Zakon o informacijskoj sigurnosti

I. OSNOVNE ODREDBE

Članak 1.

(1) Ovim se Zakonom utvrđuje pojam informacijske sigurnosti, mjere i standardi informacijske sigurnosti, područja informacijske sigurnosti, te nadležna tijela za donošenje, provođenje i nadzor mjera i standarda informacijske sigurnosti.
(2) Ovaj se Zakon primjenjuje na državna tijela, tijela jedinica lokalne i područne (regionalne) samouprave te na pravne osobe s javnim ovlastima, koje u svom djelokrugu koriste klasificirane i neklasificirane podatke.
(3) Ovaj se Zakon primjenjuje i na pravne i fizičke osobe koje ostvaruju pristup ili postupaju s klasificiranim i neklasificiranim podacima.

Članak 2.

Pojedini pojmovi u smislu ovoga Zakona imaju sljedeće značenje:
– Informacijska sigurnost je stanje povjerljivosti, cjelovitosti i raspoloživosti podatka, koje se postiže primjenom propisanih mjera i standarda informacijske sigurnosti te organizacijskom podrškom za poslove planiranja, provedbe, provjere i dorade mjera i standarda.
– Mjere informacijske sigurnosti su opća pravila zaštite podataka koja se realiziraju na fizičkoj, tehničkoj ili organizacijskoj razini.
– Standardi informacijske sigurnosti su organizacijske i tehničke procedure i rješenja namijenjena sustavnoj i ujednačenoj provedbi propisanih mjera informacijske sigurnosti.
– Područja informacijske sigurnosti predstavljaju podjelu informacijske sigurnosti na pet područja s ciljem sustavne i učinkovite realizacije donošenja, primjene i nadzora mjera i standarda informacijske sigurnosti.
– Sigurnosna akreditacija informacijskog sustava je postupak u kojem se utvrđuje osposobljenost tijela i pravnih osoba iz članka 1. stavka 2. ovoga Zakona za upravljanje sigurnošću informacijskog sustava, a provodi se utvrđivanjem primijenjenih mjera i standarda informacijske sigurnosti.
– Informacijski sustav je komunikacijski, računalni ili drugi elektronički sustav u kojem se podaci obrađuju, pohranjuju ili prenose, tako da budu dostupni i upotrebljivi za ovlaštene korisnike.

II. MJERE I STANDARDI INFORMACIJSKE SIGURNOSTI

Članak 3.

Mjerama i standardima informacijske sigurnosti utvrđuju se minimalni kriteriji za zaštitu klasificiranih i neklasificiranih podataka u tijelima i pravnim osobama iz članka 1. stavka 2. i 3. ovoga Zakona.

Članak 4.

(1) Mjere i standardi informacijske sigurnosti utvrđuju se za klasificirane i neklasificirane podatke.
(2) Mjere i standardi informacijske sigurnosti utvrđuju se sukladno stupnju tajnosti, broju, vrsti te ugrozama klasificiranih i neklasificiranih podataka na određenoj lokaciji.
(3) Za klasificirane podatke stupnja tajnosti »Povjerljivo«, »Tajno« i »Vrlo tajno«, trajno se provodi sigurnosna prosudba ugroza.

Članak 5.

Mjere i standardi informacijske sigurnosti obuhvaćaju:
– nadzor pristupa i postupanja s klasificiranim podacima,
– postupanje prilikom neovlaštenog otkrivanja i gubitka klasificiranih podataka,
– planiranje mjera prilikom izvanrednih situacija,
– ustrojavanje posebnih fondova podataka za podatke klasificirane u Republici Hrvatskoj te za klasificirane podatke koje je predala druga država, međunarodna organizacija ili institucija s kojom Republika Hrvatska surađuje.

Članak 6.

(1) Mjere i standardi informacijske sigurnosti za zaštitu neklasificiranih podataka utvrđuju se u skladu s mjerama i standardima zakonom propisanim za zaštitu osobnih podataka građana.
(2) Mjere i standardi informacijske sigurnosti za zaštitu stupnja tajnosti »Ograničeno« utvrđuju se u skladu sa stavkom 1. ovoga članka, uz:
– prethodnu provjeru primjene propisanih mjera i standarda za neklasificirane podatke,
– primjenu mjera i standarda propisanih za stupanj tajnosti »Ograničeno«.

