

Na temelju članka 10. Zakona o tajnosti podataka (NN 79/07 i NN 86/12) i članka 20., stavak 1. Zakona o vanjskim poslovima (NN 48/96, NN 72/13 i NN 127/13) donosim

PRAVILNIK

O TAJNOSTI PODATAKA U MINISTARSTVU VANJSKIH I EUROPSKIH POSLOVA RH

I. OPĆE ODREDBE

Članak 1.
(Uvodne odredbe)

Ovim Pravilnikom uređuju se klasificirani i neklasificirani podaci u Ministarstvu vanjskih i europskih poslova i diplomatskim misijama i konzularnim uredima RH (u daljnjem tekstu: Ministarstvo), razrađuju se kriteriji za određivanje stupnjeva tajnosti klasificiranih podataka iz djelokruga Ministarstva, reguliraju se postupci klasifikacije, deklasifikacije i promjene stupnja tajnosti podataka, izrada, označavanje i evidentiranje klasificiranih i neklasificiranih podataka, pristup klasificiranim podacima te nadzor nad provedbom ovog Pravilnika.

Članak 2.
(Pojam klasificiranog i neklasificiranog podatka)

Klasificirani podatak u Ministarstvu je podatak koji je označen jednim od stupnjeva tajnosti sukladno Zakonu o tajnosti podataka (u daljnjem tekstu: Zakon) i člancima 5. do 8. ovog Pravilnika, kao i podatak koji je kao klasificiran Ministarstvu predala druga država, međunarodna organizacija ili institucija.

Neklasificirani podatak u Ministarstvu je podatak bez utvrđenog stupnja tajnosti, koji se koristi i razmjenjuje isključivo u službene svrhe u okviru djelokruga Ministarstva, kao i podatak koji je Ministarstvu tako označenog predala druga država, međunarodna organizacija ili institucija.

II. NEKLASIFICIRANI PODACI

Članak 3.
(Neklasificirani podaci)

Podaci Ministarstva koji nemaju oznaku stupnja tajnosti predstavljaju neklasificirane podatke i mogu biti označeni oznakom „NEKLASIFICIRANO“ ili mogu biti bez oznake.

Neklasificirani podaci označeni oznakom „NEKLASIFICIRANO“ koriste se isključivo u službene svrhe i ne mogu se objavljivati u javnim glasilima, tiskovnim i elektroničkim medijima, internetskim stranicama i drugdje bez pismenog dopuštenja Ministarstva.

Tako označeni podaci mogu biti dostupni samo onim osobama kojima je to neophodno za obavljanje poslova iz djelokruga radnog mjesta na koje su raspoređene.

Podatak označen oznakom „NEKLASIFICIRANO“ može se učiniti dostupnim korisniku prava na pristup informacijama i ponovnu uporabu informacija, o čemu se prethodno donosi pismena odluka Ministarstva.

III. STUPNJEVI TAJNOSTI KLASIFICIRANIH PODATAKA

Članak 4. (Stupnjevi tajnosti)

Stupnjevi tajnosti klasificiranih podataka u Ministarstvu su:

- VRLO TAJNO,
- TAJNO,
- POVJERLJIVO,
- OGRANIČENO.

Članak 5. (Stupanj tajnosti „VRLO TAJNO“)

Stupnjem tajnosti „VRLO TAJNO“ klasificiraju se podaci Ministarstva čijim bi se neovlaštenim otkrivanjem nanijela nepopravljiva šteta nacionalnoj sigurnosti ili vitalnim interesima Republike Hrvatske, kao što su temelji ustavnog ustrojstva RH, neovisnost, cjelovitost i sigurnost RH, međunarodni odnosi RH, obrambena sposobnost i sigurnosno-obavještajni sustav, sigurnost građana.

Uz postojanje okolnosti iz stavka 1. ovoga članka, stupnjem tajnosti „VRLO TAJNO“ klasificiraju se:

- podaci koji se direktno tiču mjera sigurnosti i zaštite osoba, objekata i podataka u Ministarstvu, a čije bi neovlašteno otkrivanje moglo dovesti do ugrožavanja života djelatnika Ministarstva ili drugih osoba;
- Plan obrane Ministarstva.

Stupnjem tajnosti „VRLO TAJNO“ klasificiraju se i drugi podaci iz djelokruga rada Ministarstva ukoliko postoje okolnosti iz stavka 1. ovoga članka.

Članak 6. (Stupanj tajnosti „TAJNO“)

Stupnjem tajnosti „TAJNO“ klasificiraju se podaci Ministarstva čijim bi se neovlaštenim otkrivanjem teško naštetilo nacionalnoj sigurnosti ili vitalnim interesima Republike Hrvatske, kao što su temelji ustavnog ustrojstva RH, neovisnost, cjelovitost i sigurnost RH, međunarodni odnosi RH, obrambena sposobnost i sigurnosno-obavještajni sustav, sigurnost građana.

