Zakona pojedini pojmovi imaju sljedeće značenje:</p> <ol style="list-style-type: none"> 1) „<i>kibernetička sigurnost</i>“ – 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) „<i>kibernetički prostor</i>“ – 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) „<i>mrežni i informacijski sustav</i>“ – 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, obrađuju, dobivaju ili prenose elementima opisanim u točkama (a) i (b) u svrhu njihova rada, uporabe, zaštite i održavanja 	<p>U potpuno sti preuzet o</p>	

<p>opisanim u točkama (a) i (b) u svrhu njihova rada, uporabe, zaštite i održavanja;</p> <p>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;</p> <p>3. „nacionalna strategija za sigurnost mrežnih i informacijskih sustava” znači okvir kojim se pružaju strateški ciljevi i prioritete za sigurnost mrežnih i informacijskih sustava na nacionalnoj razini;</p> <p>4. „operator ključne usluge” znači javni ili privatni subjekt tipa navedenog u Prilogu II., koji ispunjava kriterije utvrđene u članku 5. stavku 2.;</p> <p>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.;</p>	<p>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</p> <p>5) „nacionalna strategija kibernetičke sigurnosti” – je okvir kojim se pružaju strateški ciljevi i prioritete za kibernetičku sigurnost na nacionalnoj razini</p> <p>6) „nadležna tijela” – su nadležna sektorska tijela, jedinstvena nacionalna kontaktna točka, nadležni CSIRT-ovi i tehnička tijela za ocjenu sukladnosti</p> <p>7) „operator ključnih usluga” – je bilo koji javni ili privatni subjekt koji ispunjava kriterije iz članka 6. ovog Zakona</p> <p>8) „davatelj digitalnih usluga” – je bilo koji privatni subjekt koji pruža neku digitalnu uslugu s Popisa iz Priloga II. ovog Zakona u Europskoj uniji</p> <p>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</p> <p>10) „privatni subjekti” – su fizičke i pravne osobe koje pružaju ili daju usluge,</p> <p>11) „sjedište” – je stalno mjesto poslovanja gdje pružatelj odnosno davatelj usluga u neodređenom vremenskom razdoblju upravlja svojom djelatnošću</p> <p>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</p> <p>13) „incident” – je bilo koji događaj koji ima stvaran negativni učinak na sigurnost mrežnih i informacijskih sustava</p>		
--	--	--	--

<p>6. „pružatelj digitalnih usluga” znači bilo koja pravna osoba koja pruža neku digitalnu uslugu;</p> <p>7. „incident” znači bilo koji događaj koji ima stvaran negativni učinak na sigurnost mrežnih i informacijskih sustava;</p> <p>8. „rješavanje incidenta” znači svi postupci koji podupiru otkrivanje, analizu i zaustavljanje incidenta te odgovor na njega;</p> <p>9. „rizik” znači bilo koja razumno prepoznatljiva okolnost ili događaj koji ima potencijalan negativni učinak na sigurnost mrežnih i informacijskih sustava;</p> <p>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;</p> <p>11. „norma” znači norma u smislu članka 2. točke 1. Uredbe (EU) br. 1025/2012;</p> <p>12. „specifikacija” znači tehnička specifikacija u smislu članka 2.</p>	<p>14) „rješavanje incidenta” – su svi postupci koji podupiru otkrivanje, analizu i zaustavljanje incidenta te odgovor na njega</p> <p>15) „rizik” – je bilo koja razumno prepoznatljiva okolnost ili događaj koji ima potencijalno negativni učinak na sigurnost mrežnih i informacijskih sustava</p> <p>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</p> <p>17) „sustav naziva domena (DNS)” – je hijerarhijsko raspoređeni sustav imenovanja na mreži koji odgovara na upite o nazivima domena</p> <p>18) „pružatelj DNS usluge” – je javni ili privatni subjekt koji pruža DNS usluge na Internetu</p> <p>19) „registri naziva vršnih domena” – su javni ili privatni subjekti koji upravljaju i rukuju registracijom naziva internetskih domena za određenu vršnu domenu (TLD)</p> <p>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</p> <p>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</p>			
---	--	--	--	--

<p>točke 4. Uredbe (EU) br. 1025/2012;</p> <p>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;</p> <p>14. „sustav naziva domena (DNS)” znači hijerarhijsko raspoređeni sustav imenovanja na mreži koji šalje upite o nazivima domena;</p> <p>15. „pružatelj DNS usluge” znači subjekt koji pruža DNS usluge na internetu;</p> <p>16. „registri naziva vršnih domena” znači subjekt koji upravlja i rukuje registracijom naziva internetskih domena za određenu vršnu domenu (TLD);</p> <p>17. „internetsko tržište” znači digitalna usluga koja potrošačima i/ili trgovcima, kako su utvrđeni</p>	<p>22) „<i>usluga računalstva u oblaku</i>” – je digitalna usluga kojom se pruža pristup nadogradivom i elastičnom skupu djeljivih računalnih resursa, usluga i aplikacija</p> <p>23) „<i>država članica</i>” – država članica Europske unije</p> <p>24) „<i>kvalificirani revizor</i>” – 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</p> <p>25) „<i>revizija sigurnosti mrežnih i informacijskih sustava</i>” – 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</p> <p>26) „<i>CSIRT</i>” – 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).</p>		
--	---	--	--

<p>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;</p> <p>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;</p> <p>19. „usluga računalstva u oblaku” znači digitalna usluga kojom se pruža pristup nadogradivom i elastičnom skupu djeljivih računalnih resursa.</p>			
--	--	--	--

<p>Članak 5.</p> <p>Identifikacija operatora ključnih usluga</p> <p>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.</p> <p>2. Kriteriji za identifikaciju operatora ključnih usluga iz članka 4. točke 4. jesu sljedeći:</p> <p>(a) subjekt pruža uslugu koja je ključna za održavanje ključnih društvenih i/ili ekonomskih djelatnosti;</p> <p>(b) pružanje takve usluge ovisi o mrežnim i informacijskim sustavima; i</p> <p>(c) incident bi imao znatan negativan učinak na pružanje te usluge.</p> <p>3. Za potrebe stavka 1. svaka država članica sastavlja popis usluga iz stavka 2. točke (a).</p>	<p style="text-align: center;"><i>Cilj i predmet</i></p> <p style="text-align: center;"><i>Članak 1.</i></p> <p>(3) Sastavni su dio ovog Zakona:</p> <p>a) Prilog I. - Popis ključnih usluga s kriterijima i pragovima za donošenje ocjene o važnosti negativnog učinka incidenta</p>	<p>U potpuno sti preuzet o</p>	
<p style="text-align: center;"><i>Primjena</i></p> <p style="text-align: center;"><i>Članak 3.</i></p> <p>(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.</p>	<p>U potpuno sti preuzet o</p>		
<p style="text-align: center;"><i>Određivanje operatora ključnih usluga</i></p> <p style="text-align: center;"><i>Članak 6.</i></p> <p>Pojedini javni ili privatni subjekt (u daljnjem tekstu: subjekt) odredit će se operatorom ključnih usluga ako:</p> <p>a) subjekt pruža neku od ključnih usluga s Popisa iz Priloga I. ovog Zakona (u daljnjem tekstu: ključna usluga)</p> <p>b) pružanje ključne usluge kod tog subjekta ovisi o mrežnim i informacijskim sustavima i</p> <p>c) incident bi imao znatan negativan učinak na pružanje ključne usluge.</p>	<p>U potpuno sti preuzet o</p>		

<p>4. Za potrebe stavka 1. ako subjekt pruža uslugu kako je navedeno u 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.</p> <p>5. Države članice redovito, a najmanje svake dvije godine nakon 9. svibnja 2018., preispituju i, prema potrebi, ažuriraju popis identificiranih operatora ključnih usluga.</p> <p>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.</p>	<p style="text-align: center;">Identifikacijski postupak <i>Članak 7.</i></p> <p>(1) Nadležna sektorska tijela provode postupak identifikacije operatora ključnih usluga po sektorima s Popisa iz Priloga I. ovog Zakona, u kojem:</p> <ul style="list-style-type: none"> 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. <p>(2) Nadležno sektorsko tijelo dužno je postupak identifikacije operatora ključnih usluga provoditi redovito, sukladno tržišnim promjenama u sektoru, a najmanje jednom u dvije godine.</p>	<p>U potpuno sti preuzet o</p>	
<p>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,</p>	<p style="text-align: center;">Popis operatora ključnih usluga <i>Članak 12.</i></p> <p>(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.</p> <p>(2) Nadležna sektorska tijela obavješćuju jedinstvenu nacionalnu kontaktnu točku o broju identificiranih operatora ključnih usluga u pojedinom sektoru, s naznakom njihove važnosti za sektor.</p>	<p>U potpuno sti preuzet o</p>	

<p>posebno dosljednosti u pristupu država članica pri identifikaciji operatora ključnih usluga. Ti podaci obuhvaćaju barem:</p> <p>(a) nacionalne mjere kojima se omogućuje identifikacija operatora ključnih usluga;</p> <p>(b) popis usluga iz stavka 3.;</p> <p>(c) broj operatora ključnih usluga identificiranih za svaki sektor iz Priloga II. te oznaku njihove važnosti u odnosu na taj sektor;</p> <p>(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).</p> <p>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.</p>	<p style="text-align: center;">Jedinstvena nacionalna kontaktna točka</p> <p style="text-align: center;"><i>Članak 30.</i></p> <p>Jedinstvena nacionalna kontaktna točka:</p> <ul style="list-style-type: none"> – 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 <p style="text-align: center;">Procjena ovisnosti o mrežnom i informacijskom sustavu</p> <p style="text-align: center;"><i>Članak 9.</i></p> <p>(2) Iznimno od stavka 1. ovog članka, nadležno sektorsko tijelo može donijeti 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.</p> <p>(3) Nadležno sektorsko tijelo, radi utvrđivanja kritičnosti prekograničnog učinka iz stavka 2. ovog članka, u suradnji s jedinstvenom nacionalnom kontaktnom točkom provodi savjetovanja s nadležnim tijelom uključene države članice.</p> <p style="text-align: center;">Zadaće nadležnog CSIRT-a</p> <p style="text-align: center;"><i>Članak 32.</i></p>	<p>U potpuno sti preuzet o</p>	
---	--	--	--

