P.Z.E. br. 236

HRVATSKI SABOR

KLASA: 022-03/21-01/153
URBROJ: 65-21-02

Zagreb, 2. prosinca 2021.

ZASTUPNICAMA I ZASTUPNICIMA
HRVATSKOGA SABORA

PREDSJEDNICAMA I PREDSJEDNICIMA
RADNIH TIJELA

Na temelju članka 178. Poslovnika Hrvatskoga sabora u prilogu upućujem ***Prijedlog zakona o provedbi Uredbe (EU) 2019/881 Europskog parlamenta i Vijeća od 17. travnja 2019. (Zakon o provedbi kibernetičke sigurnosne certifikacije)***, koji je predsjedniku Hrvatskoga sabora podnijela Vlada Republike Hrvatske, aktom od 2. prosinca 2021. 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 državnog tajnika Središnjeg državnog ureda za razvoj digitalnog društva Bernarda Gršića i zamjenicu državnog tajnika Središnjeg državnog ureda za razvoj digitalnog društva Kristinu Posavec.

PREDSJEDNIK

Gordan Jandroković

VLADA REPUBLIKE HRVATSKE

KLASA: 022-03/21-01/55
URBROJ: 50301-21/21-21-9

Zagreb, 2. prosinca 2021.

PREDSJEDNIKU HRVATSKOGA SABORA

PREDMET: Prijedlog zakona o provedbi Uredbe (EU) 2019/881 Europskog parlamenta i Vijeća od 17. travnja 2019. (Zakon o provedbi kibernetičke sigurnosne certifikacije)

Na temelju članka 85. Ustava Republike Hrvatske („Narodne novine“, br. 85/10. - pročišćeni tekst i 5/14. - Odluka Ustavnog suda Republike Hrvatske) i članka 172. Poslovnika Hrvatskoga sabora („Narodne novine“, br. 81/13., 113/16., 69/17., 29/18., 53/20. i 119/20. - Odluka Ustavnog suda Republike Hrvatske), Vlada Republike Hrvatske podnosi Prijedlog zakona o provedbi Uredbe (EU) 2019/881 Europskog parlamenta i Vijeća od 17. travnja 2019. (Zakon o provedbi kibernetičke sigurnosne certifikacije).

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 državnog tajnika Središnjeg državnog ureda za razvoj digitalnog društva Bernarda Gršića i zamjenicu državnog tajnika Središnjeg državnog ureda za razvoj digitalnog društva Kristinu Posavec.

REPUBLIKA HRVATSKA 3 VLADA REPUBLIKE HRVATSKE ZAGREB

PREDSJEDNIK

mr. sc. Andrej Plenković

VLADA REPUBLIKE HRVATSKE

PRIJEDLOG ZAKONA
O PROVEDBI UREDBE (EU) 2019/881
EUROPSKOG PARLAMENTA I VIJEĆA OD 17. TRAVNJA 2019.
(ZAKON O PROVEDBI KIBERNETIČKE SIGURNOSNE CERTIFIKACIJE)

Zagreb, prosinac 2021.

PRIJEDLOG ZAKONA
O PROVEDBI UREDBE (EU) 2019/881
EUROPSKOG PARLAMENTA I VIJEĆA OD 17. TRAVNJA 2019.
(ZAKON O PROVEDBI KIBERNETIČKE SIGURNOSNE CERTIFIKACIJE)

I. USTAVNA OSNOVA ZA DONOŠENJE ZAKONA

Ustavna osnova za donošenje Zakona o provedbi Uredbe (EU) 2019/881 Europskog parlamenta i Vijeća od 17. travnja 2019. (Zakon o provedbi kibernetičke sigurnosne certifikacije. u daljnjem tekstu: Zakon) sadržana je u odredbi članka 2. stavka 4. podstavka 1., a u vezi s člankom 37. stavkom 2. Ustava Republike Hrvatske („Narodne novine“, br. 85/10. – pročišćeni tekst i 5/14. – Odluka Ustavnog suda Republike Hrvatske).

II. OCJENA STANJA I OSNOVNA PITANJA KOJA SE TREBAJU UREDITI ZAKONOM TE POSLJEDICE KOJE ĆE DONOŠENJEM ZAKONA PROISTEĆI

a) Europska unija poduzela je niz mjera kako bi uredila odnose u kibernetičkom prostoru, povećavajući pri tome otpornost i pojačavajući svoju kibernetičku sigurnosnu pripravnost. Od prve strategije EU-a za kibernetičku sigurnost, koja je donesena 2013., u kojoj su utvrđeni strateški ciljevi i konkretne mjere za postizanje otpornosti, smanjenje kibernetičkog kriminaliteta, razvoj politike kibernetičke obrane i sposobnosti za kibernetičku obranu, razvoj industrijskih i tehnoloških resursa i uspostavu usklađene međunarodne politike kibernetičkog prostora za EU, do prijedloga najnovije iz 2020., u kojoj su dodatno naglašena tri područja: (1) otpornost, tehnološka suverenost i vodstvo; (2) izgradnja operativnih kapaciteta u svrhu sprječavanja, odvraćanja i uzvraćanja; (3) razvijanje globalnog i otvorenog kibernetičkog prostora, stalno se naglašava potreba za reguliranjem digitalne transformacije društva na način da čovjek uvijek ostane u središtu zbivanja odnosno subjekt i u kibernetičkom prostoru, pri čemu je razvidan značaj sigurnosnih parametara za izgradnju povjerenja prema tim procesima.

   U cilju povećanja povjerenja i sigurnosti na Jedinstvenom digitalnom tržištu Unije (JDT) te s obzirom na brzo širenje povezanih uređaja (internet stvari), bilo je potrebno uspostaviti okvir za sigurnosno certificiranje proizvoda, usluga i procesa informacijsko komunikacijske tehnologije (IKT) odnosno svih objekata kibernetičkog prostora. Kibernetičko sigurnosno certificiranje postaje posebno važno s obzirom na sve veću uporabu kibernetičkih tehnologija za namjene koje zahtijevaju visok stupanj pouzdanosti i sigurnosti te je u sve većem broju sektora primjetno povećanje ovisnosti o IKT proizvodima, uslugama i procesima, osobito u prometu (automatizirano upravljanje), u sustavima održavanja života i zdravlja (e-zdravstvo), u industriji (kontrolni sustavi za industrijsku automatizaciju – IACS) te u ostvarivanju ljudskih interesa i prava (e-građani).

   Direktiva o sigurnosti mrežnih i informacijskih sustava[1] (EU NIS Direktiva), transponirana Zakonom o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga („Narodne novine“, broj 64/18.) je regulirala razvrstavanje usluga odnosno objekata kibernetičkog prostora po njihovom značaju (ključne i digitalne usluge) te uspostavila sustav otpornosti (štićenje, izvješćivanje i interveniranje), specifično za najvažnije sektore. Slijednim propisom koji se na EU NIS Direktivu i naslanja, Uredbom o Agenciji Europske unije za kibernetičku sigurnost (ENISA) i o kibernetičkoj

[1] *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*

sigurnosnoj certifikaciji u području komunikacijske i informacijske tehnologije („Akt o kibernetičkoj sigurnosti“) 2019/881 od 17. travnja 2019. (u daljnjem tekstu: Uredba (EU) 2019/881) dovršena je druga faza uređivanja kibernetičkog prostora iz aspekta objekata tog prostora. Uredbom je ENISA dobila aktivniju i važniju ulogu u postizanju kibernetičke otpornosti Unije te je postala stožerno tijelo u mreži agencija država članica koje se bave kibernetičkom sigurnošću na sličan način. Glavni regulator na razini Europske unije je Europska komisija koja, uz operativnu pomoć ENISA-e i savjetodavnu pomoć Europske skupine za kibernetičku sigurnosnu certifikaciju (European Cybersecurity Certification Group, ECCG), osigurava provođenje odredbi oba ova zakona, a sukladno proklamiranim strategijama i planskim dokumentima.