Uz postojanje okolnosti iz stavka 1. ovoga članka, stupnjem tajnosti „TAJNO“ klasificiraju se:

- pojedini podaci iz područja vanjske politike i međunarodnih odnosa, uključivo oni koji se tiču službenog stava RH o određenom pitanju, a čije bi neovlašteno otkrivanje teško naštetilo nacionalnoj sigurnosti ili vitalnim interesima RH;
- pojedini podaci vezani za djelovanje RH unutar Vijeća EU-a, radnih skupina Vijeća i EU institucija;
- podaci vezani za postupak imenovanja veleposlanika, generalnih konzula, počasnih konzula i vojnih izaslanika RH;
- podaci koji se direktno tiču mjera sigurnosti i zaštite osoba, objekata i podataka u Ministarstvu, a čije bi neovlašteno otkrivanje moglo dovesti do ugrožavanja sigurnosti osoba ili sigurnosti objekata Ministarstva;
- elaborati šticenja Ministarstva i DM/KU RH i vezana dokumentacija;
- kriptografska oprema i podaci o načinu kriptografske zaštite i načinu rada kriptografskih sustava Ministarstva;
- podaci o određenim sistemskim i aplikativnim rješenjima informacijskih sustava Ministarstva;
- podaci o aktivnoj i pasivnoj komunikacijskoj opremi, računalnim poslužiteljima i opremi računalnih mreža, programskoj podršci, sustavima za uspostavljanje i zaštitu komunikacija, opremi i medijima za pohranu podataka, kao i podaci o svojoj ostaloj opremi i tehničkim rješenjima koji se primjenjuju za zaštitu podataka u Ministarstvu;
- podaci o mobilnim i fiksnim telekomunikacijskim vezama i uslugama koje se koriste za prijenos klasificiranih podataka u podatkovnom ili glasovnom obliku u Ministarstvu;
- administratorske zaporke,
- administratorski protuprovalni kodovi.

Stupnjem tajnosti „TAJNO“ klasificiraju se i drugi podaci iz djelokruga rada Ministarstva ukoliko postoje okolnosti iz stavka 1. ovoga članka.

Članak 7.

(Stupanj tajnosti „POVJERLJIVO“)

Stupnjem tajnosti „POVJERLJIVO“ klasificiraju se podaci Ministarstva čijim bi se neovlaštenim otkrivanjem naštetilo nacionalnoj sigurnosti ili vitalnim interesima Republike Hrvatske, kao što su temelji ustavnog ustrojstva RH, neovisnost, cjelovitost i sigurnost RH, međunarodni odnosi RH, obrambena sposobnost i sigurnosno-obavještajni sustav, sigurnost građana.

Uz postojanje okolnosti iz stavka 1. ovoga članka, stupnjem tajnosti „POVJERLJIVO“ klasificiraju se:

- pojedini podaci iz područja vanjske politike i međunarodnih odnosa, uključivo oni koji se tiču službenog stava RH o određenom pitanju, a čije bi neovlašteno otkrivanje naštetilo nacionalnoj sigurnosti ili vitalnim interesima RH;
- pojedini podaci vezani za djelovanje RH unutar Vijeća EU-a, radnih skupina Vijeća i EU institucija;
- analize, upute i instrukcije iz djelokruga rada uprava koje se bave diplomatskim poslovima, a izrađene temeljem aktivnosti u službi vanjskih poslova;
- pojedini podaci vezani za djelovanje RH unutar sustava UN;
- međunarodnopravna mišljenja iz djelokruga rada Sektora za međunarodno pravo;
- izvješća o nadzoru rada DM/KU RH i unutarnjih ustrojstvenih jedinica Ministarstva;
- mjesečna sigurnosna izvješća djelatnika sigurnosti DM/KU.

Stupnjem tajnosti „POVJERLJIVO“ klasificiraju se i drugi podaci iz djelokruga rada Ministarstva ukoliko postoje okolnosti iz stavka 1. ovoga članka.

Članak 8.

(Stupanj tajnosti „OGRANIČENO“)

Stupnjem tajnosti „OGRANIČENO“ klasificiraju se podaci Ministarstva čijim bi se neovlaštenim otkrivanjem naštetilo djelovanju i izvršenju zadaća Ministarstva ili drugog državnog tijela RH.

