NOVI TEKST

REPUBLIKA HRVATSKA
URED VIJEĆA ZA NACIONALNU SIGURNOST

NACRT PRIJEDLOGA

ZAKONA O TAJNOSTI PODATAKA

Zagreb, siječanj 2007.

I. USTAVNA OSNOVA ZA DONOŠENJE ZAKONA

Ustavna osnova za donošenje Zakona sadržana je u odredbama članka 37. stavak 2. Ustava Republike Hrvatske.

II. OCJENA STANJA I OSNOVNA PITANJA KOJA SE TREBAJU UREDITI ZAKONOM TE POSLJEDICE KOJE ĆE DONOŠENJEM ZAKONA PROISTEĆI

A) OCJENA STANJA

Područje koje se ovim zakonskim prijedlogom treba urediti djelomično je propisano Zakonom o zaštiti tajnosti podataka (NN 108/96) i Zakonom o sigurnosno-obavještajnom sustavu RH (NN 79/06, 105/06). 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). Tim se dokumentom ovo važno područje tajnosti podataka po prvi puta zakonski uredilo i njime su postavljena načela tajnosti podataka, vrste tajnosti i klasifikacija, postupci za određivanje tajnosti, nadležnosti pojedinih tijela te zaštitne mjere.

Zakon o zaštiti tajnosti podataka (NN 108/96) je u načelima tajnosti podataka, propisao niz rješenja preuzetih iz 80-tih godina dvadesetog stoljeća, koja nisu u skladu sa suvremenim standardima tajnosti podataka zemalja EU-a i NATO-a te drugih razvijenih demokratskih zemalja. Primjerice, to su neodgovarajuća klasifikacija prema stupnjevima i vrstama tajnosti za državne podatke, nepostojanje elementarnih načela za pristup tajnim podacima kao što su princip poslovne ili službene potrebe (need-to-know pravilo), sigurnosna provjera sa certifikatom kao osnovni uvjet te neadekvatno tretiranje temeljnih demokratskih standarda kao što su osobni podaci i pojam privatnosti općenito.

U međuvremenu je dio ove problematike, koji se odnosi na sve pravne i fizičke osobe, propisan Zakonom o zaštiti osobnih podataka (NN 103/03) i Zakonom o pravu na pristup informacijama (NN 172/03). Slijedom toga, preostalo je zakonski regulirati temeljne principe tajnosti podataka u državnoj upravi, koje donosimo prijedlogom ovog Zakona.

Tako, primjerice, Zakon o zaštiti tajnosti podataka (NN 108/96) ne definira sigurnosnu oznaku za neklasificirane podatke (neklasificirano), a u slučaju državne, vojne ili službene tajne ne utvrđuje nužnost provođenja postupka sigurnosne provjere i certificiranja osoblja. Zakon o zaštiti tajnosti podataka (NN 108/96) propisuje obavezu prema kojoj su čelnici javnih tijela i ovlašteni dužnosnici RH dužni donijeti posebne propise o utvrđivanju stupnja i vrste tajnosti, načina i mjesta označavanja tajni, trajanja tajnosti te drugih mjera zaštite tajnih podataka, ovisno o djelokrugu rada, odnosno mjestu nastanka, obrade ili čuvanja tajnih podataka, čime se ne može osigurati konzistentnost ovih postupaka na državnoj razini.

Zakon o zaštiti tajnosti podataka (NN 108/96) propisuje način određivanja zaštitnih mjera u području zaštite tajnih podataka, prema kojem su čelnici tijela javne vlasti i ovlašteni dužnosnici RH ovlašteni i dužni određivati posebne zaštitne mjere te donositi propise o

zaštitnim mjerama i propise vezane uz tajnost podataka. Posljedica ovakvog pristupa zaštiti tajnih podataka je nepostojanje zajedničkih minimalnih sigurnosnih kriterija na nacionalnoj razini u RH, jer najveći broj državnih tijela u kadrovskom smislu nije osposobljen za razvoj sigurnosnih standarda i provedbu zaštitnih mjera. Upravo stoga samo mali broj tijela sigurnosnog sustava RH u širem smislu, danas (deset godina nakon donošenja Zakona o zaštiti tajnosti podataka) ima donesene propise i implementirane određene zaštitne mjere.