Članak 7.

Mjere informacijske sigurnosti propisat će se uredbom koju donosi Vlada Republike Hrvatske, a standardi za provedbu mjera propisat će se pravilnicima koje donose čelnici središnjih državnih tijela za informacijsku sigurnost.

III. PODRUČJA INFORMACIJSKE SIGURNOSTI

Članak 8.

Područja informacijske sigurnosti za koja se propisuju mjere i standardi informacijske sigurnosti su:
– sigurnosna provjera,
– fizička sigurnost,
– sigurnost podatka,
– sigurnost informacijskog sustava,
– sigurnost poslovne suradnje.

Sigurnosna provjera

Članak 9.

(1) Sigurnosna provjera je područje informacijske sigurnosti u okviru kojeg se utvrđuju mjere i standardi informacijske sigurnosti koji se primjenjuju na osobe koje imaju pristup klasificiranim podacima.
(2) Osobe iz stavka 1. ovoga članka obvezne su ishoditi uvjerenje o sigurnosnoj provjeri osobe (certifikat).
(3) Tijela i pravne osobe iz članka 1. stavka 2. ovoga Zakona, koji koriste klasificirane podatke stupnja tajnosti » Povjerljivo«, »Tajno« i »Vrlo tajno«, dužni su ustrojiti:
– popis osoba koje imaju pristup klasificiranim podacima,
– registar zaprimljenih certifikata s rokovima važenja certifikata.

Fizička sigurnost

Članak 10.

(1) Fizička sigurnost je područje informacijske sigurnosti u okviru kojeg se utvrđuju mjere i standardi informacijske sigurnosti za zaštitu objekta, prostora i uređaja u kojem se nalaze klasificirani podaci.
(2) Tijela i pravne osobe iz članka 1. stavka 2. ovoga Zakona, koji koriste klasificirane podatke stupnja tajnosti » Povjerljivo«, »Tajno« i »Vrlo tajno«, izvršit će kategorizaciju objekata i prostora na sigurnosne zone, propisane mjerama i standardima informacijske sigurnosti.

Sigurnost podatka

Članak 11.

(1) Sigurnost podatka je područje informacijske sigurnosti za koje se utvrđuju mjere i standardi informacijske sigurnosti koje se primjenjuju kao opće zaštitne mjere za prevenciju, otkrivanje i otklanjanje štete od gubitka ili neovlaštenog otkrivanja klasificiranih i neklasificiranih podataka.
(2) Tijela i pravne osobe iz članka 1. stavka 2. ovoga Zakona, koji koriste klasificirane i neklasificirane podatke u svom djelokrugu, dužni su primijeniti procedure o postupanju s klasificiranim i neklasificiranim podacima, o sadržaju i načinu vođenja evidencije o izvršenim uvidima u klasificirane podatke te nadzoru sigurnosti podataka, propisanim mjerama i standardima informacijske sigurnosti.

Članak 12.