b) Osnovna pitanja koja se trebaju urediti ovim Zakonom, odnosno jedan od ciljeva koji se misli postići sustavom kibernetičke sigurnosne certifikacije je jačanje Jedinstvenog digitalnog tržišta EU, kako bi ono postalo značajniji čimbenik na globalnoj sceni i postalo otpornije na disruptivna djelovanja konkurentskih globalnih gospodarstava. Time se olakšava postizanje i jednog od strateških ciljeva Unije – digitalne suverenosti, odnosno mogućnosti slobodnog i samostalnog odlučivanja o svim stvarima u svezi s kibernetičkim prostorom. Posljedično navedenom, države članice EU su preuzele obvezu harmoniziranja svojih propisa i djelovanja na ovom području, te izgradnje ili prilagodbe nacionalnih sustava kibernetičke sigurnosne certifikacije zajedničkom. Očekuje se da sve „nacionalne komponente“ u dogledno vrijeme postanu „komponente na nacionalnoj razini“ dobro uvezanog i otpornog europskog sustava kibernetičke sigurnosne certifikacije. Da bi to zaista skladno funkcioniralo, bilo je potrebno odrediti načela i pravila izgradnje takvih sustava, što se Uredbom (EU) 2019/881 nastojalo i napraviti, a od država članica se očekuje provedba. Definirane su uloge raznih tijela, njihovi pravni statusi i načini asociranja, kako bi se postigla ujednačenost komponenata na razini Unije i na kraju izbjeglo štetno fragmentiranje praksi i procedura.

Prvi korak na nacionalnoj, hrvatskoj, razini jest uspostava okvira odnosno strukture koja se može uvezati na onu zajedničku od Unije te koja može ostvarivati programe na predviđeni način, prvenstveno s ciljem izgradnje domaćeg tržišta, skladno povezanog s ostalima u jedinstvenom digitalnom tržištu i provoditi njegovu regulaciju u skladu s načelima Unije, a prilagođenu domaćim okolnostima i zakonskoj praksi. Općenito, poslovi kontrole kvalitete odnosno provjere dostizanja nekog standarda koji rezultiraju nekom svjedodžbom, atestom ili certifikatom čine oko 10 % digitalnog tržišta s tendencijom rasta proporcionalnom naglašenoj brizi za sigurnost i kompleksnošću novih tehnologija. Objektivno, za hrvatsko digitalno gospodarstvo ova je diversifikacija dobrodošla te se očekuje rast u ovoj niši uz minimalne intervencije i poticaje, jer će omogućiti domaćim digitalnim poduzetnicima dostizanje poslovne i stručne razine jednake najboljima u Uniji za vrlo kratko vrijeme. Razmatrajući prevladavajuće procjene koje govore da u digitalnom gospodarstvu „nove članice“ EU odnosno one iz područja srednje i istočne Europe, zaostaju 3-4 godine i da se taj procijep ne smanjuje, uspostava sustava kibernetičke sigurnosne certifikacije obećava brisanje takve razlike barem u toj niši.

Važećim propisima u Republici Hrvatskoj nisu predviđene obveze koje bi bile kompatibilne sa zahtjevima Uredbe (EU) 2019/881, pa je izrađen ovaj Prijedlog zakona, kojim se namjerava na jedinstveni način propisati potrebno radi osiguranja provedbe Uredbe (EU) 2019/881.

Kibernetičkom sigurnosnom certifikacijom potvrđuje se da su IKT proizvodi, usluge i procesi evaluirani u skladu s europskim shemama kibernetičke sigurnosne certifikacije te da ispunjavaju utvrđene sigurnosne zahtjeve za potrebe zaštite dostupnosti, izvornosti, cjelovitosti i povjerljivosti pohranjenih, poslanih ili obrađenih podataka, funkcija ili usluga koje se nude s pomoću tih proizvoda, usluga i procesa ili kojima se s pomoću njih

može pristupiti tijekom njihova životnog ciklusa. Na temelju pojedinih europskih shema kibernetičke sigurnosne certifikacije provodi se kibernetička sigurnosna certifikacija koja predstavlja postupak izdavanja europskih kibernetičkih sigurnosnih certifikata odnosno izjava o sukladnosti za proizvođače ili pružatelje IKT proizvoda, usluga i procesa u svrhu postizanja visoke zajedničke razine kibernetičke sigurnosti diljem Europske unije za određene IKT proizvode, usluge i procese.

c) Ovim Prijedlogom zakona osigurava se provedba Uredbe (EU) 2019/881, osiguravaju se potrebne pretpostavke za trajno unaprjeđenje stanja europske kibernetičke sigurnosne certifikacije u sve širem opsegu društvenih i gospodarskih sektora njome obuhvaćenih uslijed digitalne transformacije i razvoja interneta stvari, ali se istodobno potiče i razvoj Republike Hrvatske u području digitalnog gospodarstva usklađenim pristupom između niza dionika iz javnog i privatnog sektora, imajući u vidu da u Republici Hrvatskoj izdani europski certifikat vrijedi na cijelom području jedinstvenog digitalnog tržišta Unije. Time se otvaraju mogućnosti za učinkovitiji zajednički pristup i združenom djelovanju državnog, akademskog i gospodarskog sektora, prvenstveno u razvoju novih hrvatskih proizvoda, procesa i usluga informacijsko-komunikacijske tehnologije, sukladnih s jedinstvenim zahtjevima za cijelo područje Europske unije.

   Obzirom da je Uredbom (EU) 2019/881 zadan glavni okvir jedinstvenog sustava kibernetičkog sigurnosnog certificiranja u Europskoj uniji odnosno način uspostave i provedbe sustava, prijedlogom Zakona se određuju nadležna tijela na nacionalnoj razini, pravna zaštita i sankcijski režim, koji su specifični za svaku državu članicu.

   Uz samu Uredbu (EU) 2019/881 ovaj Zakon jasno upućuje sve subjekte u Republici Hrvatskoj što im je činiti i kako postupati kada žele ili moraju pribjeći postupku certificiranja za svoje IKT proizvode, usluge ili procese ako ih namjeravaju staviti na jedinstveno tržište Europske unije.

III. OCJENA I IZVORI POTREBNIH SREDSTAVA ZA PROVEDBU ZAKONA

Tijela javnog sektora koja su obveznici primjene ovoga Zakona imati će osigurana sredstva u državnom proračunu Republike Hrvatske u okviru svojih redovnih aktivnosti. Prema organizacijskim zahtjevima Uredbe (EU) 2019/881 potrebno je proširenje funkcionalnosti Zavoda za sigurnost informacijskih sustava iz razloga što mu se ovim Zakonom stavljaju u nadležnost nove obveze i odgovornosti nacionalnog tijela za europsku kibernetičku sigurnosnu certifikaciju koje se do sada nisu obavljale:

- proširuju se obveze i zadaće stručnih službi na poslovima certificiranja, vođenje registra tijela za ocjenjivanje sukladnosti koja su akreditirane, vođenja registra u Republici Hrvatskoj izdanih europskih kibernetičkih sigurnosnih certifikata i izjava o sukladnosti
- proširuju se obveze nacionalnog tijela za suradnjom s Europskom komisijom, ENISA-om, ECCG-om te nacionalnim tijelima za kibernetičku sigurnosnu certifikaciju drugih država članica, kao i Hrvatskom akreditacijskom agencijom
- proširuju se poslovi rješavanja prigovora na europske kibernetičke sigurnosne certifikate ili izjave o sukladnosti,
- u nadležnosti nacionalnog tijela je i tehnička revizija odnosno nadzor nad sustavom europskog kibernetičkog sigurnosnog certificiranja,
- proširuju se obveze i zadaće stručnih službi u slučajevima ukinuća, ograničenja ili privremene suspenzije izdanih europskih kibernetičkih sigurnosnih certifikata ili izjava o sukladnosti.