	<p>(1) Nadležni CSIRT na sektorskoj razini, prema popisu nadležnosti iz Priloga III. ovog Zakona, obavlja sljedeće poslove:</p> <ul style="list-style-type: none"> • u suradnji s nadležnim sektorskim tijelom, određuje prekogranične utjecaje incidenata iz članka 21. ovog Zakona 			
	<p style="text-align: center;">Članak 47.</p> <p>(1) Nadležna sektorska tijela dužna su postupak identifikacije operatora ključnih usluga provesti u roku od 90 dana od dana stupanja na snagu ovog Zakona.</p> <p>(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.</p>	<p>U potpuno sti preuzet o</p>		
<p>Članak 6.</p> <p>Znatan negativan učinak</p> <p>1. Pri utvrđivanju važnosti negativnog učinka iz točke (c) članka 5. stavka 2., države članice uzimaju u obzir barem sljedeće međusektorske čimbenike:</p> <p>(a) broj korisnika koji se oslanjaju na usluge koje taj subjekt pruža;</p>	<p style="text-align: center;"><i>Određivanje važnosti negativnog učinka incidenta</i></p> <p style="text-align: center;"><i>Članak 8.</i></p> <p>(1) Za određivanje važnosti negativnog učinka koji bi incident imao na pružanje ključne usluge uzimaju se u obzir sljedeći kriteriji:</p> <ul style="list-style-type: none"> – 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, 	<p>U potpuno sti preuzet o</p>		

<p>(b) ovisnost drugih sektora iz Priloga II. o uslugama koje dotični subjekt pruža;</p> <p>(c) mogući utjecaj incidenata, u pogledu njihova stupnja i trajanja, na gospodarske i društvene aktivnosti te na javnu sigurnost;</p> <p>(d) tržišni udio tog subjekta;</p> <p>(e) zemljopisnu raširenost u smislu područja na koje bi incident mogao utjecati;</p> <p>(f) važnost subjekta za održavanje dostatne razine usluge, uzimajući u obzir raspoloživost alternativnih sredstava za pružanje te usluge.</p> <p>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.</p>	<ul style="list-style-type: none"> – 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. <p>(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.</p> <p>(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.</p>		
<p>POGLAVLJE II.</p> <p>NACIONALNI OKVIRI ZA SIGURNOST MREŽNIH I INFORMACIJSKIH SUSTAVA</p> <p>Članak 7.</p> <p>Nacionalna strategija za sigurnost mrežnih i informacijskih sustava</p>	<p style="text-align: center;"><i>Jedinstvena nacionalna kontaktna točka</i></p> <p style="text-align: center;"><i>Članak 30.</i></p> <p>Jedinstvena nacionalna kontaktna točka:</p> <ul style="list-style-type: none"> – vodi brigu o potrebi razvoja i usklađivanja nacionalne strategije kibernetičke sigurnosti s ciljevima ovog Zakona i zahtjevima Europske unije u području kibernetičke sigurnosti 	<p>Djelomično preuzeto</p>	<p>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.</p>

<p>1. Svaka država članica donosi nacionalnu strategiju za sigurnost mrežnih i informacijskih sustava, kojom se određuju strateški ciljevi te 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:</p> <p>(a) ciljevima i prioritetima nacionalnih strategija za sigurnost mrežnih i informacijskih sustava;</p> <p>(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;</p> <p>(c) određivanjem mjera u vezi s pripravnosću, odgovorom i ponovnom uspostavom, uključujući mehanizme suradnje između javnog i privatnog sektora;</p> <p>(d) određivanjem programâ edukacije, podizanja razine svijesti i osposobljavanja</p>		<p>NACIONALNE STRATEGIJE KIBERNETIČKE 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</p>
--	--	---

<p>povezanih sa strategijom sigurnosti mrežnih i informacijskih sustava;</p> <p>(e)određivanjem istraživačkih i razvojnih planova u pogledu strategije za sigurnost mrežnih i informacijskih sustava;</p> <p>(f)planom za procjenu rizika s ciljem prepoznavanja rizika;</p> <p>(g)popisom različitih sudionika u provedbi nacionalne strategije za sigurnost mrežnih i informacijskih sustava.</p> <p>2. Države članice mogu zatražiti podršku ENISA-e u razvijanju nacionalnih strategija za sigurnost mrežnih i informacijskih sustava.</p> <p>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.</p>		<p>POGLAVLJE 1. AKCIJSKOG PLANA ZA PROVEDBU NACIONALNE 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.</p>
---	--	---

	<p style="text-align: center;"><i>Članak 31.</i></p> <p>Jedinstvena nacionalna kontaktna točka je Ured Vijeća za nacionalnu sigurnost.</p>	<p>Djelomično preuzeto</p>	<p>Preuzeto u: Odluka o osnivanju Nacionalnog vijeća za kibernetičku sigurnost i Operativno-tehničke koordinacije za kibernetičku sigurnost (NN 61/16) članak/članci II.</p> <p>Zadaće Nacionalnog vijeća su:</p> <ul style="list-style-type: none"> – 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,

		<ul style="list-style-type: none"> – 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. <p>IV. Članovi Nacionalnog vijeća su:</p> <ul style="list-style-type: none"> – predstavnik Ureda Vijeća za nacionalnu sigurnost, predsjednik
--	--	---

		<ul style="list-style-type: none"> – 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
--	--	---

			<p>– predstavnik Hrvatske narodne banke, član</p> <p>– predstavnik Agencije za zaštitu osobnih podataka, član.</p>
<p>Članak 8.</p> <p>Nacionalna nadležna tijela i jedinstvene kontaktne točke</p> <p>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.</p> <p>2. Nadležna tijela nadgledaju primjenu ove Direktive na nacionalnoj razini.</p> <p>3. Svaka država određuje nacionalnu jedinstvenu kontaktnu točku za sigurnost mrežnih i informacijskih sustava („jedinствена kontaktna točka”). Države članice mogu tu ulogu dodijeliti postojećem</p>	<p><i>Cilj i predmet</i></p> <p><i>Članak 1.</i></p> <p>(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 (u daljnjem 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.</p> <p>(3) Sastavni su dio ovog Zakona:</p> <p>c) Prilog III. - Popis nadležnih tijela.</p>	U potpuno sti preuzet o	
	<p><i>Nadležna sektorska tijela</i></p> <p><i>Članak 25.</i></p> <p>(1) Nadležna sektorska tijela utvrđena su Popisom iz Priloga III. ovog Zakona.</p> <p>(2) Nadležna sektorska tijela obavljaju sljedeće poslove:</p> <p>– provode postupke identifikacije operatora ključnih usluga sukladno ovome Zakonu</p>	U potpuno sti preuzet o	

<p>tijelu. Ako država članica odredi samo jedno nadležno tijelo, to nadležno tijelo također je i jedinstvena kontaktna točka.</p> <p>4. Jedinstvena kontaktna točka izvršava funkciju povezivanja s ciljem osiguravanja prekogranične suradnje tijela države članice s relevantnim tijelima u drugim državama članicama te sa skupinom za suradnju iz članka 11. i mrežom CSIRT-ova iz članka 12.</p> <p>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.</p>	<ul style="list-style-type: none"> – 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. 		
<p>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.</p>	<p style="text-align: center;"><i>Jedinstvena nacionalna kontaktna točka</i></p> <p style="text-align: center;"><i>Članak 30.</i></p> <p>Jedinstvena nacionalna kontaktna točka:</p> <ul style="list-style-type: none"> – 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. 	<p>U potpuno sti preuzet o</p>	

