KONAČNI PRIJEDLOG

ZAKONA O TAJNOSTI PODATAKA

Zagreb, lipanj 2007.

I. KONAČNI PRIJEDLOG ZAKONA O TAJNOSTI PODATAKA

I. OSNOVNE ODREDBE

Članak 1.

(1) Ovim Zakonom utvrđuju se pojam klasificiranih i neklasificiranih podataka, stupnjevi tajnosti, postupak klasifikacije i deklasifikacije, pristup klasificiranim i neklasificiranim podacima, njihova zaštita i nadzor nad provedbom zakona.

(2) Ovaj Zakon se primjenjuje na državna tijela, tijela jedinica lokalne i područne (regionalne) samouprave, pravne osobe s javnim ovlastima te pravne i fizičke osobe koje, u skladu sa Zakonom, ostvare pristup ili postupaju s klasificiranim i neklasificiranim podacima.

Članak 2.

Pojmovi koji se koriste u ovom Zakonu imaju sljedeće značenje:

- podatak je dokument, odnosno svaki napisani, umnoženi, nacrtani, slikovni, tiskani, snimljeni, fotografirani, magnetni, optički, elektronički ili bilo koji drugi zapis podatka, saznanje, mjera, postupak, predmet, usmeno priopćenje ili informacija, koja s obzirom na svoj sadržaj ima važnost povjerljivosti i cjelovitosti za svoga vlasnika;
- klasificirani podatak je onaj koji je nadležno tijelo, u propisanom postupku, takvim označilo i za kojeg je utvrđen stupanj tajnosti, kao i podatak kojeg je Republici Hrvatskoj tako označenog predala druga država, međunarodna organizacija ili institucija s kojom Republika Hrvatska surađuje;
- neklasificirani podatak je podatak bez utvrđenog stupnja tajnosti, koji se koristi u službene svrhe, kao i podatak kojeg je Republici Hrvatskoj tako označenog predala druga država, međunarodna organizacija ili institucija s kojom Republika Hrvatska surađuje;
- klasifikacija podatka je postupak utvrđivanja jednog od stupnjeva tajnosti podatka s obzirom na stupanj ugroze i područje Zakonom zaštićenih vrijednosti;
- deklasifikacija podatka je postupak kojim se utvrđuje prestanak postojanja razloga zbog kojih je određeni podatak klasificiran odgovarajućim stupnjem tajnosti, nakon čega podatak postaje neklasificirani s ograničenom uporabom samo u službene svrhe;
- vlasnik podatka je nadležno tijelo u okviru čijeg djelovanja je klasificirani ili neklasificirani podatak nastao;
- certifikat je uvjerenje o sigurnosnoj provjeri koje omogućava pristup klasificiranim podacima.

Članak 3.

Klasificiranim podatkom ne može se proglasiti podatak radi prikrivanja kaznenog djela, prekoračenja ili zlouporabe ovlasti te drugih oblika nezakonitog postupanja u državnim tijelima.

II. STUPNJEVI TAJNOSTI

Članak 4.

Stupnjevi tajnosti klasificiranih podataka su:
- VRLO TAJNO,
- TAJNO,
- POVJERLJIVO,
- OGRANIČENO.

Članak 5.

S obzirom na stupanj ugroze zaštićenih vrijednosti stupnjevima tajnosti iz članka 4. ovog Zakona mogu se klasificirati podaci iz djelokruga državnih tijela u području obrane, sigurnosno-obavještajnog sustava, vanjskih poslova, javne sigurnosti, kaznenog postupka, te znanosti, tehnologije, javnih financija i gospodarstva ukoliko su podaci od sigurnosnog interesa za Republiku Hrvatsku.

Članak 6.

Stupnjem tajnosti „VRLO TAJNO“ klasificiraju se podaci čije bi neovlašteno otkrivanje nanijelo nepopravljivu štetu nacionalnoj sigurnosti i vitalnim interesima Republike Hrvatske, a osobito slijedećim vrijednostima:

- temelji Ustavom utvrđenog ustrojstva Republike Hrvatske,
- neovisnost, cjelovitost i sigurnost Republike Hrvatske,
- međunarodni odnosi Republike Hrvatske,
- obrambena sposobnost i sigurnosno-obavještajni sustav,
- sigurnost građana,
- osnove gospodarskog i financijskog sustava Republike Hrvatske,
- znanstvena otkrića, pronalasci i tehnologije od važnosti za nacionalnu sigurnost Republike Hrvatske.

Članak 7.

Stupnjem tajnosti „TAJNO“ klasificiraju se podaci čije bi neovlašteno otkrivanje teško naštetilo vrijednostima iz članka 6. ovog Zakona.

Članak 8.

Stupnjem tajnosti „POVJERLJIVO“ klasificiraju se podaci čije bi neovlašteno otkrivanje naštetilo vrijednostima iz članka 6. ovog Zakona.

Članak 9.

Stupnjem tajnosti „OGRANIČENO“ klasificiraju se podaci čije bi neovlašteno otkrivanje naštetilo djelovanju i izvršavanju zadaća državnih tijela u obavljanju poslova iz članka 5. ovog Zakona.

Članak 10.

Državna tijela koja provode postupak klasificikacije podataka pravilnikom će pobliže razraditi kriterije za određivanje stupnjeva tajnosti za podatke iz svog djelokruga.

III. POSTUPAK KLASIFICIRANJA I DEKLASIFICIRANJA PODATAKA

Članak 11.

Klasifikacija podataka se obavlja pri nastanku klasificiranih podataka ili prilikom periodične procjene iz članka 14. ovog Zakona.

Članak 12.

(1) U postupku klasifikacije podatka vlasnik podatka dužan je odrediti najniži stupanj tajnosti koji će osigurati zaštitu interesa koji bi neovlaštenim otkrivanjem tog podatka mogli biti ugroženi.

(2) Ukoliko klasificirani podatak sadrži određene dijelove ili priloge, čije neovlašteno otkrivanje ne ugrožava vrijednosti zaštićene ovim Zakonom, takvi dijelovi podatka neće biti označeni stupnjem tajnosti.

Članak 13.

(1) Klasificiranje podataka stupnjevima tajnosti „VRLO TAJNO“ i „TAJNO“ mogu provoditi: Predsjednik Republike Hrvatske, predsjednik Hrvatskog sabora, predsjednik Vlade Republike Hrvatske, ministri, Glavni državni odvjetnik, načelnik Glavnog stožera Oružanih snaga RH i čelnici tijela sigurnosno-obavještajnog sustava RH te osobe koje oni za tu svrhu ovlaste.

(2) Osobe iz stavka 1. ovog članka ovlast prenose pisanim putem na druge osobe isključivo u okviru njihovog djelokruga.

(3) Klasificiranje podataka stupnjevima tajnosti „POVJERLJIVO“ i „OGRANIČENO“, pored osoba iz stavka 1. i 2. ovog članka, mogu provoditi i čelnici ostalih državnih tijela.

(4) Osobe iz stavaka 1., 2. i 3., ovog članka klasificiraju podatke i za znanstvene ustanove, zavode i druge pravne osobe, kada rade na projektima, pronalascima, tehnologijama i drugim poslovima od sigurnosnog interesa za Republiku Hrvatsku.

Članak 14.

(1) Za vrijeme važenja stupnja tajnosti podatka, vlasnik podatka obvezan je trajno procjenjivati stupanj tajnosti klasificiranog podatka i izraditi perodičnu procjenu, temeljem koje se može promijeniti stupanj tajnosti ili izvršiti deklasifikacija podatka.

(2) Periodična procjena provodi se:
- za stupanj tajnosti „VRLO TAJNO“ najmanje jednom u 5 godina,
- za stupanj tajnosti „TAJNO“ najmanje jednom u 4 godine,
- za stupanj tajnosti „POVJERLJIVO“ najmanje jednom u 3 godine,
- za stupanj tajnosti „OGRANIČENO“ najmanje jednom u 2 godine.

(3) O promjeni stupnja tajnosti ili o deklasifikaciji podatka vlasnik podatka će pisanim putem izvijestiti sva tijela kojima je podatak bio dostavljen.

Članak 15.

(1) Periodična procjena izrađuje se u pisanom obliku za svaki stupanj tajnosti.

(2) Vlasnik podatka periodičnu procjenu može provesti i skupno za određene grupe podataka.

(3) Periodična procjena označava se stupnjem tajnosti podatka na koji se odnosi i prilaže se uz izvornik u arhivu vlasnika podatka.

Članak 16.