Za obavljanje navedenih novih funkcija Zavod će kao nacionalno tijelo osigurati

sredstva u Državnom proračunu za 2022. godinu u sklopu svojih redovnih aktivnosti u iznosu od 1.580.000,00 kuna, a u 2023. godini u iznosu od 2.740.000,00 kuna.

PRIJEDLOG ZAKONA O PROVEDBI UREDBE (EU) 2019/881 EUROPSKOG PARLAMENTA I VIJEĆA OD 17. TRAVNJA 2019. (ZAKON O PROVEDBI KIBERNETIČKE SIGURNOSNE CERTIFIKACIJE)

I. OPĆE ODREDBE

Predmet zakona

Članak 1.

Ovim se Zakonom utvrđuje nacionalno tijelo za kibernetičku sigurnosnu certifikaciju, zadaće i ovlasti tog tijela, upise u registre, pravnu zaštitu, nadzor i prekršajne sankcije.

Osiguranje provedbe

Članak 2.

Ovim se Zakonom osigurava provedba Uredbe (EU) 2019/881 Europskog parlamenta i Vijeća od 17. travnja 2019. o ENISA-i (Agencija Europske unije za kibersigurnost) te o kibersigurnosnoj certifikaciji u području informacijske i komunikacijske tehnologije i stavljanju izvan snage Uredbe (EU) br. 526/2013 (Akt o kibersigurnosti) (Tekst značajan za EGP) (SL L 151/15, 7.6.2019.), (u daljnjem tekstu: Uredba (EU) 2019/881).

Pojmovi

Članak 3.

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

1. *IKT* – informacijsko-komunikacijska tehnologija (u daljnjem tekstu: IKT) – djelatnost i oprema koja čini tehničku osnovu za sustavno prikupljanje, pohranjivanje, obradu, širenje i razmjenu informacija različita oblika te putem informatizacije, telekomunikacije i Interneta omogućava pristup, povezivanje i upravljanje stvarima
2. *kibernetička sigurnost* – sve aktivnosti koje su nužne za zaštitu od kibernetičkih prijetnji mrežnih i informacijskih sustava, korisnika tih sustava i drugih osoba na koje one utječu, a istovjetan je pojmu iz članka 2. točke 1. Uredbe (EU) 2019/881
3. *europska shema kibernetičke sigurnosne certifikacije* – sveobuhvatni skup pravila, tehničkih zahtjeva, normi i postupaka, koji su utvrđeni na razini Europske unije i koji se primjenjuju na certifikaciju ili ocjenjivanje sukladnosti određenih IKT proizvoda, usluga i procesa
4. *europski kibernetički sigurnosni certifikat* – dokument koji je izdalo nadležno tijelo i kojim se potvrđuje da je određenom IKT proizvodu, usluzi ili procesu provjerena sukladnost sa specifičnim sigurnosnim zahtjevima utvrđenima u europskoj shemi kibernetičke sigurnosne certifikacije
5. *akreditacija* – odobrenje za izdavanje certifikata koje izdaje nacionalno akreditacijsko tijelo tijelu za ocjenjivanje sukladnosti kako bi ono moglo legitimno nuditi usluge certificiranja na jedinstvenom tržištu Europske unije. Postupak akreditiranja je definiran u članku 2., točki 10. Uredbe (EZ) br. 765/2008 Europskog parlamenta i Vijeća od 9. srpnja

2008. o utvrđivanja zahtjeva za akreditaciju i o stavljanju izvan snage Uredbe (EEZ) br. 339/93 (Tekst značajan za EGP) (SL L 218, 13.8.2008. i SL L 169, 25.06.2019), a provodi ga nacionalno akreditacijsko tijelo koje i dodjeljuje akreditaciju

6. *autorizacija* – odobrenje za izdavanje certifikata akreditiranim tijelima za ocjenu sukladnosti ako postoji poseban ili dodatan zahtjev u europskoj shemi kibernetičke sigurnosne certifikacije za koju su ta tijela prethodno akreditirana. Postupak autoriziranja provodi nacionalno tijelo za kibernetičku sigurnosnu certifikaciju sukladno članku 60. stavku 3. Uredbe (EU) 2019/881

7. *kvalificirani revizor* - pravna ili fizička osoba koja raspolaže međunarodnim certifikatom za obavljanje revizije informacijskih sustava koji su izdani sukladno standardu ISO/IEC 27001, PCI DDS i sličnom ili stručnim certifikatom za obavljanje revizije informacijskih sustava ISACA, CISA, ICS2, CISSP i sličnima.

(2) Ostali pojmovi koji se koriste u ovom Zakonu imaju jednako značenje kao pojmovi koji se koriste u Uredbi (EU) 2019/881.

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

II. PROVEDBA

Opća odredba

Članak 4.

(1) U svrhu postizanja visoke zajedničke razine kibernetičke sigurnosti na području Europske unije za određene IKT proizvode, usluge i procese provodi se europska kibernetička sigurnosna certifikacija sukladno Uredbi (EU) 2019/881.

(2) Jamstvene razine europskih shema kibernetičke sigurnosne certifikacije sa sigurnosnim zahtjevima određene su Uredbom (EU) 2019/881.

(3) Kibernetička sigurnosna certifikacija je dobrovoljna osim ako nije drukčije određeno zakonom ili pravno obvezujućim aktom Europske unije.

(4) Na temelju pojedinih europskih shema kibernetičke sigurnosne certifikacije provodi se kibernetička sigurnosna certifikacija koja predstavlja postupak izdavanja europskih kibernetičkih sigurnosnih certifikata odnosno izjava o sukladnosti za IKT proizvode, usluge i procese na zahtjev njihovih proizvođača ili pružatelja.

(5) Kibernetičkom sigurnosnom certifikacijom potvrđuje se da su IKT proizvodi, usluge i procesi evaluirani u skladu s europskim shemama kibernetičke sigurnosne certifikacije te da ispunjavaju utvrđene sigurnosne zahtjeve za potrebe zaštite dostupnosti, izvornosti, cjelovitosti i povjerljivosti pohranjenih, poslanih ili obrađenih podataka, funkcija ili usluga koje se nude s pomoću tih proizvoda, usluga i procesa ili kojima se s pomoću njih može pristupiti tijekom njihova životnog ciklusa.

(6) Obveze podnositelja zahtjeva za izdavanjem europskih kibernetičkih sigurnosnih certifikata odnosno izdavatelja izjava o sukladnosti po obavljenom samoocjenjivanju, kao i rokovi važenja certifikata i izjava o sukladnosti određeni su Uredbom (EU) 2019/881.

Nadležna tijela

Članak 5.

(1) Nacionalno tijelo za kibernetičku sigurnosnu certifikaciju u Republici Hrvatskoj je Zavod za sigurnost informacijskih sustava (u daljnjem tekstu: Zavod).

(2) Nacionalno akreditacijsko tijelo u Republici Hrvatskoj je Hrvatska akreditacijska agencija.

(3) Tijela za ocjenjivanje sukladnosti u Republici Hrvatskoj su pravne osobe ili fizičke osobe koje su akreditirane kod Hrvatske akreditacijske agencije i, ako je primjenjivo, koje su autorizirane od strane Zavoda.

Poslovi i ovlasti Zavoda

Članak 6.

(1) Osim ovlasti utvrđenih Uredbom (EU) 2019/881, Zavod obavlja sljedeće poslove:

- utvrđuje potrebu i donosi nacionalne sheme kibernetičke sigurnosne certifikacije
- nadzire provedbu ovog Zakona i Uredbe (EU) 2019/881 na području Republike Hrvatske.

