KONAČNI PRIJEDLOG

ZAKONA O INFORMACIJSKOJ SIGURNOSTI

Zagreb, lipanj 2007.

I. KONAČNI PRIJEDLOG ZAKONA O INFORMACIJSKOJ SIGURNOSTI

I. OSNOVNE ODREDBE

Članak 1.

(1) Ovim Zakonom utvrđuje se 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 Zakon primjenjuje se 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 Zakon primjenjuje se i na pravne i fizičke osobe koje ostvaruju pristup ili postupaju s klasificiranim i neklasificiranim podacima.

Članak 2.

Pojmovi koji se koriste u ovom Zakonu 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. stavak 2. ovog 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. ovog 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. ovog 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 razradit će se pravilnicima središnjih državnih tijela za informacijsku sigurnost.

III. PODRUČJA INFORMACIJSKE SIGURNOSTI

Članak 8.

Područja informacijske sigurnosti u okviru kojih 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. ovog članka obvezne su posjedovati uvjerenje o sigurnosnoj provjeri osobe (certifikat).

(3) Tijela i pravne osobe iz članka 1. stavka 2. ovog Zakona, koja 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. ovog Zakona, koja 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 u okviru kojeg 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. ovog Zakona, koja koriste klasificirane i neklasificirane podatke u svom djelokrugu, dužna 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, propisane mjerama i standardima informacijske sigurnosti.

Sigurnost informacijskog sustava

Članak 12.

(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. ovog 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 utvrđene mjere i standardi informacijske sigurnosti za provedbu natječaja ili ugovora s klasificiranom dokumentacijom koji obvezuju pravne i fizičke osobe iz članka 1. stavka 3. ovog Zakona.

(2) Pravne i fizičke osobe koje pristupaju provedbi natječaja ili ugovora iz stavka 1. ovog članka, obvezne su posjedovati uvjerenje o sigurnosnoj provjeri pravne osobe (certifikat poslovne sigurnosti).

(3) Pravne i fizičke osobe iz stavka 1. ovog 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. ovog Zakona, ovlaštena 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, ovlaštena 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. ovog 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. ovog članka.

Zavod za sigurnost informacijskih sustava

Članak 17.

(1) Zavod za sigurnost informacijskih sustava je središnje državno tijelo za tehnička područja sigurnosti informacijskih sustava u tijelima i pravnim osobama iz članka 1. stavak 2. ovog 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,
- koordinacija prevencije i odgovora na računalne ugroze sigurnosti informacijskih sustava.

Članak 18.

(1) Zavod za sigurnost informacijskih sustava pravilnikom će regulirati standarde tehničkih područja sigurnosti informacijskih sustava iz članka 17. stavka 2. ovog 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 sa Republikom Hrvatskom.

(4) CERT usklađuje rad tijela koja rade na prevenciji i zaštiti od računalnih ugroza sigurnosti javnih informacijskih sustava u Republici Hrvatskoj te određuje pravila i načine zajedničkog rada.

Članak 21.

CERT i Zavod za sigurnost informacijskih sustava surađuju na prevenciji i zaštiti od računalnih ugroza sigurnosti informacijskih sustava te sudjeluju u izradi preporuka i normi u Republici Hrvatskoj iz područja sigurnosti informacijskih sustava.

Članak 22.

(1) Izmjenama i dopunama Statuta CARNet-a utvrdit će se djelokrug CERT-a uz prethodnu suglasnost Ureda Vijeća za nacionalnu sigurnost.

(2) Ravnatelj CARNet-a imenuje pomoćnika zaduženog za upravljanje CERT-om.

VI. PROVEDBA INFORMACIJSKE SIGURNOSTI

Članak 23.

(1) Tijela i pravne osobe iz članka 1. stavak 2. ovog Zakona dužna su primijeniti mjere i standarde informacijske sigurnosti iz članka 7. ovog Zakona.

(2) U tijelima i pravnim osobama koja nemaju odgovarajuće informatičke i tehničke mogućnosti, mjere i standarde iz stavka 1. ovog 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. ovog članka primijenit će središnje tijelo državne uprave nadležno za znanost i obrazovanje.

Članak 24.

(1) Tijela i pravne osobe iz članka 1. stavak 2. ovog Zakona pravilnikom će utvrditi provedbu mjera i standarda informacijske sigurnosti.

(2) Središnja tijela državne uprave iz članka 23. stavak 2. i 3. ovog 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. stavak 2. ovog Zakona.

(2) Poslove nadzora iz stavka 1. 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. ovog 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, temeljem izvješća iz stavka 1. ovog 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. ovog 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. ovog Zakona Ured Vijeća za nacionalnu sigurnost donijet će u roku od šest mjeseci od dana stupanja na snagu ovog Zakona.

(2) Pravilnik iz članka 25. stavka 3. ovog Zakona Ured Vijeća za nacionalnu sigurnost donijet će u roku od šest mjeseci od dana stupanja na snagu ovog Zakona.

(3) Pravilnike iz članka 18. stavak 1. ovog Zakona Zavod za sigurnost informacijskih sustava donijet će u roku od 30 dana od dana stupanja na snagu pravilnika iz stavka 1. ovog članka.

Članak 29.

(1) Izmjene i dopune Statuta CARNet-a iz članka 22. stavak 1. donijet će se u roku od tri mjeseca od dana stupanja na snagu ovog Zakona.

(2) Pravilnici iz članka 24. stavaka 1. i 2. ovog Zakona donijet će se u roku od tri mjeseca od dana donošenja Pravilnika iz članka 28. stavak 1. ovog Zakona.

Članak 30.

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

O B R A Z L O Ž E N J E

II. RAZLOZI ZBOG KOJIH SE ZAKON DONOSI I PITANJA KOJA SE NJIME RJEŠAVAJU

A) OCJENA STANJA

Područje koje se ovim zakonskim prijedlogom treba urediti djelomično je bilo propisano Zakonom o zaštiti tajnosti podataka (NN 108/96) i Zakonom o sigurnosnim službama (NN 32/02, 38/02). Donošenjem Zakona o zaštiti tajnosti podataka 1996. godine i njegovih podzakonskih propisa prestala je vrijediti Uredba o utvrđivanju mjerila za određivanje tajnih podataka obrane te posebnim i općim postupcima za njihovo čuvanje (NN 70/91). Na taj način ovo važno područje tajnosti podataka po prvi puta se u Republici Hrvatskoj uredilo Zakonom, kojim su propisana načela tajnosti podataka, vrste i razine tajnosti, postupci za određivanje tajnosti, nadležnosti tijela te zaštitne mjere. U području načela tajnosti podataka ovaj Zakon propisao je niz rješenja preuzetih iz 80-tih godina dvadesetog stoljeća, koja nisu u skladu sa suvremenim standardima tajnosti podataka zemalja EU-a, članica NATO-a i drugih razvijenih demokratskih zemalja svijeta. Primjerice, to su neodgovarajuća klasifikacija prema stupnjevima i vrstama tajnosti za tajne podatke državne uprave, nepostojanje osnovnih načela za pristup tajnim podacima kao što su „potreba pristupa u okviru djelokruga rada" (need-to-know), nepostojanje procedure izdavanja certifikata za osobe koje imaju pristup tajnim podacima te nezadovoljavajuće tretiranje temeljnih demokratskih standarda kao što su zaštita osobnih podataka građana i pojam privatnosti općenito. Dio ove materije koji se odnosi na sve pravne i fizičke osobe u Republici Hrvatskoj, u međuvremenu je propisan Zakonom o zaštiti osobnih podataka (NN 103/03) i Zakonom o pravu na pristup informacijama (NN 172/03). Slijedom toga, potrebno je propisati temeljne principe tajnosti podataka državne uprave koji se trebaju razraditi novim Zakonom o tajnosti podataka. Taj Zakon treba na suvremen i međunarodno prihvaćen način tretirati pojmove klasificiranih i neklasificiranih podataka državne uprave, stupnjeve tajnosti i principe klasificiranja, kao i načela pristupa klasificiranim podacima.

Zakon o zaštiti tajnosti podataka (NN 108/96) nadalje propisuje način određivanja mjera za zaštitu tajnosti podataka i to na način da čelnicima javnih tijela i ovlaštenim dužnosnicima Republike Hrvatske daje ovlast za određivanje posebnih zaštitnih mjera i rok od tri mjeseca za donošenje propisa o zaštitnim mjerama i drugih propisa vezanih za tajnost podataka. Ovakva odredba ima za posljedicu neodgovarajuće stanje u kojemu se Republika Hrvatska danas nalazi, a to je nepostojanje standarda za zaštitu podataka u državnoj upravi, neprimjeren pristup tajnosti podataka u državnoj upravi i samim time loša percepcija javnosti o pojmovima privatnosti i tajnosti. Rezultat ovakvih odredbi Zakona je da tijela državne uprave samostalno donose mjere i standarde zaštite tajnosti podataka koji stoga na razini državnog sektora nisu standardizirani. U tijelima u kojima su takvi propisi doneseni i implementirani to je rezultiralo različitom učinkovitošću zaštitnih mjera i međusobno neusklađenim organizacijskim i tehničkim sigurnosnim rješenjima. Poseban problem na koji se svih ovih godina nije obraćala pažnja je i to što je samo mali broj tijela državne uprave uopće osposobljen za donošenje i implementaciju mjera i standarda zaštite tajnosti podataka. U praksi su podzakonski propisi doneseni i u određenoj mjeri provedeni samo u tijelima sigurnosnog sustava u širem smislu (sigurnosno-obavještajne agencije, ministarstva obrane, unutarnjih i vanjskih poslova). Najveći broj tijela državne uprave u Republici Hrvatskoj nema

ljudske potencijale i potrebna znanja za donošenje i implementaciju ovakvih mjera i standarda te propise nije niti donio, ili je mjere zaštite pokušao implementirati kroz vanjsku komercijalnu uslugu, kupljenu na tržištu bez jasnih kriterija i tehničkih zahtjeva, te upitne primjerenosti državnim potrebama. Zaključno se može reći da problem postoji na dvije razine. Prva su nedovoljni ljudski potencijali i znanje za koncipiranje sigurnosnih mjera za zaštitu podataka u većini tijela, a druga je da i pri definiranim standardima zaštite podataka veliki broj tijela nema stručne potencijale za implementaciju, održavanje i unaprjeđivanje zaštitnih mjera.