(1) Kad postoji interes javnosti, vlasnik podatka dužan je ocjeniti razmjernost između prava na pristup informacijama i zaštite vrijednosti propisanih u člancima 6., 7., 8. i 9. ovog Zakona te odlučiti o zadržavanju stupnja tajnosti, promjeni stupnja tajnosti, deklasifikaciji ili oslobađanju od obveze čuvanja tajnosti podatka.

(2) Prije donošenja odluke iz stavka 1. ovog članka vlasnik podatka je dužan zatražiti mišljenje Ureda Vijeća za nacionalnu sigurnost.

(3) Vlasnik podatka dužan je o postupku iz stavka 1. ovog članka izvjestiti i druga nadležna tijela propisana zakonom.

Članak 17.

Način označavanja stupnjeva tajnosti klasificiranih podataka, propisat će se uredbom koju donosi Vlada Republike Hrvatske.

IV. PRISTUP PODACIMA

Članak 18.

(1) Pristup klasificiranim podacima imaju osobe kojima je to nužno za obavljanje poslova iz njihovog djelokruga te koje imaju izdano Uvjerenje o obavljenoj sigurnosnoj provjeri (u daljnjem tekstu: certifikat).

(2) Državna tijela, tijela jedinica lokalne i područne (regionalne) samouprave, pravne osobe s javnim ovlastima te pravne i fizičke osobe (u daljnjem tekstu: podnositelji zahtjeva) ovlašteni su za podnošenje zahtjeva za izdavanje certifikata za zaposlenike, koji u okviru svog djelokruga imaju pravo pristupa klasificiranim podacima.

(3) Zahtjev za izdavanje certifikata podnosi se, u pisanom obliku, Uredu Vijeća za nacionalnu sigurnost.

Zahtjev sadrži: ime i prezime osobe, dužnost ili poslove u okviru kojih pristupa klasificiranim podacima i stupanj tajnosti za koji se traži certifikat.

(4) Certifikat se izdaje za stupnjeve tajnosti „VRLO TAJNO“, „TAJNO“ i „POVJERLJIVO“ na rok od pet godina.

Certifikat se ne označava stupnjem tajnosti već predstavlja neklasificirani podatak.

(5) Certifikat izdaje Ured Vijeća za nacionalnu sigurnost na temelju ocjene o nepostojanju sigurnosnih zapreka za pristup klasificiranim podacima.

Postojanje sigurnosnih zapreka utvrđuje se na temelju sigurnosne provjere koju obavlja nadležna sigurnosno-obavještajna agencija.

(6) Sigurnosne zapreke u smislu ovog zakona su: neistinito navođenje podataka u upitniku za sigurnosnu provjeru; činjenice koje su posebnim zakonom propisane kao zapreke za prijam u državnu službu; te izrečene stegovne sankcije i druge činjenice koje predstavljaju osnovu za sumnju u povjerljivosti ili pouzdanosti osobe za postupanje s klasificiranim podacima.

Članak 19.

(1) Ako tijelo iz članka 18. stavka 5. ovog Zakona, na temelju izvješća o rezultatima sigurnosne provjere ocijeni da postoje sigurnosne zapreke, rješenjem će odbiti izdavanje certifikata.

(2) Osoba kojoj je rješenjem odbijeno izdavanje certifikata ima pravo pokrenuti upravni spor u roku od 30 dana od primitka rješenja.

(3) U postupku pred Upravnim sudom, sud će, prilikom utvrđivanja činjenica i izvođenja dokaza kojima bi mogla nastati šteta za rad sigurnosno-obavještajnih agencija i nacionalnu sigurnost, poduzeti mjere i radnje iz svoje nadležnosti kojima će spriječiti nastanak štete.

Članak 20.

(1) Pristup klasificiranim podacima bez certifikata imat će u okviru obavljanja poslova iz njihovog djelokruga saborski zastupnik, ministar, državni tajnik središnjeg državnog ureda, sudac i Glavni državni odvjetnik.

(2) Osobe iz stavka 1. ovog članka dužne su, prije pristupanja klasificiranim podacima, potpisati izjavu Uredu Vijeća za nacionalnu sigurnost kojom potvrđuju da su upoznati s odredbama ovog Zakona i drugih propisa kojima se uređuje zaštita klasificiranih podataka te se obvezuju raspolagati klasificiranim podacima sukladno navedenim propisima.

Članak 21.

Sadržaj i izgled certifikata iz članka 18. ovog Zakona te izjave iz članka 20. stavak 2. ovog Zakona, propisat će se uredbom koju donosi Vlada Republike Hrvatske.

Članak 22.

(1) Pristup klasificiranim podacima druge države i međunarodne organizacije, imaju osobe kojima je to nužno za obavljanje poslova iz njihovog djelokruga, te kojima je izdan certifikat propisan međunarodnim ugovorom ili sigurnosnim sporazumom.

(2) Certifikat iz stavka 1. ovog članka izdaje Ured Vijeća za nacionalnu sigurnost na temelju zahtjeva nadležnog tijela.

(3) Zahtjev iz stavka 2. ovog članka može se podnijeti samo za osobe kojima je prethodno izdan odgovarajući certifikat u postupku iz članka 18. ovog Zakona.

Članak 23.

(1) Pristup neklasificiranim podacima imaju osobe kojima je to nužno u službene svrhe radi obavljanje poslova iz njihovog djelokruga.

(2) Pristup neklasificiranim podacima imaju i zainteresirani ovlaštenici prava na informaciju na temelju podnesenog zahtjeva za ostvarivanje prava na pristup informacijama sukladno zakonu.

Članak 24.

Predsjednik Republike Hrvatske, predsjednik Hrvatskog sabora i predsjednik Vlade Republike Hrvatske, izuzeti su od postupka propisanog za izdavanje certifikata.

V. ZAŠTITA PODATAKA

Članak 25.

Način i provedba zaštite klasificiranih i neklasificiranih podataka propisat će se zakonom koji regulira područje informacijske sigurnosti.

Članak 26.

Dužnosnici i zaposlenici državnih tijela, tijela jedinica lokalne i područne (regionalne) samouprave, pravnih osoba s javnim ovlastima, kao i pravne i fizičke osobe koje ostvare pristup ili postupaju s klasificiranim i neklasificiranim podacima, dužni su čuvati tajnost klasificiranog podatka za vrijeme i nakon prestanka obavljanja dužnosti ili službe, sve dok je podatak utvrđen jednim od stupnjeva tajnosti ili dok se odlukom vlasnika podatka ne oslobode obveze čuvanja tajnosti.

Članak 27.

(1) Ako se klasificirani podatak uništi, otuđi ili učini dostupnim neovlaštenim osobama, vlasnik podatka poduzima sve potrebne mjere za otklanjanje nastajanja mogućih štetnih posljedica, pokreće postupak za utvrđivanje odgovornosti i istodobno izvještava Ured Vijeća za nacionalnu sigurnost.

(2) Ako se klasificirani podatak uništi, otuđi ili učini dostupnim neovlaštenim osobama u tijelu koje nije vlasnik podatka, odgovorna osoba tog tijela dužna je odmah o tome izvijestiti vlasnika podatka koji pokreće postupak iz stavka 1. ovog članka.

Članak 28.

(1) Ured Vijeća za nacionalnu sigurnost će prilikom izdavanja certifikata ili potpisivanja izjave iz članka 20. stavka 2. ovog Zakona upoznati osobe sa standardima postupanja s klasificiranim podacima te s pravnim i drugim posljedicama neovlaštenog raspolaganja istim.

(2) Postupak iz stavka 1. ovog članka, provodi se najmanje jednom godišnje za vrijeme važenja certifikata.

VI. NADZOR NAD PROVEDBOM ZAKONA

Članak 29.

Državna tijela, tijela jedinica lokalne i područne (regionalne) samouprave i pravne osobe s javnim ovlastima, vode evidenciju o izvršenim uvidima i postupanju s klasificiranim podacima.

Članak 30.

(1) Ured Vijeća za nacionalnu sigurnost provodi nadzor nad postupcima klasifikacije i deklasifikacije podataka, načinom ostvarivanja pristupa klasificiranim i neklasificiranim podacima, provedbi mjera za zaštitu pristupa klasificiranim podacima te izvršavanja obveza proizašlih iz međunarodnih ugovora i sporazuma o zaštiti klasificiranih podataka.

(2) U provođenju nadzora predstojnik Ureda Vijeća za nacionalnu sigurnost ovlašten je:
- utvrditi činjenično stanje,
- dati upute u svrhu otklanjanja utvrđenih nedostataka i nepravilnosti koje su nadzirana tijela dužna u određenom roku ukloniti,
- pokrenuti postupak utvrđivanja odgovornosti vlasnika podatka,
- poduzeti druge mjere i radnje, za koje je posebnim propisima ovlašten.