(2) Na nacionalne sheme kibernetičke sigurnosne certifikacije, njima određenu kibernetičku sigurnosnu certifikaciju, kao i tijela za ocjenu sukladnosti te izdane kibernetičke sigurnosne certifikate ili izjave o sukladnosti prema nacionalnim shemama kibernetičke sigurnosne certifikacije na odgovarajući način primjenjuju se odredbe ovog Zakona i Uredbe (EU) 2019/881.

Dodjela akreditacije

Članak 7.

(1) Hrvatska akreditacijska agencija dodjeljuje akreditaciju tijelima za ocjenjivanje sukladnosti na vrijeme od pet godina ako ispunjavaju zahtjeve iz Priloga Uredbe (EU) 2019/881.

(2) Hrvatska akreditacijska agencija akreditaciju može ukinuti, ograničiti ili privremeno suspendirati ako uvjeti za akreditaciju nisu više ispunjeni.

Izvješćivanje i prijava u europski registar

Članak 8.

(1) Hrvatska akreditacijska agencija će izvijestiti Zavod o započinjanju svakog akreditacijskog postupka, pridržavajući se pritom odgovarajućih propisa o tajnosti.

(2) Hrvatska akreditacijska agencija će bez odgode obavijestiti Zavod o svakoj izdanoj akreditaciji provedenoj u svrhu kibernetičke sigurnosne certifikacije.

(3) Zavod će obavijestiti Europsku komisiju o svakoj izdanoj akreditaciji provedenoj u svrhu kibernetičke sigurnosne certifikacije i, ako je primjenjivo, autorizaciji za obavljanje poslova europskog kibernetičkog sigurnosnog certificiranja, u skladu s odredbama članka 61. Uredbe (EU) 2019/881.

Posebni i dodatni uvjeti ili zahtjevi

Članak 9.

(1) Ako europska shema kibernetičke sigurnosne certifikacije sadrži posebne ili dodatne zahtjeve sukladno članku 54. stavku 1. točki (f) Uredbe (EU) 2019/881 Zavod će provesti postupak utvrđivanja ispunjavanja tih posebnih ili dodatnih zahtjeva i izdati autorizaciju tijelu za ocjenjivanje sukladnosti u slučaju zadovoljenja uvjeta.

(2) Pri izdavanju akreditacije u uvjetima iz stavka 1. ovog članka Hrvatska akreditacijska agencija mora jasno navesti obvezu ishođenja dodatne autorizacije, a tako akreditirano tijelo za ocjenu sukladnosti ne smije nuditi uslugu certifikacije bez dobivene autorizacije.

(3) U slučaju kada se zahtijeva izdavanje kibernetičkog sigurnosnog certifikata visoke jamstvene razine u skladu s europskom shemom kibernetičke sigurnosne certifikacije, certifikat će izdati Zavod ili tijelo za ocjenu sukladnosti sukladno odredbama članka 56. stavka 6. Uredbe (EU) 2019/881.

(4) U slučaju zahtjeva za izdavanjem kibernetičkog sigurnosnog certifikata od strane javnog tijela, dopušta se podugovaranje dijelova certifikacijskog procesa sukladno točki 9. Priloga Uredbe (EU) 2019/881 osim samog izdavanja certifikata.

Nacionalni registri

Članak 10.

(1) Zavod vodi registar tijela za ocjenjivanje sukladnosti akreditiranih i, ako je primjenjivo, autoriziranih u Republici Hrvatskoj.

(2) Zavod vodi registar europskih kibernetičkih sigurnosnih certifikata izdanih u Republici Hrvatskoj te su mu tijela iz stavka 1. ovog članka obvezna bez odgode dostaviti ovjerenu digitalnu kopiju svakog izdanog certifikata.

(3) Zavod vodi registar izjava o sukladnosti izdanih u Republici Hrvatskoj te su sve pravne i fizičke osobe po provedenom samoocjenjivanju obvezne bez odgode dostaviti ovjerenu digitalnu kopiju svake izdane izjave o sukladnosti.

Pravo na podnošenje pritužbi

Članak 11.

(1) Sve fizičke i pravne osobe imaju pravo podnijeti pritužbu izdavatelju europskog kibernetičkog sigurnosnog certifikata ili izdavatelju izjave o sukladnosti, koji ih moraju informirati o statusu zaprimljene pritužbe i mogućnosti vođenja postupka pred nadležnim sudom ako priroda predmeta pritužbe to zahtjeva.

(2) Tijela iz stavka 1. ovog članka obvezna su donijeti opći akt kojim uređuju postupak po pritužbi.

(3) Za vrijeme trajanja suspenzije ili ograničenja europskog kibernetičkog sigurnosnog certifikata ili izjave o sukladnosti IKT proizvoda, usluga ili procesa nije dopušteno njihovo stavljanje na tržište prije okončanja postupaka iz ovog članka.

(4) U slučaju nepostupanja po pritužbi iz stavka 1. ovog članka, sve fizičke i pravne osobe imaju pravo podnijeti prigovor Zavodu.

Prigovor

Članak 12.

(1) Sve fizičke i pravne osobe mogu podnijeti prigovor Zavodu na europski kibernetički sigurnosni certifikat izdan od strane Zavoda ili akreditiranog tijela za ocjenjivanje sukladnosti ako je certifikat izdan sukladno članku 56. stavku 6. Uredbe (EU) 2019/881 te na izjavu o sukladnosti izdanu od proizvođača ili pružatelja IKT proizvoda, usluga ili procesa sukladno članku 53. Uredbe (EU) 2019/881.

(2) Zavod o prigovoru odlučuje rješenjem, protiv kojeg nije dopuštena žalba, ali se može pokrenuti upravni spor.

(3) Za vrijeme trajanja suspenzije ili ograničenja europskog kibernetičkog sigurnosnog certifikata ili izjave o sukladnosti IKT proizvoda, usluga ili procesa nije dopušteno njihovo stavljanje na tržište prije okončanja postupaka iz ovog članka.

Tehnička revizija

Članak 13.

(1) Zavod provodi tehničku reviziju nad izdavateljima europskog kibernetičkog sigurnosnog certifikata i izdavateljima izjave o sukladnosti radi usklađenosti s odredbama ovog Zakona i Uredbe (EU) 2019/881.

(2) Tijekom postupka tehničke revizije ovlaštene osobe Zavoda mogu pristupiti prostorima, opremi, sustavima i dokumentaciji tijela iz stavka 1. ovog članka radi provjere usklađenosti postupanja s odredbama ovog Zakona i Uredbe (EU) 2019/881.

(3) Izdavatelji europskog kibernetičkog sigurnosnog certifikata i izdavatelji izjave o sukladnosti obvezni su Zavodu omogućiti nesmetan pristup prostorima, opremi, sustavima i dokumentaciji nužnima za provođenje revizije.

(4) Zavod može koristiti i rezultate revizije obavljene od strane kvalificiranih revizora.

(5) Zavod će po provedenoj tehničkoj reviziji izraditi izvješće o reviziji koje sadrži:

- ocjenu sukladnosti s odredbama propisa,
- korektivne mjere s rokom izvršenja i
- druge upute,

koje će dostaviti i izdavateljima nad kojima je provedena revizija.

(6) U slučajevima potrebe osiguranja provedbe korektivnih mjera, Zavod će izdati rješenje, protiv kojeg nije dopuštena žalba, već se može pokrenuti upravni spor.

(7) U slučaju utvrđenog prekršaja Zavod podnosi prijavu Državnom odvjetniku koji može podnijeti optužni prijedlog.

III. PREKRŠAJNE ODREDBE

Članak 14.

(1) Novčanom kaznom u iznosu od 100.000,00 do 500.000,00 kuna kaznit će se za prekršaj

pravna osoba koja

- nudi certificiranje IKT proizvoda, usluga i procesa za europsku shemu kibernetičke sigurnosne certifikacije za koju nema validnu akreditaciju sukladno članku 7. stavku 1. ovog Zakona i, ako je primjenjivo, validnu autorizaciju sukladno članku 60. Uredbe (EU) 2019/881 odnosno članku 9. stavku 1. ovog Zakona
- nudi na tržištu IKT proizvode, usluge i procese za koje joj je europski kibernetički sigurnosni certifikat ili izjava o sukladnosti suspendirana ili ograničena prema članku 11. stavku 3. ili članku 12. stavku 3. ovog Zakona.