Ovakvo stanje predstavlja sigurnosni problem za Republiku Hrvatsku, ali i vrlo skup pristup, u kojem se na nekoordiniran i nesustavan način realiziraju i financiraju različita organizacijska i tehnička sigurnosna rješenja u tijelima državne uprave. U takvom stanju Republika Hrvatska ne može uspostaviti i osigurati minimalne zahtjeve informacijske sigurnosti na nacionalnoj razini, što je temeljni zahtjev EU-a i NATO-a u aktualnim integracijskim procesima. U tom smislu može se reći da postojeći zakonski okvir u području informacijske sigurnosti nije usklađen sa zahtjevima NATO-a i EU-a, a međunarodno standardiziran i zahtijevan institucionalni okvir u području informacijske sigurnosti u Republici Hrvatskoj tek nastaje, što predstavlja veliku zapreku koju treba nužno otkloniti na putu daljnjeg približavanja euro-atlantskim integracijama.

Starim Zakonom o sigurnosnim službama (NN 32/02, 38/02), na temelju iskustava u NATO programu Partnerstvo za mir, kojemu je Republika Hrvatska pristupila u svibnju 2000. godine, propisani su prvi temelji organizacije informacijske sigurnosti na nacionalnoj razini, koji su bili uvjet pristupa Republike Hrvatske Akcijskom planu za članstvo u NATO-u (MAP) 2002. godine. Ovim Zakonom osnovan je Ured Vijeća za nacionalnu sigurnost, nadležan između ostalog za provedbu sigurnosnih mjera potrebnih za zaštitu tajnih dokumenata u razmjeni između Republike Hrvatske i stranih obrambenih organizacija, te Središnji registar za prijem i pohranu dokumenata. Pored toga, Ured je postao nadležan za tehničke poslove u području informacijske sigurnosti do osnivanja posebnog tehničkog tijela, Zavoda za informacijsku sigurnost i kripto-zaštitnu tehnologiju, koji Uredu u tim poslovima treba pružati tehničku potporu. Ovakvim propisom Republika Hrvatska je započela izgradnju zajedničke organizacije na nacionalnoj razini za potrebe suradnje s NATO-om i sukladno zahtjevima NATO-a. Ovim Zakonom u Republici Hrvatskoj uvedeni su međunarodno prihvaćeni standardi za postojanje središnjeg državnog tijela za informacijsku sigurnost (National Security Authority – NSA) i središnjeg državnog tijela za tehnička područja informacijske sigurnosti (National Communication Security Authority – NCSA ili Infosec Authority – IA). U razdoblju od donošenja ovog Zakona 2002. godine pa do danas, Ured je preuzeo i proveo većinu svojih nadležnosti u ovom području, dok je formiranje Zavoda tek započeto. Zbog pravnih nedorečenosti u odredbama ovog Zakona, Zavod nikada nije formiran, inicijalna proračunska sredstva nisu korištena, a poslove Zavoda u okviru suradnje s NATO-om obavljali su privremeni ravnatelj Zavoda i Ured Vijeća za nacionalnu sigurnost. Najveći problem spomenutih odredbi Zakona o sigurnosnim službama je pokušaj parcijalnog rješavanja pojma informacijske sigurnosti, u okvirima suradnje s NATO-om i u okvirima sigurnosnog sustava Republike Hrvatske. S vremenom se, osobito kroz provedbu Akcijskog plana za članstvo u NATO-u, pokazalo da se zahtjevi informacijske sigurnosti postavljaju za državnu upravu u cjelini te da je nužno uskladiti pristup u području informacijske sigurnosti na nacionalnoj razini sa zahtjevima ne samo NATO-a, već i EU-a.

Godine 2004. stručna skupina sastavljena od relevantnih stručnjaka državnog i akademskog sektora, u organizaciji Središnjeg državnog ureda za e-Hrvatsku, započela je izradu

sveobuhvatnog Nacionalnog programa informacijske sigurnosti u Republici Hrvatskoj. Cilj je bio sustavno razraditi potrebne izmjene zakonodavnog i institucionalnog okvira u Republici Hrvatskoj, kako bi se sustav državne uprave u Republici Hrvatskoj kompletno uskladio sa standardima razvijenih demokratskih zemalja, a napose sa zemljama EU-a i članicama NATO-a. Nacionalni program informacijske sigurnosti u Republici Hrvatskoj, nakon javne rasprave, prihvatila je 31. ožujka 2005. Vlada Republike Hrvatske (www.e-hrvatska.hr). Strateški, dugoročni cilj Programa je izgradnja čvrstih temelja za razvoj informacijskog društva u Republici Hrvatskoj (programi EU-a: e-Europe 2005 te i2010, program RH e-Hrvatska 2007), bez čega je upitan gospodarski prosperitet Republike Hrvatske u idućem desetljeću. Taktički, kratkoročno, programom je planiran niz mjera kojima će se postupno, u roku od nekoliko godina, uz najmanje moguće izmjene zakonodavnog i institucionalnog okvira, Republiku Hrvatsku dovesti do suvremenog, međunarodno prihvaćenog koncepta informacijske sigurnosti, kao temelja vlastitog sustava nacionalne sigurnosti, ali i razvoja društva u cjelini. Sukladnost zahtjevima međunarodnih integracijskih procesa u NATO i EU postavljena je kao uvjet u Nacionalnom programu te njegova provedba osigurava Republici Hrvatskoj uređenje nacionalnih pitanja iz područja informacijske sigurnosti na način sukladan NATO i EU zahtjevima.

Nacionalnim programom preporučene su pripremne radnje kao minimalni skup mjera koje je potrebno provesti kako bi Republika Hrvatska uopće mogla započeti prilagodbu međunarodnim zahtjevima, standardima i praksi postupanja u području informacijske sigurnosti. Pripremnim radnjama označeni su međunarodno prihvaćeni standardi koji sve zemlje obvezuju na propisivanje zakonodavnog okvira koji se odnosi na sustavan i unificiran pristup državnoj upravi u cjelini te na određivanje tijela s ovlastima za propisivanje i usmjeravanje sigurnosnih standarda na nacionalnoj razini. U tom smislu pripremne radnje odnose se na odgovarajuće zakonske promjene kojima treba potpuno izmijeniti Zakon o zaštititi tajnosti podataka iz 1996. godine, doraditi Zakon o sigurnosnim službama iz 2002. godine u području informacijske sigurnosti te međusobno uskladiti nove prijedloge zakona koji će činiti budući zakonski sustav informacijske sigurnosti u Republici Hrvatskoj. Predviđeno je da se ovaj novi zakonski sustav sastoji od tri nova zakona: Zakona o tajnosti podataka, Zakona o informacijskoj sigurnosti i već donesenog Zakona o sigurnosno-obavještajnom sustavu Republike Hrvatske (NN79/2006 i NN105/2006).

Zakon o sigurnosno-obavještajnom sustavu Republike Hrvatske, ujednačio je pristup području informacijske sigurnosti unutar sigurnosnog sustava Republike Hrvatske s pristupom koji se planira na nacionalnoj razini te prilagodio ustroj i ovlasti pojedinih tijela sigurnosnog sustava, koja u području informacijske sigurnosti imaju nadležnosti na nacionalnoj razini u Republici Hrvatskoj. To su prvenstveno Ured Vijeća za nacionalnu sigurnost, kao središnje državno tijelo za informacijsku sigurnost, odgovorno za donošenje i usmjeravanje mjera i standarda informacijske sigurnosti i Zavod za sigurnost informacijskih sustava, kao središnje državno tijelo za tehnička područja sigurnosti informacijskog sustava. Tako predradnje, započete Zakonom o sigurnosno-obavještajnom sustavu Republike Hrvatske, trebaju rezultirati potpuno funkcionalnim središnjim državnim tijelima za informacijsku sigurnosti (NSA, NCSA) sa svim potrebnim ovlastima, osobljem te infrastrukturom potrebnom za rad, jer će ta tijela biti pokretač razvoja informacijske sigurnosti, predloženog Konačnim prijedlogom Zakona o informacijskoj sigurnosti.

B) *OSNOVNA PITANJA ČIJE SE UREĐENJE PREDLAŽE OVIM ZAKONOM I POSLJEDICE KOJE PROIZLAZE NJEGOVIM DONOŠENJEM*

Zakon o informacijskoj sigurnosti, kao novina u hrvatskom pravnom poretku, uređuje na cjelovit način područje informacijske sigurnosti u Republici Hrvatskoj kao suštinski dio sustava nacionalne sigurnosti, ali i kao temelj izgradnje suvremenog informacijskog društva. Zakon u cijelosti definira nadležna tijela, njihove međusobne odnose, način i smjer pojedinačnog i zajedničkog funkcioniranja te nadležnosti nadzora. Informacijska sigurnost tako predstavlja stanje odgovarajuće povjerljivosti, cjelovitosti i raspoloživosti podatka, koje se postiže primjenom propisanih mjera i standarda informacijske sigurnosti te odgovarajućom organizacijskom podrškom za poslove planiranja, provedbe, provjere i dorade mjera i standarda.