(3) U Uredu Vijeća za nacionalnu sigurnost ustrojavaju se registri izdanih certifikata, rješenja o odbijanju izdavanja certifikata, potpisanih izjava iz članka 20. st. 2 ovog Zakona te obavljenih upoznavanja sa standardima iz članka 28. ovog Zakona.

VII. PRIJELAZNE I ZAVRŠNE ODREDBE

Članak 31.

(1) Uredba Vlade Republike Hrvatske iz članka 17. i članka 21. ovog Zakona donijet će se u roku od 30 dana od dana stupanja na snagu ovog Zakona.

(2) Pravilnik iz članka 10. ovog Zakona čelnici nadležnih tijela donijet će u roku od 60 dana od dana stupanja na snagu ovog Zakona.

(3) Čelnici nadležnih tijela dužni su utvrditi popis dužnosti i poslova iz njihova djelokruga za koje je potreban certifikat, u roku od 90 dana.

Članak 32.

Stupnjevi tajnosti određeni međunarodnim ugovorima koje je Republika Hrvatska potpisala prije donošenja ovog Zakona, stupnjevi tajnosti podataka dobivenih međunarodnom razmjenom prije stupanja na snagu ovog Zakona, kao i stupnjevi tajnosti podataka koji su nastali prije stupanja na snagu ovog Zakona, prevode se na način:
- „DRŽAVNA TAJNA“ u „VRLO TAJNO“,
- „SLUŽBENA TAJNA – VRLO TAJNO“ i „VOJNA TAJNA – VRLO TAJNO“ u „TAJNO“,
- „SLUŽBENA TAJNA – TAJNO“ i „VOJNA TAJNA – TAJNO“ u „POVJERLJIVO“,
- „SLUŽBENA TAJNA – POVJERLJIVO“ i „VOJNA TAJNA – POVJERLJIVO“ u „OGRANIČENO“.

Članak 33.

(1) Certifikati koje je Ured Vijeća za nacionalnu sigurnost izdao do stupanja na snagu ovog Zakona vrijede do isteka roka označenog na certifikatu.

(2) Interna dopuštenja za pristup tajnim podacima koja su izdana na temelju Zakona o zaštiti tajnosti podataka (Narodne novine 108/96), vrijede do izdavanja certifikata po ovom Zakonu.

(3) Podzakonski propisi doneseni na temelju Zakona o zaštiti tajnosti podataka (Narodne novine 108/96) vrijedit će do donošenja odgovarajućih podzakonskih propisa na temelju ovoga Zakona.

Članak 34.

Stupanjem na snagu ovog Zakona prestaju važiti odredbe Zakona o zaštiti tajnosti podataka (Narodne novine 108/96) osim odredbi navedenih u glavi 8. i 9. istog Zakona.

Članak 35.

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

O B R A Z L O Ž E NJ 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 do sada je bilo propisano Zakonom o zaštiti tajnosti podataka (NN 108/96) čijim je donošenjem prestala važiti Uredba o utvrđivanju mjerila za određivanje tajnih podataka obrane te posebnim i općim postupcima za njihovo čuvanje (NN 70/91), a područje tajnosti podataka uredilo se normom zakonskog ranga te se obuhvatila materija tajnih podataka, njihovih vrsta, postupaka za određivanje tajnosti, dužnosti za čuvanje tajnosti podataka i načina provjere tajnosti podataka od strane predstavnika sredstava javnog priopćavanja.

Zakon o zaštiti tajnosti podataka (NN 108/96) ne zadovoljava suvremene standarde po pitanju tajnosti podataka po više osnova.

Prvo, Zakon po uzoru na standarde koji su važili u razdoblju prije demokratskih promjena, razlikuje vrste tajni (državna tajna, službena tajna, vojna tajna, poslovna tajna) i stupnjeve tajnosti (državna tajna, vrlo tajno, tajno i povjerljivo) što je neodgovarajuće standardima koji se primjenjuje u zemljama članicama EU i NATO koji u području tajni iz djelokruga državnih tijela ne poznaju posebne vrste već samo četiri stupnja tajnosti podataka. Uz određena neznatna odstupanja u nazivlju na engleskom jeziku uobičajena je klasifikacija na sljedeće stupnjeve: TOP SECRET, SECRET, CONFIDENTIAL i RESTRICTED te UNCLASSIFIED za podatke koji nisu tajni već se njihova upotreba ograničava za službene svrhe.

Iz navedene nekompatibilnosti proizlaze problemi kod prevođenja ili usklađivanja klasifikacijskih oznaka iz dva izvorno različita klasifikacijska sustava slijedom čega RH ima poteškoće kod sklapanja i primjene ugovora o razmjeni klasificiranih podataka sa stranim zemljama i organizacijama, a osobito u postupku pravnog usklađivanja sa standardima zemalja EU i NATO koje prethodi punopravnom članstvu objema organizacijama.

Drugo, postojeći Zakon ne propisuje kao uvjet za pristup tajnim podacima provedbu sigurnosne provjere takvih osoba i izdavanje odgovarajuće isprave ili certifikata kojim bi se potvrdilo sigurnosnu pouzdanost osobe za pristup tajnim podacima što je također sigurnosni standard navedenih zemalja i uvjet za razmjenu klasificiranih i neklasificiranih podataka, a time i za integriranje sa sustavima navedenih organizacija i njihovih članica.

Treće, iako postojeći Zakon neposredno određuje dio podataka koji se po Zakonu imaju smatrati tajnama određene vrste, istovremeno dopušta i da se tajni podaci određuju na temelju drugih propisa i općih akata tijela javne vlasti ne utvrđujući za to potrebne kriterije niti središnji nadzor što otvara mogućnost za vrlo široko i neujednačeno određivanje tajnih podatka u različitim područjima djelovanja državnih tijela.

Četvrto, Zakon široko određuje krug tijela ovlaštenih za utvrđivanje vrsta i stupnjeva tajnosti definirajući ih kao javna tijela čime se otvara mogućnost utvrđivanja tajnosti i u područjima koja to nisu po standardima zemalja EU koje polaze od načela da je tajnost izuzetak, a ne

pravilo, što se smatra važnim u kontekstu ostvarivanja javne kontrole nad radom državnih tijela kao bitne sastavnice demokratske i pravne države.

Dakle, područja djelovanja državnih tijela u kojima je nužno, zbog opravdanih javnih interesa, predvidjeti mogućnost klasificiranja dijela podataka, potrebno je preciznije odrediti kako bi se područje tajnosti reduciralo na stvarno potrebnu mjeru, a izbjeglo široku primjenu klasifikacije koja ne bi bila u funkciji zaštite opravdanih javnih interesa već bi mogla poslužiti u cilju prikrivanja neefikasnosti ili nezakonitosti u radu.

Nadalje, Zakon ne propisuje niz drugih suvremenih stečevina i standarda poput sustava nadzora nad postupcima određivanja i čuvanja tajnih podataka, raspolaganja tajnim podacima samo u okviru zakonom utvrđenog djelokruga i samo u mjeri koja je nužna za obavljanje poslova iz navedenog djelokruga (*need to know*), propisivanja posebne vrste podataka namijenjenih korištenju u službene svrhe i slično.

Navedeno stanje doprinijelo je ustrojavanju sustava tajnosti podataka koji je nekonzistentan i u pojedinim segmentima neefikasan te koji po standardima i nekim pokazateljima odudara od onih u zemljama EU i NATO. Tako je evidentna primjena različitih kriterija u klasificiranju i raspolaganju podacima, visok omjer podataka klasificiranih najvećim stupnjem i vrstom tajnosti te u nekim područjima rada državnih tijela evidentno nizak stupanj razvijenosti i primjene propisanih standarda i općenito kulture raspolaganja tajnim podacima.

Tako, samo mali broj državnih tijela, deset godina nakon donošenja Zakona o zaštiti tajnosti podataka, ima donesene propise i implementirane zaštitne mjere, navedeni propisi su slabo ujednačeni, a najveći broj tijela državne uprave nema odgovarajuće ljudske potencijale i znanja za provedbu potrebnih poslova u cilju zaštite tajnih podataka. S ovim u vezi svakako je problem nedostatka središnjeg stručnog i nadzornog tijela koje bi svojim ovlastima, odgovornostima i kompetencijama, imalo osigurati ujednačenu i visoko standardiziranu zaštitu tajnih podataka.