<p>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. Komisija objavljuje popis određenih jedinstvenih kontaktnih točaka.</p>	<p>stavkom 1. točkama 8., 10. i 11. ovog Zakona, osim za sektor poslovnih usluga za središnja državna tijela</p> <ul style="list-style-type: none"> – 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 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. <p style="text-align: center;"><i>Članak 31.</i></p> <p>Jedinstvena nacionalna kontaktna točka je Ured Vijeća za nacionalnu sigurnost.</p>										
	<p style="text-align: center;">Prilog III.</p> <p style="text-align: center;">Popis nadležnih tijela</p> <p style="text-align: center;">Jedinstvena nacionalna kontaktna točka – Ured Vijeća za nacionalnu sigurnost</p> <table border="1" data-bbox="593 1212 1489 1404"> <thead> <tr> <th data-bbox="593 1212 817 1332">Sektor ključnih usluga</th> <th data-bbox="817 1212 1030 1332">Nadležno sektorsko tijelo</th> <th data-bbox="1030 1212 1265 1332">CSIRT</th> <th data-bbox="1265 1212 1489 1332">Tehničko tijelo za ocjenu sukladnosti</th> </tr> </thead> <tbody> <tr> <td data-bbox="593 1332 817 1404">Energetika</td> <td data-bbox="817 1332 1030 1404">tijelo državne uprave</td> <td data-bbox="1030 1332 1265 1404">Zavod za sigurnost</td> <td data-bbox="1265 1332 1489 1404">Zavod za sigurnost</td> </tr> </tbody> </table>	Sektor ključnih usluga	Nadležno sektorsko tijelo	CSIRT	Tehničko tijelo za ocjenu sukladnosti	Energetika	tijelo državne uprave	Zavod za sigurnost	Zavod za sigurnost	<p>U potpuno sti preuzet o</p>	
Sektor ključnih usluga	Nadležno sektorsko tijelo	CSIRT	Tehničko tijelo za ocjenu sukladnosti								
Energetika	tijelo državne uprave	Zavod za sigurnost	Zavod za sigurnost								

		nadležno za energetiku	informatijskih sustava	informatijskih sustava			
	Prijevoz	tijelo državne uprave nadležno za promet	Zavod za sigurnost informatijskih sustava	Zavod za sigurnost informatijskih 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 informatijskih sustava	Zavod za sigurnost informatijskih sustava			
	Opskrba vodom za piće i njezina distribucija	tijelo državne uprave nadležno za vodno gospodarstvo	Zavod za sigurnost informatijskih sustava	Zavod za sigurnost informatijskih sustava			
	Digitalna infrastruktura	Središnji državni ured za razvoj digitalnog društva	Nacionalni CERT	Hrvatska akademska i istraživačka mreža – CARNet			
	Poslovne usluge za središnja državna tijela	Središnji državni ured za razvoj digitalnog društva	Zavod za sigurnost informatijskih sustava ili Nacionalni CERT*	Zavod za sigurnost informatijskih sustava ili Nacionalni CERT**			

	<table border="1" data-bbox="582 191 1500 462"> <tr> <th data-bbox="582 191 784 311">Davatelji digitalnih usluga</th> <th data-bbox="784 191 1019 311">Nadležno sektorsko tijelo</th> <th data-bbox="1019 191 1243 311">CSIRT</th> <th data-bbox="1243 191 1500 311">Tehničko tijelo za ocjenu sukladnosti</th> </tr> <tr> <td data-bbox="582 311 784 462"></td> <td data-bbox="784 311 1019 462">tijelo državne uprave nadležno za gospodarstvo</td> <td data-bbox="1019 311 1243 462">Nacionalni CERT</td> <td data-bbox="1243 311 1500 462">Zavod za sigurnost informacijskih sustava</td> </tr> </table> <p data-bbox="582 502 1500 726">*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.</p> <p data-bbox="582 726 1500 989">**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.</p>	Davatelji digitalnih usluga	Nadležno sektorsko tijelo	CSIRT	Tehničko tijelo za ocjenu sukladnosti		tijelo državne uprave nadležno za gospodarstvo	Nacionalni CERT	Zavod za sigurnost informacijskih sustava		
Davatelji digitalnih usluga	Nadležno sektorsko tijelo	CSIRT	Tehničko tijelo za ocjenu sukladnosti								
	tijelo državne uprave nadležno za gospodarstvo	Nacionalni CERT	Zavod za sigurnost informacijskih sustava								
<p data-bbox="78 1029 224 1069">Članak 9.</p> <p data-bbox="78 1101 537 1181">Timovi za odgovor na računalne sigurnosne incidente (CSIRT-ovi)</p> <p data-bbox="78 1204 548 1356">1. Svaka država članica imenuje jedan ili više CSIRT-ova koji udovoljavaju zahtjevima iz točke 1. Priloga I. i koji obuhvaćaju barem</p>	<p data-bbox="952 1029 1142 1069"><i>Cilj i predmet</i></p> <p data-bbox="974 1085 1120 1125"><i>Članak 1.</i></p> <p data-bbox="582 1149 1500 1364">(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 (u daljnjem tekstu: nadležni CSIRT) i tehničkog tijela za ocjenu sukladnosti, nadzor nad operatorima ključnih</p>	<p data-bbox="1523 1029 1635 1212">U potpunosti preuzet o</p>									

<p>sektore iz Priloga II. i usluge iz Priloga III., odgovornih za rješavanje rizika i incidenata u skladu s točno propisanim postupkom. CSIRT se može osnovati unutar nadležnog tijela.</p> <p>2. Države članice imenovanim CSIRT-ovima osiguravaju odgovarajuće resurse za učinkovito izvršavanje zadaća iz Priloga I. točke 2.</p> <p>Države članice osiguravaju učinkovitu, djelotvornu i sigurnu suradnju svojih CSIRT-ova u mreži CSIRT-ova iz članka 12.</p> <p>3. Države članice osiguravaju da CSIRT-ovi imaju pristup prikladnoj, sigurnoj i otpornoj infrastrukturi za komunikaciju i informiranje na nacionalnoj razini.</p> <p>4. Države članice obavješćuju Komisiju o mandatu i glavnim elementima postupka za rješavanje incidenata svojih CSIRT-ova.</p> <p>5. Države članice mogu zatražiti podršku ENISA-e u razvijanju nacionalnih CSIRT-ova.</p>	<p>usluga i davateljima digitalnih usluga u provedbi ovog Zakona i prekršajne odredbe.</p> <p>(3) Sastavni su dio ovog Zakona:</p> <p>c) Prilog III. - Popis nadležnih tijela.</p>			
	<p style="text-align: center;">Zadaci nadležnog CSIRT-a</p> <p style="text-align: center;">Članak 32.</p> <p>(1) Nadležni CSIRT na sektorskoj razini, prema popisu nadležnosti iz Priloga III. ovog Zakona, obavlja sljedeće poslove:</p> <ul style="list-style-type: none"> – 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 	<p>U potpuno sti preuzet o</p>		

	<p>obavijesti, a osobito informacije koje bi mogle doprinijeti djelotvornom rješavanju incidenta</p> <ul style="list-style-type: none"> - 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 		
--	--	--	--

	<ul style="list-style-type: none"> – 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. <p>(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.</p> <p>(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.</p>			
	<p style="text-align: center;"><i>Osiguravanje uvjeta za obavljanje poslova nadležnog CSIRT-a</i></p> <p style="text-align: center;"><i>Članak 33.</i></p> <p>Nadležni CSIRT je dužan:</p> <ul style="list-style-type: none"> – 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 	<p>U potpuno sti preuzet o</p>		

- 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.

Prilog III.

Popis nadležnih tijela

Jedinstvena nacionalna kontaktna točka – Ured Vijeća za nacionalnu sigurnost

Sektor ključnih usluga	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

U potpuno
sti preuzet
o

	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			
	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**			
	Davatelji digitalnih usluga	Nadležno sektorsko tijelo	CSIRT	Tehničko tijelo za ocjenu sukladnosti			
		tijelo državne uprave	Nacionalni CERT	Zavod za sigurnost			

		nadležno za gospodarstvo		informativskih sustava		
<p>Članak 10.</p> <p>Suradnja na nacionalnoj razini</p> <p>1. Ako su odvojeni, nadležno tijelo, jedinstvena kontaktna točka i CSIRT-ovi iste države članice surađuju u pogledu ispunjavanja obveza propisanih u ovoj Direktivi.</p> <p>2. Države članice osiguravaju da bilo nadležna tijela ili CSIRT-ovi primaju obavijesti o incidentima podnesene u skladu s ovom</p>	<p style="text-align: center;"><i>Nadležna sektorska tijela</i></p> <p style="text-align: center;"><i>Članak 25.</i></p> <p>(2) Nadležna sektorska tijela obavljaju sljedeće poslove:</p> <ul style="list-style-type: none"> – surađuju i razmjenjuju relevantne informacije s drugim nadležnim tijelima iz ovog Zakona <p style="text-align: center;"><i>Jedinstvena nacionalna kontaktna točka</i></p> <p style="text-align: center;"><i>Članak 30.</i></p> <p>Jedinstvena nacionalna kontaktna točka:</p> <ul style="list-style-type: none"> – surađuje s drugim nadležnim tijelima iz ovog Zakona, 				<p>U potpuno sti preuzet o</p>	

<p>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 pružatelji digitalnih usluga, u skladu s člankom 16. stavcima 3. i 6.</p> <p>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.</p>	<p style="text-align: center;">Obveza obavješćivanja <i>Članak 21.</i></p> <p>(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.</p> <p>(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.</p> <p>(3) Obveza obavješćivanja iz ovog članka odnosi se na incidente na mrežnim i informacijskim sustavima iz članka 17. ovog Zakona.</p>	<p>U potpuno sti preuzet o</p>		
<p>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.</p>	<p style="text-align: center;">Zadace nadležnog CSIRT-a <i>Članak 32.</i></p> <p>(1) Nadležni CSIRT na sektorskoj razini, prema popisu nadležnosti iz Priloga III. ovog Zakona, obavlja sljedeće poslove:</p> <ul style="list-style-type: none"> – 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 	<p>U potpuno sti preuzet o</p>		

	<p>– dostavlja jedinstvenoj nacionalnoj kontaktnoj točki podatke o glavnim elementima postupaka rješavanja incidenata koje provodi,</p>		
	<p style="text-align: center;"><i>Jedinstvena nacionalna kontaktna točka</i></p> <p style="text-align: center;"><i>Članak 30.</i></p> <p>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 poslovnih usluga za središnja državna tijela</p>	<p>U potpuno sti preuzet o</p>	
<p>POGLAVLJE III.</p> <p>SURADNJA</p> <p>Članak 11.</p> <p>Skupina za suradnju</p> <p>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</p>		<p>Nije potrebn o preuzim anje</p>	<p>U pitanju obveze koje su provedene na razini nadležnih EU institucija. Predstavnic RH već sudjeluju u radu Skupine za suradnju, dok je predmetnim Nacrtom zakona isto uključeno kroz zadaće jedinstvene nacionalne kontaktne točke.</p>