Uz postojanje okolnosti iz stavka 1. ovoga članka, stupnjem tajnosti „OGRANIČENO“ klasificiraju se:

- pojedini podaci iz područja vanjske politike i međunarodnih odnosa, uključivo oni koji se tiču službenog stava RH o određenom pitanju, a čije bi neovlašteno otkrivanje naštetilo djelovanju i izvršenju zadaća Ministarstva;
- pojedini podaci vezani za djelovanje RH unutar Vijeća EU-a, radnih skupina Vijeća i EU institucija;
- analize, upute i instrukcije iz djelokruga rada uprava koje se bave diplomatskim poslovima, a izrađene temeljem aktivnosti u službi vanjskih poslova;
- pojedini podaci vezani za djelovanje RH unutar sustava UN;
- međunarodnopravna mišljenja iz djelokruga rada Sektora za međunarodno pravo;
- podaci vezani za postupak zbog kršenja pravne stečevine EU (infringement);
- Godišnje izvješće Ministarstva (ili pojedini dijelovi);
- Plan rada Ministarstva (ili pojedini dijelovi);
- Dnevni briefing Ministarstva;
- Dnevne aktivnosti Ministarstva;
- revizijska izvješća DM/KU RH;
- programi posjeta stranih dužnosnika;
- informacijsko – komunikacijski podsustav Ministarstva – IKOS Politička dokumentacija;
- kadrovski informacijski sustav;
- zbirke osobnih podataka;
- urudžbeni zapisnik klasificiranih predmeta;
- ostali podaci koji se direktno tiču mjera sigurnosti i zaštite osoba, objekata i podataka u Ministarstvu;
- podaci sigurnosnog karaktera koji se dostavljaju sigurnosnim tijelima RH;

- tlocrti objekata Ministarstva;
- cjeloviti interni telefonski imenik i adresar Ministarstva;
- organigram Ministarstva s osobnim podacima djelatnika i službenim brojevima telefona i telefaksa koji nisu javno dostupni;
- korisničke zaporke;
- korisnički protuprovalni kodovi;
- zahtjevi za provođenje sigurnosne provjere;
- zahtjevi za izdavanje certifikata za pristup klasificiranim podacima;
- podaci o ACID zaštićenoj komunikaciji;
- podaci o postupanju s dokumentima koji se distribuiraju kriptografskim sustavima Ministarstva.

Stupnjem tajnosti „OGRANIČENO“ klasificiraju se i drugi podaci iz djelokruga rada Ministarstva ukoliko postoje okolnosti iz stavka 1. ovoga članka.

Članak 9.

(Uvažavanje stupnja tajnosti međunarodnog podatka pri klasificiranju podatka Ministarstva)

Ako se podatak Ministarstva izrađuje na temelju klasificiranog međunarodnog podatka ili sadrži njegove pojedine dijelove, prilikom određivanja stupnja tajnosti podatka Ministarstva obvezno se uzima u obzir stupanj tajnosti predmetnog međunarodnog podatka.

U tom slučaju, klasificirani podatak Ministarstva ne može imati nižu oznaku stupnja tajnosti od oznake stupnja tajnosti međunarodnog podatka.

Članak 10.

(Natječaji i ugovori s klasificiranom dokumentacijom)

Natječaji i ugovori s klasificiranom dokumentacijom koji se temeljem zakonskih i podzakonskih propisa iz područja informacijske sigurnosti sklapaju za obavljanje radova, nabavu robe, opreme ili usluga klasificiranog karaktera, klasificiraju se istim stupnjem tajnosti kojim je klasificiran predmet nabave, odnosno predmet ugovora.

IV. POSTUPAK KLASIFIKACIJE I DEKLASIFIKACIJE PODATAKA

Članak 11.

(Klasifikacija podataka)

Klasifikacija podataka u Ministarstvu je postupak kojim se podatku određuje jedan od stupnjeva tajnosti podataka s obzirom na stupanj ugroze koji bi nastupio ako bi podaci bili neovlašteno otkriveni.

Klasifikacija podataka u Ministarstvu obavlja se prilikom nastanka klasificiranog podatka ili prilikom periodične procjene propisane člankom 14. Zakona.

Članak 12.
(Ovlast za obavljanje klasifikacije)

Klasifikaciju podataka u Ministarstvu u okviru svog djelokruga rada provode Ministar vanjskih i europskih poslova (u daljnjem tekstu: ministar) i druge osobe u Ministarstvu koje ministar za to ovlasti pisanom odlukom.

Članak 13.
(Deklasifikacija podataka)

Deklasifikacija podataka u Ministarstvu je postupak kojim se utvrđuje prestanak postojanja razloga zbog kojih je određeni podatak Ministarstva klasificiran stupnjem tajnosti, nakon čega podatak postaje neklasificiran.

Deklasifikaciju podataka Ministarstva provodi ministar pisanom odlukom.

Ministar može iznimno za provođenje određenih slučajeva deklasifikacije podataka ovlastiti točno određene osobe u Ministarstvu u okviru njihova djelokruga rada, a ovlast prenosi isključivo pisanim putem, za konkretan slučaj.

Osobe iz stavka 2. i 3. ovoga članka mogu provesti skupnu deklasifikaciju ili promjenu stupnja tajnosti većeg broja klasificiranih podataka.

Članak 14.
(Postupak deklasifikacije podataka)

Zahtjevi i prijedlozi za deklasifikaciju ili snižavanje stupnja tajnosti dostavljaju se savjetniku za informacijsku sigurnost. Zahtjev mora biti u pisanom obliku i mora biti obrazložen. Savjetnik za informacijsku sigurnost će izraditi stručno mišljenje o podnesenom zahtjevu u roku ne dužem od 8 dana i dostaviti ga ministru zajedno sa zahtjevom.