(2) 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.

(3) Novčanom kaznom u iznosu od 10.000,00 do 100.000,00 kuna kaznit će se za prekršaj iz stavka 1. ovog članka fizička osoba obrtnik ili osoba koja obavlja drugu samostalnu djelatnost.

Članak 15.

(1) Novčanom kaznom u iznosu od 50.000,00 do 250.000,00 kuna kaznit će se za prekršaj pravna osoba koja

- ometa provođenje tehničke revizije od strane Zavoda protivno odredbi članka 13. stavka 3. ovog Zakona
- ne postupi po izdanom rješenju iz članka 13. stavka 6. 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 i odgovorna osoba u pravnoj osobi.

(3) Novčanom kaznom u iznosu od 5.000,00 do 50.000,00 kuna kaznit će se za prekršaj iz stavka 1. ovog članka fizička osoba obrtnik ili osoba koja obavlja drugu samostalnu djelatnost.

Članak 16.

(1) Novčanom kaznom u iznosu od 10.000,00 do 100.000,00 kuna kaznit će se za prekršaj izdavatelj europskog kibernetičkog sigurnosnog certifikata ili izjave o sukladnosti koji

- ne dostavi ovjerenu digitalnu kopiju svakog izdanog kibernetičkog sigurnosnog certifikata ili ovjerenu digitalnu kopiju svake izdane izjave o sukladnosti u skladu s odredbom članka 10. stavka 2. ili članka 10. stavka 3. ovog Zakona
- ne donesu opći akt kojim uređuju postupak po pritužbi u skladu s odredbom članka 11. stavka 2. ovog Zakona.

(2) Novčanom kaznom u iznosu od 2.000,00 do 10.000,00 kuna kaznit će se za prekršaj iz stavka 1. ovog članka i odgovorna osoba u pravnoj osobi.

(3) 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.

IV. PRIJELAZNA I ZAVRŠNA ODREDBA

Članak 17.

(1) Vlada Republike Hrvatske, na prijedlog ravnatelja Zavoda, uz suglasnost Savjeta za koordinaciju sigurnosno-obavještajnih agencija, uskladit će Uredbu o unutarnjem ustrojstvu Zavoda s odredbama ovog Zakona, u roku od 90 dana od njegovog stupanja na snagu.

(2) Ravnatelj Zavoda uskladit će Pravilnik o unutarnjem redu Zavoda s Uredbom iz stavka 1. ovog članka uz suglasnost Vlade Republike Hrvatske u roku od 60 dana od stupanja na snagu Uredbe.

Članak 18.

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

O B R A Z LO Ž E N J E

Uz članak 1.

Ovim se člankom određuje sadržaj Zakona; provedba Uredbe o Agenciji Europske unije za kibernetičku sigurnost (ENISA) i o kibernetičkoj sigurnosnoj certifikaciji u području komunikacijske i informacijske tehnologije („Akt o kibernetičkoj sigurnosti“) 2019/881 od 17. travnja 2019.

Uz članak 2.

Ovim člankom se utvrđuje svrha ovog Zakona, a ta je osiguranje provedbe Uredbe (EU) 2019/881 u Republici Hrvatskoj na jednak način kao u svim Državama članicama EU.

Uz članak 3.

Ovim se člankom određuju značenja pojedinih pojmova korištenih u Zakonu. Posebna pozornost je posvećena usklađivanju pojmova s uvriježenim terminima hrvatskog pravnog nazivlja sadržanog u drugim važećim zakonskim propisima u Republici Hrvatskoj (lat. *terminus technicus*) jer je zbog odabira pojedinih naziva pri prijevodu Uredbe s engleskog izvornika bilo potrebno napraviti ispravke kako bi se osigurala harmonizacija te povezanost s hrvatskim pravnim okvirom, a posljedično i provedivost. Prilagodba je napravljena osobito prema stajalištu Nacionalnog vijeća za kibernetičku sigurnost da se u Republici Hrvatskoj koristi pridjev „kibernetički“, a ne „kiber“. Još 23. studenog 2001. godine u Budimpešti je donesena Konvencija o kibernetičkom kriminalu Vijeća Europe čiji popisnik je i Republika Hrvatska koja se tom zgodom opredijelila za pridjev „kibernetički“. Konvencija je ratificirana od strane Republike Hrvatske i objavljena u „Narodnim novinama – Međunarodni ugovori“, broj 9/02. To je dosljedno poštivao i Zakon o kibernetičkoj sigurnosti operatera ključnih usluga i davatelja digitalnih usluga donesen 2018. godine („Narodne novine“, broj 64/18.). Druga značajna situacija odnosi se na upotrebu pojma „program“ u prijevodu Uredbe dok je hrvatski uvriježeni *terminus tehnicus* – „shema“. Tim više što Uredba (EU) 2019/881 pojam „program“ (*programme*) koristi primjerice kod kontinuiranog programa rada Unije za europsku kibernetičku sigurnosnu certifikaciju, a kojeg sadržajno razlikuje od europskih „shema“ (*scheme*) kibernetičke sigurnosne certifikacije. Ovim se člankom određuje i jednaka primjena izraza koji imaju rodno značenje na muški i ženski rod.

Uz članak 4.

Članak ukratko naznačuje svrhu europske kibernetičke sigurnosne certifikacije u smislu Uredbe (EU) 2019/881. Govori i o jamstvenim razinama europskih shema kibernetičke sigurnosne certifikacije sa sigurnosnim zahtjevima, dobrovoljnosti kibernetičke sigurnosne certifikacije osim ako EU pravo izrijekom drukčije ne određuje, postupku izdavanja europskih kibernetičkih sigurnosnih certifikata odnosno izjava o sukladnosti za proizvođače ili pružatelje IKT proizvoda, usluga i procesa, njihovim obvezama, kao i rokovima važenja certifikata i izjava o sukladnosti.

Uz članak 5.

Članak određuje nadležna tijela u Republici Hrvatskoj. Kao nacionalno tijelo za kibernetičku sigurnosnu certifikaciju određuje se Zavod za sigurnost informacijskih sustava. Zavod se određuje kao nacionalno tijelo za kibernetičku sigurnosnu certifikaciju sukladno ranijoj odluci Vlade Republike Hrvatske od 19. rujna 2019. kojom je Zavod bio određen za tijelo koje privremeno obavlja te poslove, što je bilo osobito važno za vrijeme predsjedanja Republike Hrvatske Europskom unijom 2020. godine, kako pojedino područje aktivnosti EU tijekom predsjedanja ne bi ostalo nepokriveno od strane Republike Hrvatske i njenog predstavnika u Europskoj skupini za kibernetičku sigurnosnu certifikaciju *(European Cybersecurity Certification Group, ECCG).*

Članak upućuje i da je nacionalno akreditacijsko tijelo u Republici Hrvatskoj za potrebe kibernetičkog sigurnosnog certificiranja kod kojeg je potrebno provesti postupak akreditacije tijela za ocjenjivanje sukladnosti Hrvatska akreditacijska agencija (HAA) koje je kao takva određena primjenom Uredbe (EU) 765/2008 odnosno Zakonom o akreditaciji (Narodne novine, br. 158/03., 75/09. i 56/13.) i Uredbom o osnivanju Hrvatske akreditacijske agencije (Narodne novine, br. 158/04., 44/05. i 30/10.).
U slučaju kada tijela za ocjenu sukladnosti trebaju ispuniti posebne ili dodatne zahtjeve iz europskih shema kibernetičke sigurnosne certifikacije u smislu članka 54. stavka 1. točke (f) Uredbe (EU) 2019/881 autorizaciju će im prema članku 60. stavku 3. Uredbe (EU) 2019/881 izdati nacionalno tijelo za kibernetičku sigurnosnu certifikaciju, odnosno Zavod, ako ispunjavaju takve zahtjeve.