<p>sustava u Uniji, uspostavlja se skupina za suradnju.</p> <p>Skupina za suradnju izvršava svoje zadaće na temelju dvogodišnjih programa rada iz stavka 3. drugog podstavka.</p> <p>2. Skupina za suradnju sastoji se od predstavnika država članica, Komisije i ENISA-e.</p> <p>Skupina za suradnju može, prema potrebi, pozvati predstavnike relevantnih zainteresiranih strana da sudjeluju u njezinu radu.</p> <p>Komisija osigurava tajništvo.</p> <p>3. Zadaće su skupine za suradnju:</p> <p>(a) pružanje strateških smjernica za aktivnosti mreže CSIRT-ova osnovane prema članku 12.;</p> <p>(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.;</p> <p>(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;</p>			
--	--	--	--

<p>(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;</p> <p>(e)razmjena informacija i najbolje prakse u pogledu podizanja svijesti i osposobljavanja;</p> <p>(f)razmjena informacija i najbolje prakse u pogledu istraživanja i razvoja u vezi sa sigurnošću mrežnih i informacijskih sustava;</p> <p>(g)prema potrebi, razmjena iskustava o pitanjima povezanim sa sigurnošću mrežnih i informacijskih sustava u relevantnim institucijama, tijelima, uredima i agencijama Unije;</p> <p>(h)rasprava o normama i specifikacijama iz članka 19. s predstavnicima relevantnih europskih organizacija za normizaciju;</p> <p>(i)prikupljanje informacija o najboljoj praksi u pogledu rizika i incidenata;</p> <p>(j)provjera, na godišnjoj osnovi, sažetih izvješća iz članka 10. stavka 3. drugog podstavka;</p>			
---	--	--	--

- (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

<p>aranžmani potrebni za funkcioniranje skupine za suradnju. Ti se provedbeni akti donose u skladu s postupkom ispitivanja iz članka 22. stavka 2.</p> <p>Za potrebe prvog podstavka Komisija dostavlja prvi nacrt provedbenog akta odboru iz članka 22. stavka 1. do 9. veljače 2017.</p>			
<p>Članak 12.</p> <p>Mreža CSIRT-ova</p> <p>1. S ciljem doprinosa razvoju povjerenja i pouzdanja među državama članicama te promicanju brze i učinkovite operativne suradnje osniva se mreža nacionalnih CSIRT-ova.</p> <p>2. Mreža CSIRT-ova sastoji se od predstavnika 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.</p> <p>3. Zadaće su mreže CSIRT-ova:</p> <p>(a)razmjena informacija o uslugama CSIRT-ova te njihovim</p>		<p>Nije potrebno preuzimanje</p>	<p>U pitanju obveze koje se provode na razini nadležnih EU institucija. Predstavnicima RH već sudjeluju u radu Mreže CSIRT-ova, dok je predmetnim Nacrtom zakona isto uključeno kroz definirane zadatke nadležnih CSIRT-ova.</p>

<p>aktivnostima i sposobnostima za suradnju;</p> <p>(b) na zahtjev predstavnika CSIRT-a iz države članice na koju bi 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;</p> <p>(c) razmjena i stavljanje na raspolaganje na dobrovoljnoj osnovi informacija o pojedinačnim incidentima koje nisu povjerljive;</p> <p>(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;</p> <p>(e) pružanje podrške državam članicama u rješavanju prekograničnih incidenata na temelju dobrovoljne uzajamne pomoći;</p> <p>(f) rasprava o daljnjim oblicima operativne suradnje te njihovo</p>			
--	--	--	--

<p>istraživanje i utvrđivanje, među ostalim u odnosu na:</p> <p>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;</p> <p>(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;</p> <p>(h) rasprava o poukama stečenima u vježbama koje se odnose na sigurnost mrežnih i informacijskih sustava, među ostalim i onima koje organizira ENISA;</p> <p>(i) na zahtjev pojedinačnog CSIRT-a, rasprava o sposobnostima i pripravnosti tog CSIRT-a;</p> <p>(j) izdavanje smjernica radi olakšavanja konvergencije operativnih praksi s ciljem primjene odredaba ovoga članka u pogledu operativne suradnje.</p> <p>4. Za potrebe preispitivanja iz članka 23. i najkasnije 9. kolovoza 2018., a nakon toga svakih godinu i pol, mreža CSIRT-ova priprema</p>			
--	--	--	--

<p>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.</p> <p>5. Mreža CSIRT-ova utvrđuje vlastiti poslovnik.</p>			
<p>Članak 13.</p> <p>Međunarodna suradnja</p> <p>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.</p>		<p>Nije potrebn o preuzim anje</p>	<p>Odredba se odnosi na nadležne EU institucije.</p>
<p>POGLAVLJE IV.</p> <p>SIGURNOST MREŽNIH I INFORMACIJSKIH SUSTAVA OPERATORA KLJUČNIH USLUGA</p>	<p style="text-align: center;">Obveza provedbe mjera</p> <p style="text-align: center;"><i>Članak 14.</i></p> <p>(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.</p> <p>(2) Mjere iz stavka 1. ovog članka sastoje se minimalno od:</p>	<p>U potpuno sti preuzet o</p>	

<p>Članak 14.</p> <p>Sigurnosni zahtjevi i obavješćivanje o incidentima</p> <p>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.</p> <p>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</p>	<ul style="list-style-type: none"> – 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. 		
	<p style="text-align: center;">Mjere za upravljanje rizikom operatora ključnih usluga</p> <p style="text-align: center;"><i>Članak 15.</i></p> <p>Operatori ključnih usluga dužni su poduzimati tehničke i organizacijske mjere za upravljanje rizicima koje moraju obuhvatiti mjere za:</p> <ul style="list-style-type: none"> – utvrđivanje rizika od incidenata – sprječavanje, otkrivanje i rješavanje incidenata i – ublažavanje učinka incidenata na najmanju moguću mjeru. 	<p>U potpuno sti preuzet o</p>	
	<p style="text-align: center;">Opseg primjene mjera</p> <p style="text-align: center;"><i>Članak 17.</i></p> <p>(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.</p>	<p>U potpuno sti preuzet o</p>	

<p>usluga s ciljem osiguravanja kontinuiteta tih usluga.</p>	<p align="center">Primjena mjera prema procjeni rizika</p>	<p>U</p>	
<p>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.</p>	<p align="center"><i>Članak 18.</i></p> <p>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.</p>	<p>potpuno sti preuzet o</p>	
<p>4. Kako bi se odredila važnost učinka nekog incidenta, osobito se uzimaju u obzir sljedeći parametri:</p> <p>(a) broj korisnika pogođenih prekidom osnovnih usluga; (b) trajanje incidenta; (c) zemljopisna raširenost u smislu područja na koje bi incident mogao utjecati.</p>	<p align="center">Odgovornost za primjenu mjera</p> <p align="center"><i>Članak 19.</i></p> <p>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.</p>	<p>U potpuno sti preuzet o</p>	
<p>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</p>	<p align="center">Utvrđivanje mjera</p> <p align="center"><i>Članak 20.</i></p> <p>(1) Mjere za postizanje visoke razine kibernetičke sigurnosti operatora ključnih usluga i način njihove provedbe pobliže se propisuju uredbom koju donosi Vlada Republike Hrvatske (u daljnjem tekstu: Vlada).</p>	<p>Djelomi čno preuzet o</p>	<p>Bit će preuzeto u: Uredba o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga (18.06.2018)</p>
<p>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</p>	<p align="center">Obveza obavješćivanja</p> <p align="center"><i>Članak 21.</i></p> <p>(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.</p> <p>(2) Ako je incident na mrežnom i informacijskom sustavu davatelja digitalne usluge imao znatan učinak na pružanje neke ključne usluge,</p>	<p>U potpuno sti preuzet o</p>	

<p>kontinuitet ključnih usluga u toj državi članici. Pritom nadležno tijelo ili CSIRT, u skladu s pravom Unije 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.</p>	<p>operator ključne usluge dužan je o tom incidentu obavijestiti nadležni CSIRT.</p> <p>(3) Obveza obavješćivanja iz ovog članka odnosi se na incidente na mrežnim i informacijskim sustavima iz članka 17. ovog Zakona.</p>		
<p>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.</p>	<p style="text-align: center;">Kriteriji za određivanje učinka incidenata</p> <p style="text-align: center;"><i>Članak 22.</i></p> <p>(1) Kriteriji za određivanje incidenata koji imaju znatan učinak na pružanje ključnih usluga propisuju se uredbom Vlade iz članka 20. stavka 1. ovog Zakona.</p>	<p>Djelomično preuzet</p>	<p>Bit će preuzeto u: Uredba o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga (18.06.2018)</p>
<p>Na zahtjev nadležnog tijela ili CSIRT-a jedinstvena kontaktna točka obavijesti iz prvog podstavka prosljeđuje jedinstvenim kontaktnim točkama drugih pogođenih država članica.</p>	<p style="text-align: center;">Obavijesti o incidentima</p> <p style="text-align: center;"><i>Članak 23.</i></p> <p>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.</p>	<p>Djelomično preuzet</p>	<p>Bit će preuzeto u: Uredba o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga (18.06.2018)</p>
<p>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</p>	<p style="text-align: center;">Zadace nadležnog CSIRT-a</p> <p style="text-align: center;"><i>Članak 32.</i></p> <p>(1) Nadležni CSIRT na sektorskoj razini, prema popisu nadležnosti iz Priloga III. ovog Zakona, obavlja sljedeće poslove:</p> <ul style="list-style-type: none"> – ako to dopuštaju okolnosti, nakon primitka obavijesti o incidentu dostavlja operatoru ključnih usluga relevantne 	<p>U potpunosti preuzet</p>	