Ministar donosi odluku o deklasifikaciji ili snižavanju stupnja tajnosti službenog podatka ili o odbijanju zahtjeva, koja se dostavlja podnositelju zahtjeva u roku od 30 dana od podnošenja zahtjeva.

Odluka o deklasifikaciji dostavlja se savjetniku za informacijsku sigurnost i ustrojstvenoj jedinici koja je stvaratelj klasificiranog podatka. Ustrojstvena jedinica koja je stvaratelj klasificiranog podatka provodi daljnje postupanje sukladno odredbama ovog Pravilnika.

Stvaratelj klasificiranog podatka ima obvezu obavještanja svih primatelja klasificiranog podatka o izvršenoj promjeni stupnja tajnosti.

Ukoliko nije moguće utvrditi stvaratelja klasificiranog podatka, savjetnik za informacijsku sigurnost preuzima izvršavanje obveza iz stavaka 3. i 4. ovoga članka.

Članak 15.

(Evidentiranje deklasifikacije podatka u evidencijama uredskog poslovanja)

Svaka deklasifikacija podatka ili promjena stupnja tajnosti podatka obavezno se evidentira u urudžbenom zapisniku i drugim postojećim evidencijama uredskog poslovanja.

Evidentiranje promjene stupnja tajnosti podatka u urudžbenom zapisniku provodi ustrojstvena jedinica koja je stvaratelj podatka koji se deklasificira.

Članak 16.

(Interes javnosti, pravo na pristup informacijama i zahtjev za skidanje oznake tajnosti podatka)

Postupak utvrđivanja opravdanosti skidanja oznake tajnosti s klasificiranog podatka u Ministarstvu provodi se kada postoji:

- interes javnosti za objavom podataka,
- zahtjev korisnika prava na pristup informacijama i ponovnu uporabu informacija na temelju Zakona o pravu na pristup informacijama,
- zahtjev suda ili druge institucije.

Postupak utvrđivanja opravdanosti skidanja oznake tajnosti provodi se na temelju pisanog obrazloženog zahtjeva podnositelja koji se dostavlja savjetniku za informacijsku sigurnost.

Kada postoji interes javnosti za objavom podataka Ministarstvo je dužno zatražiti mišljenje Ureda Vijeća za nacionalnu sigurnost u skladu s člankom 16. stavkom 2. Zakona.

Članak 17.

(Označavanje deklasificiranog podatka)

U postupku deklasifikacije prvotna oznaka stupnja tajnosti se precrta, a ispod nje se upisuje oznaka „DEKLASIFICIRANO“.

Kada se u postupku periodične procjene klasificiranom podatku promjeni ili skine stupanj tajnosti, na dokumentu ili drugom zapisu klasificiranog podatka precrtava se prvotna oznaka stupnja tajnosti i ispod nje se upisuje novi stupanj tajnosti. Ispod nove oznake upisuje se klasa i urudžbeni broj dokumenta temeljem kojeg je izvršena promjena ili skidanje stupnja tajnosti.

Savjetnik za informacijsku sigurnost vodi evidenciju o skinutim i sniženim stupnjevima tajnosti klasificiranih podataka.

Članak 18.

(Periodična procjena)

Periodična procjena klasificiranih podataka u Ministarstvu provodi se:

- za stupnjeve tajnosti „VRLO TAJNO“, „TAJNO“ i „POVJERLJIVO“ najmanje jednom u 5 godina,

- za stupanj tajnosti „OGRANIČENO“ najmanje jednom u 2 godine.

Periodična procjena klasificiranih podataka evidentira se na obrascu koje se nalazi u Prilogu I ovog Pravilnika.

Članak 19. (Provedba periodične procjene)

Stvaratelji klasificiranih podataka iz članka 12. ovog Pravilnika obvezni su trajno procjenjivati stupanj tajnosti klasificiranih podataka iz svog djelokruga rada.

Ministar donosi pisanu odluku o provođenju periodične procjene stupnjeva tajnosti klasificiranih podataka nastalih u Ministarstvu u skladu s rokovima iz članka 17. ovog Pravilnika.

Odluka o provedbi periodične procjene sadržava:

- obvezu stvaratelja klasificiranog podatka da izradi pisanu procjenu na temelju koje će se odlučiti o promjeni stupnja tajnosti, deklasifikaciji ili zadržavanju postojećeg stupnja tajnosti,
- rok do kada se periodična procjena mora obaviti,
- obvezu izrade pisanog izvješća o provedenoj periodičnoj procjeni.

Periodična procjena može se provesti i skupno za određene grupe podataka.

U postupku periodične procjene, sukladno pisanoj procjeni stvaratelja klasificiranog podatka, Ministar može donijeti odluku kojom mijenja stupanj tajnosti podatka ili deklasificira podatak.