Pri tome je važno uočiti kako i neklasificirani podaci, čija je uporaba ograničena u službene svrhe, imaju veliku važnost te se i na njih primjenjuje odgovarajući (manji) skup mjera i standarda koje služe očuvanju svojstava privatnosti, cjelovitosti i raspoloživosti podataka koji nisu tajni, ali mogu biti privatni[1]. Mjere i standardi neklasificiranih podataka usklađuju se ovim Zakonom sa prije propisanim mjerama zaštite osobnih podataka građana u Zakonu o zaštiti osobnih podataka (NN 103/03) i pripadnim podzakonskim aktima, čime se postiže učinkovit i ekonomičan koncept informacijske sigurnosti, sukladan konceptima koji se primjenjuju u razvijenim zemljama, a napose u zemljama članicama EU.

Mjere i standardi informacijske sigurnosti razrađuju se kroz podjelu na pet međunarodno prihvaćenih područja informacijske sigurnosti u državnoj upravi: sigurnosna provjera, fizička sigurnost, sigurnost podatka, sigurnost informacijskog sustava i sigurnost poslovne suradnje. Zakon daje temeljna organizacijska i strukovna načela potrebna za daljnju razradu mjera i standarda u okviru područja informacijske sigurnosti. Razrada mjera izvršit će se uredbom Vlade RH u roku od tri mjeseca od donošenja ovog Zakona, a razrada standarda za realizaciju tih mjera izvršit će se pravilnicima središnjih državnih tijela u roku daljnjih šest, odnosno sedam mjeseci. Ukupan rok predviđen za izradu cjelokupnog regulativnog okvira informacijske sigurnosti iznosi oko 12 mjeseci od donošenja ovog Zakona (rok uključuje i prethodnu unutarnju organizaciju središnjih državnih tijela za informacijsku sigurnost i CERT-a). Ovaj Zakon veliku pažnju posvećuje opisanom podzakonskom okviru. Stoga se detaljno razrađuje vrsta i hijerarhija propisa te nadležnost i rokovi njihova donošenja, kako uslijed kompleksnosti i višeslojnosti propisa ne bi došlo do međusobne kolizije ili nedostatka pojedinih propisa. Ovakav pristup je međunarodno pravno prihvaćen i osigurava sustavno uvođenje informacijske sigurnosti od općih prema posebnim propisima, kao i od funkcionalnih prema provedbenim te od organizacijskih prema tehničkim. Na taj način se, između ostalog, osigurava i trajnije prihvaćanje pojedinih općih načela informacijske sigurnosti i njihova što manja ovisnost o tehnološkim i organizacijskim promjenama pojedinih poslovnih procesa koje su česte i neizbježne.

U svrhu pripremanja spomenutih podzakonskih propisa informacijske sigurnosti koji će se primjenjivati u realizaciji propisanih mjera i standarda, prijedlogom Zakona se definiraju tijela koja će imati ovlasti središnjih državnih tijela za informacijsku sigurnost, odgovornih za koordinaciju i usmjeravanje aktivnosti, te donošenje pravilnika sa standardima informacijske sigurnosti. Ovim Zakonom se propisuje da Ured Vijeća za nacionalnu sigurnost (UVNS)

[1] Primjer su javni elektronički servisi državne uprave koji mogu koristiti osobne podatke građana koji se nalaze u okviru nekog državnog tijela, gdje ih je potrebno i adekvatno zaštiti. Ovo se odnosi i na službene podatke u radu državnih tijela koji nisu namijenjeni objavljivanju (primjerice radne inačice različitih prijedloga akata).

postaje središnje državno tijelo za informacijsku sigurnost koje u međunarodno pravnoj nomenklaturi zemalja članica EU-a i NATO-a predstavlja: National Security Authority – NSA, tijelo odgovorno za koordinaciju svih aktivnosti oko primjene i donošenja mjera i standarda informacijske sigurnosti u tijelima iz članka 1. stavak 2. ovog Zakona te za koordinaciju svih drugih tijela koja imaju nadležnost ili sudjeluju u izradi ili provedbi propisa informacijske sigurnosti. Ovim Zakonom se propisuje da Zavod za sigurnost informacijskih sustava (ZSIS) postaje središnje državno tijelo za tehnička područja sigurnosti informacijskog sustava (National Communication Security Authority – NCSA ili Infosec Authority - IA). Zavod djeluje u uskoj koordinaciji s Uredom, kao krovnim tijelom, a osim općih poslova na standardima sigurnosti informacijskog sustava tijela iz članka 1. stavak 2. ovog Zakona, nadležan je i za sigurnosne akreditacije klasificiranih informacijskih sustava (Security Accreditation Authority - SAA), za upravljanje kriptomaterijalima (National Distribution Authority – NDA) te za poslove tijela za odgovornog za prevenciju i odgovor na računalne ugroze sigurnosti u privatnom[2] informacijskom sustavu državne uprave (CERT - Computer Emergency Response Team).

Kako bi se potrebna pažnja posvetila prevenciji i otklanjanju sigurnosnih problema vezanih uz sigurnost javnih informacijskih sustava u Republici Hrvatskoj, koji se nužno koriste i u realizaciji državnih informacijskih sustava te omogućila učinkovita međunarodna suradnja Republike Hrvatske u ovom području, zakonskim Prijedlogom osniva se nacionalni CERT[3]. Pored uključenja u EU, NATO i međunarodnu mrežu CERT-ova, CERT bi djelovao u uskoj koordinaciji sa središnjim državnim tijelima za informacijsku sigurnost na problematici prevencije i odgovora na računalne ugroze sigurnosti javnih i privatnih informacijskih sustava državne uprave RH. Kao javna ustanova, organizirana na temeljima postojećeg, međunarodno afirmiranog akademskog CERT-a koji je sastavni dio Hrvatske akademske i istraživačke mreže – CARNet, nacionalni CERT će biti ključna institucija za promoviranje informacijske sigurnosti u najširim društvenim slojevima Republike Hrvatske, ali i međunarodnim okvirima.

Jedan od najvažnijih zadataka informacijske sigurnosti je osiguravanje sustavne primjene mjera u okviru informatizacije državne uprave i javnog sektora u širem smislu. Za razliku od privatnog sektora, gdje se mjere informacijske sigurnosti trebaju promovirati i poticati u svrhu preventive i zaštite građanstva i gospodarstva, ovdje se radi o propisivanju i provedbi obvezujućih propisa u tijelima iz članka 1. stavak 2. i 3. ovog Zakona. Stoga je nužno zakonom propisati koncept provedbe mjera i standarda informacijske sigurnosti koji će, između ostalog, osigurati sustavnu informatizaciju državne uprave, u okviru koje će mjere informacijske sigurnosti biti planirane i primijenjene na propisani način. Ovim Zakonom je propisan međunarodno prihvaćen način kojim se definiraju nadležna središnja tijela za potporu u poslovima planiranja i implementacije informacijskih sustava (CIS[4] Planning and Implementation), koja ove poslove obavljaju u tijelima iz članka 1. stavak 2. ovog Zakona, koja nemaju primjerene vlastite stručne potencijale za planiranje i implementaciju. Središnje tijelo za ove poslove u Republici Hrvatskoj je Središnji državni ured za e-Hrvatsku (SDUeH), nadležan za razvitak informacijskog sustava državne uprave, dok u okviru obrazovnog i

---

[2] Izgradnja zaštićene privatne informacijske infrastrukture (državne!) jedna je od obveza RH u okviru pristupanja EU sukladno Zakonu o potvrđivanju Memoranduma o razumijevanju između RH i EU o sudjelovanju RH u programu IDABC, NN, Međunarodni ugovori br. 2, 28.02.2007 (IDABC program EU-a, inf. mreža TESTA)

[3] Naziv CERT, iako izvorno potječe od kratice engleskog jezika Computer Emergency Response Team, danas je međunarodno priznat kao naziv ove vrste poslova i upotrebljava se u nacionalnim nazivima tijela koja imaju ovlasti ove vrste u nacionalnim okvirima (EU, Austrija, Grčka, Malta, Italija, Švicarska, Portugal, Njemačka, Švedska, ...). Ovaj naziv je uvriježen i u RH jer je već niz godina u upotrebi kao CARNet CERT, koji bi ovim zakonskim Prijedlogom trebao iz akademskog prerasti u nacionalni CERT.

[4] Communication and Information Systems – CIS, komunikacijski i informacijski sustavi

akademskog sektora ove poslove provodi Ministarstvo znanosti, obrazovanja i športa. Oba nadležna tijela za izvršenje ovih poslova mogu koristiti druga izvršna tijela i tvrtke čiji će rad koordinirati i usklađivati sa zakonskim obvezama u području informacijske sigurnosti.