<p>sprečavanje incidenta ili rješavanje incidenta koji je u tijeku.</p> <p>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.</p>	<p>informacije u pogledu daljnjeg postupanja po njegovoj obavijesti, a osobito informacije koje bi mogle doprinijeti djelotvornom rješavanju incidenta</p> <ul style="list-style-type: none"> – 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, 			
--	---	--	--	--

	<p style="text-align: center;"><i>Jedinstvena nacionalna kontaktna točka</i></p> <p style="text-align: center;"><i>Članak 30.</i></p> <p>Jedinstvena nacionalna kontaktna točka:</p> <ul style="list-style-type: none"> – na zahtjev nadležnog CSIRT-a, obavijesti o incidentima iz članka 21. ovog Zakona prosljeđuje jedinstvenim nacionalnim kontaktnim točkama drugih pogodjenih država članica, osim za sektor poslovnih usluga za središnja državna tijela 	<p>U potpuno sti preuzet o</p>	
	<p style="text-align: center;"><i>Informiranje javnosti o incidentu</i></p> <p style="text-align: center;"><i>Članak 24.</i></p> <p>(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.</p>	<p>U potpuno sti preuzet o</p>	
	<p style="text-align: center;"><i>Članak 41.</i></p> <p>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.</p>	<p>U potpuno sti preuzet o</p>	

<p>Članak 15.</p> <p>Provedba i izvršavanje</p> <p>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.</p> <p>2. Države članice osiguravaju da nadležno tijelo ima ovlasti i sredstva da od operatora ključnih uloga zatraži dostavu:</p>	<p style="text-align: center;"><i>Nadležna sektorska tijela</i></p> <p style="text-align: center;"><i>Članak 25.</i></p> <p>(2) Nadležna sektorska tijela obavljaju sljedeće poslove:</p> <ul style="list-style-type: none"> – 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. 	<p>U potpuno sti preuzet o</p>	
<p>(a)informacija potrebnih za procjenu sigurnosti njihovih mrežnih i informacijskih sustava, među ostalim dokumentirane sigurnosne politike;</p> <p>(b)dokaza o učinkovitoj provedbi sigurnosnih politika, primjerice rezultata revizije sigurnosti koju su obavili nadležno tijelo ili kvalificirani revizor te, u slučaju da je obavljala kvalificirani revizor,</p>	<p style="text-align: center;"><i>Nadzor</i></p> <p style="text-align: center;"><i>Članak 26.</i></p> <p>(1) Nadzor nad operatorom ključnih usluga provodi se jednom svake dvije godine.</p> <p>(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.</p>	<p>U potpuno sti preuzet o</p>	

<p>stavljanje tih rezultata, zajedno s dokazima na kojima se temelje, na raspolaganje nadležnom tijelu.</p> <p>Prilikom traženja takvih informacija ili dokaza nadležno tijelo navodi svrhu zahtjeva i određuje koje su informacije potrebne.</p> <p>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.</p> <p>4. Nadležna tijela blisko surađuju s tijelima za zaštitu podataka u rješavanju incidenata koji za posljedicu imaju ugrožavanja osobnih podataka.</p>	<p>Obveze operatora ključnih usluga i davatelja digitalnih usluga u okviru nadzora</p> <p><i>Članak 27.</i></p> <p>(1) Operatori ključnih usluga i davatelji digitalnih usluga dužni su u okviru nadzora nadležnom sektorskom tijelu, na njegov zahtjev, dostaviti:</p> <ul style="list-style-type: none"> – podatke potrebne za procjenu razine sigurnosti njihovih mrežnih i informacijskih sustava, uključujući dokumentirane sigurnosne politike i – dokaze o učinkovitoj provedbi sigurnosnih mjera. <p>(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.</p> <p>(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.</p> <p>(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.</p> <p>(5) Nadležno sektorsko tijelo nadzor davatelja digitalne usluge, koji ima sjedište ili svog predstavnika u Republici Hrvatskoj, a čiji se mrežni i informacijski sustavi nalaze u drugoj ili više država članica, može provoditi u suradnji s nadležnim tijelima tih država članica.</p>	<p>U potpuno sti preuzet o</p>	
--	--	--	--

	<p style="text-align: center;"><i>Predmet nadzora</i></p> <p style="text-align: center;"><i>Članak 28.</i></p> <p>(1) U okviru nadzora, nadležna sektorska tijela nadziru pravilnost provedbe propisanih:</p> <ul style="list-style-type: none"> – 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. <p>(2) U provedbi nadzora, nadležna sektorska tijela:</p> <ul style="list-style-type: none"> – izdaju obvezujuću uputu operatoru ključnih usluga kada utvrde da on: <ul style="list-style-type: none"> 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. <p>(3) Nadležna sektorska tijela dužna su u aktima iz stavka 2. podstavka 1. i 2. ovog članka naznačiti rok za postupanje.</p>	<p>U potpuno sti preuzet o</p>	
--	--	--	--

	<p style="text-align: center;">Obavljanje nadzora</p> <p style="text-align: center;"><i>Članak 29.</i></p> <p>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.</p>	<p>U potpuno sti preuzet o</p>	
<p>POGLAVLJE V.</p> <p>SIGURNOST MREŽNIH I INFORMACIJSKIH SUSTAVA PRUŽATELJA DIGITALNIH USLUGA</p> <p>Članak 16.</p> <p>Sigurnosni zahtjevi i obavješćivanje o incidentima</p> <p>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</p>	<p style="text-align: center;">Obveza provedbe mjera</p> <p style="text-align: center;"><i>Članak 14.</i></p> <p>(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.</p> <p>(2) Mjere iz stavka 1. ovog članka sastoje se minimalno od:</p> <ul style="list-style-type: none"> – 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. 	<p>U potpuno sti preuzet o</p>	
	<p style="text-align: center;">Mjere za upravljanje rizikom davatelja digitalnih usluga</p> <p style="text-align: center;"><i>Članak 16.</i></p> <p>Davatelji digitalnih usluga dužni su prilikom poduzimanja tehničkih i organizacijskih mjera za upravljanje rizicima voditi računa osobito o:</p> <ul style="list-style-type: none"> – sigurnosti sustava i objekata – rješavanju incidenata – upravljanju kontinuitetom poslovanja – praćenju, reviziji i testiranju 	<p>U potpuno sti preuzet o</p>	

<p>vođenje računa o sljedećim elementima:</p> <p>(a) sigurnosti sustava i objekata; (b) rješavanju incidenata; (c) upravljanju kontinuitetom poslovanja; (d) praćenju, reviziji i testiranju; (e) sukladnosti s međunarodnim standardima.</p> <p>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.</p> <p>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</p>	<p>– sukladnosti s međunarodnim standardima.</p>			
	<p style="text-align: center;">Pojmovi</p> <p style="text-align: center;">Članak 5.</p> <p>U smislu ovog Zakona pojedini pojmovi imaju sljedeće značenje:</p> <p>1) „<i>davatelj digitalnih usluga</i>”- je bilo koji privatni subjekt koji pruža neku digitalnu uslugu s Popisa iz Priloga II. ovog Zakona u Europskoj uniji</p> <p style="text-align: center;">Prilog II.</p> <p style="text-align: center;">Popis digitalnih usluga</p> <p>1. Internetsko tržište</p> <p>2. Internetska tražilica</p> <p>3. Usluge računalstva u oblaku</p>	<p>U potpuno sti preuzet o</p>		

<p>Unije. Obavijesti sadržavaju informacije s pomoću kojih nadležno tijelo ili CSIRT mogu odrediti važnost svakog prekograničnog učinka. Strana koja šalje obavijest ne podliježe zbog toga povećanoj odgovornosti.</p> <p>4. Radi utvrđivanja je li učinak incidenta znatan, u obzir se osobito uzimaju sljedeći parametri:</p> <p>(a) broj korisnika na koje incident utječe, osobito ako je riječ o korisnicima koji se na te usluge oslanjaju za pružanje vlastitih usluga;</p> <p>(b) trajanje incidenta;</p> <p>(c) zemljopisna raširenost u smislu područja na koje bi incident mogao utjecati;</p> <p>(d) opseg poremećaja u funkcioniranju usluge;</p> <p>(e) opseg utjecaja na gospodarsko i društveno djelovanje.</p>	<p style="text-align: center;">Obveza obavješćivanja</p> <p style="text-align: center;"><i>Članak 21.</i></p> <p>(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.</p> <p>(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.</p> <p>(3) Obveza obavješćivanja iz ovog članka odnosi se na incidente na mrežnim i informacijskim sustavima iz članka 17. ovog Zakona.</p>	<p>U potpuno sti preuzet o</p>	
	<p style="text-align: center;">Obavijesti o incidentima</p> <p style="text-align: center;"><i>Članak 23.</i></p> <p>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.</p>	<p>Djelomično preuzet o</p>	<p>Bit će preuzeto u: Uredba o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga (18.06.2018)</p>
<p>Obveza obavješćivanja o incidentu primjenjuje se samo ako pružatelj digitalnih usluga ima pristup informacijama potrebnima za procjenu učinka incidenta spram kriterija iz prvog podstavka.</p> <p>5. Ako se operator ključnih usluga oslanja na trećeg pružatelja</p>	<p style="text-align: center;">Kriteriji za određivanje učinka incidenata</p> <p style="text-align: center;"><i>Članak 22.</i></p> <p>(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.</p>	<p>Nije potrebno preuzimanje</p>	<p>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</p>