B) Osnovna pitanja čije se uređenje predlaže ovim Zakonom i posljedice koje proizlaze njegovim donošenjem

Ovim Zakonom se uređuje jedinstveni sustav utvrđivanja, imenovanja i zaštite klasificiranih i neklasificiranih podataka, postupaka utvrđivanja stupnjeva tajnosti (postupci klasifikacije i deklasifikacije), ostvarivanja uvjeta za pristup tajnim podacima te nadzora nad primjenom zakona. Zakonom se uređuju pitanja tajnih podataka iz područja djelovanja državnih tijela dok će se reguliranje ostalih vrsta tajnih podataka iz privatnog i poslovnog područja regulirati odvojeno, sukladno EU standardima.

Određuju se novi stupnjevi tajnosti podataka usklađeni sa suvremenim standardima glede kriterija i nomenklatura tajnih podataka u zemljama EU-a i NATO-a.

Prema novoj klasifikaciji uvode se stupnjevi tajnosti: **VRLO TAJNO, TAJNO, POVJERLJIVO i OGRANIČENO.**

Stupnjevima tajnosti vrlo tajno, tajno i povjerljivo, štite se podaci čijim bi otkrivanjem nastupila šteta (stupnjevana kao nepopravljiva šteta, teška šteta i šteta) za nacionalnu sigurnost i vitalne interese RH dok se stupnjem tajnosti ograničeno štite podaci čijim bi otkrivanjem nastupila šteta djelovanju i izvršavanju zadaća državnih tijela, međutim samo u precizno određenim područjima rada (poslovi obrane, sigurnosno-obavještajnog sustava, vanjski poslovi, javna sigurnost, kazneni postupak te znanost, tehnologija, javne financije i gospodarstvo samo ako se radi o podacima od sigurnosnog interesa za Republiku Hrvatsku).

Na propisani način sužavaju se područja rada državnih tijela u okviru kojih je moguće klasificirati podatke i vrši se usmjeravanje na one poslove koji sukladno standardima ustanovljenim u demokratskim sustavima trebaju zaštitu kao pretpostavku učinkovitosti i održivosti s obzirom na druge javne i državne interese.

Navedeni stupnjevi tajnosti utvrđivati će se u postupku klasifikacije na temelju jedinstvenih kriterija utvrđenih ovim zakonom te Pravilnicima nadležnih tijela kojima će se kriteriji utvrđeni ovim zakonom izraziti u posebnostima iz užeg djelokruga svakog tijela. Jedinstvenost i zakonitost kriterija osiguravati će se nadzornom ulogom Ureda Vijeća za nacionalnu sigurnost kao središnjeg državnog tijela zaduženog za utvrđivanje i provedbu standarda informacijske sigurnosti.

Osim klasificiranih podataka utvrđenih po kriterijima i u postupcima koji odražavaju normativno stanje zemalja članica EU i NATO, propisuje se i posebna kategorija neklasificiranog podatka namijenjenog korištenju u službene svrhe, čime se pravno artikulira načelo izraženo u engleskom jeziku kroz sintagmu *need to know* i standard usvojen kroz politiku informacijske sigurnosti NATO i EU.

S time u vezi potrebno je naglasiti kako neklasificirani podatak ne predstavlja izuzetak iz odredbe članka 8. Zakona o pravu na pristup informacijama, odnosno pristup neklasificiranim podacima je dostupan svakome tko podnese zahtjev propisan odredbama ZPPI-a.

S druge strane se, međutim, ustanovljavanjem neklasificiranih podataka, štite neklasificirani službeni podaci od neodgovornog raspolaganja afirmirajući pravilo njihovog namjenskog korištenja i sprječavanja zlouporaba te poticanja kulture odgovornog postupanja sa službenim podacima.

Zakon isključuje mogućnost da bi se tajnim podatkom označavali podaci koji bi ukazivali na kaznena djela, prekoračenja i zlouporabe ovlasti ili druge oblike nezakonitog postupanja u državnim tijelima.

Važan segment u demokratskom pristupu reguliranja tajnosti podataka jest njihovo vremensko ograničavanje. U tom smislu Zakon propisuje obveznu trajnu i periodičnu procjenu svrhovitosti dodijeljenog stupnja tajnosti pojedinom podatku te s time u vezi donošenje periodične procjene u pisanom obliku u zakonskim rokovima precizno propisanim za svaki stupanj tajnosti.

Kad postoji interes javnosti, vlasnik podatka dužan je ocjeniti razmjernost između prava na pristup informacijama i štete koja bi otkrivanjem informacija javnosti nastupila šteta po zaštićene vrijednosti, te sukladno tome i na temelju prethodnog mišljenja UVNS-a, odlučiti o zadržavanju stupnja tajnosti, promjeni stupnja tajnosti, deklasifikaciji, ili oslobađanju od obveze čuvanja tajnosti. Osim mišljenja UVNS-a propisana je i obveza izvješćivanja o tome i drugih nadležnih tijela propisanih zakonom.

Zakon propisuje uvjerenje ili certifikat o obavljenoj sigurnosnoj provjeri kao uvjet za dopuštenje pristupa klasificiranim podacima. Za izdavanje certifikata nadležnim se određuje Ured Vijeća za nacionalnu sigurnost. Odluka o izdavanju certifikata donosi se na temelju obavljene sigurnosne provjere (obavljaju ih nadležne sigurnosno-obavještajne agencije-op.) kojom se utvrđuju činjenice potrebne za donošenje ocjene o postojanju sigurnosnih zapreka odnosno o utjecaju utvrđenih činjenica na povjerljivost i pouzdanost osobe za pristup podacima odnosno za raspolaganje istim u skladu sa Zakonom.

U slučaju neizdavanja certifikata nadležno tijelo obvezno je donijeti poseban upravni akt odnosno rješenje na koje osoba kojoj je izdavanje certifikata odbijeno ima pravo pokrenuti upravni spor. U upravnom sporu obvezuje se Upravni sud na mjere zaštite podataka čijim bi otkrivanjem mogle nastupiti štete za rad sigurnosno-obavještajnih agencija i nacionalne sigurnosti. Na ovaj način se odluka UVNS-a o neizdavanju certifikata, a budući da odlučuje o statusnim pitanjima građana, podiže na rang upravnog akta i ostvaruje ustavno jamstvo sudske kontrole nad zakonitosti pojedinačnih akata upravnih vlasti (čl. 19. st. 2 Ustava RH).

Pristup klasificiranim podacima i izdavanje certifikata, bez propisanog postupka za izdavanje certifikata, imaju Predsjednik Republike, predsjednik Hrvatskog sabora i predsjednik Vlade.

Saborski zastupnici, ministri, državni tajnici središnjih državnih ureda, suci i Glavni državni odvjetnik imaju pravo pristupa nacionalnim klasificiranim podacima u okviru svog djelokruga bez certifikata, dakle, bez provođenja sigurnosne provjere, ali uz izjavu kojom potvrđuju upoznatost s odredbama ovog Zakona i drugih propisa kojima se uređuje zaštita klasificiranih podataka.

Za pristup klasificiranim podacima druge države ili međunarodne organizacije, UVNS izdaje poseban certifikat propisan međunarodnim ugovorima, a na temelju zahtjeva nadležnog tijela za izdavanjem certifikata osobi kojoj je isti potreban u okviru poslova predviđenih međunarodnim ugovorom te na temelju prethodno izdanog certifikata za pristup nacionalnim klasificiranim podacima.

Izdavanje certifikata za osobe koje ostvaruju pristup klasificiranim podacima propisano je i Zakonom o sigurnosno-obavještajnom sustavu RH, a dio je prakse većine zemalja članica EU i NATO. Također, potreba njihovog izdavanja kao rezultata prethodno provedenog sustava sigurnosne provjere, implicite proizlazi i iz odredbi Sigurnosnog sporazuma između RH i NATO-a te Ugovora između RH i EU o sigurnosnim postupcima za razmjenu tajnih podataka.

Prilikom izdavanja certifikata ili potpisivanja navedenih izjava Ured Vijeća za nacionalnu sigurnost obvezan je obaviti i sigurnosno informiranje osoba o postupanju s klasificiranim podacima te o pravnim i drugim posljedicama neovlaštenog raspolaganja tim podacima.

Ovaj Zakon se primjenjuje na državna tijela, tijela jedinica lokalne i područne (regionalne) samouprave te pravne osobe s javnim ovlastima, kao i na fizičke i pravne osobe koje ostvaruju pristup ili postupaju s klasificiranim i neklasificiranim podacima. Klasificiranje podataka je ovlast državnih tijela dok se ostali naprijed navedeni subjekti javljaju kao ovlaštenici prava na raspolaganje, a time i čuvanje i postupanje s klasificiranim podacima sukladno zakonu.