Kako bi se osigurao stalni ciklus planiranja, provođenja, provjere i dorade (PDCA[5]), organizacijski se mora uključiti element nadzora informacijske sigurnosti. Ovaj Zakon propisuje organizacijski model koji je usklađen sa zahtjevima EU-a i NATO-a. U tijelima i pravnim osobama iz članka 1. stavak 2. ovog Zakona propisuje se obveza postavljanja savjetnika za informacijsku sigurnost, koji mogu biti centralni (CISO[6]), za više tijela, ili lokalni (LISO[7]). Ove koordinatore će imenovati sama tijela, ali prema uvjetima koji se određuju na nacionalnoj razini, pravilnikom Ureda Vijeća za nacionalnu sigurnost, koji je nadležan za stručno usmjeravanje i praćenje rada ovih savjetnika. Poslovi koje obavljaju savjetnici za informacijsku sigurnost, poslovi su nadzora organizacije, implementacije i učinkovitosti propisanih mjera u okviru pet područja informacijske sigurnosti u tijelima i pravnim osobama iz članka 1. stavak 2. ovog Zakona, te izvještavanje čelnika tijela i središnjeg državnog tijela za informacijsku sigurnost, o stanju i učinkovitosti primijenjenih mjera i standarda te o mogućim poboljšanjima istih. Smisao nadzora informacijske sigurnosti prvenstveno je u stalnom usmjeravanju propisanih i primijenjenih mjera i standarda informacijske sigurnosti te koordinaciji rada i ispomoći stručnog i sigurnosnog osoblja u samim tijelima iz članka 1. stavak 2. ovog Zakona, zaduženog za održavanje i administriranje organizacijskih i tehničkih mjera i sustava realiziranih u određenom tijelu. U tom smislu, nadzor se obavlja u unaprijed planiranim terminima, a o rezultatima nadzora donosi se izvješće koje se dostavlja čelniku tijela te središnjem državnom tijelu za informacijsku sigurnost. Središnje državno tijelo za informacijsku sigurnost (UVNS), uz pomoć tijela za tehnička područja sigurnosti informacijskog sustava (ZSIS), savjetnika za informacijsku sigurnost te tijela za planiranje i implementaciju, zaduženo je za koordinaciju postupka otklanjanja nepravilnosti ili nedostatnosti u provedbi mjera ili u nadležnoj regulativi. Čelnici tijela i pravnih osoba odgovorni su za otklanjanje utvrđenih nedostataka u području svoje nadležnosti. U slučaju utvrđenih nepravilnosti na klasificiranom informacijskom sustavu za koji je provedena sigurnosna akreditacija, ZSIS u suradnji s UVNS-om, ovisno o vrsti nepravilnosti, utvrđuje daljnju valjanost akreditacije. U tom smislu naglašavamo da nema posebnih rokova za provedbu sigurnosne akreditacije već se u informacijskom sustavu podaci utvrđenih razina niti ne mogu početi obrađivati, pohranjivati ili prenositi, ako prethodno nije provedena sigurnosna akreditacija tog informacijskog sustava. Stoga je sigurnosna akreditacija, kao i općenito svaka druga vrsta akreditacije, u stvari dozvola za korištenje klasificiranih podataka stupnjeva tajnosti „Povjerljivo", „Tajno" i „Vrlo tajno" u određenom informacijskom sustavu.

Drugim riječima, ovim Zakonom propisuju se:

- mjere i standardi informacijske sigurnosti te područja informacijske sigurnosti (sigurnosna provjera, fizička sigurnost, sigurnost podatka, sigurnost informacijskog sustava i sigurnost poslovne suradnje), te se dalje razrađuju podzakonskim aktima (uredbe Vlade RH, pravilnici Središnjih državnih tijela za informacijsku sigurnost)
- poslovi i ovlasti središnjih državnih tijela za informacijsku sigurnost (Ured Vijeća za nacionalnu sigurnost, Zavod za sigurnost informacijskih sustava),

[5] Plan, Do, Check, Act – PDCA, stalni ciklus planiranja, provođenja, provjere i dorade određenih standarda
[6] Central Information Security Officer
[7] Local Information Security Officer

- osnivanje tijela za prevenciju i odgovor na računalne ugroze sigurnosti javnih informacijskih sustava u RH (nacionalni CERT) te način upravljanja i njegova koordinacija sa središnjim državnim tijelima za informacijsku sigurnost,
- koncept provedbe informacijske sigurnosti,
- koncept nadzora informacijske sigurnosti.

Donošenjem predloženog Zakona u sustav državne uprave uvode se nove vrste tijela – središnja državna tijela za informacijsku sigurnost, čije ovlasti preuzimaju Ured Vijeća za nacionalnu sigurnost, kao krovno koordinacijsko tijelo, te Zavod za sigurnost informacijskih sustava, kao specijalizirano pomoćno tijelo za tehnička područja sigurnosti informacijskog sustava. Kako bi ova tijela mogla obavljati propisane poslove predlaganja akata i donošenja odgovarajućih pravilnika za primjenu u tijelima iz članka 1. stavak 2. ovog Zakona, potrebno je provesti izmjene i dopune Zakona o sustavu državne uprave, po uzoru na promjene koje su provedene u prosincu 2003. godine, tijekom uvođenja središnjih državnih ureda u sustav državne uprave (NN 199/2003).

Donošenjem ovog Zakona cjelovito će se urediti potpuno novo područje u Republici Hrvatskoj. Nadležna tijela u području informacijske sigurnosti u Republici Hrvatskoj predstavljaju središnja državna tijela za informacijsku sigurnost: Ured Vijeća za nacionalnu sigurnost (UVNS) i Zavod za sigurnost informacijskih sustava (ZSIS), kao okosnica i ključna tijela, zatim Nacionalni CERT u okviru Hrvatske akademske i istraživačke mreže (CARNet), kao tijelo nadležno za prevenciju i odgovor na računalne ugroze sigurnosti javnih informacijskih sustava u RH, Središnji državni ured za e-Hrvatsku i Ministarstvo znanosti, obrazovanja i športa, kao središnja tijela za planiranje i implementaciju propisanih mjera i standarda informacijske sigurnosti u državnom, odnosno obrazovnom i akademskom sektoru te savjetnici za informacijsku sigurnost u svojstvu nadzora primijenjenih mjera i standarda informacijske sigurnosti u tijelima iz članka 1. stavak 2. ovog Zakona.

Zakonom se, pored redovitog nadzora informacijske sigurnosti, kojim se osigurava stalni ciklus planiranja, provođenja, provjere i dorade (PDCA) propisa i stanja informacijske sigurnosti u tijelima, po prvi puta uvodi i proces sigurnosne akreditacije klasificiranih[8] informacijskih sustava tijela iz članka 1. stavak 2. ovog Zakona. Ovakav pristup dugoročno će iznimno povoljno utjecati na bolje planiranje i sustavniju provedbu projekata u tijelima iz članka 1. stavak 2. ovog Zakona, kako u području informatizacije, tako i u području adaptacije i izgradnje objekata. Tu se primarno misli na uvođenje dodatnih kriterija u nabavi i projektiranju, kriterija koji prate ne samo sigurnosne aspekte uporabe različitih uređaja i sustava te korištenja vanjskih usluga, već prije svega mjerila kvalitete i pouzdanosti uređaja i sustava tijekom njihova životnog ciklusa. U tom smislu, utjecaj mjera i standarda informacijske sigurnosti na troškove informatizacije, adaptacije ili izgradnje objekata ne treba promatrati odvojeno od same funkcionalnosti sustava, objekata, procesa ili osoba na koje se odnose, jer te mjere i standardi predstavljaju nužan uvjet realizacije pojedinih projekata i poslovnih procesa.

Sadržaj mjera i standarda informacijske sigurnosti ovisi o tome da li se u tijelu koriste klasificirani ili neklasificirani podaci te o tome koja je razina tajnosti klasificiranih podataka. Sadržaj ovisi i o broju te o vrsti zapisa klasificiranih i neklasificiranih podataka, ali i o ugrozama na određenoj lokaciji. U tom smislu sadržaj mjera i standarda informacijske sigurnosti može biti bitno različit u nekim tijelima, no za grupe istovrsnih tijela mogu se očekivati vrlo slična rješenja obzirom da je korištenje klasificiranih i neklasificiranih

[8] Samo za tri viša stupnja tajnosti: „Povjerljivo, „Tajno“ i „Vrlo tajno“

podataka u sličnom djelokrugu također međusobno slično (odstupanja mogu biti u karakteristikama objekata ili primjerice različitoj razini informatiziranosti dvaju tijela sličnog djelokruga).

Prijedlog Zakona uređuje područje informacijske sigurnosti u Republici Hrvatskoj u skladu sa stvarnim i predviđenim potrebama Republike Hrvatske, kako u području vlastite nacionalne sigurnosti i razvoja informacijskog društva, tako i u skladu sa zahtjevima međunarodnih integracijskih procesa, odnosno sukladnosti sa sigurnosnim politikama NATO-a i EU-a, prihvaćenih u okviru sigurnosnih sporazuma[9]. U metodološkom smislu ovaj Zakon koncipira sustav instrumenata raspoloživih u sustavima informacijske sigurnosti zemalja EU-a i NATO-a te je optimiziran sa stajališta potreba Republike Hrvatske. Prijedlog u potpunosti slijedi strukovne potrebe i zahtjeve za učinkovitošću mjera i standarda informacijske sigurnosti u uvjetima naraslih i izmijenjenih prijetnji i izazova uslijed tehnološke i informacijske revolucije. Nužnost različitih oblika državnih ili vojnih integracija, međunarodne suradnje na suzbijanju ugroza kao što su organizirani kriminal ili terorizam, pa do različitih pojavnih oblika računalnog i kibernetičkog kriminala kojima smo već sada okruženi, traži uvođenje minimalnih sigurnosnih zahtjeva informacijske sigurnosti u svakoj državi koja želi participirati u međunarodnoj zajednici te osposobljenu i međunarodno usklađenu nacionalnu organizaciju nadležnih tijela, koja će takve minimalne zahtjeve ne samo uspostaviti već i trajno održavati.

Propisivanjem sustava informacijske sigurnosti sa širokim zahvatom u tijela i pravne osobe iz članka 1. stavak 2. ovog Zakona te dobrom koordinacijom središnjih državnih tijela za informacijsku sigurnost i nacionalnog CERT-a nadležnog za javne informacijske sustave u Republici Hrvatskoj, osigurava se temelj za daljnje poticanje informacijske sigurnosti u cjelokupnom društvu kroz procese normizacije u Republici Hrvatskoj i javno-privatnog partnerstva. Na taj se način osiguravaju preduvjeti za strateški nacionalni interes stvaranja informacijskog društva.