Odluka iz stavka 5. ovog članka dostavlja se savjetniku za informacijsku sigurnost i ustrojstvenoj jedinici koja je stvaratelj klasificiranog podatka. Ustrojstvena jedinica koja je stvaratelj klasificiranog podatka provodi daljnje postupanje sukladno odredbama ovog Pravilnika.

V. IZRADA, OZNAČAVANJE I EVIDENTIRANJE KLASIFICIRANIH I NEKLASIFICIRANIH PODATAKA

Članak 20. (Označavanje primatelja klasificiranih podataka)

Klasificirani podaci stupnjeva tajnosti „VRLO TAJNO“, „TAJNO“ i „POVJERLJIVO“ moraju biti naslovljeni na točno određenog primatelja po imenu i prezimenu i nazivu ustrojstvene jedinice primatelja.

Članak 21. (Stupnjevi tajnosti i kratice)

Oznaka stupnja tajnosti stavlja se u gornjem desnom kutu i ispisuje se velikim tiskanim slovima. Kada dokument ima više stranica, oznaka stupnja tajnosti stavlja se na svaku stranicu dokumenta u gornji desni kut tako da se ispisuje ili otiskuje štambiljem.

Kratice stupnjeva tajnosti su:

- za VRLO TAJNO – VT,
- za TAJNO – T,
- za POVJERLJIVO – POV,
- za OGRANIČENO – OGR,

Kratice se koriste za vođenje evidencija klasificiranih podataka i obavezno se stavljaju u klasu dokumenta prije klasifikacijske oznake te odvajaju ravnom crticom (-) od oznake klasifikacije prema sadržaju, u skladu s Uredbom o uredskom poslovanju.

Članak 22.

(Evidentiranje klasificiranih podataka)

Evidentiranje klasificiranih podataka obavlja se upisivanjem u urudžbeni zapisnik klasificiranih predmeta.

Za klasificirane podatke stupnja tajnosti „VRLO TAJNO“ i „TAJNO“ obavezno se vodi:

- popis svih osoba koje su ostvarile uvid u pojedini podatak, prema prilogu II. ovog Pravilnika. Prilog II. vodi se za svaki podatak zasebno.

Za klasificirane podatke stupnja tajnosti „POVJERLJIVO“ obavezno se vodi:

- popis krajnjih korisnika ovlaštenih za pristup klasificiranim podacima, prema prilogu III. ovog Pravilnika. Popis definira načelnik Sektora, odnosno nadležni pomoćnik ministra, uz zadovoljavanje svih propisanih uvjeta za pristup klasificiranim podacima stupnja tajnosti „POVJERLJIVO“, iz članka 35., stavka 1. ovog Pravilnika.

Za klasificirane podatke stupnja tajnosti „OGRANIČENO“ obavezno se vode evidencije o krajnjim korisnicima kojima je podatak dostavljen, sukladno propisima o uredskom poslovanju.

Članak 23.

(Osnovne zaštitne oznake)

Osnovne zaštitne oznake klasificiranih podataka su:

- puna oznaka stupnja tajnosti,
- kratica stupnja tajnosti,
- oznaka broja primjerka u odnosu na ukupan broj primjeraka klasificiranog dokumenta ili drugog zapisa klasificiranog podatka,
- oznaka broja stranice u odnosu na ukupan broj stranica klasificiranog dokumenta,
- oznaka broja, vrste, naziva i stupnja tajnosti priloga klasificiranog dokumenta.

Članak 24.

(Broj primjeraka i broj stranica)

Broj primjerka u odnosu na ukupan broj primjeraka klasificiranog dokumenta stavlja se u gornjem desnom kutu ispod oznake stupnja tajnosti.

Kada je potrebno u gornjem desnom kutu ispisati dodatne zaštitne oznake, broj primjerka se ispisuje ispod njih.

Svaka stranica klasificiranog dokumenta u donjem desnom kutu mora imati oznaku broja stranice u odnosu na ukupan broj stranica dokumenta.

Članak 25.
(Prilozi)

Broj, vrsta, naziv i stupanj tajnosti priloga navode se na posljednjoj stranici klasificiranog dokumenta u donjem lijevom kutu, ispod potpisa ovlaštene osobe.

Prilog se navodi ukupnim brojem priloga, punim nazivom priloga, kraticom stupnja tajnosti i vrstom. Kada se radi o više priloga, za svakoga od njih je potrebno upisati navedene oznake. Ako priloge ne sačinjavaju samo pisani dokumenti, potrebno je navesti njihovu vrstu (CD, fotografije, mape...).

Standardni izgled klasificiranog dokumenta sa svim osnovnim i dodatnim zaštitnim oznakama nalazi se u prilogu IV. ovog Pravilnika.

Članak 26.
(Dodatne zaštitne oznake)

Stvaratelji klasificiranih podataka iz članka 12. ovog Pravilnika mogu klasificirane podatke označiti dodatnim zaštitnim oznakama.