Čelnici državnih tijela obvezuju se utvrditi popise poslova u okviru kojih se ostvaruje pristup klasificiranim podacima odnosno osoba kojima je za rad na tim mjestima potrebno prethodno izdati certifikat o obavljenoj sigurnosnoj provjeri.

Ovaj Zakon ne propisuje pojmove poslovne i profesionalne tajne, za razliku od Zakona o zaštiti tajnosti podataka (NN 108/96), budući to nije uobičajeno u zakonima većine zemalja članica EU i NATO. Stoga će ostati na snazi odredbe iz glave 8. i 9. navedenog Zakona o zaštiti tajnosti podataka (NN 108/96) dok se ta materija ne regulira drugim odgovarajućim zakonima.

Segment zaštite podataka u većoj mjeri regulirat će Zakon o sustavu informacijske sigurnosti, koji je sadržajno potpuno usklađen i komplementaran s ovim Zakonom te će sukladno svom djelokrugu na nacionalnoj razini regulirati postupke kreiranja i donošenja mjera i standarda informacijske sigurnosti, njihove implementacije i nadzora.

Nadzor nad provedbom ovog Zakona u nadležnosti je tijela koja raspolažu klasificiranim podacima i Ureda Vijeća za nacionalnu sigurnost.

II OBJAŠNJENJE POJEDINIH ODREDBI

I. OSNOVNE ODREDBE

Prijedlogom Nacrta Zakona o tajnosti podataka uvode se pojmovi klasificiranih i neklasificiranih podataka, reguliraju stupnjevi tajnosti, postupak klasifikacije, odnosno deklasifikacije, pristup i zaštita nad podacima te provedba nadzora. U članku 1. određuje se i djelokrug primjene Zakona. Člankom 2. definiraju se temeljni pojmovi predmetnog Zakona (podatak, dokument, klasificirani i neklasificirani podatak, klasifikacija, deklasifikacija, vlasnici podatka, certifikat). Odredbe iz članka 3. predstavljaju zaštitu od zlouporabe postupka klasificiranja u smislu da bi se klasificirali podaci o počinjenim kaznenim djelima ali i drugim nezakonitostima u radu državnih tijela.

II. STUPNJEVI TAJNOSTI

Odredbe iz članka 4. određuju stupnjeve tajnosti koji se uvode ovim Zakonom (ograničeno, povjerljivo, tajno i vrlo tajno).
U članku 5. određuje se djelokrug državnih tijela u okviru kojega Zakon dopušta klasifikaciju podataka (obrana, sigurnosno-obavještajni poslovi, vanjski poslovi, javna sigurnost, kazneni postupak te znanost, tehnologija, javne financije i gospodarstvo samo ukoliko su od važnosti za sigurnost Republike Hrvatske). Na ovaj način isključuje se mogućnost klasificiranja podataka izvan navedenih područja rada državnih tijela.
U člancima 6. do 9. propisani su kriteriji za određivanje četiri stupnja tajnosti podataka. Navedeni stupnjevi mogu se podijeliti u dvije kategorije. U jednoj kategoriji su stupnjevi tajnosti vrlo tajno, tajno i povjerljivo, a u drugoj stupanj tajnosti ograničeno. Kod stupnjeva tajnosti vrlo tajno, tajno i povjerljivo radi se o podacima čijim bi otkrivanjem nastupila šteta po nacionalnu sigurnost i vitalne interese Republike Hrvatske, a kod stupnja tajnosti ograničeno o podatku čijim bi otkrivanjem nastupila šteta djelovanju i izvršavanju zadaća državnih tijela i to u poslovima iz članka 5.
Stupnjevi tajnosti vrlo tajno, tajno i povjerljivo međusobno se razgraničavaju na temelju stupnja štete po nacionalnu sigurnost i vitalne interese RH koja bi nastala njihovim otkrivanjem (nepopravljiva šteta kod vrlo tajno, teška šteta kod tajno i šteta kod povjerljivo).

Osim navedenih zakonom utvrđenih kriterija za klasifikaciju podataka u članku 10. propisuje se obveza državnih tijela koja će provoditi postupak klasifikacije, da za poslove odnosno podatke iz svog djelokruga, pravilnikom pobliže razrade zakonom utvrđene kriterije za određivanje stupnjeva tajnosti.

III. POSTUPAK KLASIFICIRANJA I DEKLASIFICIRANJA PODATAKA

Odredbe članaka 11. i 12. propisuju temeljne odrednice postupka klasifikacije podataka kao što su vrijeme provođenja postupka klasifikacije, određivanja najnižeg stupnja tajnosti kojim će se osigurati zaštita interesa koji se klasificiranjem štite, te pravilo diferenciranog pristupa klasifikaciji podataka na način da pojedini sastavni dijelovi podatka ne podliježu zakonskim kriterijima za klasificiranje ako su odvojivi od cjeline i ako po svom sadržaju nisu tajni po kriterijima određenim ovim zakonom.
Odredbe iz članka 13. diferenciraju krug ovlaštenika za postupak klasifikacije s obzirom na stupanj klasificiranih podataka na način da stupnjeve tajnosti tajno i vrlo tajno mogu odrediti samo čelnici institucija propisanih zakonom ili osobe na koje prenesu ovlast pisanim putem za podatke u okviru njihovog djelokruga. Stupnjeve tajnosti povjerljivo i ograničeno dopušteno je klasificirati i čelnicima drugih državnih tijela u okviru njihovog djelokruga, sukladno kriterijima utvrđenim zakonom i razrađenim posebnim pravilnikom.
Bitno je naglasiti da iste osobe klasificiraju i podatke za vanjske subjekte koji rade za državna tijela na poslovima koji su od sigurnosnog značaja i interesa za Republiku Hrvatsku.
U člancima 14. i 15. propisuje se obveza vlasnika podatka da vrši trajnu procjenu svrhovitosti dodijeljenog stupnja tajnosti, a u zakonom utvrđenim rokovima i obveza donošenja pisane periodične procjene (5 godina za vrlo tajno, 4 godine za tajno, 3 godine za povjerljivo i 2 godine za ograničeno).
U članku 16. propisuje se da kad postoji interes javnosti, vlasnik podatka dužan je ocjeniti razmjernost između interesa javnosti i prava na pristup informacijama s jedne strane te interesa zaštite tajnosti podataka odnosno vrijednosti opisanih u člancima 6. i 9. čija se zaštita postiže postupkom klasifikacije. Na temelju navedene ocjene i prethodnog mišljenja UVNS-a, vlasnik podatka je dužan donijeti odluku o zadržavanju stupnja tajnosti, promjeni stupnja tajnosti, deklasifikaciji ili oslobađanju od obveze čuvanja tajnosti.
U stavku 3. ovoga članka propisuje se i obveza izvješćivanja o provedenom postupku drugog nadležnog tijela propisanog zakonom, čime se u ovom Zakonu stvara pretpostavka za eventualno naknadno uvođenje u pravni sustav posebne institucije zadužene za provođenje testa javnog interesa odnosno testa razmjernosti između interesa javnosti te interesa zaštićenih podataka i vrijednosti na koje se oni odnose.
U članku 17. propisuje se da će se način označavanja pojedinih stupnjeva tajnosti podataka propisati uredbom Vlade.

IV. PRISTUP PODACIMA

Odredbe iz članaka 18. do 22. propisuju model ostvarivanja pristupa klasificiranim podacima na temelju posjedovanja uvjerenja ili certifikata o obavljenoj sigurnosnoj provjeri koju provodi nadležna sigurnosno-obavještajna agencija na zahtjev Ureda Vijeća za nacionalnu sigurnost, a na temelju zahtjeva državnog tijela za izdavanje certifikata osobama koje ostvaruju pristup klasificiranim podacima.

Certifikat se izdaje na temelju ocjene UVNS-a o nepostojanju, Zakonom utvrđenih, sigurnosnih zapreka za pristup klasificiranim podacima. Zaprekama se propisuju: neistinito navođenje podataka u upitniku za sigurnosnu provjeru, zapreke propisane za prijem u državnu službu, te izrečene stegovne sankcije i utvrđene druge činjenice koje predstavljaju osnovu za sumnju u povjerljivost ili pouzdanost osobe za postupanje s klasificiranim podacima.