Ovakvo stanje ne zadovoljava zahtjeve NATO-a i EU-a za provedbu minimalnih sigurnosnih standarda jer pristup sigurnosti u državnim tijelima nije izjednačen i nisu određeni minimalni sigurnosni zahtjevi koje moraju zadovoljiti sva državna tijela, kao i informacijska infrastruktura u RH. Tijela koja su donijela vlastite propise različito uređuju ovu problematiku, imaju različito učinkovita sigurnosna rješenja te time i različitu primjenu mjera i standarda zaštite tajnosti podataka u praksi. Najveći broj tijela državne uprave nema potrebne kadrovske resurse, kao ni potrebna znanja za primjenu mjera.

Zakon o zaštiti tajnosti podataka (NN 108/96) propisuje da nadzor nad provedbom zaštite tajnih podataka obavlja čelnik tog tijela ili osoba koju on za to ovlasti. S druge strane, Zakonom o sigurnosno-obavještajnom sustavu RH (NN 79/06, 105/06) regulirano je da poslove redovitog nadzora organizacije i implementacije propisanih mjera informacijske sigurnosti u državnim tijelima provodi Sigurnosno-obavještajna agencija (SOA) te u tom smislu treba obaviti usklađivanje odredaba ovih dvaju Zakona, kako bi se razjasnilo tko, pod kojim uvjetima i u kojoj mjeri provodi nadzor. Kod usklađivanju Zakona potrebno je postići razdvajanje nadležnosti u poslovima kreiranja i propisivanja mjera i standarda informacijske sigurnosti te njihove implementacije i nadzora.

Zakon o zaštiti tajnosti podataka (NN 108/96) nije propisao međunarodno prihvaćenu podjelu na četiri stupnja tajnosti podataka (TOP SECRET, SECRET, CONFIDENTIAL, RESTRICTED, UNCLASSIFIED), već je umjesto toga uveo komplicirani sustav više vrsta tajnosti (državna, vojna, službena) s jednim odnosno tri stupnja tajnosti po vrsti. Iz toga proizlaze i problemi u potpisivanju međunarodnih sigurnosnih sporazuma, pri čemu se pokušavaju izjednačiti dva izvorno različita sustava tajnosti. Na ovaj način RH ne može osigurati odgovarajuću pravnu i praktičnu zaštitu klasificiranih podataka EU-a, NATO-a i drugih zemalja, jer nacionalno propisane vrste tajnosti nemaju jednak tretman u kazneno-procesnom sustavu RH, kao ni u praksi rada državnih tijela.

Tako se nedostatnost Zakona o zaštiti tajnosti podataka (NN 108/96) posebno očituje u slabim ili otežanim mogućnostima sankcioniranja u slučaju nestanka ili otkrivanja tajnoga podatka. Mogućnost za tek djelomično sankcioniranje pravnih ili fizičkih osoba koji su sudjelovali u otkrivanju tajnih podataka postoji samo u slučaju nestanka ili otkrivanja državne tajne, koja je, u stvari, sukladna međunarodnom stupnju tajnosti „Top Secret", dok su ostala tri međunarodna stupnja tajnosti nezadovoljavajuće riješena u ovom dijelu.

Osim postupka klasifikacije Zakon o zaštiti tajnosti podataka (NN 108/96) koji nije zadovoljavajuće riješen, Zakon ne regulira postupak uklanjanja stupnjeva tajnosti podataka (deklasifikacije).

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

Ovim Zakonom se uređuje područje tajnosti podataka kroz određivanje pojmova klasificiranih i neklasificiranih podataka. Određuju se novi stupnjevi tajnosti podataka usklađeni sa suvremenim standardima tajnosti podataka zemalja EU-a i NATO-a te drugih razvijenih demokratskih zemalja.

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

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 (tvrtke) koje ostvaruju pristup ili postupaju s klasificiranim i neklasificiranim podacima.

Prateći standarde zemalja EU-a i NATO-a i uzimajući u obzir praksu u suvremenoj državnoj i poslovnoj komunikaciji, bilo je nužno definirati pojam podatak, od kojeg polazi sam koncept zaštite. Ovaj Zakon daje jasnu podjelu podataka, ovisno o njihovoj klasificiranosti prema stupnju tajnosti ili bez tajnosti te uvodi pojmove podatak, klasificirani podatak i neklasificirani podatak.