Sigurnost informacijskog sustava

(1) Sigurnost informacijskog sustava je područje informacijske sigurnosti u okviru kojeg se utvrđuju mjere i standardi informacijske sigurnosti klasificiranog i neklasificiranog podatka koji se obrađuje, pohranjuje ili prenosi u informacijskom sustavu te zaštite cjelovitosti i raspoloživosti informacijskog sustava u procesu planiranja, projektiranja, izgradnje, uporabe, održavanja i prestanka rada informacijskog sustava.
(2) Sigurnosna akreditacija informacijskog sustava provodi se za informacijski sustav u kojem se koriste klasificirani podaci stupnja tajnosti »Povjerljivo«, »Tajno« i »Vrlo tajno«.
(3) Osobe koje sudjeluju u procesu iz stavka 1. ovoga članka trebaju posjedovati certifikat razine »Vrlo tajno« ili za jedan stupanj više od najviše razine tajnosti klasificiranih podataka koji se obrađuju, pohranjuju ili prenose u informacijskim sustavima pod njihovom nadležnosti.
(4) Mjere fizičke zaštite prostora u kojima se nalaze informacijski sustavi poduzet će se sukladno najvišoj razini tajnosti klasificiranih podataka koji se u njima obrađuju, pohranjuju ili prenose.
(5) Središnja državna tijela za informacijsku sigurnost ustrojavaju registar certificirane opreme i uređaja koji se koriste u klasificiranom informacijskom sustavu razine »Povjerljivo«, »Tajno« i »Vrlo tajno«.
Registar certificirane opreme i uređaja ustrojava se na temelju preuzimanja odgovarajućih registara međunarodnih organizacija ili vlastitim certificiranjem u skladu s odgovarajućim međunarodnim normama.

Sigurnost poslovne suradnje
Članak 13.

(1) Sigurnost poslovne suradnje je područje informacijske sigurnosti u kojem se primjenjuju propisane mjere i standardi informacijske sigurnosti za provedbu natječaja ili ugovora s klasificiranom dokumentacijom koji obvezuju pravne i fizičke osobe iz članka 1. stavka 3. ovoga Zakona.
(2) Pravne i fizičke osobe koje pristupaju provedbi natječaja ili ugovora iz stavka 1. ovoga članka, obvezne su ishoditi uvjerenje o sigurnosnoj provjeri pravne osobe (certifikat poslovne sigurnosti).
(3) Pravne i fizičke osobe iz stavka 1. ovoga članka za osoblje, objekte i prostore obvezne su primijeniti utvrđene mjere i standarde informacijske sigurnosti za određeni stupanj tajnosti klasificiranih podataka.
(4) Tijela i pravne osobe iz članka 1. stavka 2. ovoga Zakona, ovlašteni su za podnošenje zahtjeva za izdavanje certifikata poslovne sigurnosti za pravne i fizičke osobe kojima dostavljaju klasificirane podatke stupnja tajnosti » Povjerljivo«, »Tajno« i »Vrlo tajno«.
(5) Pravne i fizičke osobe koje sudjeluju u međunarodnim poslovima za koje je obvezan certifikat poslovne sigurnosti, ovlaštene su za podnošenje zahtjeva za izdavanje certifikata.
(6) Certifikat poslovne sigurnosti izdaje središnje državno tijelo za informacijsku sigurnost.

IV. SREDIŠNJA DRŽAVNA TIJELA ZA INFORMACIJSKU SIGURNOST

Ured Vijeća za nacionalnu sigurnost
Članak 14.

Ured Vijeća za nacionalnu sigurnost je središnje državno tijelo za informacijsku sigurnost koje koordinira i usklađuje donošenje i primjenu mjera i standarda informacijske sigurnosti u Republici Hrvatskoj i u razmjeni klasificiranih i neklasificiranih podataka između Republike Hrvatske i stranih zemalja i organizacija.

Članak 15.

(1) Ured Vijeća za nacionalnu sigurnost donosi Pravilnik o standardima sigurnosne provjere, Pravilnik o standardima fizičke sigurnosti, Pravilnik o standardima sigurnosti podataka, Pravilnik o standardima organizacije i upravljanja područjem sigurnosti informacijskih sustava te Pravilnik o standardima sigurnosti poslovne suradnje.
(2) Ured Vijeća za nacionalnu sigurnost trajno usklađuje propisane mjere i standarde informacijske sigurnosti u Republici Hrvatskoj s međunarodnim standardima i preporukama informacijske sigurnosti te sudjeluje u nacionalnoj normizaciji područja informacijske sigurnosti.

Članak 16.

(1) Ured Vijeća za nacionalnu sigurnost koordinira i usklađuje rad tijela i pravnih osoba iz članaka 17., 20., 23. i 25. ovoga Zakona.
(2) Ured Vijeća za nacionalnu sigurnost surađuje s mjerodavnim institucijama stranih zemalja i organizacija u području informacijske sigurnosti te koordinira međunarodnu suradnju ostalih tijela i pravnih osoba iz stavka 1. ovoga članka.