U postupku pred Upravnim sudom (čl. 19. st. 3) potrebno je zaštititi tajnost podataka čijim bi otkrivanjem nastupila nerazmjerna šteta za interese sigurnosno-obavještajnih agencija i nacionalne sigurnosti odnosno uravnotežiti zahtjev za očuvanjem tajnosti rada sigurnosno-obavještajnih agencija i zahtjev za sudskom kontrolom nad zakonitošću pojedinačnih akata upravnih vlasti (čl. 19. Ustava RH).

U članku 20. regulira se pristup klasificiranim podacima saborskim zastupnicima, ministrima, državnim tajnicima središnjih državnih ureda, sucima i Glavnom državnom odvjetniku. Oni imaju pravo pristupa nacionalnim klasificiranim podacima, u okviru svog djelokruga, bez certifikata, dakle, bez provođenja sigurnosne provjere, ali uz izjavu kojom potvrđuju upoznatost s odredbama ovog Zakona i drugih propisa kojima se uređuje zaštita klasificiranih podataka.

Za pristup klasificiranim podacima druge države i međunarodne organizacije, Ured Vijeća za nacionalnu sigurnost izdaje poseban certifikat propisan međunarodnim ugovorom ili sigurnosnim sporazumom (čl. 22). Uvjet za izdavanje međunarodnog certifikata je posjedovanje nacionalnog certifikata iz članka 18. ovog Zakona i zahtjev nadležnog tijela za izdavanje odgovarajućeg međunarodnog certifikata osobi u okviru poslova iz njezinog djelokruga.

Pristup neklasificiranim podacima zakonom se omogućuje osobama kojima je to nužno u okviru poslova iz njihovog službenog djelokruga te zainteresiranim ovlaštenicima prava na pristup informacijama na temelju zakonito podnesenog zahtjeva za ostvarivanje prava na pristup informacijama (čl. 23.).

U članku 24. propisuje se pristup klasificiranim podacima Predsjedniku Republike, predsjedniku Hrvatskog sabora i predsjedniku Vlade, na način da su oni izuzeti od propisanog postupka za izdavanje certifikata.

V. ZAŠTITA PODATAKA

U člancima 25. do 28. propisuje se obveza čuvanja klasificiranih podataka za vrijeme i nakon prestanka obavljanja dužnosti sve dok je podatak klasificiran ili dok se osobu ne oslobodi obveze čuvanja tajnosti klasificiranih podataka; zatim postupak utvrđivanja odgovornosti nakon što se klasificirani podatak uništi, otuđi ili učini dostupnim neovlaštenim osobama; te sigurnosno informiranje (upoznavanje) osoba kojima se izdaje certifikat ili koje imaju pristup klasificiranim podacima bez certifikata (čl. 20) o standardima zakonitog postupanja s klasificiranim podacima i zakonskim posljedicama neovlaštenog raspolaganja istima.

VI. NADZOR NAD PROVEDBOM ZAKONA

U odredbama 29. i 30. propisuje se ostvarivanje nadzora nad primjenom ovog Zakona unutar tijela koja raspolažu klasificiranim podacima (vođenje evidencija o izvršenim uvidima i postupanju s klasificiranim podacima, čl. 29.) te ostvarivanje nadzora od strane Ureda Vijeća za nacionalnu sigurnost (čl. 30) nad postupcima klasifikacije i deklasifikacije, ostvarivanjem pristupa klasificiranim i neklasificiranim podacima, provedbi mjera zaštite te izvršavanja obveza proizišlih iz međunarodnih ugovora i sporazuma. U provođenju nadzora UVNS je ovlašten utvrditi činjenično stanje, dati upute u svrhu otklanjanja utvrđenih nedostataka i nepravilnosti, pokrenuti postupak utvrđivanja odgovornosti te poduzeti druge mjere i radnje za koje je ovlašten drugim propisima.
U svrhu provođenja nadzora nad provedbom Zakona u UVNS-u se ustrojavaju središnji registri izdanih certifikata, donesenih rješenja o odbijanju izdavanja certifikata, potpisanih izjava o upoznatosti s odredbama ovog zakona i drugih propisa o raspolaganju klasificiranim podacima, te o obavljenom sigurnosnom informiranju (upoznavanju) ovlaštenika na pristup klasificiranim podacima glede standarda zaštite i raspolaganja klasificiranim podacima te pravnim i drugim posljedicama neovlaštenog raspolaganja istima.

VII. PRIJELAZNE I ZAVRŠNE ODREDBE

U članku 31. st. 1 propisuje se rok od 30 dana za donošenje uredbe kojom će se propisati način označavanja stupnjeva tajnosti klasificiranih podataka (propisana u članku 17.) te sadržaj i izgled sigurnosnih certifikata (propisana u članku 21.).
U stavku 2. istog članka propisuje se rok od 60 dana za donošenje pravilnika iz članka 10. kojim se imaju pobliže razraditi zakonski kriteriji za klasificiranje podataka u okviru djelokruga državnih tijela ovlaštenih za provođenje postupka klasifikacije.
U stavku 3. istog članka propisuje se rok od 90 dana za utvrđivanje popisa dužnosti i poslova iz djelokruga pojedinih državnih tijela za obavljanje kojih je potrebno izdavanje certifikata sukladno uvjetima utvrđenim zakonom.

U članku 32. preimenuju se dosadašnje vrste i stupnjevi tajnosti propisane Zakonom o zaštiti tajnosti podataka NN (108/96) sukladno novim stupnjevima tajnosti propisanim ovim zakonom.

U članku 33. propisuju se rokovi važenja ranije izdanih certifikata, internih dopuštenja za pristup tajnim podacima i podzakonskih propisa donesenih na temelju Zakona o zaštiti tajnosti podataka.

U članku 34. propisuje se ostanak na snazi odredbi iz glava 8. i 9. Zakona o zaštiti tajnosti podataka NN(108/89) u kojima su propisana pitanja u vezi s poslovnom i profesionalnom tajnom.

III OCJENA POTREBNIH SREDSTAVA ZA PROVOĐENJE ZAKONA

Ocjenjuje se da donošenje odnosno provedba ovog Zakona neće iziskivati osiguranje zasebnih sredstava u državnom proračunu Republike Hrvatske.

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

Na temelju ocjena koje su na tekst prijedloga Zakona iznesene na saborskim odborima te potom u prvom čitanju na saborskoj raspravi, napravljena je analiza iznesenih ocjena odnosno primjedbi i prijedloga te su mnoge prihvaćene i potom uvrštene u Konačni prijedlog Zakona.

Prihvaćene su primjedbe Odbora za ljudska prava i prava nacionalnih manjina te saborskih zastupnika Nenada Stazića, Mate Arlovića, Pere Kovačevića i Šime Lučina da je stupanj tajnosti ograničeno određen preširoko te se u članku 9. prijedloga izostavljaju podaci koji se odnose na rad tijela jedinica lokalne i područne (regionalne) samouprave i na pravne osobe s javnim ovlastima, te se u članku 9. konačnog Prijedloga stupnjem tajnosti ograničeno propisuju samo podaci čijim bi neovlaštenim otkrivanjem nastupile štete u radu i izvršavanju zadaća državnih tijela. Na tragu iste primjedbe članak 5. koji propisuje djelokrug državnih tijela u okviru kojeg je moguće klasificirati podatke, referira se u konačnom Prijedlogu i na stupanj tajnosti ograničeno čime se taj stupanj tajnosti svodi na striktno određene poslove iz djelokruga državnih tijela (obrana, sigurnosno-obavještajni poslovi, vanjski poslovi, javna sigurnost, kazneni postupak te znanost, tehnologija, javne financije i gospodarstvo samo ako su od sigurnosnog interesa za RH) i time se otklanja mogućnost širokog tumačenja kriterija za određivanje stupnja tajnosti ograničeno i time mogućnost zlouporaba u primjeni zakona.

Na tragu iznesenih primjedbi na široku određenost stupnjeva tajnosti uvrštene su izmjene u članku 6. st. 1 alineja 7 na način da se pod vrijednostima koje se štite stupnjevima tajnosti povjerljivo, tajno i vrlo tajno uzimaju samo ona znanstvena otkrića, pronalasci i tehnologije koja su od važnosti za nacionalnu sigurnost, a izbacuje se iz ranijeg prijedloga otkrića, pronalaske i tehnologije od znanstvenog interesa za RH.

Prihvaćene su primjedbe iznesene od strane Odbora za informiranje, informatizaciju i medije, te zastupnika Pere Kovačevića, Šime Lučina i Dorotee Pešić Bukovac da je krug ovlaštenika na klasifikaciju široko određen i da su tijela lokalne vlasti u tom smislu dobila preširoke ovlasti.