Uz članak 6.

Člankom je određeno da Zavod ima ovlasti koje utvrđuje Uredba (EU) 2019/881, a oni su sadržani primjerice u njenim člancima 56. stavcima 5. i 6., članku 57., člancima 58., 60. stavku 3., člancima 61. 62., 63., 64., kao i drugima u mjeri u kojoj su primjenljivi. Pored toga Zavod je ovlašten obavljati poslove utvrđivanja potrebe za donošenje, kao i samo donošenje nacionalne sheme kibernetičke sigurnosne certifikacije, donošenje uputa za potrebe provedbe Zakona i Uredbe (EU) 2019/881 te nadzora nad provedbom ovog Zakona. Određena je odgovarajuća primjena odredaba ovog Zakona i Uredbe (EU) 2019/881 na nacionalne sheme kibernetičke sigurnosne certifikacije, njima određenu kibernetičku sigurnosnu certifikaciju, kao i tijela za ocjenu sukladnosti te izdane kibernetičke sigurnosne certifikate ili izjave o sukladnosti prema nacionalnim shemama kibernetičke sigurnosne certifikacije.

Uz članak 7.

Članak upućuje da nacionalno akreditacijsko tijelo (HAA) dodjeljuje akreditacije tijelima za ocjenjivanje sukladnosti (pravnim ili fizičkim osobama – obrtnicima, fizičkim osobama koje obavljaju samostalnu djelatnost ili samim fizičkim osobama primjerice koji su inovatori) na vrijeme od pet godina, a da bi mogli obavljati poslove europske kibernetičke sigurnosne certifikacije. Akreditacija se dodjeljuje u slučaju ispunjavanja uvjeta iz Priloga Uredbe (EU) 2019/881. HAA dodijeljenu akreditaciju može ukinuti, ograničiti ili privremeno suspendirati ako uvjeti za akreditaciju nisu više ispunjeni.

Uz članak 8.

Članak obvezuje HAA izvijestiti Zavod o svakom započetom postupku izdavanja akreditacije, a Zavod se određuje tijelom koje je dužno obavijestiti Europsku komisiju o svakoj izdanoj akreditaciji za pojedinu shemu europske kibernetičke certifikacije u svrhu objave u Službenom listu EU. Ako je zbog zahtjeva iz sheme bilo potrebno izdati i autorizaciju, Zavod će to također navesti u prijavi.

Uz članak 9.

Ovim člankom se pobliže određuju procedura i obveze obavljanja tražene provjere posebnih i dodatnih zahtjeva propisanih člankom 54. stavkom 1. točkom (f) Uredbe (EU) 2019/881.

Uz članak 10.

Ovim člankom se određuju koje registre vodi Zavod i obvezu dostavljanja ovjerenih digitalnih kopija certifikata izdanih od tijela za ocjenu sukladnosti i izjava o sukladnosti izdanih od proizvođača IKT proizvoda, usluga i procesa.

Uz članak 11.

Članak predviđa da sve fizičke i pravne osobe zbog povrede ovog Zakona i Uredbe (EU) 2019/881 mogu podnijeti pritužbu tijelu za ocjenjivanje sukladnosti na izdani certifikat odnosno izdavatelju izjave o sukladnosti na izdanu izjavu. Tijela za ocjenjivanje sukladnosti,

nositelji europskih kibernetičkih sigurnosni certifikata i izdavatelji izjava o sukladnosti obvezni su donijeti opći akt kojim uređuju postupak po pritužbi. Ako se pak pritužba odnosi na ograničeni ili suspendirani certifikat ili izjavu o sukladnosti nekog IKT proizvoda, usluge ili procesa, brani se proizvođaču stavljanje tog proizvoda na tržište do razrješenja spora. Predviđeno je ulaganje prigovora Zavodu u slučaju da izdavatelji certifikata ili izjave o sukladnosti ne donesu odluku ili na drugi način obavijeste stranke o statusu pritužbe.

Uz članak 12.

U slučaju kad je Zavod izdavatelj certifikata ili je izdavatelj tijelo za ocjenu sukladnosti s kojim je Zavod sklopio poseban ugovor kako je predviđeno člankom 56. stavkom 6. Uredbe (EU) 2019/881, tada nezadovoljna stranka ulaže prigovor izravno Zavodu. Zavod će pritom donijeti rješenje protiv kojeg nije dopuštena žalba, već je moguće pokrenuti upravni spor. Upravni spor nezadovoljna stranka može pokrenuti i u slučaju kada Zavod ne donese rješenje (šutnja administracije). Kao i u slučaju pritužbe iz prethodnog članka, ako se prigovor odnosi na ograničenje ili suspenziju certifikata ili izjave o sukladnosti nekog IKT proizvoda, usluge ili procesa, brani se proizvođaču stavljanje tog proizvoda na tržište do razrješenja spora.

Uz članak 13.

Tehnička revizija je glavna spoznajna metoda predviđena ovim Zakonom, kojom Zavod dolazi do potrebnih informacija kako bi mogao obavljati svoje zadaće. Odredbom članka propisane su neposredne ovlasti Zavoda pri provođenju tehničke revizije, kao i obveze izdavatelja certifikata ili izjava o sukladnosti nad kojima se tehnička revizija provodi. Navedena je i mogućnost korištenja tuđih nalaza, u ovom slučaju kvalificiranih revizora. Propisana je i izrada izvješća, koje sadrži barem ocjenu sukladnosti s odredbama propisa i korektivne mjere s rokom izvršenja, ako ih bude, a koje se mora dostaviti revidiranoj stranci. Ako Zavod smatra nužnim osigurati provođenje mjera danim u izvješću, može donijeti i rješenje o obvezi provođenja predmetne mjere.

Uz članke 14.-16.

U ovim člancima propisane su prekršajne sankcije za nepoštivanje odredbi Uredbe (EU) 2019/881 i ovog Zakona, na način dostatan kako bi se odredbe Uredbe (EU) 2019/881 mogle provoditi u suglasju sa zakonopravnim sustavom Republike Hrvatske, a pritom zadržala univerzalnost postupanja unutar jedinstvenog digitalnog tržišta EU. Predviđeno je obaviti usklađivanje sankcijskih odredbi na razini Europske unije pri sljedećoj reviziji Uredbe.

Uz članak 17.

Završnim odredbama određeni su rokovi donošenja provedbenih akata. Uzimajući u obzir da je Zakonom o sigurnosno-obavještajnom sustavu Republike Hrvatske ("Narodne novine" broj 79/06 i 105/06) osnovan Zavod za sigurnost informacijskih sustava te je tim Zakonom propisan i djelokrug poslova Zavoda, a da je djelatnost Hrvatske akreditacijske agencije, u skladu sa Zakonom o akreditaciji („Narodne novine“, br. 158/03.,75/09. i 56/13.), propisana Uredbom o osnivanju Hrvatske akreditacijske agencije („Narodne novine“, br. 158/04., 44/05. i 30/10.), napominje se kako je nakon stupanja na snagu ovoga Nacrta prijedloga zakona, u rokovima koji su mogući, potrebno uskladiti i navedene zakone odnosno podzakonski osnivački akt u mjeri i ako je nužno.

Uz članak 18.

Ovim se člankom određuje stupanje na snagu Zakona.