Ovaj Zakon donosi promjenu u označavanju stupnjeva tajnosti klasificiranih podataka. Prethodno je postignuta suglasnost niza državnih tijela (Ministarstvo obrane, Ministarstvo unutarnjih poslova, Ured Predsjednika RH, Središnji državni ured za upravu, Središnji državni ured za e-Hrvatsku, Ministarstvo vanjskih poslova i europskih integracija, Protuobavještajna agencija, Obavještajna agencija[1], Vojna sigurnosna agencija[2], Državno odvjetništvo i dr.) oko potrebe potpunog usklađivanja označavanja tajnosti podataka s iskustvima i pravilima ustrojenima u zemljama EU-a i NATO-a, čime se klasifikacija podataka svodi na određivanje stupnjeva tajnosti, a odustaje se od pristupa određivanja tajnosti po vrsti (državna tajna, službena tajna, vojna tajna).

Jasno je prepoznata neusklađenost pristupa koji daje Zakon o zaštiti tajnosti podataka (NN 108/96) i potreba koje proizlaze iz komunikacije s drugim zemljama i organizacijama, kao i odredbi sigurnosnih sporazuma koje je RH potpisala s NATO-om, drugim zemljama članicama NATO-a i EU-a te sigurnosnog sporazuma koji je u travnju 2006. godine potpisan s Europskom Unijom.

Pojmovi poslovne i profesionalne tajne, kako ih definira Zakon o zaštiti tajnosti podataka (NN 108/96), nije uobičajeno regulirati na ovaj način u sustavima zapadnih demokracija. Stoga napominjemo kako se Nacrt prijedloga Zakona o tajnosti podataka ograničio samo na reguliranje tajnosti podataka u državnom sustavu i za one pravne i fizičke osobe koje su u poslovnom odnosu s bilo kojim tijelom državnog sustava. Tajnost podataka pravnih i fizičkih osoba izvan državnog sustava (privatni sektor) regulira se internim pravilima, u skladu i oslanjajući se pri tom na pravni sustav zemlje (zaštita intelektualnog i industrijskog vlasništva, patenti i dr.).

---

[1] Temeljem novog Zakona o sigurnosno-obavještajnom sustavu Sigurnosno-obavještajna agencija (SOA) preuzela je poslove koje su do tada obavljale Protuobavještajna agencija (POA) i Obavještajna agencija (OA)

[2] Temeljem novog Zakona o sigurnosno-obavještajnom sustavu djeluje pod nazivom Vojna sigurnosno-obavještajna agencija (VSOA)

Ovaj Zakon prepoznaje vlasnika podatka kao tijelo koje stvara podatak. Ako je to tijelo, sukladno odredbama ovog Zakona, ovlašteno za klasifikaciju, tada ono, kao vlasnik podatka, u smislu ovog Zakona postaje odgovorno za njegovu klasifikaciju, deklasifikaciju i periodičnu procjenu tajnosti. Ujedno, vlasnik podatka dužan je izraditi procjenu štetnosti neovlaštenog otkrivanja podatka kako bi mogao odrediti stupanj njegove tajnosti.

Ovaj Zakon uvodi pojam Uvjerenja o sigurnosnoj provjeri (Certifikat) koji zaposlenici u tijelima javne vlasti moraju posjedovati kako bi mogli pristupati klasificiranim podacima. Certifikat izdaje Ured Vijeća za nacionalnu sigurnost (UVNS) nakon provedenog postupka sigurnosne provjere. Ova praksa je već primijenjena slijedom odredbi Sigurnosnog sporazuma RH i NATO-a za pristup klasificiranim podacima NATO-a, a i Sigurnosni sporazum s EU-om ima slične odredbe. Izuzetak od postupka izrade sigurnosne provjere sveden je na najmanju moguću mjeru (predsjednici države, Sabora i Vlade), unatoč smjernicama EU-a i NATO-a koje predlažu sustav bez izuzetaka.

Zaštitu podataka ne regulira ovaj Zakon, već Zakon o sustavu informacijske sigurnosti, koji se donosi u paketu i koji će na nacionalnoj razini regulirati postupke kreiranja i donošenja mjera i standarda informacijske sigurnosti, implementacije u određenim tijelima te stalnog nadzora.