Dodatne zaštitne oznake klasificiranih podataka su:

- zabrana ili ograničavanje umnožavanja dokumenata ili drugih zapisa klasificiranih podataka,
- zabrana ili ograničavanje daljnje distribucije klasificiranog podatka drugim primateljima,
- obaveza povrata klasificiranog podatka nakon obavljenog uvida,
- rok tajnosti koji je vlasnik klasificiranog podatka odredio pri nastanku podatka.

Članak 27.
(Upisivanje dodatnih oznaka)

Dodatne zaštitne oznake ispisuju se u gornjem desnom kutu dokumenta, na svakoj stranici, velikim tiskanim slovima ispod oznake stupnja tajnosti.

Članak 28.

(Zabrana ili ograničavanje umnožavanja klasificiranog podatka)

Stvaratelj klasificiranog podatka može zabraniti ili ograničiti umnožavanje podatka upisivanjem teksta „ZABRANJENO UMNOŽAVANJE“ ili „OGRANIČENO UMNOŽAVANJE“ u gornjem desnom kutu dokumenta ispod oznake stupnja tajnosti.

Članak 29.

(Umnožavanje klasificiranih podataka stupnja tajnosti „VRLO TAJNO“)

Umnožavanje klasificiranih podataka stupnja tajnosti „VRLO TAJNO“ dopušteno je isključivo uz pismenu suglasnost stvaratelja klasificiranog podatka.

Članak 30.

(Odobranje umnožavanja i evidencija kopija klasificiranog podatka)

Umnožavanje klasificiranih podataka odobravaju čelnici ustrojstvenih jedinica koje su zaprimile klasificirani podatak, ako je to nužno za obavljanje određenih poslova i zadaća i ako na zaprimljenom primjerku klasificiranog podatka nema oznake zabrane umnožavanja. Na zaprimljenom izvorniku, u gornjem desnom slobodnom dijelu dokumenta čelnik ustrojstvene jedinice vlastoručno ispisuje tekst „odobravam kopiranje“, upisuje broj odobrenih kopija, imena i prezimena osoba koje ih zadužuju, te stavlja svoj potpis.

Nakon što je na izvorniku upisano sve navedeno iz stavka 3. ovog članka, izvornik se umnožava u odobrenom broju kopija.

Ako je čelnik odobrio kopiranje samo dijela dokumenta na kojem nije vidljiva oznaka tajnosti izvornika, na kopiji se štambiljem otiskuje stupanj tajnosti kojim je označen izvornik.

O broju kopija klasificiranih podataka i njihovim zaduženjima vodi se evidencija u sklopu urudžbenog zapisnika klasificiranih predmeta.

Članak 31.

(Povrat nakon uvida)

Stvaratelj klasificiranog podatka može od primatelja zahtijevati povrat podatka nakon uvida na način da u gornjem desnom kutu dokumenta ispod oznake stupnja tajnosti upiše oznaku „VRATITI NAKON UVIDA“.

U evidencijama odnosno urudžbenom zapisniku klasificiranih predmeta stavlja se napomena „vraćeno nakon uvida“ i upisuje se datum povrata dokumenta.

Članak 32.

(Zabrana i ograničavanje distribucije klasificiranog podatka)

Za zabranu ili ograničavanje distribucije klasificiranog podatka koristi se oznaka „ISKLJUČIVO“. U produžetku oznake „ISKLJUČIVO“ upisuje se službeni naziv ili kratica primatelja klasificiranog podatka.

Članak 33.
(Rok tajnosti)

Rok tajnosti klasificiranog podatka dodatna je zaštitna oznaka kojom se određuje vremensko trajanje određenog stupnja tajnosti podatka.

Članak 34.
(Različiti stupnjevi tajnosti dokumenta)

Klasificirani dokument, pojedini dio ili prilog mogu biti označeni različitim stupnjevima tajnosti. U takvom slučaju dokument kao cjelina označava se najvišim stupnjem tajnosti pojedinog dijela ili priloga.

Ako dijelovi dokumenta imaju različiti stupanj tajnosti, svaki od dijelova se odvaja u zaseban dio i ispred svakog dijela teksta na desnu stranu se stavlja oznaka stupnja tajnosti tog dijela dokumenta.

Ako neki dio klasificiranog dokumenta nema oznaku tajnosti, ispred tog dijela stavlja se oznaka „NEKLASIFICIRANO“.

Članak 35.
(Pakiranje i označavanje omotnica klasificiranog podatka)

Klasificirani podaci stupnjeva tajnosti „VRLO TAJNO“, „TAJNO“ i „POVJERLJIVO“ koji se dostavljaju tijelima na različitim lokacijama pakiraju se u dvije neprozirne i čvrste omotnice. Unutarnji omot mora nositi odgovarajuću oznaku stupnja tajnosti, klasu i urudžbeni broj, puni naziv i adresu pošiljatelja i primatelja te propisani broj otisaka službenog pečata Ministarstva na spojevima omotnice. Na vanjskom omotu mora biti istaknut naziv i adresa primatelja i pošiljatelja, evidencijski broj pošiljke iz dostavne knjige te jedan otisak službenog pečata na spojevima omotnice. Vanjski omot ne smije imati oznaku stupnja tajnosti niti na bilo koji drugi način ukazivati da se radi o klasificiranim podacima.

