NN 63/2022 (3.6.2022.), Zakon o provedbi Uredbe (EU) 2019/881 Europskog parlamenta i Vijeća od 17. travnja 2019. (Zakon o provedbi kibernetičke sigurnosne certifikacije)

HRVATSKI SABOR

908

Na temelju članka 89. Ustava Republike Hrvatske, donosim

ODLUKU

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

Proglašavam Zakon o provedbi Uredbe (EU) 2019/881 Europskog parlamenta i Vijeća od 17. travnja 2019. (Zakon o provedbi kibernetičke sigurnosne certifikacije), koji je Hrvatski sabor donio na sjednici 27. svibnja 2022.

Klasa: 011-02/22-02/48
Urbroj: 71-10-01/1-22-2
Zagreb, 31. svibnja 2022.

Predsjednik
Republike Hrvatske
Zoran Milanović, v. r.

ZAKON

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, upisi u registre, pravna zaštita, 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 ovoga 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 podataka i 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 definiran je 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. 6. 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 koje su, ako je to propisano odredbama ovoga Zakona, dodatno 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 ovoga 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 izvijestit će Zavod o započinjanju svakog akreditacijskog postupka, pridržavajući se pritom odgovarajućih propisa o tajnosti.

(2) Hrvatska akreditacijska agencija obavijestit će 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 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. ovoga 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) 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 primjene odredbe članka 56. stavka 5. točke (a) Uredbe (EU) 2019/881 Zavod može tijelu za ocjenu sukladnosti ugovorom povjeriti obavljanje pojedinog postupka ili dijela postupka kibernetičke sigurnosne certifikacije, osim izdavanja samog certifikata.

Nacionalni registri

Članak 10.

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

(2) Zavod vodi registar europskih kibernetičkih sigurnosnih certifikata izdanih u Republici Hrvatskoj te su mu tijela iz stavka 1. ovoga članka obvezna 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 dostaviti ovjerenu digitalnu kopiju svake izdane izjave o sukladnosti.