<p>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.</p>			<p>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.)</p>
<p>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.</p> <p>7. Nakon savjetovanja s dotičnim pružateljem digitalnih usluga, nadležno tijelo ili CSIRT te, prema potrebi, tijela ili CSIRT-ovi drugih pogođenih država članica, mogu 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</p>	<p style="text-align: center;">Zadaci nadležnog CSIRT-a</p> <p style="text-align: center;"><i>Članak 32.</i></p> <p>(1) Nadležni CSIRT na sektorskoj razini, prema popisu nadležnosti iz Priloga III. ovog Zakona, obavlja sljedeće poslove:</p> <ul style="list-style-type: none"> – 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 	<p>U potpunosti preuzeto</p>	

<p>incidenta koji je u tijeku ili ako je objavljivanje incidenta zbog nekog drugog razloga u javnome interesu.</p> <p>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.</p>	<p style="text-align: center;">Jedinstvena nacionalna kontaktna točka</p> <p style="text-align: center;"><i>Članak 30.</i></p> <p>Jedinstvena nacionalna kontaktna točka:</p> <ul style="list-style-type: none"> – na zahtjev nadležnog CSIRT-a, obavijesti o incidentima iz članka 21. ovog Zakona prosljeđuje jedinstvenim kontaktnim točkama drugih pogodjenih država članica, osim za sektor poslovnih usluga za središnja državna tijela 	<p>U potpuno sti preuzet o</p>	
<p>9. Komisija može donijeti provedbene akte kojima se utvrđuju oblici i postupci primjenjivi na zahtjeve za obavješćivanje. Ti se provedbeni akti donose u skladu s postupkom ispitivanja iz članka 22. stavka 2.</p>	<p style="text-align: center;">Informiranje javnosti o incidentu</p> <p style="text-align: center;"><i>Članak 24.</i></p> <p>(2) Nadležni CSIRT te, prema potrebi, CSIRT-ovi drugih pogodjenih 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.</p>	<p>U potpuno sti preuzet o</p>	
<p>10. Ne dovodeći u pitanje članak 1. stavak 6., države članice ne nameću nikakve dodatne sigurnosne zahtjeve ni zahtjeve za obavješćivanje pružateljima digitalnih usluga.</p> <p>11. Poglavlje V. ne primjenjuje se na mikropoduzeća i mala poduzeća</p>	<p style="text-align: center;"><i>Članak 41.</i></p> <p>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.</p>	<p>U potpuno sti preuzet o</p>	

<p>kako su definirana u Preporuci Komisije 2003/361/EZ (19).</p>	<p style="text-align: center;">Primjena</p> <p style="text-align: center;"><i>Članak 3.</i></p> <p>(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.</p>	<p>U potpuno sti preuzet o</p>	
<p>Članak 17.</p> <p>Provedba i izvršavanje</p> <p>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.</p> <p>2. Za potrebe stavka 1. nadležna tijela imaju potrebne ovlasti i sredstva da mogu od pružatelja digitalnih usluga tražiti:</p> <p>(a) dostavu informacija potrebnih za procjenu sigurnosti njihovih mrežnih i informacijskih sustava,</p>	<p style="text-align: center;">Nadležna sektorska tijela</p> <p style="text-align: center;"><i>Članak 25.</i></p> <p>(2) Nadležna sektorska tijela obavljaju sljedeće poslove:</p> <ul style="list-style-type: none"> – 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. 	<p>U potpuno sti preuzet o</p>	

<p>među ostalim dokumentirane sigurnosne politike;</p> <p>(b)otklanjanje svakog nepoštovanja zahtjeva utvrđenih u članku 16.</p> <p>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.</p>	<p style="text-align: center;">Nadzor</p> <p style="text-align: center;"><i>Članak 26.</i></p> <p>(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 postupuje sukladno Provedbenoj uredbi Komisije iz članka 20. stavka 2. ovog Zakona i/ili odredbama ovog Zakona.</p>	<p>U potpuno sti preuzet o</p>	
	<p style="text-align: center;">Obveze operatora ključnih usluga i davatelja digitalnih usluga u okviru nadzora</p> <p style="text-align: center;"><i>Članak 27.</i></p> <p>(1) Operatori ključnih usluga i davatelji digitalnih usluga dužni su u okviru nadzora nadležnom sektorskom tijelu, na njegov zahtjev, dostaviti:</p> <ul style="list-style-type: none"> – podatke potrebne za procjenu razine sigurnosti njihovih mrežnih i informacijskih sustava, uključujući dokumentirane sigurnosne politike i – dokaze o učinkovitoj provedbi sigurnosnih mjera. <p>(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.</p> <p>(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.</p> <p>(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.</p>	<p>U potpuno sti preuzet o</p>	

	<p>(5) Nadležno sektorsko tijelo nadzor davatelja digitalne usluge, koji ima sjedište ili svog predstavnika u Republici Hrvatskoj, a čiji se mrežni i informacijski sustavi nalaze u drugoj ili više država članica, može provoditi u suradnji s nadležnim tijelima tih država članica.</p>			
	<p style="text-align: center;"><i>Predmet nadzora</i></p> <p style="text-align: center;"><i>Članak 28.</i></p> <p>(1) U okviru nadzora, nadležna sektorska tijela nadziru pravilnost provedbe propisanih:</p> <ul style="list-style-type: none"> – 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. <p>(2) U provedbi nadzora, nadležna sektorska tijela:</p> <ul style="list-style-type: none"> – 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. <p>(3) Nadležna sektorska tijela dužna su u aktima iz stavka 2. podstavka 1. i 2. ovog članka naznačiti rok za postupanje.</p>	<p>U potpuno sti preuzet o</p>		

<p>Članak 18.</p> <p>Nadležnost i teritorijalnost</p> <p>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.</p>	<p><i>Primjena</i></p> <p><i>Članak 3.</i></p> <p>(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.</p>	<p>U potpuno sti preuzet o</p>	
<p>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.</p> <p>3. Imenovanje predstavnika od strane pružatelja digitalnih usluga ne dovodi u pitanje pravne postupke</p>	<p><i>Pojmovi</i></p> <p><i>Članak 5.</i></p> <p>U smislu ovog Zakona pojedini pojmovi imaju sljedeće značenje:</p> <p>8) „<i>davatelj digitalnih usluga</i>” - je bilo koji privatni subjekt koji pruža neku digitalnu uslugu s Popisa iz Priloga II. ovog Zakona u Europskoj uniji</p> <p>12) „<i>predstavnik</i>“ – 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</p>	<p>U potpuno sti preuzet o</p>	

<p>koji bi se mogli pokrenuti protiv samog pružatelja digitalnih usluga.</p>	<p style="text-align: center;">Prilog II. Popis digitalnih usluga</p> <p>1. Internetsko tržište 2. Internetska tražilica 3. Usluge računalstva u oblaku</p>	<p>U potpuno sti preuzet o</p>	
<p>POGLAVLJE VI.</p> <p>NORMIZACIJA I OBAVJEŠĆIVANJE NA DOBROVOLJNOJ OSNOVI</p> <p>Članak 19.</p> <p>Normizacija</p> <p>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.</p> <p>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</p>		<p>Nije preuzet o</p>	<p>Bit će preuzeto u: Uredba o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga (18.06.2018)</p>

<p>postojeće norme, uključujući nacionalne norme država članica, kojima bi se ta područja mogla obuhvatiti.</p>			
<p>Članak 20.</p> <p>Obavješćivanje na dobrovoljnoj osnovi</p> <p>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.</p> <p>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.</p>		<p>Nije preuzet o</p>	<p>Bit će preuzeto u: Uredba o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga (18.06.2018)</p>

<p>Subjektu koji je obavijest podnio dobrovoljno ne nameću se zbog tog obavješćivanja nikakve obveze kojima ne bi podlijegao da nije podnio tu obavijest.</p>			
<p>POGLAVLJE VII.</p> <p>ZAVRŠNE ODREDBE</p> <p>Članak 21.</p> <p>Sankcije</p> <p>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.</p>	<p style="text-align: center;">PREKRŠAJNE ODREDBE</p> <p style="text-align: center;">Članak 42.</p> <p>(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:</p> <ul style="list-style-type: none"> – 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. <p>(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.</p> <p>(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.</p> <p style="text-align: center;">Članak 43.</p> <p>(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:</p>	<p>U potpuno sti preuzet o</p>	

	<ul style="list-style-type: none"> - 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. <p>(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.</p> <p>(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.</p> <p style="text-align: center;">Članak 44.</p> <p>(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:</p> <ul style="list-style-type: none"> - 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. <p>(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.</p> <p>(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.</p>		
--	---	--	--

	<p style="text-align: center;">Članak 45.</p> <p>(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:</p> <ul style="list-style-type: none"> – 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. <p>(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.</p> <p>(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.</p>		
<p>Članak 22.</p> <p>Postupak odbora</p> <p>1. Komisiji pomaže Odbor za sigurnost mrežnih i informacijskih sustava. Navedeni odbor je odbor u smislu Uredbe (EU) br. 182/2011.</p> <p>2. Pri upućivanju na ovaj stavak primjenjuje se članak 5. Uredbe (EU) br. 182/2011.</p>		<p>Nije potrebna o preuzimanje</p>	<p>U pitanju odredba Direktive koja se provodi na razini nadležnih EU institucija.</p>

<p>Članak 23.</p> <p>Preispitivanje</p> <p>1. Do 9. svibnja 2019. Komisija podnosi Europskom parlamentu i Vijeću izvješće s procjenom dosljednosti u pristupu država članica pri identifikaciji operatora ključnih usluga.</p> <p>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 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</p>		<p>Nije potrebno preuzimanje</p>	<p>U pitanju odredba Direktive koja se provodi od strane nadležnih EU institucija.</p>