Zavod za sigurnost informacijskih sustava
Članak 17. (NN 79/07, 14/24)

(1) Zavod za sigurnost informacijskih sustava je središnje državno tijelo za tehnička područja sigurnosti informacijskih sustava u tijelima i pravnim osobama iz članka 1. stavka 2. ovoga Zakona.
(2) Tehnička područja sigurnosti informacijskih sustava su:
– standardi sigurnosti informacijskih sustava,
– sigurnosne akreditacije informacijskih sustava,
– upravljanje kriptomaterijalima koji se koriste u razmjeni klasificiranih podataka.

Članak 18.

(1) Zavod za sigurnost informacijskih sustava pravilnikom će regulirati standarde tehničkih područja sigurnosti informacijskih sustava iz članka 17. stavka 2. ovoga Zakona.
(2) Zavod za sigurnost informacijskih sustava trajno usklađuje standarde tehničkih područja sigurnosti informacijskih sustava u Republici Hrvatskoj s međunarodnim standardima i preporukama te sudjeluje u nacionalnoj normizaciji područja sigurnosti informacijskih sustava.

Članak 19.

Zavod za sigurnost informacijskih sustava obavlja poslove sigurnosne akreditacije informacijskih sustava u suradnji s Uredom Vijeća za nacionalnu sigurnost.

V. NACIONALNI CERT
Članak 20.

(1) CERT je nacionalno tijelo za prevenciju i zaštitu od računalnih ugroza sigurnosti javnih informacijskih sustava u Republici Hrvatskoj.
(2) CERT je zasebna ustrojstvena jedinica koja se ustrojava u Hrvatskoj akademskoj i istraživačkoj mreži (u daljnjem tekstu: CARNet).
(3) CERT usklađuje postupanja u slučaju sigurnosnih računalnih incidenata na javnim informacijskim sustavima nastalih u Republici Hrvatskoj, ili u drugim zemljama i organizacijama, kad su povezani s Republikom Hrvatskom.
(4) CERT usklađuje rad tijela koja rade na prevenciji i zaštiti od računalnih ugroza sigurnosti javnih informacijskih sustava u Repub-lici Hrvatskoj te određuje pravila i načine zajedničkog rada.

Članak 21. NN (79/07, 14/24)

Prestao važiti.

Članak 22.

Ravnatelj CARNet-a imenuje pomoćnika zaduženog za uprav-ljanje CERT-om.

VI. PROVEDBA INFORMACIJSKE SIGURNOSTI
Članak 23.

(1) Tijela i pravne osobe iz članka 1. stavka 2. ovoga Zakona dužni su primijeniti mjere i standarde informacijske sigurnosti iz članka 7. ovoga Zakona.
(2) U tijelima i pravnim osobama koji nemaju odgovarajuće informatičke i tehničke mogućnosti, mjere i standarde iz stavka 1. ovoga članka primijenit će središnje tijelo državne uprave nadležno za razvoj informacijskog sustava.
(3) U području obrazovnog i akademskog sektora mjere i standarde iz stavka 1. ovoga članka primijenit će središnje tijelo državne uprave nadležno za znanost i obrazovanje.

Članak 24.

(1) Tijela i pravne osobe iz članka 1. stavka 2. ovoga Zakona pravilnikom će utvrditi provedbu mjera i standarda informacijske sigurnosti.
(2) Središnja tijela državne uprave iz članka 23. stavka 2. i 3. ovoga Zakona pravilnikom će utvrditi način provedbe mjera i standarda informacijske sigurnosti u drugim tijelima.

VII. NADZOR INFORMACIJSKE SIGURNOSTI

Članak 25.

(1) Poslovi nadzora informacijske sigurnosti su poslovi nadzora organizacije, provedbe i učinkovitosti propisanih mjera i standarda informacijske sigurnosti u tijelima i pravnim osobama iz članka 1. stavka 2. ovoga Zakona.
(2) Poslove nadzora iz stavka 1. ovoga članka provode savjetnici za informacijsku sigurnost.
(3) Ured Vijeća za nacionalnu sigurnost pravilnikom će propisati kriterije za ustrojavanje radnih mjesta savjetnika za informacijsku sigurnost iz stavka 2. ovoga članka.