Klasificirani podaci stupnja tajnosti „OGRANIČENO“ pakiraju se i dostavljaju u jednoj neprozirnoj i čvrstoj omotnici. Oznake na omotnici ne smiju na bilo koji način ukazivati da se radi o klasificiranim podacima stupnja tajnosti „OGRANIČENO“.

VI. PRISTUP KLASIFICIRANIM PODACIMA

Članak 36.
(Pristup klasificiranim podacima)

Pristup klasificiranim podacima stupnjeva tajnosti „VRLO TAJNO“, „TAJNO“ i „POVJERLJIVO“ mogu imati osobe koje zadovoljavaju sljedeće uvjete:

1. imaju izdano odgovarajuće Uvjerenje o obavljenoj sigurnosnoj provjeri (u daljnjem tekstu: certifikat) od strane Ureda Vijeća za nacionalnu sigurnost;
2. pristup tim podacima nužan im je za obavljanje poslova iz njihova djelokruga rada (načelo „need to know“);
3. ovlaštene su za pristup tim podacima;
4. sigurnosno su informirane.

Pristup klasificiranim podacima stupnja tajnosti „OGRANIČENO“ mogu imati osobe koje zadovoljavaju sljedeće uvjete:

1. potpisale su Izjavu o postupanju s klasificiranim podacima stupnja tajnosti „OGRANIČENO“ ili imaju izdan certifikat;
2. pristup tim podacima nužan im je za obavljanje poslova iz njihova djelokruga rada (načelo „need to know“);
3. ovlaštene su za pristup tim podacima;
4. sigurnosno su informirane.

Ispunjavanje uvjeta iz točaka 2. i 3. potvrđuje neposredno nadređeni rukovoditelj.

Sigurnosno informiranje je postupak u kojem se osoba upoznaje s mjerama i standardima informacijske sigurnosti, te svojim obvezama i zakonskim posljedicama u slučaju nepridržavanja istih. Sigurnosno informiranje provodi savjetnik za informacijsku sigurnost ili druga, za to, ovlaštena osoba. Po završetku sigurnosnog informiranja potpisuje se Izjava o postupanju s klasificiranim podacima, kojom se potvrđuje da je informirana osoba upoznata s minimalnim standardima postupanja s klasificiranim podacima.

Članak 37.

(Zahtjev za izdavanje certifikata)

Zahtjev za izdavanje certifikata za pristup klasificiranim podacima podnose čelnici ustrojstvenih jedinica.

Zahtjev treba sadržavati:

- ime i prezime osobe
- naziv radnog mjesta na koje je osoba raspoređena i naziv ustrojstvene jedinice
- vrstu certifikata koji se traži (nacionalni, EU ili NATO)
- stupanj tajnosti za koji se traži certifikat.

Zahtjev za izdavanje certifikata podnosi se za osobe koje se raspoređuju na dužnosti i poslove obuhvaćene Popisom dužnosti i poslova iz djelokruga rada Ministarstva vanjskih i europskih poslova RH za koje je potreban certifikat za pristup klasificiranim podacima.

Članak 38.

(Registar certifikata)

Sukladno članku 9. Zakona o informacijskoj sigurnosti Ministarstvo ustrojava i vodi popis osoba koje imaju pristup klasificiranim podacima i registar zaprimljenih certifikata s rokovima važenja certifikata.

VII. MEĐUNARODNO RAZMJENJIVI PODACI

Članak 39.

(Međunarodno razmjenjivi podaci)

Međunarodno razmjenjivi podaci su službeni podaci Ministarstva koji se na temelju međunarodnog ugovora dostavljaju drugoj državi ili međunarodnoj organizaciji.

Ured Vijeća za nacionalnu sigurnost RH središnje je državno tijelo nadležno za zaključivanje međunarodnih sigurnosnih ugovora temeljem kojih se razmjenjuju klasificirani podaci.

Kada je službeni dokument, vlasnik kojeg je Ministarstvo, dostavljen drugoj državi ili međunarodnoj organizaciji, na arhivski primjerak otiskuje se sigurnosna oznaka „RAZMIJENJEN PODATAK“, bez obzira na postojeće sigurnosne oznake na službenom dokumentu.

VIII. MEĐUNARODNI KLASIFICIRANI I NEKLASIFICIRANI PODACI

Članak 40.

(EU i NATO klasificirani i neklasificirani podaci)

Postupanje s klasificiranim i neklasificiranim EU i NATO podacima, koji se putem sustava Registara zaprimaju i distribuiraju u službi vanjskih poslova, propisano je odredbama Pravilnika o standardima sigurnosti podataka Ureda Vijeća za nacionalnu sigurnost RH.