Stoga se zaključno može reći da je temeljni cilj Zakona o informacijskoj sigurnosti zaštita klasificiranih i neklasificiranih podataka u tijelima i pravnim osobama iz članka 1. stavka 2. i 3. ovog Zakona, koja se osigurava utvrđivanjem i provođenjem mjera i standarda informacijske sigurnosti u okviru područja informacijske sigurnosti.

Strateške mjere, za koje se ovim Zakonom otvara prostor, za društvo su još važnije i obuhvaćaju podizanje sigurnosne edukacije u državnom sektoru, ali i šire, suradnju državnog i akademskog sektora u razvoju područja informacijske sigurnosti, poticanje procesa nacionalne normizacije, poticanje sektorskih mjera informacijske sigurnosti u gospodarstvu, te, kao najvažnije, stvaranje temelja za razvoj informacijskog društva u Republici Hrvatskoj. Ove temelje čine sigurnosna edukacija i razvoj svijesti o sigurnosti u najširim slojevima društva te stvaranje povjerenja građana i poslovnog sektora u elektroničku javnu upravu, javne informacijske sustave i jedinstveni informacijski prostor, kao nedjeljive sastavnice informacijskog društva nužne za razvoj tržišta, ali i rast i zapošljavanje u ovom propulzivnom segmentu društva danas.

---

[9] Zakon o potvrđivanju ugovora između Republike Hrvatske i Europske Unije o sigurnosnim postupcima za razmjenu tajnih podataka, NN Međunarodni ugovori 9/2006, 3. 10. 2006.
Zakon o potvrđivanju sporazuma o sigurnosti između Republike Hrvatske i Organizacije sjevernoatlantskog ugovora, NN Međunarodni ugovori 7/2003, 23. 07. 2003.

III. OBJAŠNJENJE POJEDINIH ODREDBI

I. OSNOVNE ODREDBE

Prijedlogom nacrta Zakona o informacijskoj sigurnosti uvodi se i regulira područje informacijske sigurnosti u Republici Hrvatskoj. U članku 1. određuje se djelokrug primjene Zakona na državna tijela, tijela jedinica lokalne i područne (regionalne) samouprave te pravne osobe s javnim ovlastima. Zakon se primjenjuje i na pravne i fizičke osobe koje ostvare pristup ili postupaju s klasificiranim i neklasificiranim podacima. U članku 2. definiraju se pojam informacijske sigurnosti, mjere i standardi te područja informacijske sigurnosti, kao i sigurnosna akreditacija informacijskog sustava. Informacijska sigurnost tako u smislu ovog Zakona predstavlja stanje odgovarajuće povjerljivosti, cjelovitosti i raspoloživosti podataka, koje se postiže primjenom propisanih mjera i standarda informacijske sigurnosti te odgovarajućom organizacijskom podrškom za poslove planiranja, provedbe, provjere i dorade mjera i standarda. Uvodi se pojam područja informacijske sigurnosti, u svrhu stvaranja sustavnih i međusobno koordiniranih područja u okviru kojih se utvrđuju propisane mjere i standardi s ciljem zaštite klasificiranih i/ili neklasificiranih podataka. Drugi pojmovi koji se koriste u ovom Zakonu definirani su u Zakonu o tajnosti podataka, kao temeljnom zakonu koji se bavi podacima (klasificirani i neklasificirani podatak, stupnjevi tajnosti i sl.).

II. MJERE I STANDARDI INFORMACIJSKE SIGURNOSTI

Člankom 3. definira se svrha donošenja mjera i standarda informacijske sigurnosti, a to je utvrđivanje minimalnih sigurnosnih kriterija za zaštitu klasificiranih i neklasificiranih podataka u tijelima i pravnim osobama iz članka 1. stavka 2. i 3. ovog Zakona. Člancima 4. do 6. utvrđuju se okviri i temeljna načela za razradu mjera i standarda informacijske sigurnosti koji će se propisati podzakonskim aktima. Mjere i standardi utvrđuju se primarno za klasificirane i neklasificirane podatke, ali ovise i o čimbenicima kao što su broj podataka, vrsta podataka (oblik zapisa), odnosno ugroze na određenoj lokaciji (članak 4.). Mjere i standardi razrađuju se tako da obuhvaćaju procedure nadzora pristupa i postupanja s klasificiranim podacima, postupanje prilikom kompromitiranja klasificiranih podataka, planiranje mjera prilikom izvanrednih situacija, te ustrojavanje posebnih fondova za nacionalne i međunarodne klasificirane podatke (članak 5.). Mjere i standardi informacijske sigurnosti za zaštitu neklasificiranih podataka sukladne su zakonom propisanoj zaštiti osobnih podataka građana (članak 6. stavak 1.) te se na taj način realizacijom istih mjera i standarda ostvaruju uvjeti za korištenje neklasificiranih i osobnih podataka građana, što je nužnost praktično u svakom tijelu i pravnoj osobi iz članka 1. stavka 2. i 3. ovog Zakona. Nadalje, u članku 6. stavak 2., omogućava se ostvarivanje uvjeta za korištenje klasificiranih podataka stupnja tajnosti „Ograničeno“ na temelju istih mjera koje važe za neklasificirane podatke, uz dodatnu provjeru primijenjenih mjera i standarda te primjenu dodatno propisanih mjera i standarda za ovaj stupanj tajnosti. Člankom 7. utvrđuju se nadležna tijela (Vlada RH i središnja državna tijela za informacijsku sigurnost – UVNS i ZSIS) i akti (uredba i pravilnici) kojima će se razraditi mjere i standardi informacijske sigurnosti.

III. PODRUČJA INFORMACIJSKE SIGURNOSTI

Člankom 8. utvrđuju se i definiraju područja informacijske sigurnosti. U člancima 9. do 13. za svako područje informacijske sigurnosti definiraju se temeljni okviri mjera i standarda koji obvezuju tijela i pravne osobe iz članka 1. stavka 2. i 3. ovog Zakona. Sigurnosna provjera temelji se na odredbama Zakona o tajnosti podataka i Zakona o sigurnosno-obavještajnom sustavu, te se u ovom Zakonu i podzakonskim aktima primarno definiraju organizacijske i tehničke obveze tijela i pravnih osoba iz članka 1. stavka 2. Fizička sigurnost u članku 10. definira osnovni zahtjev za kategorizaciju objekata i prostora na sigurnosne zone, ovisno o tome koja vrsta podataka se koristi. Podzakonskim aktima će se razraditi mjere i standardi koji će se morati primjenjivati u pojedinoj kategoriji sigurnosne zone. Sigurnost podatka u članku 11. uvodi tijelima i pravnim osobama iz članka 1. stavka 2. ovog Zakona obvezu upravljanja podacima u svojoj nadležnosti. Razrada mjera i standarda informacijske sigurnosti za ovo područje bit će u skladu sa odredbama Zakona o tajnosti podataka te Zakona o zaštiti osobnih podataka, kao zakona koji uređuju postupanje sa klasificiranim, neklasificiranim i osobnim podacima građana te će biti postavljena u okvire ovog područja informacijske sigurnosti i okvire zahtjeva za mjere i standarde definirane ovim Zakonom. Sigurnost informacijskih sustava u članku 12. uvodi u okviru ovog područja načela kao što su sigurnosna akreditacija informacijskog sustava, certificiranje informatičko-tehničkog osoblja, fizičku zaštitu te registar certificirane opreme i uređaja za klasificirane informacijske sustave. Sigurnost poslovne suradnje u članku 13. prati koncept certifikacije osoba za pristup klasificiranim podacima, koji je propisan u Zakonu o tajnosti podataka, te utvrđuje obvezu izdavanja certifikata poslovne suradnje za pravne i fizičke osobe, kao i procedure koje se provode za slučajeve u kojima su ovi certifikati potrebni (informacijska sigurnost u RH i učestvovanje tvrtki registriranih u RH na međunarodnim klasificiranim projektima i natječajima). Razrada podzakonskih akata za sva područja informacijske sigurnosti temeljit će se na načelima uvedenim u poglavljima II. i III.

IV. SREDIŠNJA DRŽAVNA TIJELA ZA INFORMACIJSKU SIGURNOST

U člancima 14. do 16. određuju se nadležnosti UVNS-a kao središnjeg državnog tijela za informacijsku sigurnost (hrvatski NSA – National Security Authority) koje je odgovorno za usklađivanje aktivnosti donošenja i primjene mjera i standarda informacijske sigurnosti u tijelima iz članka 1. stavak 2. i 3. ovog Zakona, kao i za usklađenost aktivnosti oko primjene mjera i standarda informacijske sigurnosti u razmjeni klasificiranih podataka između RH i stranih zemalja i organizacija. Tako se člankom 15. stavkom 1. propisuje da UVNS donosi pravilnike iz područja informacijske sigurnosti. Također se člankom 15. stavak 2. definira odnos prema nacionalnom normizacijskom procesu, a člankom 16. se utvrđuje UVNS kao krovno tijelo nadležno za koordinaciju aktivnosti donošenja i primjene mjera i standarda u svim područjima informacijske sigurnosti i koordinaciju drugih tijela s određenim nadležnostima u okviru informacijske sigurnosti.