PRILOZI - **Izvješće o provedenom savjetovanju sa zainteresiranom javnošću**

- **Izjava o usklađenosti prijedloga propisa s pravnom stečevinom Europske unije**

OBRAZAC IZVJEŠĆA O PROVEDENOM SAVJETOVANJU SA ZAINTERESIRANOM JAVNOŠĆU	
Naslov dokumenta	Izvješće o provedenom javnom savjetovanju o Prijedlogu Zakona o provedbi Uredbe (EU) 2019/881 Europskog parlamenta i Vijeća od 17. travnja 2019.
Stvaratelj dokumenta, tijelo koje provodi savjetovanje	Središnji državni ured za razvoj digitalnog društva
Svrha dokumenta	Izvješće o provedenom javnom savjetovanju o Prijedlogu Zakona o provedbi Uredbe (EU) 2019/881 Europskog parlamenta i Vijeća od 17. travnja 2019.
Datum dokumenta	19.10.2021.
Verzija dokumenta	1.0
Vrsta dokumenta	Izvješće
Naziv nacrta zakona, drugog propisa ili akta	Prijedlog Zakona o provedbi Uredbe (EU) 2019/881 Europskog parlamenta i Vijeća od 17. travnja 2019.
Jedinstvena oznaka iz Plana donošenja zakona, drugih propisa i akata objavljenog na internetskim stranicama Vlade	/
Naziv tijela nadležnog za izradu nacrta	Središnji državni ured za razvoj digitalnog društva
Koji su predstavnici zainteresirane javnosti bili uključeni u postupak izrade odnosno u rad stručne radne skupine za izradu nacrta?	U postupku izrade, jednako kao i u radu stručne radne skupine sudjelovali su predstavnici Ministarstva gospodarstva, poduzetništva i obrta, Ministarstva mora, prometa i infrastrukture, Ministarstva obrane, Ministarstva pravosuđa i uprave, Ministarstva unutarnjih poslova, Ministarstva zdravstva, Ministarstva znanosti i obrazovanja, Hrvatske akademske i istraživačke mreže (CARNet), Hrvatske akreditacijske agencije, Hrvatske regulatorne agencije za mrežne djelatnosti (HAKOM), Ureda Vijeća za nacionalnu sigurnost (UVNS), Zavoda za sigurnost informacijskih sustava (ZSIS), Sigurnosno-obavještajne agencije (SOA), Operativno-tehničkog centra za nadzor telekomunikacija (OTC) i Središnjeg državnog ureda za razvoj digitalnog društva.

Je li nacrt bio objavljen na internetskim stranicama ili na drugi odgovarajući način? Ako jest, kada je nacrt objavljen, na kojoj internetskoj stranici i koliko je vremena ostavljeno za savjetovanje? Ako nije, zašto?	Da, na portalu e-Savjetovanja u razdoblju od 28.09.2021. do 13.10.2021., te na mrežnim stranicama Središnjeg državnog ureda za razvoj digitalnog društva.
Koji su predstavnici zainteresirane javnosti dostavili svoja očitovanja?	Hrvatski telekom d.d. Tamara Kajmić Košutić
ANALIZA DOSTAVLJENIH PRIMJEDBI Primjedbe koje su prihvaćene Primjedbe koje nisu prihvaćene i obrazloženje razloga za neprihvaćanje	Odgovori na pristigle primjedbe/komentare objavljeni su u izvješću o provedenom savjetovanju.
Troškovi provedenog savjetovanja	/

Izvješće o provedenom savjetovanju - Savjetovanje o prijedlogu Zakona o provedbi Uredbe (EU) 2019/881 Europskog parlamenta i Vijeća od 17. travnja 2019.

Redni broj	Korisnik/Sekcija/Komentar	Odgovor
1	**Hrvatski Telekom d.d.** **II. PROVEDBA, Članak 4.** Predlažemo da se predmetnim Zakonom detaljno definira pojam sheme kibernetičke sigurnosti.	**Nije prihvaćen** Definicija je dana u članku 3. stavku 1. točki 3. kao „europska shema kibernetičke sigurnosne certifikacije“, gdje se ispravlja netočan izraz u hrvatskoj inačici Uredbe (EU) 2019/881 naveden u članku 2. stavku 1. točki 9. kao „europski program kibersigurnosne certifikacije“, dok je u engleskoj inačici naveden točan izraz kao „European cybersecurity certification scheme“. Izraz „shema“ je uobičajen tehnički izraz koji se koristi u postupcima certifikacije i dosljedno se kao takav koristi u svim područjima reguliranim europskim propisima pa ga stoga valja zadržati i u području kibernetičke sigurnosti. Točan sadržaj shema kojima se ova Uredba i Zakon bave je naveden u članku 54. Uredbe (EU) 2019/881 i nije ga potrebno ponavljati.
2	**Hrvatski Telekom d.d.** **II. PROVEDBA, Članak 6.** Predlažemo da se predmetnim Zakonom detaljno propiše način utvrđivanja potrebe za donošenjem nacionalne sheme kibernetičke sigurnosti, postupak donošenja iste na način da su u postupak, između ostalih, uključeni predstavnici IKT industrije, kao i obveza Zavoda da provede javnu rasprave prije donošenja navedene sheme.	**Nije prihvaćen** Ovim Zakonom se osigurava provedba Uredbe (EU) 2019/881 osobito glede ispunjavanja nacionalne obveze navedene u članku 65. Uredbe i nema drugih ambicija. U članku 6. stavku 1. podstavku 1. ovog Zakona se doista spominje mogućnost izrade nacionalnih shema, no to će se morati riješiti zasebnim propisom ako interes za takvim nečim bude postojao pored važećih europskih shema kibernetičke sigurnosne certifikacije.

3	**Hrvatski Telekom d.d.** **II. PROVEDBA, Članak 11.** U svrhu transparentnosti i jednoznačnog tumačenja i primjene predmetnog Zakona, predlažemo da se Zakonom jasno definiraju nadležna tijela koja su izdavatelji europskog kibernetičkog sigurnosnog certifikata, odnosno izdavatelji izjave o sukladnosti. Predlažemo dopunu članka 11. stavaka 2. na način da se obvežu tijela iz članka 11. stavka 1. da su prije donošenja općeg akta obvezna provesti javnu raspravu. Predlažemo da se predmetnim Zakonom u svrhu transparentnosti i jednoznačnog tumačenja i primjene Zakona jasno propišu uvjeti suspenzije ili ograničenja europskog kibernetičkog sigurnosnog certifikata ili izjave o sukladnosti, kao i tijela ovlaštena za odlučivanje o navedenom. Ujedno naglašavamo kako je Uredbom 2019/881 naglašena potreba uzimanja u obzir utjecaja mjera na proizvođače ili pružatelje IKT proizvoda, IKT usluga i IKT procesa te na korisnike u smislu troška mjera, kao i društvenih ili gospodarskih koristi koje proizlaze iz očekivane poboljšane razine sigurnosti ciljanih IKT proizvoda, IKT usluga ili IKT procesa. Predlažemo brisanje cjelokupne odredbe članka 11. stavka 3. Prijedloga Zakona s obzirom da Uredba 2019/881 ne daje ovlaštenje državama članicama da odlučuju o zabrani stavljanja na tržište IKT proizvoda, usluga i procesa.	**Nije prihvaćen** Ovim Zakonom se ne definiraju tijela – izdavatelji europskog kibernetičkog sigurnosnog certifikata niti neka druga nadležna tijela, jer je sve detaljno propisano Uredbom (EU) 2019/881. Certifikat (tehnički naziv za potvrdu ili svjedodžbu) da neki IKT proizvod, usluga ili proces zadovoljava uvjete i zahtjeve iz tražene sheme izdaju akreditirane (licencirane za taj posao) pravne osobe. Ako se naknadno utvrdi da neki već certificirani IKT proizvod, usluga ili proces više ne zadovoljava uvjete pod kojima je uopće dobio certifikat, tada samo i isključivo ona pravna osoba koja je certifikat izdala ima ga pravo i povući, privremeno ili trajno, ovisno o ozbiljnosti kršenja početnih uvjeta. Dakle, ne radi se o zabrani stavljanja na tržište nekog proizvoda per se, već je u pitanju zabrana lažnog reklamiranja i oglašavanja odnosno dovođenja potrošača u zabludu, što je pak predmet drugih propisa. S druge strane, ako je posjedovanje validnog certifikata nekim propisom proglašeno obveznim, tada se njegovim gubitkom de facto gubi dopuštenje za rad pa je proizvođač ili pružatelj tog IKT proizvoda, usluge ili procesa dužan obavijestiti potrošača o toj činjenici.
4	**Hrvatski Telekom d.d.** **II. PROVEDBA, Članak 12.** Predlažemo da se predmetnim Zakonom u svrhu transparentnosti i jednoznačnog tumačenja i primjene Zakona jasno propišu uvjeti suspenzije ili ograničenja europskog kibernetičkog sigurnosnog certifikata ili izjave o sukladnosti, kao i tijela ovlaštena za odlučivanje o navedenom. Ujedno naglašavamo kako je Uredbom 2019/881 naglašena potreba uzimanja u obzir utjecaja mjera na proizvođače ili pružatelje IKT proizvoda, IKT usluga i IKT procesa te na korisnike u smislu troška mjera, kao i društvenih ili gospodarskih koristi koje proizlaze iz očekivane poboljšane razine sigurnosti ciljanih IKT proizvoda, IKT usluga ili IKT procesa. Predlažemo brisanje cjelokupnog članka 12. stavka 4. Prijedloga Zakona s obzirom da Uredba 2019/881 ne daje ovlaštenje državama članicama da odlučuju o zabrani stavljanja na tržište IKT proizvoda, usluga i procesa.	**Nije prihvaćen** Daje se isti odgovor kao za komentar pod brojem 3, jer je o istome odnosno komentari su vezani.