Članak 41.

(Pristup klasificiranim podacima druge države ili međunarodne organizacije)

Pravo pristupa klasificiranim podacima druge države ili međunarodne organizacije imaju osobe koje osim uvjeta iz članka 35. ovog Pravilnika imaju i izdan odgovarajući certifikat iz članka 22. Zakona.

IX. ZAŠTITA PODATAKA I NADZOR PROVEDBE PRAVILNIKA

Članak 42.

(Mjere i postupci zaštite podataka)

Primjena i pridržavanje mjera i postupaka zaštite podataka obvezujući su za svakoga tko takav podatak koristi ili mu postane dostupan.

Članak 43.

(Povreda sigurnosti klasificiranog podatka)

Povreda sigurnosti klasificiranog podatka nastaje kada se isti uništi, otuđi, izgubi ili učini dostupnim neovlaštenoj osobi.

Svaka osoba koja sazna za povredu sigurnosti podatka dužna je o tome odmah obavijestiti savjetnika za informacijsku sigurnost.

Svaka osoba koja sazna da se klasificirani podatak ne čuva na propisani način dužna je poduzeti mjere da ne dođe do povrede sigurnosti podatka i o tome odmah obavijestiti savjetnika za informacijsku sigurnost.

Članak 44.

(Utvrđivanje povrede sigurnosti klasificiranog podatka)

U slučaju povrede sigurnosti klasificiranog podatka savjetnik za informacijsku sigurnost će u suradnji s nadležnim tijelima provesti daljnji postupak u cilju utvrđivanja svih okolnosti te će poduzeti mjere potrebne za otklanjanje mogućih štetnih posljedica, sukladno odredbama Zakona o vanjskim poslovima, Zakona o tajnosti podataka, Zakona o informacijskoj sigurnosti i Kaznenog zakona RH.

O poduzetim mjerama i utvrđenim činjenicama iz stavka 1. ovoga članka izvješćuje se ministar te se, u slučaju takvih zaključaka, predlaže pokretanje postupka disciplinske i/ili kaznene odgovornosti.

Članak 45.

(Nadzor)

Nadzor nad pridržavanjem i provedbom ovog Pravilnika, sukladno Zakonu o informacijskoj sigurnosti i Uredbi o unutarnjem ustrojstvu Ministarstva vanjskih i europskih poslova provodi savjetnik za informacijsku sigurnost Ministarstva.

Članak 46.

(Pravilnik o primjeni mjera i standarda informacijske sigurnosti)

Mjere i standardi informacijske sigurnosti za pristup, postupanje, distribuciju, pohranu i uništavanje klasificiranih i neklasificiranih podataka propisuju se posebnim pravilnikom o primjeni mjera i standarda informacijske sigurnosti.

X. PRIJELAZNE I ZAKLJUČNE ODREDBE

Članak 47.
(Klasificirani podaci drugih tijela državne uprave)

Postupanje s klasificiranim podacima drugih tijela državne uprave navedenim u stavku 2. članku 1. Zakona, a koji se distribuiraju u službi vanjskih poslova, propisano je odredbama Zakona.

Članak 48.
(Raniji stupnjevi tajnosti podataka)

Stupnjevi tajnosti podataka koji su utvrđeni prije stupanja na snagu ovog Pravilnika prevode se na način utvrđen člankom 32. Zakona.

Članak 49.
(Priprema sredstava za rad)

Ministarstvo mora pripremiti sve potrebne štambilje za svoj rad sukladno odredbama Uredbe o načinu označavanja klasificiranih podataka, sadržaju i izgledu uvjerenja o obavljenoj sigurnosnoj provjeri i izjave o postupanju s klasificiranim podacima i ovoga Pravilnika („VRLO TAJNO“, „TAJNO“, „POVJERLJIVO“, „OGRANIČENO“, „NEKLASIFICIRANO“, „KOPIJA“, „RAZMIJENJEN PODATAK“, „ISKLUČIVO“, „ISTEK ROKA TAJNOSTI“, „ZABRANJENO UMNOŽAVANJE“, „OBVEZAN POVRAT NAKON UVIDA“) u roku od tri mjeseca od stupanja na snagu ovog Pravilnika.

Članak 50.
(Prestanak važenja ranijih odredbi)

Stupanjem na snagu ovog Pravilnika prestaje važiti Pravilnik o utvrđivanju kriterija za određivanje stupnjeva tajnosti podataka u službi vanjskih poslova (Klasa:011-02/08-03/3563; Urbroj:521-VII-01-08) od 11.07.2008.

Članak 51.
(Stupanje na snagu)

Ovaj pravilnik stupa na snagu danom donošenja.

KLASA: 833-05/13-05/18
URBROJ: 521-GT-02-01-02-16-9
Zagreb, 01.04.2016.

MINISTAR VANJSKIH I EUROPSKIH POSLOVA

dr.sc. Miro Kovač