<p>izvješće dostavlja do 9. svibnja 2021.</p>			
<p>Članak 24.</p> <p>Prijelazne mjere</p> <p>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 zadatke utvrđene u članku 11. stavku 3. odnosno članku 12. stavku 3. najkasnije do 9. veljače 2017.</p> <p>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</p>	<p style="text-align: center;">Jedinstvena nacionalna kontaktna točka</p> <p style="text-align: center;">Članak 30.</p> <p>Jedinstvena nacionalna kontaktna točka:</p> <ul style="list-style-type: none"> – 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, 	<p>U potpuno sti preuzet o</p>	
	<p style="text-align: center;">Zadaci nadležnog CSIRT-a</p> <p style="text-align: center;">Članak 32.</p> <p>(1) Nadležni CSIRT na sektorskoj razini, prema popisu nadležnosti iz Priloga III. ovog Zakona, obavlja sljedeće poslove:</p> <ul style="list-style-type: none"> – 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 	<p>U potpuno sti preuzet o</p>	

<p>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.</p> <p>3. Do 9. veljače 2017., a za potrebe ovog članka države članice osiguravaju odgovarajuću zastupljenost u skupini za suradnju i mreži CSIRT-ova.</p>			
<p>Članak 25.</p> <p>Prenošenje</p> <p>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.</p> <p>One primjenjuju te mjere od 10. svibnja 2018.</p>	<p style="text-align: center;"><i>Usklađenost s propisima Europske unije</i></p> <p style="text-align: center;"><i>Članak 2.</i></p> <p>Ovim Zakonom se u hrvatsko zakonodavstvo preuzima 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.).</p>	<p>Djelomično preuzet o</p>	<p>Bit će preuzeto u: Uredba o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga (18.06.2018)</p>

<p>Kada države članice donose te mjere, one sadržavaju upućivanje na ovu Direktivu ili se na nju upućuje prilikom njihove službene objave. Načine tog upućivanja određuju države članice.</p> <p>2. Države članice Komisiji dostavljaju tekst glavnih odredaba nacionalnog prava koje donesu u području na koje se odnosi ova Direktiva.</p>	<p style="text-align: center;">Utvrđivanje mjera</p> <p style="text-align: center;">Članak 20.</p> <p>(1) Mjere za postizanje visoke razine kibernetičke sigurnosti operatora ključnih usluga i način njihove provedbe pobliže se propisuju uredbom koju donosi Vlada Republike Hrvatske (u daljnjem tekstu: Vlada).</p> <p>(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.).</p>	<p>Djelomično preuzet o</p>	<p>Bit će preuzeto u: Uredba o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga (18.06.2018)</p>
	<p style="text-align: center;">Kriteriji za određivanje učinka incidenata</p> <p style="text-align: center;">Članak 22.</p> <p>(1) Kriteriji za određivanje incidenata koji imaju znatan učinak na pružanje ključnih usluga propisuju se uredbom Vlade iz članka 20. stavka 1. ovog Zakona.</p> <p>(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.</p>	<p>Djelomično preuzet o</p>	<p>Bit će preuzeto u: Uredba o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga (18.06.2018)</p>

	<p style="text-align: center;"><i>Obavijesti o incidentima</i></p> <p style="text-align: center;"><i>Članak 23.</i></p> <p>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.</p>	Djelomično preuzeto	Bit će preuzeto u: Uredba o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga (18.06.2018)
	<p style="text-align: center;"><i>Članak 46.</i></p> <p>Vlada će Uredbu iz članka 20. stavka 1. ovog Zakona donijeti u roku od 30 dana od dana stupanja na snagu ovog Zakona.</p>	Djelomično preuzeto	Bit će preuzeto u: Uredba o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga (18.06.2018)
<p>Članak 26.</p> <p>Stupanje na snagu</p> <p>Ova Direktiva stupa na snagu dvadesetog dana od dana objave u Službenom listu Europske unije.</p>		Nije potrebno preuzimanje	U pitanju odredba Direktive koja utvrđuje njezino stupanja na snagu.
<p>Članak 27.</p> <p>Adresati</p> <p>Ova je Direktiva upućena državama članicama.</p>		Nije potrebno preuzimanje	U pitanju odredba Direktive koja utvrđuje adresate na koje se Direktiva odnosi.

<p>PRILOG I.</p> <p>ZAHTJEVI U POGLEDU TIMOVA ZA ODGOVOR NA RAČUNALNE SIGURNOSNE INCIDENTE (CSIRT-ovi) I NJIHOVE ZADAĆE</p> <p>Zahtjevi u pogledu CSIRT-ova i njihove zadaće propisno su i jasno definirani i poduprti nacionalnom politikom i/ili zakonodavstvom. Oni obuhvaćaju sljedeće:</p> <p>1. Zahtjevi u pogledu CSIRT-ova:</p> <p>(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.</p> <p>(b) Prostori CSIRT-ova i informacijski sustavi za potporu smješteni su na sigurnim lokacijama.</p> <p>(c) Kontinuitet rada:</p>	<p style="text-align: center;"><i>Zadaće nadležnog CSIRT-a</i></p> <p style="text-align: center;"><i>Članak 32.</i></p> <p>(1) Nadležni CSIRT na sektorskoj razini, prema popisu nadležnosti iz Priloga III. ovog Zakona, obavlja sljedeće poslove:</p> <ul style="list-style-type: none"> – 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 	<p>U potpuno sti preuzet o</p>	
---	---	--------------------------------	--

<p>i. CSIRT-ovi su opremljeni odgovarajućim sustavom za upravljanje zahtjevima i njihovim preusmjeravanjem, kako bi se olakšale primopredaje.</p> <p>ii. CSIRT-ovi imaju dovoljno zaposlenika kako bi se osigurala dostupnost u svako doba.</p> <p>iii. CSIRT-ovi se oslanjaju na infrastrukturu čiji je kontinuitet osiguran. U tu svrhu dostupni su redundantni sustavi i rezervni radni prostor.</p> <p>(d) CSIRT-ovi imaju mogućnost da, ako to žele, sudjeluju u međunarodnim mrežama za suradnju.</p> <p>2. Zadaće CSIRT-ova:</p> <p>(a) Zadaće CSIRT-ova obuhvaćaju barem:</p> <p>i. praćenje incidenata na nacionalnoj razini;</p> <p>ii. pružanje ranih upozorenja i najava te informiranje relevantnih dionika o rizicima i incidentima;</p> <p>iii. odgovaranje na incidente;</p>	<ul style="list-style-type: none"> – 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. 		
--	---	--	--

<p>iv.pružanje dinamičke analize rizika i incidenata te pregleda situacije;</p> <p>v.sudjelovanje u mreži CSIRT-ova.</p> <p>(b)CSIRT-ovi uspostavljaju suradnju s privatnim sektorom.</p> <p>(c)CSIRT-ovi s ciljem olakšavanja suradnje promiču usvajanje i primjenu zajedničkih ili normiranih praksi za:</p>	<p>(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.</p> <p>(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.</p>			
<p>i.postupke rješavanja incidenata i rizika;</p> <p>ii.planove za klasifikaciju incidenata, rizika i informacija.</p>	<p style="text-align: center;"><i>Osiguravanje uvjeta za obavljanje poslova nadležnog CSIRT-a</i></p> <p style="text-align: center;"><i>Članak 33.</i></p> <p>Nadležni CSIRT je dužan:</p> <ul style="list-style-type: none"> – 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: <ul style="list-style-type: none"> 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 	<p>U potpuno sti preuzet o</p>		

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

PRILOG II.
VRSTE SUBJEKATA ZA
POTREBE ČLANKA 4. TOČKE 4.

Sektor Podsekto Vrsta subjekta
r
I Energeti (aelektri —elektroenerget
. ka) čna sko poduzeće
energij kako je
a definirano u
članku 2. točki
35.
Direktive 2009
/72/EZ
Europskog
parlamenta i
Vijeća (1),
koje obavlja
funkciju
„opskrbe”
kako je
definirana u
članku 2. točki
19. te
Direktive

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
potpuno
sti
preuzet
o

Prilog I.