U člancima 17. do 19. određuju se nadležnosti ZSIS-a kao središnjeg državnog tijela za tehnička područja sigurnosti informacijskih sustava (hrvatski NCSA – National Communications Security Authority), koje djeluje u koordinaciji s UVNS-om (NSA) i koje skrbi o standardima sigurnosti informacijskih sustava tijela i pravnih osoba iz članka 1. stavak 2. ovog Zakona, sigurnosnim akreditacijama informacijskih sustava, upravljanju kriptomaterijalima, kao i o koordinaciji prevencije i odgovora na računalne ugroze sigurnosti informacijskih sustava u tijelima i pravnim osobama iz članka 1. stavak 2. ovog Zakona. Tako

se člankom 18. stavkom 1. propisuje da ZSIS donosi pravilnik kojim regulira standarde tehničkih područja sigurnosti informacijskih sustava. Također se člankom 18. stavkom 2. i člankom 19. definira odnos prema nacionalnom normizacijskom i akreditacijskom procesu te utvrđuje nadležnost ZSIS-a za poslove sigurnosnih akreditacija klasificiranih informacijskih sustava (nacionalni SAA – Security Accreditation Authority), što obavlja u suradnji s krovnim tijelom - UVNS-om.

V. NACIONALNI CERT

U člancima 20. do 22. CARNet-u se proširuju ovlasti i time se definira nova nacionalna funkcionalnost za prevenciju i odgovor na računalne ugroze javnih informacijskih sustava u RH (u daljnjem tekstu CERT). CERT se kao zasebna ustrojstvena jedinica ustrojava u Hrvatskoj akademskoj i istraživačkoj mreži (u daljnjem tekstu CARNet). Člankom 21. se utvrđuje potrebna koordinacija CERT-a i ZSIS-a u području sigurnosti informacijskih sustava i normizaciji ovog područja u RH, a u članku 22. definirana je razrada poslova CERT-a i postavljanje čelnog čovjeka, čime se osigurava međusobna usklađenost rada nacionalnog CERT-a i središnjih državnih tijela za informacijsku sigurnost UVNS-a i ZSIS-a.

VI. PROVEDBA INFORMACIJSKE SIGURNOSTI

Člankom 23. propisuje se obveza provođenja propisanih standarda informacijske sigurnosti temeljem uredbe Vlade RH koja utvrđuje mjere informacijske sigurnosti i pravilnika kojima se razrađuju standardi za provođenje mjera, a koje donose UVNS i ZSIS. U članku 23. stavku 2. definira se da u tijelima i pravnim osobama iz članka 1. stavak 2. ovog Zakona, koja nemaju odgovarajuće informatičke i tehničke mogućnosti, nadležnost za poslove provedbe sigurnosti informacijskih sustava ima Središnji državni ured za e-Hrvatsku, dok u području obrazovnog i akademskog sektora nadležnost za poslove provedbe informacijske sigurnosti ima Ministarstvo znanosti, obrazovanja i športa. Člankom 24. utvrđuje se obaveza tijela za donošenje pravilnika kojim će utvrditi provedbu mjera i standarda informacijske sigurnosti u svojoj nadležnosti, kao i obveza središnjih tijela državne uprave za donošenjem pravilnika o načinu provedbe mjera i standarda informacijske sigurnosti u drugim tijelima.

VII. NADZOR INFORMACIJSKE SIGURNOSTI

Člankom 25. definiran je nadzor informacijske sigurnosti koji se provodi u tijelima i pravnim osobama iz članka 1. stavak 2. ovog Zakona, kao nadzor organizacije, provedbe i učinkovitosti propisanih mjera i standarda (stavak 1.). Poslove nadzora provode savjetnici informacijske sigurnosti u tim tijelima i pravnim osobama (stavak 2.). U članku 26. stavcima 1., 2. i 3. utvrđuje se način izvješćivanja, odgovornosti i postupanje vezano za rezultate nadzora.

VIII. PRIJELAZNE I ZAVRŠNE ODREDBE

Prijelaznim i završnim odredbama u člancima 27. do 30. definira se dinamika donošenja regulativnog okvira informacijske sigurnosti propisanog Zakonom. Potrebno je napomenuti da je dužina rokova za razradu regulativnog okvira informacijske sigurnosti (ukupno 7 mjeseci) uvjetovana činjenicom da se radi o potpuno novom području u RH za koji je

potrebno međusobno koordinirati zajednički rad čitavog niza tijela koja do sada nisu postojala ili nisu obavljala ove poslove na nacionalnoj razini. Članak 27. propisuje rok od tri mjeseca za donošenje uredbe Vlade RH o mjerama informacijske sigurnosti iz članka 7. Članak 28. propisuje rok od šest mjeseci za donošenje pravilnika UVNS-a iz članka 15. stavka 1. (stavak 1.) te isti rok za pravilnik iz članka 25. stavka 3. U članku 28. stavku 3. propisuje se rok od 30 dana nakon donošenja pravilnika UVNS-a, za donošenje pravilnika ZSIS-a (ukupno sedam mjeseci od donošenja Zakona). Članak 29. propisuje u stavku 1. rok od tri mjeseca za izmjenu statuta CARNet-a u poslovima CERT-a. U članku 29. stavku 2. propisuje se tijelima i pravnim osobama, rok od tri mjeseca nakon donošenja pravilnika iz članka 28. stavka 1., za donošenje pravilnika o provedbi mjera i standarda informacijske sigurnosti u okviru svoje nadležnosti, odnosno u članku 28. stavku 2. propisuje isti rok središnjim tijelima državne uprave (SDUeH i MZOŠ) za pravilnik za provedbu mjera i standarda informacijske sigurnosti u drugim tijelima.

IV. OCJENA POTREBNIH SREDSTAVA ZA PROVOĐENJE ZAKONA

Ocjenjuje se da donošenje i provedba ovog Zakona neće zahtijevati osiguravanje dodatnih sredstava u Državnom proračunu Republike Hrvatske.

Zakonom o sigurnosno-obavještajnom sustavu Republike Hrvatske predviđeno je osnivanje Zavoda za sigurnost informacijskih sustava (ZSIS) kao pravnog sljednika Zavoda za informacijsku sigurnost i kripto-zaštitnu tehnologiju, a Ured Vijeća za nacionalnu sigurnost postojeća je institucija, čije su nadležnosti iz Zakona o informacijskoj sigurnosti usklađene s novim Zakonom o sigurnosno-obavještajnom sustavu Republike Hrvatske (NN 79/06).

Jedino novo tijelo je Nacionalni CERT, koji je nova ustrojstvena jedinica postojeće ustanove Hrvatske akademske i istraživačke mreže (CARNet) i koji će se temeljiti na radu akademskog CERT-a koji postoji već niz godina. CARNet je proračunski u nadležnosti Ministarstva znanosti, obrazovanja i športa, s kojim je usuglašena potrebna promjena statuta, slijedom koje su planirani dodatni troškovi uslijed proširenja broja djelatnika i djelokruga poslova postojećeg CARNet-ovog CERT-a. Ovi troškovi su planirani u Državnom proračunu za 2007. godinu pod stavkom 080 75 – 1444 – A628063 REDOVNA DJELATNOST NACIONALNOG CERTA, 1.530667 kn, te stavkom 080 75 – 1444 – K628066 NACIONALNI CERT – ZAJEDNIČKA RK INFRASTRUKTURA, 1.850.000 kn.

V. RAZLIKE IZMEĐU RJEŠENJA KOJA SE PREDLAŽU U ODNOSU NA PRIJEDLOG ZAKONA I RAZLOZI ZBOG KOJIH SU RAZLIKE NASTALE

Na temelju ocjena koje su na tekst prvog prijedloga Zakona iznesene na saborskim odborima te potom u prvom čitanju na saborskoj raspravi, napravljena je analiza iznesenih ocjena, odnosno primjedbi i sugestija, te su gotovo sve prihvaćene i ugrađene u konačni prijedlog Zakona.

U skladu s primjedbama iznesenim u raspravama zastupnika Nenada Stazića, Antuna Kapraljevića i Ingrid Antičević Marinović na nejasnu terminologiju koja se koristi i koja dovodi do nerazumljivosti Zakona, izvršene su značajne korekcije u terminologiji koja se upotrebljava u konačnom prijedlogu Zakona, a cijeli tekst konačnog prijedloga Zakona je dodatno nomotehnički dorađen. Naslov je zbog razumljivosti korigiran u „Zakon o informacijskoj sigurnosti" kako bi se jasno odredila razlika između općeg područja informacijske sigurnosti koje se odnosi na ljude, organizaciju i tehnologiju i tehničkog pojma informacijskog sustava. Temeljem ovih primjedbi izvršene su i značajne korekcije pojmovnika u članku 2., gdje su definicije pročišćene i složene slijedom toga kako se uvode u tekstu konačnog prijedloga Zakona. Jasnoći konačnog teksta doprinose i dva potpuno nova poglavlja: II. Mjere i standardi informacijske sigurnosti i III. Područja informacijske sigurnosti.

Prihvaćene su primjedbe Odbora za ljudska prava i prava nacionalnih manjina, te zastupnika dr.sc. Zlatka Kramarića i Dorotee Pešić Bukovac vezane za Nacionalnu politiku informacijske sigurnosti da bi bilo primjerenije da je donesena prije ovog Zakona. U konačnom tekstu zakona stoga se odustalo od propisivanja donošenja Nacionalne politike informacijske sigurnosti kao posebnog akta te su umjesto toga u konačni prijedlog Zakona ugrađena dva nova poglavlja: II. Mjere i standardi informacijske sigurnosti i III. Područja informacijske sigurnosti. Slijedom novog dijela teksta konačnog prijedloga Zakona i ostale odredbe Zakona prilagođene su i dobile su dodatnu jasnoću, obzirom na sadržaje koji su sada uključeni u Zakon, a koji su trebali biti razrađeni u Nacionalnoj politici informacijske sigurnosti kao zasebnom dokumentu. Ovakvim pristupom postiglo se i bitno skraćivanje rokova za izradu podzakonskih akata, dok su opći strateški ciljevi i koncepcija ostali nepromijenjeni, jer ih u stvari definira Nacionalni program informacijske sigurnosti koji je prošao javnu raspravu i usvojen je na Vladi RH u ožujku 2005. godine.

