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

Sadržaj

I. OPĆE ODREDBE

Članak 1.

Predmet Zakona

Ovim se Zakonom utvrđuje nacionalno tijelo za kibernetičku sigurnosnu certifikaciju, zadaće i ovlasti tog tijela, upisi u registre, pravna zaštita, nadzor i prekršajne sankcije.

Članak 2.

Osiguranje provedbe

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).

Članak 3.

Pojmovi

(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

Članak 4.

Opća odredba

(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.

Članak 5.

Nadležna tijela

(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.

Članak 6.

Poslovi i ovlasti Zavoda

(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.

Članak 7.

Dodjela akreditacije

(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.

Članak 8.

Izvješćivanje i prijava u europski registar

(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.

Članak 9.

Posebni i dodatni uvjeti ili zahtjevi

(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.

Članak 10.

Nacionalni registri

(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.

Članak 11.

Pravo na podnošenje pritužbi

(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. ovoga 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 ovoga članka.

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

Članak 12.

Prigovor

(1) Sve fizičke i pravne osobe mogu podnijeti prigovor Zavodu na europski kibernetički sigurnosni certifikat koji je izdao Zavod ili akreditirano tijelo za ocjenjivanje sukladnosti ako je certifikat izdan sukladno članku 56. stavku 6. Uredbe (EU) 2019/881 te na izjavu o sukladnosti koju je izdao proizvođač ili pružatelj 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 pred nadležnim upravnim sudom.

(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 ovoga članka.

Članak 13.

Tehnička revizija

(1) Zavod provodi tehničku reviziju nad izdavateljima europskog kibernetičkog sigurnosnog certifikata i izdavateljima izjave o sukladnosti radi usklađenosti s odredbama ovoga 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. ovoga članka radi provjere usklađenosti postupanja s odredbama ovoga 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 koje su objavili kvalificirani revizori.

(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.

(6) Izvješće iz stavka 5. ovoga članka dostavit će se i izdavateljima nad kojima je provedena revizija.

(7) U slučajevima potrebe osiguranja provedbe korektivnih mjera Zavod će donijeti rješenje protiv kojeg nije dopuštena žalba, već se može pokrenuti upravni spor pred nadležnim upravnim sudom.

(8) U slučaju utvrđenog prekršaja Zavod podnosi prijavu Državnom odvjetniku koji podnosi 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. ovoga Zakona ili validnu autorizaciju sukladno članku 60. Uredbe (EU) 2019/881 odnosno članku 9. stavku 1. ovoga 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. ovoga Zakona.

(2) Novčanom kaznom u iznosu od 10.000,00 do 25.000,00 kuna kaznit će se za prekršaj iz stavka 1. ovoga 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. ovoga 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. ovoga Zakona

– ne postupi po izdanom rješenju iz članka 13. stavka 7. ovoga Zakona.

(2) Novčanom kaznom u iznosu od 5000,00 do 25.000,00 kuna kaznit će se za prekršaj iz stavka 1. ovoga članka i odgovorna osoba u pravnoj osobi.

(3) Novčanom kaznom u iznosu od 5000,00 do 50.000,00 kuna kaznit će se za prekršaj iz stavka 1. ovoga 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. ovoga Zakona

– ne donese opći akt kojim uređuje postupak po pritužbi u skladu s odredbom članka 11. stavka 2. ovoga Zakona.

(2) Novčanom kaznom u iznosu od 2000,00 do 10.000,00 kuna kaznit će se za prekršaj iz stavka 1. ovoga članka i odgovorna osoba u pravnoj osobi.

(3) Novčanom kaznom u iznosu od 5000,00 do 25.000,00 kuna kaznit će se za prekršaj iz stavka 1. ovoga članka fizička osoba obrtnik ili osoba koja obavlja drugu samostalnu djelatnost.

Članak 17.

(1) Novčanom kaznom u iznosu od 13.270,00 do 66.360,00 eura 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. ovoga Zakona ili validnu autorizaciju sukladno članku 60. Uredbe (EU) 2019/881 odnosno članku 9. stavku 1. ovoga 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. ovoga Zakona.

(2) Novčanom kaznom u iznosu od 1320,00 do 3.310,00 eura kaznit će se za prekršaj iz stavka 1. ovoga članka i odgovorna osoba u pravnoj osobi.

(3) Novčanom kaznom u iznosu od 1320,00 do 13.270,00 eura kaznit će se za prekršaj iz stavka 1. ovoga članka fizička osoba obrtnik ili osoba koja obavlja drugu samostalnu djelatnost.

Članak 18.

(1) Novčanom kaznom u iznosu od 6630,00 do 33.180,00 eura kaznit će se za prekršaj pravna osoba koja:

– ometa provođenje tehničke revizije od strane Zavoda protivno odredbi članka 13. stavka 3. ovoga Zakona

– ne postupi po izdanom rješenju iz članka 13. stavka 7. ovoga Zakona.

(2) Novčanom kaznom u iznosu od 660,00 do 3310,00 eura kaznit će se za prekršaj iz stavka 1. ovoga članka i odgovorna osoba u pravnoj osobi.

(3) Novčanom kaznom u iznosu od 660,00 do 6630,00 eura kaznit će se za prekršaj iz stavka 1. ovoga članka fizička osoba obrtnik ili osoba koja obavlja drugu samostalnu djelatnost.

Članak 19.

(1) Novčanom kaznom u iznosu od 1320,00 do 13.270,00 eura 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. ovoga Zakona

– ne donese opći akt kojim uređuje postupak po pritužbi u skladu s odredbom članka 11. stavka 2. ovoga Zakona.

(2) Novčanom kaznom u iznosu od 260,00 do 1320,00 eura kaznit će se za prekršaj iz stavka 1. ovoga članka i odgovorna osoba u pravnoj osobi.

(3) Novčanom kaznom u iznosu od 660,00 do 3310,00 eura kaznit će se za prekršaj iz stavka 1. ovoga članka fizička osoba obrtnik ili osoba koja obavlja drugu samostalnu djelatnost.

IV. PRIJELAZNA I ZAVRŠNA ODREDBA

Članak 20.

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

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

(3) Odredbe članaka 14., 15. i 16. ovoga Zakona prestaju važiti na dan uvođenja eura.

Članak 21.

Ovaj Zakon stupa na snagu osmoga dana od dana objave u »Narodnim novinama«, osim članaka 17., 18. i 19. ovoga Zakona koje stupaju na snagu na dan uvođenja eura.