Tako je u članku 13. st. 1 izostavljena ovlast odgovornih osoba u znanstvenim ustanovama, zavodima i institucijama kada rade na projektima, pronalascima i tehnologijama od sigurnosnog i znanstvenog interesa RH, te je u čl. 13. st. 4 konačnog prijedloga propisano da klasifikaciju za znanstvene ustanove, zavode i druge pravne osobe kada rade na projektima, pronalascima, tehnologijama i drugim poslovima od sigurnosnog interesa za RH, obavljaju čelnici državnih tijela i osobe koji oni za to pismeno ovlaste za podatke u okviru njihovog djelokruga.
U članku 13. st. 3 ukinuta je odredba po kojoj su čelnici tijela jedinica lokalne (regionalne) samouprave te čelnici pravnih osoba s javnim ovlastima bili ovlašteni klasificirati podatke stupnja tajnosti ograničeno.
Također je slijedom reduciranja kruga ovlaštenika na klasificiranje u članku 16. Prijedloga izostavljena ovlast tijela lokalne i područne (regionalne) samouprave i pravne osobe s javnim ovlastima da internim aktima utvrde kriterije za određivanje stupnjeva tajnosti unutar svog djelokruga te je u članku 10. konačnog Prijedloga propisana obveza isključivo državnih tijela

da u okviru svog djelokruga i uz suglasnost UVNS-a donesu pravilnike kojima će pobliže razraditi zakonom utvrđene kriterije za određivanje stupnjeva tajnosti podataka unutar svog djelokruga.

U članku 11. konačnog Prijedloga je postupak klasifikacije, osim pri nastanku podatka, propisan i kod periodične procjene podatka čime se tekst zakona jezično usklađuje s namjeravanim načinom uređenja ovog dijela materije.

U članku 14. st. 1 uvedena je obveza vlasnika podatka da provodi trajnu procjenu svrhovitosti dodijeljenog stupnja tajnosti, a u čl. 14. st. 2 smanjen je rok za stupanj tajnosti povjerljivo s 4 na tri godine. Na ovaj način se usvaja dio preporuka posebnog predstavnika OESS-a za slobodu medija.

Odbor za ljudska prava i prava nacionalnih manjina te zastupnici Šime Lučin, Dorotea Pešić Bukovac i Nenad Stazića ukazali su na potrebu postojanja neovisnog tijela koje bi provodilo test interesa javnosti. Ovu primjedbu uputile su i udruge civilnog društva (GONG, Transparency International Croatia i drugi) i posebni predstavnik OESS-a za slobodu medija. Primjedbe su uvažene u skladu s nadležnošću ovog Zakona na način da se u članku 16. uvodi obveza vlasnika podatka da u slučaju kada postoji interes javnosti, ocijeni razmjernost između interesa javnosti odnosno prava na pristup informacijama s jedne strane i zaštićenih vrijednosti s druge strane te da, uz prethodno mišljenje UVNS-a, donese konačnu odluku o daljnjem statusu podatka kao i da o navedenom postupku izvijesti druga tijela određena zakonom (čl. 16. st. 3).

Prihvaćene su i primjedbe Odbora za ljudska prava i prava nacionalnih manjina te zastupnika Šime Lučina, Ante Markova, Dorotee Pešić Bukovac i Mate Arlovića, o nedostatnim mehanizmima kontrole nad provedbom zakona, te su članci 17. i 18. izmijenjeni na način da je uvedena sudska kontrola nad postupkom izdavanja certifikata o obavljenoj sigurnosnoj provjeri na temelju kojeg se dopušta pristup klasificiranim podacima odnosno mogućnost pokretanja upravnog spora protiv rješenja kojim se odbija izdavanje certifikata. Ovim su prihvaćene i sugestije dostavljene od strane Hrvatske obrtničke komore.

U članku 18. st. 6 konačnog Prijedloga propisane su sigurnosne zapreke za izdavanje certifikata, čime se eliminira moguća primjedba nedovoljne pravne određenosti tog dijela materije.

Uvažene su primjedbe zastupnika Šime Lučina, Ante Markova, Nikole Vuljanića i Mate Arlovića po pitanju izuzeća saborskih zastupnika od postupka sigurnosnog provjeravanja i izdavanja certifikata te se u članku 20. propisuje da saborski zastupnici, ministri, državni tajnici središnjih državnih ureda, suci i Glavni državni odvjetnik imaju pravo pristupa nacionalnim klasificiranim podacima u okviru svog djelokruga bez certifikata, dakle, bez provođenja sigurnosne provjere, te uz izjavu kojom potvrđuju upoznatost s odredbama ovog Zakona i drugih propisa kojima se uređuje zaštita klasificiranih podataka.

Djelomično je prihvaćena primjedba saborskog zastupnika Pere Kovačevića da međunarodni ugovori ne dopuštaju izuzetke od postupka sigurnosnog provjeravanja te se u članku 22. propisuje izdavanje posebnih certifikata na temelju međunarodnih ugovora za pristup klasificiranim podacima stranih država ili organizacija. Uvjet za izdavanje ovih certifikata je posjedovanje nacionalnog certifikata iz članka 18. konačnog Prijedloga i zahtjev nadležnog

tijela koji se treba temeljiti na potrebi pristupa određene osobe klasificiranim podacima stranih zemalja ili organizacija.

Predsjedniku Republike, predsjedniku Hrvatskog sabora i predsjedniku Vlade RH izdaje se certifikat bez provođenja sigurnosne provjere (članak 24. konačnog prijedloga).

Prihvaćena je primjedba iznesena na Odboru za ljudska prava i prava nacionalnih manjina i Odboru za informiranje, informatizaciju i medije o neodređenosti pojma neklasificiranog podatka te je isti jasnije definiran u članku 2. st. 1 alineja 3 te u članku 23. u smislu reguliranja prava pristupa takvim podacima (u službene svrhe radi obavljanja poslova iz propisanog djelokruga i zainteresiranim ovlaštenicima prava na pristup informacijama na temelju zakonito podnesenog zahtjeva).

U članku 28. konačnog Prijedloga u cilju pojačavanja mjera zaštite tajnih podataka propisuje se postupak upoznavanja s sigurnosnim standardima osoba koje ostvaruju pristup klasificiranim podacima prilikom izdavanja certifikata, prilikom potpisivanja izjave iz članka 20. st. 2 te periodično jednom godišnje za vrijeme važenja certifikata.

U članku 30. st. 1 i 2 konačnog Prijedloga poboljšane su ranije odredbe o provedbi nadzora od strane UVNS-a propisane u člancima 22. i 23. Prijedloga, a u čl. 30. st. 3 propisuje se u UVNS-u ustrojavanje registara izdanih certifikata, rješenja o odbijanju izdavanja certifikata, potpisanih izjava o upoznatosti s pravilima postupanja s klasificiranim podacima te obavljenih sigurnosnih upoznavanja ili informiranja.

U prijelaznim i završnim odredbama izmijenjen je članak 24. na način da se u članku 31. st. 1 umjesto dvije propisuje donošenje jedne uredbe Vlade te u čl. 31. st. 3 konačnog prijedloga propisano je utvrđivanje popisa dužnosti i poslova iz djelokruga državnih tijela za koja je potrebno izdavanje certifikata u roku od 90 dana od stupanja na snagu ovog Zakona.

U prijelaznim i završnim odredbama konačnog prijedloga (čl. 32.) propisuje se nastavak važenja odredbi iz poglavlja 8. i 9. Zakona o zaštiti tajnosti podataka kojima je obuhvaćena materija poslovnih i profesionalnih tajni. Ovim je uvažen zahtjev Hrvatskih sindikata.

V PRIJEDLOZI I MIŠLJENJA KOJA NISU PRIHVAĆENA I RAZLOZI

Nije prihvaćen prijedlog Odbora za ljudska prava i prava nacionalnih manjina i zastupnika Nikole Vuljanića da se utvrde kaznene sankcije za kršenje odredbi iz članka 21. (čl. 27. u konačnom prijedlogu) za slučaj uništenja, otuđenja ili činjenja dostupnih neovlaštenim osobama tajnih podataka, iz razloga što je tajnost podataka već utvrđeni predmet ili objekt zaštite Kaznenog zakona Republike Hrvatske.

Nije prihvaćen prijedlog Odbora za ljudska prava i prava nacionalnih manjina da se preispita potreba uređenja, ovim Zakonom, poslovne tajne iz razloga što poslovna tajna po kriterijima većine komparativnog zakonodavstva nije regulirana zajedno s tajnama iz djelokruga državnih tijela već odvojeno, najčešće u okviru propisa o tržišnom poslovanju.