Usvojene su primjedbe na tragu rasprave i zaključaka Odbora za ljudska prava i prava nacionalnih manjina, te zastupnika Pere Kovačevića, Ante Markova, Dorotee Pešić Bukovac i dr. sc. Zlatka Kramarića o predugim rokovima i nedostatnoj sadržajnosti Zakona. U konačni prijedlog Zakona u tom smislu ugrađena su već spomenuta dva nova poglavlja: II. Mjere i standardi informacijske sigurnosti i III. Područja informacijske sigurnosti, te je redefiniran koncept podzakonskih propisa (članci 7., 15., 18. i 28.), čime se u konačnom prijedlogu Zakona daje jasan opis sadržaja koji će se razrađivati podzakonskim aktima, bolja struktura, nazivi i opisi tih akata, te kao najvažnije značajno skraćeni rokovi za donošenje podzakonskih akata. Tako je, temeljem ovih izmjena u konačnom prijedlogu Zakona (prvenstveno dodavanjem sadržaja u poglavljima II. i III., izrada cjelokupnog regulativnog okvira skraćena gotovo dvostruko, odnosno na 7 mjeseci od dana donošenja ovog Zakona. Uzimajući u obzir čitav niz problema opisanih u obrazloženju ovog Zakona, a koji se svode na to da u području koje pokrivaju Zakon o tajnosti podataka i Zakon o informacijskoj sigurnosti, RH kasni u odnosu na razvijene zemlje 20-tak godina, daljnje skraćivanje rokova nije realno.

Prihvaćene su primjedbe zastupnice Dorotee Pešić Bukovac da se poslovi provedbe informacijske sigurnosti ne mogu zakonom dodjeljivati državnim tvrtkama (FINA, APIS), te primjedbe na tragu rasprave zastupnika Ante Markova o potrebi veće suradnje državnog i gospodarskog sektora. Stoga je predmetni stavak izostavljen u konačnom prijedlogu Zakona u novom članku 23., jer Zakon već propisuje područje informacijske sigurnosti „Sigurnost poslovne suradnje", u okviru kojeg će se, između ostalog, definirati i uvjeti za poslove provedbe informacijske sigurnosti koje mogu obavljati sve pravne i fizičke osobe na tržištu koje takve uvjete zadovolje.

Usvojene su primjedbe Odbora za informiranje, informatizaciju i medije, te primjedbe iznesene u raspravi zastupnika Nenada Stazića i Ingrid Antičević Marinović o neprihvatljivom i nepotrebnom konceptu nadzora informacijske sigurnosti u koji su uključene i sigurnosno-obavještajne službe. Sukladno tome, u konačnom prijedlogu Zakona prihvaćen je model koji se temelji isključivo na osobama koje su zaposlenici samih tijela i pravnih osoba (savjetnici za informacijsku sigurnost) i koje stručno usmjerava UVNS kao središnje državno tijelo za informacijsku sigurnost. Ovaj model je preuzet od EU, a nakon dodatnih konzultacija s NATO-om koje su u međuvremenu obavljene, usvojen je kao jedinstven za sva tijela (članci 25. i 26.).

Prihvaćene su primjedbe na strukturu Zakona i da je nejasno propisan obuhvat primjene informacijske sigurnosti iz rasprave zastupnika Nenada Stazića te su u tekstu konačnog prijedloga Zakona uvedena dva potpuno nova poglavlja: II. Mjere i standardi informacijske sigurnosti i III. Područja informacijske sigurnosti, u okviru kojih se uvodi jasno tumačenje po kojem obuhvat primjene mjera i standarda informacijske sigurnosti ovisi prvenstveno o vrsti (klasificirani ili neklasificirani) i stupnju tajnosti podatka. U članku 4. razrađena su i dodatna načela za obuhvat primjene mjera i standarda informacijske sigurnosti.

Djelomično je prihvaćen prijedlog zastupnika Stazića da strukturu Zakona treba podijeliti prema grupama tijela ovisno o pripadnosti pojedinom stupu ili razini vlasti iako je ovakvo razmišljanje o dosegu mjera i standarda prihvatljivo i proizlazi iz Nacionalnog programa informacijske sigurnosti. U tom smislu konačan prijedlog Zakona uvodi jasno tumačenje po kojem obuhvat primjene mjera i standarda informacijske sigurnosti ovisi o vrsti i stupnju tajnosti podatka. Ovakav pristup je standardan za zemlje članice EU-a i NATO-a, a iz njega na određeni način prirodno proizlazi i to da određena istovrsna grupa državnih tijela po svom djelokrugu koristi samo neke, slične ili iste vrste podataka. Mjere i standardi informacijske sigurnosti vezani su dakle na klasificirane ili neklasificirane podatke, a onda slijedom toga i na osobe, prostore ili informacijske sustave u kojima se takvi podaci koriste. U našem slučaju kada imamo Zakon o tajnosti podataka i Zakon informacijskoj sigurnosti, to direktno proizlazi i iz toga što ovaj Zakon ne daje ovlast za klasificiranje i korištenje klasificiranih i neklasificiranih podataka već se bavi samo njihovom zaštitom. Dakle, intencija ovog Zakona nije da daje ovlasti tijelima za korištenje pojedine vrste podataka, već da propiše obvezne (minimalne) sigurnosne kriterije za ona tijela koja u svom djelokrugu koriste takve podatke. Pri tome se primjenjuje niz kriterija kao što je primjerice propisano u članku 4. stavak 2. (npr. količina klasificiranih podataka na određenoj lokaciji). Upravo iz tih razloga u članku 6. se utvrđuju važna načela za razradu mjera i standarda informacijske sigurnosti, koja će se (osobito stavak 1.) odnositi na većinu tijela iz članka 1. stavak 2. ovog Zakona. Ova načela bitna su ne samo za sigurnost, već i za ekonomičnost primjene mjera i standarda informacijske sigurnosti.

Djelomično su prihvaćene primjedbe Odbora za informiranje, informatizaciju i medije na kraticu CERT koja nije pojašnjena u tekstu zakona, jer je iscrpno pojašnjenje dano u obrazloženju. U konačnom prijedlogu Zakona opisni naziv „tijelo za prevenciju i odgovor na računalne ugroze sigurnosti informacijskih sustava" konzistentnije se upotrebljava, ali je zadržana kratica CERT iz razloga prvotno pojašnjenih u obrazloženju.

VI. PRIJEDLOZI I MIŠLJENJA KOJA NISU PRIHVAĆENA I RAZLOZI

Nisu prihvaćene primjedbe zastupnika Dorotee Pešić Bukovac i Antuna Kapraljevića da postoje sumnje u razloge donošenja ovog Zakona u ovom obliku jer ne nosi oznaku usklađivanja s EU, a u obrazloženju se stalno poziva na EU i NATO. Uvođenje suvremenog sustava klasificiranih podataka u državnoj upravi i njihove zaštite nije legislativni zahtjev EU, već zahtjev koji proizlazi iz Zakona o potvrđivanju Ugovora između Republike Hrvatske i Europske Unije o sigurnosnim postupcima za razmjenu tajnih podataka (NN Međunarodni ugovori 9/2006, 18. 10. 2006). Provedba tog Zakona znači prihvaćanje uvjeta koje propisuje sigurnosna politika EU (Council Decision, 19 March 2001, adopting the Council's security regulations, 2001/264/EC, eur-lex.europa.eu) te u tom smislu RH mora osigurati pretpostavke za to u nacionalnom zakonodavstvu. Ovo je tzv. implicitni zahtjev, koji spada u vrstu zahtjeva koji proizlaze iz određenih politika ili programa EU, za razliku od eksplicitnih zahtjeva u kojima se traži donošenje pojedinih zakona, kao što je primjerice Zakon o pravu na pristup informacijama. Implicitni zahtjevi su uobičajeni u dijelu nacionalne sigurnosti (zaštite države), dok su ovi eksplicitni uobičajeni u dijelu zaštite demokratskih standarda građana ili primjerice zaštite otvorenog tržišta. Zbog neprimjerenih koncepata koji proizlaze iz još uvijek aktualnog Zakona o zaštiti tajnosti podataka iz 1996.g., a koji se novim Zakonom o tajnosti podataka i Zakonom o informacijskoj sigurnosti funkcionalno zamjenjuje, RH ne može provesti sljedeću fazu u sklopu spomenutog Zakona o potvrđivanju Ugovora između Republike Hrvatske i Europske Unije o sigurnosnim postupcima za razmjenu tajnih podataka, tj. ne može potpisati Sporazum o provedbi ovog Zakona[10] koji EU očekuje već nekoliko mjeseci.

[10] Security arrangements between the Office of the National Security Council of the Republic of Croatia, the EU Council General Secretariat Security Office and the European Commission Security Directorate for the protection of classified information exchanged between the Republic of Croatia and the EU

Očitovanje na mišljenje UREDA ZA ZAKONODAVSTVO
(dopis Ureda od 31. svibnja 2007., klasa: 008-02/07-01/01, Urbroj: 50501-07-574-02)

Temeljem dostavljenog mišljenja Ureda za zakonodavstvo na Konačni prijedlog Zakona o informacijskoj sigurnosti, uvažili smo veliki broj sugestija i prijedloga te izvršili korekcije Konačnog prijedloga. Za primjedbe Ureda za koje smatramo da ih ne treba mijenjati u tekstu samog Zakona, ponudili smo dodatna obrazloženja te smo u tim slučajevima korigirali pripadne dijelove obrazloženja Konačnog prijedloga Zakona, kako bi cjeloviti materijal bio jasniji.