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

Sektor	Podsekto tor	Ključna usluga	Kriteriji za utvrđivanje važnosti negativnog učinka incidenta	Pragovi za utvrđivanje važnosti negativnog učinka incidenta
Energeti ka	Elektri čna energij a	Proizvodnj a električne energije	Instalirana snaga proizvodnog postrojenja	300 MW

U
potpuno
sti
preuzet
o

<p>—operatori distribucijskog sustava kako su definirani u članku 2. točki 6. Direktive 2009/72/EZ</p> <p>—operatori prijenosnog sustava kako su definirani u članku 2. točki 4. Direktive 2009/72/EZ</p> <p>(b) nafta —operatori naftovoda</p> <p>—operatori proizvodnje nafte, rafinerija i tvornicâ nafte te njezina skladištenja i prijenosa</p> <p>(c) plin —poduzeća za opskrbu kako su definirana člankom 2. točkom 8. Direktive 2009/73/EZ Europskog</p>			<p>Prijenos električne energije</p>	Bez iznimke	-			
			<p>Distribucija električne energije</p>	Prekid napajanja	Više od 100.000 obračunskih mjernih mjesta			

<p>parlamenta i Vijeća (2)</p> <p>—operatori distribucijskog sustava kako su definirani u članku 2. točki 6. Direktive 2009 /73/EZ</p> <p>—operatori transportnog sustava kako su definirani u članku 2. točki 4. Direktive 2009 /73/EZ</p> <p>—operatori sustava skladišta plina kako su definirani u članku 2. točki 10. Direktive 2009 /73/EZ</p> <p>—operatori terminala za UPP kako su definirani u članku 2. točki 12.</p>				<p>Ovisnosti drugih djelatnosti ili područja o pružanju usluge</p>	<p>Distribucija za:</p> <p>§ bolnice</p> <p>§ zračne luke i kontrole leta</p> <p>§ objekte banaka s podatkovnim centrima</p> <p>§ policijske uprave</p> <p>§ aktivne vojne objekte</p> <p>§ aktivna vodocrpilišta i centre upravljanja</p> <p>§ objekte operatora telekomunik acijskog sustava</p> <p>§ objekte tijela sigurnosno- obavještajno g sustava,</p> <p>§ objekte profesionalni h vatrogasnih postrojbi,</p> <p>§ objekte Državne uprave za zaštitu i spašavanje</p>		
--	--	--	--	--	--	--	--

<p>Direktive 2009/73/EZ</p> <p>—poduzeća za prirodni plin kako su definirana u članku 2. točki 1. Direktive 2009/73/EZ</p> <p>—operatori postrojenja za rafiniranje i obradu prirodnog plina</p> <p>2. Prijevoz (a zračni promet)</p> <p>—zračni prijevoznici kako su definirani u članku 3. točki 4. Uredbe (EZ) br. 300/2008 Europskog parlamenta i Vijeća (3)</p> <p>—upravno tijelo zračne luke kako je definirano u članku 2. točki 2. Direktive</p>				(Služba 112) ili § objekte određene nacionalnom kritičnom infrastrukturom		
	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		

<p>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 usluge kontrole</p>			Skladištenje naftne i naftnih derivata	Ukupni skladišni kapacitet naftne pojednog terminala u m ³	1.000.000 m ³							
				Ukupni skladišni kapacitet naftnih derivata pojednog skladišta (na istoj lokaciji) u m ³	60.000 m ³							
		Plin						Broj krajnjih kupaca priklučen 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
								Prihvati otprema UPP-a	Kapacitet uplinjavanja UPP u m ³ /h			Više od 500.000 m ³ /h

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

(c vodni) prijevoz putnika unutarnjim plovnicima, morem i duž obale te kompanije za prijevoz tereta unutarnjim plovnicima, 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 upravljaju te kompanije	su definirani u članku 3. točki 12. Direktive 2012/34/EU —kompanije za prijevoz putnika unutarnjim plovnicima, morem i duž obale te kompanije za prijevoz tereta unutarnjim plovnicima, 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 upravljaju te kompanije			Upravljanje infrastrukturom zračne luke, uključujući i 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

<p>—upravljачka 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</p> <p>—služba za nadzor i upravljanje pomorskim prometom kako je definirana u članku 3. točki (o) Direktive</p>		Željeznički promet	<p>Upravljanje i održavanje željezničke infrastrukture, uključujući i upravljanje prometom i prometno-upravljačkim i signalno-sigurnosnim podsustavom</p>	Upravitelj željezničke infrastrukture za javni prijevoz – bez iznimke				
			<p>Usluge prijevoza robe i/ili putnika željeznicom</p>	Broj voznih jedinica (vlakova)	20 dnevno			

<p>(d cestov —) ni prijev oz</p> <p>2002/59/EZ Europskog parlamenta i Vijeća (10) —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)</p> <p>3 Bankarst . vo kreditne institucije kako su definirane člankom 4.</p>			Upravljanje e 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 željeznico m	Broj voznih jedinica (vlakova)	20 dnevno		
		Vodni prijevo z	Nadzor kretanja brodova (VTS usluga)	Godišnji broj dolazaka brodova iz međunarodn e plovidbe	najmanje 4.000		

4 Infrastruktura financijskog tržišta	točkom 1. Uredbe (EU) br. 575/2013 Europskog parlamenta i Vijeća (13) —operatori mjesta 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 pružatelja zdravstvene zaštite kako su							

6 Opskrba vodom za piće i njezina distribucija	zaštite definirani u (uključuj članku 3. točki ući (g) Direktive bolnice i 2011/24/EU privatne Europskog klinike) parlamenta i Vijeća (16) 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 ključnim uslugama — IXP-ovi		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	Broj korisnika	15% ukupno prevezenih putnika i/ili vozila godišnje		

<p>7 Digitalna infrastruktura</p> <p>—pružatelj DNS usluga —registri naziva TLD-ova</p>			<p>unutarnji morskim vodama i teritorijalnom moru Republike Hrvatske koji se obavlja na unaprijed utvrđenim linijama prema javno objavljenim uvjetima reda plovidbe i cjenikom usluga</p>	<p>Tržišni udio</p>	<p>Minimalno 15% tržišnog udjela</p>			
<p>(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.).</p> <p>(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.).</p> <p>(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.).</p> <p>(4) Direktiva 2009/12/EZ Europskog parlamenta i Vijeća od 11. ožujka 2009. o naknadama</p>			<p>Praćenje i lociranje plovila u unutarnjoj plovidbi</p>	<p>Broj plovila na unutarnjim plovnim putovima u Republici Hrvatskoj tijekom godine</p>	<p>100</p>			

<p>zračnih luka (SL L 70, 14.3.2009., str. 11.).</p> <p>(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.).</p> <p>(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.).</p> <p>(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.).</p> <p>(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.).</p> <p>(9) Direktiva 2005/65/EZ Europskog parlamenta i Vijeća od 26. listopada 2005. o jačanju</p>			<p>Obavijesti brodarstvu u unutarnjoj plovidbi</p>	<p>Broj izdanih obavijesti brodarstvu tijekom godine</p>	<p>100</p>		
			<p>Pristup elektroničkim navigacijskim kartama u unutarnjoj plovidbi</p>	<p>Pokrivenost unutarnjih vodnih putova u Republici Hrvatskoj</p>	<p>Pokrivenost 500 riječnih km</p>		
			<p>Baza podataka o trupu plovila u unutarnjoj plovidbi</p>	<p>Broj plovila unesenih u bazu podataka tijekom godine</p>	<p>50</p>		
			<p>Međunarodno elektroničko izvješćavanje u unutarnjoj plovidbi</p>	<p>Broj ERI poruka upućenih prema RIS centrima dnevno</p>	<p>50</p>		
		<p>Cestovni</p>		<p>Broj voznih jedinica</p>	<p>100</p>		

<p>sigurnosne zaštite luka (SL L 310, 25.11.2005, str. 28.).</p> <p>(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.).</p> <p>(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.).</p> <p>(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.).</p> <p>(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</p>	<p>prijevoz</p>	<p>Javni prijevoz putnika</p>	<p>Broj putnika godišnje</p>	<p>5.000.000</p>					
		<p>Korištenje cestovne infrastrukture</p>	<p>Upravitelj ceste na TEN-T mreži – bez iznimke</p>	<p>-</p>					<p>20.000 PGDP (prosječni godišnji dnevni promet)</p>
			<p>Broj vozila na glavnoj cesti koja vodi do središta naseljenog mjesta većeg od 35.000 stanovnika</p>	<p>20.000 PGDP (prosječni godišnji dnevni promet)</p>					
			<p>Zemljopisna raširenost korištenja usluga</p>	<p>Teritorij cijele države ili grada većeg od 35.000 stanovnika</p>					
		<p>Upravljanje prometnim tokovima ili informiran</p>	<p>Uspostavljen centar za kontrolu i upravljanje prometom 24/7 – bez iznimke</p>						

<p>Uredbe (EU) br. 648/2012 (SL L 176, 27.6.2013., str. 1.).</p> <p>(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.).</p> <p>(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.).</p> <p>(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.).</p> <p>(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.).</p>			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	Sistemske važne kreditne institucije – bez iznimke	-		
Infrastruktura financijski			Usluge mjesta trgovanja	Bez iznimke	-			

	kog tržišta		Usluge središnjih drugih ugovornih strana (CCP)	Bez iznimke	-			
	Zdravstv eni sektor		Primarna zdravstven a zaštita – informativ ski sustav	Broj propisanih recepta za lijevakove godišnje	50.000.000			
Broj posjeta ordinacijama opće obiteljske medicine godišnje				35.000.000				
Pokrivenost ustanova primarne zdravstvene zaštite pojedini 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	-		

				Broj sigurnosno-tehničkih listova pregledanih i uvrštenih u registar sigurnosno-tehničkih listova (STL) godišnje	9.000			
			Zaštita od opasnih kemikalija	Broj opasnih kemikalija prikupljenih i uvrštenih u registar opasnih kemikalija proizvedenih ili uvezenih/unešenih 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 distribucijski h centara	330.000		
				Broj distribucijski h centara na broj veledrogerija	3		
			Cijepljenje i zarazne bolesti	Obuhvat primovakcin acijom 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 članica	Veći od 15		
		Usluge u sustavima državne informacijske infrastrukture	Usluge u sustavu e-Građani	Broj 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	<i>Cilj i predmet</i> <i>Članak 1.</i> (3) Sastavni su dio ovog Zakona: b) Prilog II. - Popis digitalnih usluga					U potpuno sti preuzet o	

3. Usluge računalstva u oblaku	<p style="text-align: center;">Prilog II.</p> <p style="text-align: center;">Popis digitalnih usluga</p> <p>1. Internetsko tržište</p> <p>2. Internetska tražilica</p> <p>3. Usluge računalstva u oblaku</p>	U potpuno sti preuzet o		
--------------------------------	--	-------------------------------------	--	--