Nadzor nad pristupom klasificiranim podacima u nadležnosti je samih tijela, dok nadzor provedbe ovog Zakona, kao i ostalih podzakonskih akata koji iz njega proizlaze, obavlja Ured Vijeća za nacionalnu sigurnost.

S tekstom Nacrta prijedloga Zakona upoznate su udruge civilnog društva i predstavnici medija, kojima je predstavljen novi koncept i princip tajnosti podataka. Udruge civilnog društva (Hrvatski helsinški odbor, GONG, Transparency International) te Hrvatska obrtnička komora, dali su svoje primjedbe na neke odredbe prethodnog prijedloga, pri čemu su određeni prijedlozi prihvaćeni, naročito po pitanjima:

- ograničenja na mogućnost proglašavanja nekog podatka klasificiranim (uvedena nova odredba u članku 3., te u članku 15., stavak 2.);

- utvrđena su područja u kojima se mogu pojaviti klasificirani podaci (članak 5.);

- jasnije su definirane ovlaštene osobe i tijela koja mogu obavljati postupak klasifikacije i deklasifikacije, odnosno, određivanje stupnjeva tajnosti za podatke (članak 10.);

- naglašena je važnost periodične procjene daljnjeg trajanja klasificiranosti nekog podatka, što su vlasnici podataka dužni provoditi za sve stupnjeve tajnosti podataka najmanje jednom u razdoblju od dvije do pet godina (članak 12. stavak 2.);

- uvedena je odredba u članku 19. stavku 2. koja govori kada i pod kojim uvjetima vlasnik podatka može odlučiti o uklanjanju stupnja tajnosti podatka ili oslobađanja obveze čuvanja tajnosti podatka.

Pored ovih, predlagač je unio izmjene kojima se dodatno i jasnije definiraju područja u kojima se osobito mogu pojaviti tri viša stupnja tajnosti (VRLO TAJNO, TAJNO i POVJERLJIVO). Ove izmjene su uvedene u člancima 6., 7. i 8.

U razmatranju primjedbi i prijedloga koje su se odnosile na prethodni Nacrt prijedloga Zakona, ističemo kako je predlagač unio one izmjene koje ne mogu utjecati na definirani koncept i princip tajnosti podataka koji se ovim prijedlogom Zakona uvodi.

U vezi s odredbama Zakona o pravu na pristup informacijama (ZPPI) potrebno je naglasiti kako se odredbe članka 8. ZPPI-a ne primjenjuju na podatke koji se ovim prijedlogom Zakona definiraju kao neklasificirani podaci. Sukladno tome, pristup do neklasificiranih podataka je moguć za svakoga tko provede proceduru definiranu odredbama ZPPI-a.

III. OCJENA POTREBNIH SREDSTAVA ZA PROVOĐENJE ZAKONA

Ocjenjuje se da donošenje, odnosno provedba ovog Zakona neće zahtijevati osiguranje posebnih sredstava u Državnom proračunu Republike Hrvatske u 2007. godini.

IV. TEKST NACRTA PRIJEDLOGA ZAKONA O TAJNOSTI PODATAKA S OBRAZLOŽENJEM

Tekst Nacrta prijedloga Zakona dan je u obliku Nacrta prijedloga Zakona o tajnosti podataka s obrazloženjem.

NACRT PRIJEDLOGA
ZAKONA O TAJNOSTI PODATAKA

I. OSNOVNE ODREDBE

Članak 1.

(1) Ovim Zakonom se utvrđuje pojam podatka, klasificiranog i neklasificiranog podatka, sadržaj i stupnjevi tajnosti podataka, postupak klasifikacije i deklasifikacije, pristup klasificiranim podacima, odgovornost vlasnika podatka te provedba nadzora.

(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 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.
- Neklasificirani podatak je podatak bez utvrđenog stupnja tajnosti, za koji su zakonom ili drugim propisima utvrđena ograničenja uporabe samo u službene svrhe.
- Klasificirani, odnosno neklasificirani podatak, je i onaj 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.
- Vlasnici podatka su državna tijela, tijela jedinica lokalne i područne (regionalne) samouprave, kao i pravne osobe s javnim ovlastima, u okviru čijeg djelovanja je podatak nastao.
- Certifikat je uvjerenje o sigurnosnoj provjeri koje omogućava pristup klasificiranim podacima osobama kojima je pristup takvim podacima nužan za obavljanje poslova iz vlastitog djelokruga rada.