Članak 26.

(1) Savjetnik za informacijsku sigurnost podnosi izvješće o rezultatima provedenog nadzora čelniku tijela ili pravne osobe te središnjem državnom tijelu za informacijsku sigurnost.
(2) Središnje državno tijelo za informacijsku sigurnost, na temelju izvješća iz stavka 1. ovoga članka, ovlašteno je:
– dati upute u svrhu otklanjanja utvrđenih nedostataka i nepravilnosti, koje su nadzirana tijela i pravne osobe dužne u određenom roku otkloniti,
– provesti postupak preispitivanja daljnje valjanosti sigurnosne akreditacije informacijskog sustava,
– pokrenuti postupak utvrđivanja odgovornosti,
– poduzeti druge mjere i radnje za koje je posebnim propisima ovlašteno.
(3) Čelnik tijela ili pravne osobe dužan je poduzeti mjere za otklanjanje nedostataka utvrđenih u provedbi nadzora.

VIII. PRIJELAZNE I ZAVRŠNE ODREDBE

Članak 27.

Uredbu iz članka 7. ovoga Zakona Vlada Republike Hrvatske donijet će u roku od tri mjeseca od dana stupanja na snagu ovog Zakona.

Članak 28.

(1) Pravilnike iz članka 15. stavak 1. ovoga Zakona Ured Vijeća za nacionalnu sigurnost donijet će u roku od šest mjeseci od dana stupanja na snagu ovoga Zakona.
(2) Pravilnik iz članka 25. stavka 3. ovoga Zakona Ured Vijeća za nacionalnu sigurnost donijet će u roku od šest mjeseci od dana stupanja na snagu ovoga Zakona.
(3) Pravilnike iz članka 18. stavka 1. ovoga Zakona Zavod za sigurnost informacijskih sustava donijet će u roku od 30 dana od dana stupanja na snagu pravilnika iz stavka 1. ovoga članka.

Članak 29.

(1) Obvezuje se CARNet da uskladi svoj statut i dostavi Uredu Vijeća za nacionalnu sigurnost na suglasnost u roku od tri mjeseca od dana stupanja na snagu ovoga Zakona.
(2) Pravilnici iz članka 24. stavka 1. i 2. ovoga Zakona donijet će se u roku od devet mjeseci od dana stupanja na snagu ovoga Zakona.

Članak 30.

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

Prijelazne i završne odredbe iz Zakona o kibernetičkoj sigurnosti NN 14/24

Članak 115.

Prestanak važenja propisa

(1) Danom stupanja na snagu ovoga Zakona prestaju važiti:

– Zakon o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga (»Narodne novine«, br. 64/18.)

– članak 17. stavak 2. podstavak 4. i članak 21. Zakona o informacijskoj sigurnosti (»Narodne novine«, br. 79/07.)

– članak 41. Zakona o elektroničkim komunikacijama (»Narodne novine«, br. 76/22.)

– Uredba o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga (»Narodne novine«, br. 68 /18.) i

– Odluka o osnivanju Nacionalnog vijeća za kibernetičku sigurnost i Operativno-tehničke koordinacije za kibernetičku sigurnost (»Narodne novine«, br. 61/16., 28/18., 110/18., 79/19. i 136/20.).

(2) Odluka o mjerama i aktivnostima za podizanje nacionalnih sposobnosti pravovremenog otkrivanja i zaštite od državno sponzoriranih kibernetičkih napada, Advanced Persistent Threat (ATP) kampanja te drugih kibernetičkih ugroza, klasa: 022-03/21-04/91, urbroj: 50301-29/09-21-2, od 1. travnja 2021., ostaje na snazi do stupanja na snagu uredbe iz članka 113. stavka 1. ovoga Zakona.

Članak 116.

Stupanje na snagu Zakona

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