Nije prihvaćen prijedlog Odbora za ljudska prava i prava nacionalnih manjina da se razmotri propisivanje instrumenata koji će osigurati nadzor podzakonskih akata od strane Hrvatskog

sabora i Pučkog pravobranitelja iz razloga što će podzakonski akti prema konačnom prijedlogu zakona biti javno objavljeni te će biti moguće bilo kojoj zainteresiranoj osobi pokrenuti redovni postupak za ocjenu zakonitosti ili ustavnosti dok Pučki pravobranitelj i po svojoj redovnoj nadležnosti ima pravo uvida i davanja ocjene na bilo koji opći ili pojedinačni akt tijela javne uprave u dijelu u kojem se to tiče sloboda i prava građana.

Nije prihvaćena primjedba zastupnika Pere Kovačevića da nisu utvrđeni temelji i mjerila za određivanje pojedinih stupnjeva tajnosti te da bi ih sve trebalo propisati zakonom, a ne podzakonskim normama. Primjedba nije prihvaćena jer zakon u člancima 5. do 9. propisuje kriterije ili mjerila za sve stupnjeve tajnosti na način i u mjeri koja je uobičajena u komparativnom zakonodavstvu dok se dodatno određivanje kriterija u podzakonskim normama javlja kao nužno zbog velikih razlika i posebnosti u radu pojedinih državnih tijela čime se izbjegava neodređenost i pretjerana uopćenost pravnih propisa. S obzirom da pravilnici o kriterijima za određivanje stupnjeva tajnosti moraju biti u skladu s ovim Zakonom, da u tom pogledu UVNS provodi nadzor te da se pravilnici javno objavljuju neće biti mogućnosti odstupanja od zakonskih kriterija, a s druge strane će se osigurati mogućnost izražavanja posebnosti pojedinih državnih tijela u skladu s vlastitim opisima poslova.

Nije usvojena primjedba zastupnika Ante Markova da se u zakonu navedu objekti interesa državnih tijela (špijunaža, terorizam,, ekstremizam, organizirani kriminal i slično) u okviru kojih bi se klasificirali podaci, jer zakon po uzoru na komparativno zakonodavstvo, propisuje područja rada državnih tijela u kojima se klasificiraju podaci u odnosu na stupanj štete koja bi otkrivanjem podataka nastupila po interese nacionalne sigurnosti. Daljnja razrada stupnja tajnosti podataka s obzirom na navedene i druge predmete interese državnih tijela, predviđena je za podzakonske norme dok bi predloženim načinom svojom detaljnošću opterećivala opću strukturu zakonskog teksta.
Nije usvojen prijedlog zastupnika Ante Markova za propisivanjem posebnog parlamentarnog nadzora jer isti nije uobičajen u komparativnom zakonodavstvu, odnosno već postoje u zakonu adekvatni sustavi nadzora kao i mogućnost korištenja nadzora Hrvatskog sabora u okviru njegovih općih ustavnih nadležnosti.

Nije prihvaćen prijedlog zastupnika Šime Lučina da se izradi registar osoba koji bi mogli proglašavati stupnjeve tajnosti jer zbog znatnog smanjivanja broja takvih osoba u konačnom prijedlogu zakona, nema potrebe da se posebnim registrima dodatno nadzire cjelokupni proces klasificiranja podataka.

Nije prihvaćen prijedlog zastupnice Dorotee Pešić Bukovac da se zakonski propiše vođenje jedinstvenog registra klasificiranih podataka zbog toga što se drži da bi na taj način negativni učinci od troškova administriranja te centralizacije tih podataka s obzirom na sigurnosno načelo ograničenog pristupa podacima (*need to know*), bili nerazmjerni očekivanoj koristi osobito s obzirom na nadzorne ovlasti UVNS-a koje u slučaju opravdane potrebe podrazumijevaju dolazak do svih podataka ekvivalentnih registru klasificiranih podataka.

Nisu prihvaćene primjedbe zastupnice Ingrid Antičević Marinović usmjerene na ulogu sigurnosno-obavještajnih agencija u provedbi dijela poslova zaštite klasificiranih podataka jer se radi o poslovima iz redovnog djelokruga službi takvog tipa kao niti primjedba o tome da ovaj Zakon dezavuira Zakon o pravu na pristup informacijama osobito nakon što je u konačnom prijedlogu smanjen opseg poslova u okviru kojih je moguće obavljati klasifikaciju kao i broj i vrsta odnosno osoba koje mogu obaviti postupak klasifikacije.

Nisu prihvaćene primjedbe zastupnika Mate Arlovića da pravilnik o kriterijima za određivanje stupnjeva tajnosti treba biti usuglašen s Uredbom iz članka 29. zakona jer se Uredbom propisuju sadržaji koji nisu osnova za donošenje navedenog pravilnika odnosno radi se o sadržajno različitoj materiji.
Nisu prihvaćene primjedbe zastupnika Mate Arlovića da prijedlog zakona nije usklađen s Ustavom RH i da je u suprotnosti s zakonom o pravu na pristup informacijama te primjedbe na pojam vlasništva nad informacijama. Naime, predlagatelj Zakona ne vidi u kojem dijelu eventualno odredbe ovog zakona ne bi bile u skladu s Ustavom i navedenim Zakonom dok je termin vlasnika podatka rezultat pojmovne i terminološke uskladbe s odgovarajućim propisima zemalja članica EU dok nije izvjesno da bi takav termin bio u neskladu s hrvatskim pravnim poretkom.

PREDMET: Konačni prijedlog Zakona o tajnosti podataka
-osvrt na mišljenje Ureda za zakonodavstvo Vlade RH

Veza: dopis Ureda za zakonodavstvo klasa: 200-01/07-01/01 ur. broj: 50501-07-593-02 od 8. lipnja ove godine

Slijedom mišljenja Ureda za zakonodavstvo, UVNS je kao stručni nositelj izrade konačnog prijedloga Zakona, uvažio dio primjedbi i uvrstio ih u konačni tekst na način kako slijedi:

- u članku 2. podstavci 2. i 7. ujednačeni su izričaji na način da se u oba navedena podstavka sada govori o „nadležnim tijelima"
- u članku 2. početne riječi u podstavcima napisane su malim slovom
- u članku 2. podstavak 4. izostavljen je podstavak 4. te je njegov sadržaj odgovarajuće nadodan u podstavcima 2. i 3.
- u članku 15. st. 1. odnosno 16 st. 1. po numeraciji nakon obavljenih ispravaka izostavljena je riječ „ograničenja" čime tekst odredbe postaje jasniji
- sukladno ocjeni Ureda za zakonodavstvo izbrisan je članak 16. st. 2. kao nepotreban (o objavljivanju pravilnika o utvrđivanju kriterija za klasifikaciju u Narodnim novinama) jer se po općim propisima ionako imaju objaviti osim ako to ne bi bilo izrijekom drugačije propisano
- izbrisan je stavak 7. u članku 17., odnosno 18. prema novoj numeraciji, kojim je bilo određeno da se u slučaju dvojbi u ocjeni o postojanju sigurnosnih zapreka neće izdati certifikat
- u članku 12. st. 3. izostavljen je završni dio rečenice koji glasi „te službi i agencija odgovornih Vladi RH"
- članak 28. je prebačen iz VII poglavlja (prijelazne i završne odredbe) u IV poglavlje (pristup podacima), članak 24.
- sadržaj članka 29. st. 1. kojim se utvrđuju ovlasti za donošenje uredbe Vlade preraspoređeni su u odgovarajuća poglavlja u člancima 17. i 21.
- na više mjesta je u tekstu ujednačen izričaj koji se odnosi na pojmove „klasificirati" i „odrediti stupanj tajnosti"
- promijenjen je tekst članka 25, po novoj numeraciji 28., na način da je pojam „sigurnosno informiranje" zamijenjen s „upoznavanjem sa standardima postupanja s klasificiranim podacima"
- u članku 31. st. 2 , po novoj numeraciji 33. st. 2, ispravljen je naziv medija u kojem će se zakon objaviti.

Dio primjedbi Ureda za zakonodavstvo Ured Vijeća za nacionalnu sigurnost kao stručni nositelj izrade konačnog prijedloga Zakona, nije mogao prihvatiti jer su smjerale na izmjene koje strukovno i na razini pravnih načela (npr. pozivanje na načela ustavnog i kaznenog prava u materiji upravnog prava) nisu održive.