Članak 3.

Klasificiranim podatkom ne može se proglasiti podatak radi prikrivanja kaznenog djela, prekoračenja ili zlouporabe ovlasti ili bilo kojeg drugog nezakonitog djelovanja.

II. STUPNJEVI TAJNOSTI

Članak 4.

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

Članak 5.

Stupnjevima tajnosti „VRLO TAJNO“, „TAJNO“ i „POVJERLJIVO“ mogu se, s obzirom na stupanj ugroze, klasificirati podaci iz područja nacionalne sigurnosti, obrane, vanjskih poslova, izvida i istraga kaznenih djela, kao i podaci od osobitog interesa za Republiku Hrvatsku u području znanosti, istraživanja, tehnologije, gospodarstva i financija.

Članak 6.

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

- temelji Ustavom utvrđenog ustrojstva Republike Hrvatske,
- neovisnost, cjelovitost i sigurnost Republike Hrvatske,
- međunarodni ugled i diplomatski odnosi Republike Hrvatske,
- obrambena sposobnost i sigurnosno-obavještajni sustav,
- život i sigurnost građana,
- osnove gospodarskog i financijskog sustava Republike Hrvatske,
- otkrića, pronalasci i tehnologija od sigurnosnog i znanstvenog interesa za Republiku Hrvatsku.

Članak 7.

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

Članak 8.

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

Članak 9.

Stupnjem tajnosti „OGRANIČENO“ određuju se podaci čije bi neovlašteno otkrivanje moglo naštetiti djelovanju i izvršavanju zadaća državnih tijela, tijela jedinica lokalne i područne (regionalne) samouprave i pravnih osoba s javnim ovlastima.

III. POSTUPAK KLASIFICIRANJA I DEKLASIFICIRANJA PODATAKA

Članak 10.

Klasifikacija podataka se obavlja pri nastanku klasificiranih podataka ili na početku aktivnosti u kojoj se koriste klasificirani podaci.

Članak 11.

(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 12.

Uredbu o načinu označavanja stupnja tajnosti klasificiranih podataka donosi Vlada Republike Hrvatske.

Članak 13.

(1) Stupanj tajnosti „VRLO TAJNO“ određuju predsjednik Republike Hrvatske, predsjednik Hrvatskog sabora, predsjednik Vlade Republike Hrvatske te ministri, načelnik Glavnog stožera Oružanih snaga RH, čelnici tijela sigurnosno-obavještajnog sustava RH.

(2) Stupanj tajnosti „TAJNO“ i „POVJERLJIVO“ mogu, pored osoba iz stavka 1. ovog članka, odrediti i čelnici ostalih državnih tijela, te čelnici službi i agencija odgovorni Vladi Republike Hrvatske.

(3) Stupanj tajnosti „OGRANIČENO“ pored osoba iz stavka 1. i 2. ovog članka mogu odrediti i čelnici tijela jedinica lokalne i područne (regionalne) samouprave te pravnih osoba s javnim ovlastima.

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

Članak 14.

(1) Za vrijeme važenja jednog od stupnjeva tajnosti podatka, vlasnik podatka obvezan je provoditi periodičnu procjenu svrhovitosti dodijeljenog stupnja tajnosti klasificiranog podatka (u daljnjem tekstu periodična procjena).

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

(3) Vlasnik podatka donosi odluku o promjeni stupnja tajnosti ili o deklasifikaciji podatka te o tome pisanim putem izvješćuje 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.

Državna tijela, tijela jedinica lokalne i područne (regionalne) samouprave i pravne osobe s javnim ovlastima će, u okviru svog djelokruga rada, uz prethodnu suglasnost Ureda Vijeća za nacionalnu sigurnost, donijeti Pravilnik o kriterijima za određivanje stupnjeva tajnosti.

IV. PRISTUP PODACIMA

Članak 17.

(1) Pristup klasificiranim podacima imaju osobe kojima je pristup takvim podacima nužan za obavljanje poslova iz vlastitog djelokruga rada te koje za tu svrhu imaju izdano odgovarajuće Uvjerenje o sigurnosnoj provjeri (u daljnjem tekstu: Certifikat).