5	**Hrvatski Telekom d.d.** **III. PREKRŠAJNE ODREDBE, Članak 14.** Predlažemo brisanje članka 14. stavka 1. Prijedloga Zakona u dijelu koji predviđa da će se novčanom kaznom u iznosu od 100.000,00 do 500.000,00 kuna kazniti za prekršaj pravna osoba koja nudi na tržištu IKT proizvode, usluge i procese za koje joj je europski kibernetički sigurnosni certifikat ili izjava o sukladnosti opozvana ili ograničena prema članku 11. stavku 3. ili članku 12. stavku 3. ovog Zakona, a s obzirom da, kako je u prethodnim komentarima navedeno - Uredba 2019/881 ne daje ovlaštenje državama članicama da odlučuju o zabrani stavljanja na tržište IKT proizvoda, usluga i procesa pa posljedično niti ovlaštenje o odlučivanju o predloženim novčanim kaznama. Ujedno naglašavamo kako je Uredbom 2019/881 naglašena potreba uzimanja u obzir utjecaja mjera na proizvođače ili pružatelje IKT proizvoda, IKT usluga i IKT procesa te na korisnike u smislu troška mjera, kao i društvenih ili gospodarskih koristi koje proizlaze iz očekivane poboljšane razine sigurnosti ciljanih IKT proizvoda, IKT usluga ili IKT procesa, kao i da predviđene kazne moraju biti učinkovite, proporcionalne i odvraćajuće	**Nije prihvaćen** Daje se isti odgovor kao za komentar pod brojem 3, jer je prijedlog posljedica iste primjedbe koja je već obrađena odnosno komentari su vezani. Dodatno se daje informacija o postojanju obveze usklađivanja visina kazni na jedinstvenom digitalnom tržištu EU, što će Europska komisija i napraviti kad bude dobila sve provedbene propise država članica. Po dogovoru oko usklađivanju sankcijskih režima na razini EU, predložit će se izmjena ili dopuna ovog Zakona kako bi se takvo ujednačavanje i provelo.
6	**Tamara Kajmić Košutić** **III. PREKRŠAJNE ODREDBE, Članak 14.** Nejasno je što znači da će se kazniti firma koja nudi na tržištu IKT proizvod, uslugu i proces za koje je certifikat opozvan ili ograničen. Da li se odredba iz čl 14 st 1 odnosi samo na IKT proizvode, usluge i procese koji se prethodno imali certifikat ili izjavu o sukladnosti pa im je opozvana ili ograničena? Što točno znači stavljanje na tržište? Da li korisnici koji već koriste IKT proizvod mogu nastaviti s njegovim korištenjem?	**Nije prihvaćen** Ne treba pojašnjavati ono što je jasno iz same Uredbe (EU) 2019/881 ili je uređeno propisima o regulaciji tržišta, obveznim odnosima, zaštiti potrošača i slično... Proizvođač ili pružatelj za svoj IKT proizvod, uslugu ili proces traži certifikaciju (i plaća ju) od „tijela za ocjenjivanje sukladnosti“ (naravno, akreditirane pravne osobe za taj posao) kako bi pojačao prodaju na tržištu te je stoga ta inačica, naziv i trgovačko ime IKT proizvoda, usluge ili procesa vezano uz izdani certifikat. Gubitkom certifikata, proizvođač ili pružatelj više ne smije pod tim istim ili vrlo sličnim nazivom, oznakom ili imenom nuditi istu inačicu IKT proizvoda, usluge ili procesa, jer bi to bilo dovođenje potrošača u zabludu odnosno varanje. IKT proizvod, usluga ili proces koji je izgubio certifikat se načelno može nastaviti koristiti (odluka na potrošaču) no svi potrošači moraju biti informirani o činjenici i razlogu gubitka certifikata za proizvod koji koriste (predmet drugih propisa, navodim kao primjer). Samo u slučaju kad se nekim zakonskim propisom zahtijeva posjedovanje validnog certifikata, tada bi se IKT proizvod, usluga ili proces kojemu je suspendiran certifikat morao prestati koristiti, jer mogu nastati štete zbog kojih je takva obveza i uvedena (primjerice robotski uređaji u medicini, autopiloti u zrakoplovima i sl.).

IZJAVA O USKLAĐENOSTI PRIJEDLOGA PROPISA S PRAVNOM STEČEVINOM EUROPSKE UNIJE

1. Naziv prijedloga propisa

Nacrt prijedloga Zakona o provedbi Uredbe (EU) 2019/881Europskog parlamenta i Vijeća od 17. travnja 2019. (Zakon o provedbi kibernetičke sigurnosne certifikacije)

2. Stručni nositelj izrade prijedloga propisa

SREDIŠNJI DRŽAVNI URED ZA RAZVOJ DIGITALNOG DRUŠTVA

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 2021. godinu.
Rok: IV. kvartal 2021.

4. Preuzimanje odnosno provedba pravne stečevine Europske unije

a) Odredbe primarnih izvora prava Europske unije

Ugovor o funkcioniranju Europske unije
članak/članci Članak 16.

b) Sekundarni izvori prava Europske unije

Uredba (EU) 2019/881Europskog parlamenta i Vijeća od 17. travnja 2019. o ENISA-i (Agencija Europske unije za kibersigurnost) te o kibersigurnosnoj certifikaciji u području informacijske i komunikacijske tehnologije i stavljanju izvan snage Uredbe (EU) br. 526/2013 (Akt o kibersigurnosti) (Tekst značajan za EGP) (SL L 151, 7.6.2019.)

32019R0881

c) Ostali izvori prava Europske unije

5. Prilog:

-

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

Bernard Gršić

Državni tajnik

(potpis)

REPUBLIKA HRVATSKA 1 ZAGREB SREDIŠNJI DRŽAVNI URED ZA RAZVOJ DIGITALNOG DRUŠTVA

17 -11- 2021

(datum i pečat)

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

Andreja Metelko-Zgombić

Državna tajnica

(potpis)

REPUBLIKA HRVATSKA 27 ZAGREB MINISTARSTVO VANJSKIH I EUROPSKIH POSLOVA

19. 11. 2021

(datum i pečat)