Prihvaćene sugestije i primjedbe:

Vezano na članak 1. stavak 2., potvrđujemo pretpostavku Ureda da se u ovom Zakonu koriste termini prema definicijama uvedenim u Zakonu o tajnosti podataka, koji je specijalni zakon za područje tajnosti podataka u državnoj upravi. Ova dva Zakona stoga se i predlažu u paketu.

U članku 4. stavku 1. korigirali smo pojmove „nacionalni i međunarodni klasificirani i neklasificirani podaci" te uveli terminologiju sukladnu Zakonu o tajnosti podataka „klasificirani i neklasificirani podaci", pri čemu je Zakonom o tajnosti podataka definirano da klasificirani i neklasificirani podaci obuhvaćaju podatke u nadležnim tijelima RH, koji su označeni kao takvi u propisanom postupku, kao i podatke koje je Republici Hrvatskoj tako označene predala druga država, međunarodna organizacija ili institucija s kojom Republika Hrvatska surađuje. To znači da se mjere i standardi propisuju za sve takve klasificirane i neklasificirane podatke sukladno načelima iz članaka 3. do 6. ovog Zakona.

Prihvatili smo primjedbu da neki pojmovi nisu dovoljno definirani u Zakonu te smo umjesto uvođenja dodatnih pojmova u članak 2., izvršili korekcije teksta i uskladili ga s terminologijom Zakona o tajnosti podataka kao specijalnim zakonom, odnosno korigirali neke pojmove (članak 4. stavak 3.), ili ih izostavili (članak 4. stavak 2.). Izostavljeni pojmovi, kao strukovni pojmovi, bit će razrađeni Uredbama i Pravilnicima te neće opterećivati tekst Zakona.

Vezano na komentar o članku 10. stavku 2., o istovjetnosti načina i postupanja u različitim tijelima, izvršili smo dodatno usklađivanje ovog Zakona i Zakona o tajnosti podataka te smo doradili novi članak 11. stavak 2. ovog Zakona, koji propisuje obvezu primjene procedura za postupanje s klasificiranim i neklasificiranim podacima. Procedure se razrađuju u okviru mjera i standarda informacijske sigurnosti (članak 2. podstavak 2. i 3., članak 7., članak 15. stavak 1., članak 18. stavak 1., članak 27., članak 28. stavci 1. i 3.), čija primjena je uvjetovana korištenjem odgovarajuće vrste (klasificirani, neklasificirani) i razine podataka (stupanj tajnosti) i ovisi o načelima definiranim člancima 3. do 6. To znači da će mjere u pojedinim tijelima biti istovrsne u smislu osiguravanja minimalnih kriterija za zaštitu (članak 3.), ali se mogu razlikovati, primjerice, u ovisnosti o broju klasificiranih podataka, ili u ovisnosti o tome da li se u nekom tijelu koriste podaci u papirnatom ili elektroničkom obliku. Radi lakšeg planiranja, provedbe i nadzora sve mjere i standardi podijeljeni su na pet područja informacijske sigurnosti, sukladno međunarodno (NATO, EU) prihvaćenoj praksi.

Što se tiče primjedbi na definiciju pojma sigurnosne akreditacije u članku 2. podstavak 5. i na nejasan proces sigurnosne akreditacije reguliran Zakonom, smatramo da je taj proces dobro definiran počevši od pojma (članak 2. podstavak 5.), uvjeta kad se provodi (članak 12. stavak 2.), subjekta koji to provode (članak 17. stavak 2. i članak 19.) te samih obveza tijela u kojima, i na temelju kojih, će se provoditi sigurnosna akreditacija (članci 23., 24. i članak 29. stavak 2.), zatim nadzora, kojim se redovito procjenjuje stanje informacijskog sustava i eventualno osporava daljnja sigurnosna akreditacija informacijskog sustava (članak 26. stavak 2. podstavak 2.), i to sve u okvirima definiranim člankom 12. stavkom 2. (samo za tri utvrđene, više razine stupnja tajnosti klasificiranih podataka). Pojam akreditacije kao opći pojam, poznat je u hrvatskom zakonodavstvu (Hrvatska agencija za akreditacije i mjerodavna regulativa), te nije potrebno uvoditi dodatna pojašnjenja u ovaj Zakon, jer je ova akreditacija, kao i svaka druga, dozvola za rad u definiranim okvirima, a ovdje se definiraju okviri u kojima se izdaje takva dozvola za rad u ovom Zakonu (tijela koja koriste klasificirane podatke u elektroničkom obliku i to samo za razine tri viša stupnja tajnosti – „Povjerljivo", „Tajno" i „Vrlo tajno"). U tom smislu naglašavamo da nema rokova za provedbu sigurnosne akreditacije već se u informacijskom sustavu podaci utvrđenih razina tajnosti niti ne mogu početi obrađivati, pohranjivati ili prenositi ako nije prethodno provedena sigurnosna akreditacija tog informacijskog sustava. Ipak, zbog jasnoće, a temeljem sugestija Ureda za zakonodavstvo, korigirano je obrazloženje Konačnog prijedloga na stranici 16.

Obrazloženje članaka 20. do 22. (Nacionalni CERT) korigirano je na prijedlog Ureda za zakonodavstvo, jer se ne osniva novo nacionalno tijelo već se CARNet-u proširuju ovlasti i time se definira nova nacionalna funkcionalnost za prevenciju i odgovor na računalne ugroze javnih informacijskih sustava u RH (Nacionalni CERT).

Dorađene su Prijelazne i završne odredbe (članci 27. do 30.) te su ovlasti za donošenje podzakonskih akata prebačene u tekst Zakona dok su u Prijelaznim i završnim odredbama ostali rokovi i veze na članke u tekstu Zakona.

Obrazloženje sugestija i primjedbi koje nisu prihvaćene:

Primjedbe na članak 13. stavak 2. o pravnoj zaštiti pravnih osoba kojima se odbije certifikat poslovne sigurnosti, mišljenja smo da ne stoje, jer se radi o konceptu koji proizlazi iz međunarodnih obveza RH prema kojima RH treba osigurati odgovarajuću sigurnost poslovne suradnje na klasificiranim projektima za svoja državna tijela, ali isto tako i za tvrtke registrirane u RH koje se uključuju u klasificirane međunarodne natječaje i poslove ove vrste (NATO, EU). Pristup je usklađen sa zahtjevima sigurnosne politike EU-a i NATO-a, prihvaćene Zakonom o potvrđivanju Ugovora između Republike Hrvatske i Europske Unije o sigurnosnim postupcima za razmjenu tajnih podataka (NN Međunarodni ugovori 9/2006, 18. 10. 2006) te Zakonom o potvrđivanju sporazuma o sigurnosti između Republike Hrvatske i Organizacije sjevernoatlantskog ugovora, NN Međunarodni ugovori 7/2003, 23. 07. 2003.). Napominjemo da se u slučaju certifikata pravne osobe, primjenjuje pristup uobičajen za poslovni sektor, sukladan pristupu koji se koristi kod svih vrsta poslovnih certifikata. Temeljno je da se ovdje radi o privilegiji, a ne o pravu, te se ovi certifikati ne mogu uspoređivati s certifikatima osoba gdje to može biti na određeni način povezano s radnim mjestom i mora biti usklađeno s radno-pravnog stajališta te sa stajališta ljudskih prava (Zakon o tajnosti podataka). Kod certifikata pravne osobe

iz ovog Zakona, kao i kod svih vrsta poslovnog certificiranja (primjerice norme kvalitete ISO 9000 ili norme informacijske sigurnosti ISO 27001) u RH i u svijetu, nije uobičajena terminologija „odbijanja certifikata", već se izdavanje certifikata smatra procesom usklađivanja pravne osobe s određenim propisima ili normama te se certifikat o tome izdaje tek onda kada je pravna osoba zadovoljila proces usklađivanja s određenim propisima što zavisi o nizu faktora, ali primarno o unutarnjoj organizaciji i veličini same pravne osobe i uobičajeno traje 6 mjeseci ili više.

Što se tiče problema odgovornosti za primjenu mjera i standarda, kazni i slično, konstatiramo da je tajnost podataka utvrđeni predmet zaštite Kaznenog zakona, a Zakon o zaštiti osobnih podataka uveo je kazne za nepridržavanje mjera koje se propisuju za sve pravne i fizičke osobe u segmentu zaštite osobnih podataka građana. Nije uobičajeno određivati novčane kazne čelnicima državnih tijela za neprimjenjivanje mjera i standarda zaštite klasificiranih i neklasificiranih podataka u državnoj upravi, već se u praksi razvijenih zemalja primjenjuje koncept odgovornosti čelnih osoba (članak 26. stavak 3.), a tu odgovornost utvrđuje nacionalno NSA tijelo (članak 26. stavak 2.) te prosljeđuje na odlučivanje o daljnjem statusu čelnika njegovom nadređenom tijelu (npr. Vlada i sl.).

Vezano za primjedbe na ovlasti donošenja pravilnika iz članka 15. stavak 1. i članka 18. stavak 1., u obrazloženju ovog Zakona ukazano je na potrebne izmjene Zakona o sustavu državne uprave i način kako se to predlaže provesti (stranica 17.).

Vezano za primjedbe na ovlasti UVNS-a iz članka 15., potvrđujemo da se člancima 14. do 16. utvrđuju ovlasti koje su međunarodno standardizirane kao funkcionalnost nacionalnog NSA tijela (National Security Authority ili Središnje državno tijelo za informacijsku sigurnost), što je uvjet pristupa u EU i NATO te proizlazi iz prethodno spomenutih zakona koje je ratificirao Hrvatski sabor. Stoga te ovlasti ne možemo tretirati kao prevelike, već kao nužne u suvremenoj državnoj upravi.