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

(3) Certifikat se izdaje za stupnjeve tajnosti „VRLO TAJNO“, „TAJNO“ i „POVJERLJIVO“.

(4) Zahtjev za izdavanje Certifikata podnosi se u pisanom obliku Uredu Vijeća za nacionalnu sigurnost.

Članak 18.

(1) Certifikat se izdaje na temelju obavljene sigurnosne provjere, kada nema sigurnosnih zapreka za pristup podacima.
Certifikat se dostavlja podnositelju zahtjeva.

(2) Odredba stavka 1. ovog članka ne primjenjuje se na predsjednika Republike Hrvatske, predsjednika Hrvatskog sabora i predsjednika Vlade Republike Hrvatske.

(3) Radi izvršenja nužnih i neodgodivih zadaća Ured Vijeća za nacionalnu sigurnost može, na prijedlog podnositelja zahtjeva, izdati privremeni certifikat za stupanj tajnosti „POVJERLJIVO“.

(4) Certifikat se ne označava stupnjem tajnosti već predstavlja neklasificirani podatak.

(5) Certifikat se izdaje na rok od pet godina.
Privremeni certifikat se izdaje na rok od tri mjeseca.

(6) Podnositelj zahtjeva, u slučaju uskraćivanja izdavanja certifikata, može podnijeti prigovor Savjetu za koordinaciju sigurnosno-obavještajnih agencija, putem Ureda Vijeća za nacionalnu sigurnost, u roku od 15 dana od dana primitka obavijesti o uskraćivanju izdavanja certifikata.

Članak 19.

(1) 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.

(2) Kada je to u interesu javnosti, drugog tijela, pojedinca ili u znanstvene svrhe, vlasnik podatka dužan je razmotriti odgovarajući zahtjev te, ukoliko ne postoji ugroza definirana u člancima 6., 7., 8. i 9. ovog Zakona, donijeti odluku o uklanjanju stupnja tajnosti podatka ili osloboditi osobu obveze čuvanja tajnosti podatka.

V. ZAŠTITA PODATAKA

Članak 20.

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

Članak 21.

(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.

VI. NADZOR NAD PRISTUPOM PODACIMA

Članak 22.

(1) 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.

(2) Uredbu o sadržaju i načinu vođenja evidencije o izvršenim uvidima i postupanju s klasificiranim podacima donosi Vlada Republike Hrvatske.

Članak 23.

(1) Inspekcijski nadzor postupka klasifikacije i deklasifikacije podataka te pristupa osoba klasificiranim podacima provodi Ured Vijeća za nacionalnu sigurnost.

(2) U provođenju inspekcijskog nadzora predstojnik Ureda Vijeća za nacionalnu sigurnost ovlašten je:
- narediti otklanjanje utvrđenih nedostataka, odnosno nepravilnosti u određenom roku,
- pokrenuti postupak utvrđivanja odgovornosti vlasnika podatka,
- poduzeti druge mjere, odnosno izvršiti druge radnje, za koje je posebnim propisima ovlašten.

VII. PRIJELAZNE I ZAVRŠNE ODREDBE

Članak 24.

(1) Vlada Republike Hrvatske donijet će uredbe iz članka 12. i članka 22. stavak 2. ovog Zakona, u roku od 30 dana od dana stupanja na snagu ovog Zakona.

(2) Čelnici nadležnih tijela donijet će Pravilnik iz članka 16. u roku od 60 dana od dana stupanja na snagu ovog Zakona.

Članak 25.

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 26.

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

(2) Interni certifikati koje su do stupanja na snagu ovoga Zakona izdala tijela ovlaštena Zakonom o zaštiti tajnosti podataka (NN 108 iz 1996.g.), vrijede do izdavanja certifikata po ovom Zakonu.

Članak 27.

Stupanjem na snagu ovog Zakona prestaje važiti Zakon o zaštiti tajnosti podataka (NN 108 iz 1996.g.).

Članak 28.

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

OBRAZLOŽENJE

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 temeljnih 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 temeljnih demokratskih prava.

II. STUPNJEVI TAJNOSTI

Odredbe iz članka 4. određuju stupnjeve tajnosti koji se uvode ovim Zakonom. Člankom 5. su uvedena dva temeljna kriterija za određivanje stupnjeva tajnosti: stupanj ugroze i područje primjene. Odredbe iz članaka 6., 7. i 8. definiraju područja i stupnjeve ugroze svakog od tri viša stupnja tajnosti podataka, dok se kriterij za određivanje najnižeg stupnja tajnosti – „OGRANIČENO", definira člankom 9., tako da je ovaj stupanj tajnosti uži po svom obuhvatu i odnosi se na djelovanje državnih tijela, tijela jedinica lokalne i područne (regionalne) samouprave te pravnih osoba s javnim ovlastima

III. POSTUPAK KLASIFICIRANJA I DEKLASIFICIRANJA PODATAKA

Odredbe članaka 10. i 11. propisuju temeljna načela klasifikacije podataka kao što su vrijeme kad se poduzima klasifikacija podatka, načelo određivanja najnižeg stupnja tajnosti i načelo izuzimanja dijelova ili priloga od klasificiranja u određenim slučajevima. Odredbe iz članka 13. ograničavaju područje primjene klasificiranih podataka u okviru pojedinih tijela i pravnih osoba. U odredbama članaka 14. i 15. uvodi se postupak periodične procjene svrhovitosti dodjele stupnja tajnosti za sve klasificirane podatke, propisuje se vremenska gradacija periodične procjene s obzirom na stupanj tajnosti te načini provedbe i postupanja (pisani oblik, pojedinačno ili skupno, arhiviranje uz izvornik, izvještavanje). U člancima 12. i 16. propisuju se podzakonski akti, uredbe Vlade RH i pravilnici tijela, koja uz suglasnost UVNS-a, detaljnije propisuju označavanje stupnjeva tajnosti i kriterija za određivanje stupnjeva tajnosti u području djelokruga rada pojedinog tijela.

IV. PRISTUP PODACIMA

Odredbe iz članaka 17. i 18. propisuju tko i pod kojim uvjetima može imati pristup klasificiranim podacima te opisuju postupak dobivanja Uvjerenja o sigurnosnoj provjeri (certifikata) i njegove karakteristike. Trajni izuzeci od provođenja sigurnosne provjere uvedeni su u članku 18. stavak 2., dok su privremeni i djelomični utvrđeni odredbom članka

19. stavak 2. Odredbe iz članka 19. propisuju tko je dužan čuvati tajnost podatka te pod kojim uvjetima vlasnik podatka može provesti deklasifikaciju ili oslobađanje od čuvanja tajnosti podatka izvan procedure periodične procjene i instituta sigurnosne provjere.

V. ZAŠTITA PODATAKA

Odredbe iz članka 21. upućuju na potrebu izgradnje nacionalnog regulativnog okvira informacijske sigurnosti, što se provodi drugim zakonom koji regulira područje informacijske sigurnosti. Odredbe članka 22. propisuju postupak u slučaju nestanka podatka ili njegova neovlaštenog otkrivanja, u slučajevima kada se taj postupak provodi u tijelu koje je vlasnik podatka, odnosno u tijelu koje je korisnik podatka.

VI. NADZOR NAD PRISTUPOM PODACIMA

Odredbe članaka 23. i 24. propisuju obvezu vođenja evidencije u tijelima iz članka 1., stavka 2., o uvidu u klasificirane podatke, o svakom postupanju s njima te o provedbi inspekcijskog nadzora odredaba ovog Zakona i određivanju tijela odgovornog za provedbu inspekcijskog nadzora.

VII. PRIJELAZNE I ZAVRŠNE ODREDBE

Odredbe iz članka 24. propisuju rokove u kojima Vlada RH treba donijeti odgovarajuće uredbe te rokove u kojima nadležna tijela trebaju donijeti odgovarajuće pravilnike za provedbu ovog Zakona. Odredbe iz članka 25. propisuju način na koji se obavlja prevođenje stupnjeva tajnosti propisanih ovim Zakonom sa stupnjevima korištenima prije njegova donošenja i onima preuzetim u obvezama iz međunarodnih ugovora koje je do donošenja ovog Zakona potpisala Republika Hrvatska. U članku 26. utvrđuje se valjanost postojećih certifikata UVNS-a. a u članku 27. propisuje se prestanak važenja Zakona o zaštiti tajnosti podataka (NN 108/96), stupanjem na snagu ovog Zakona.