Predlog

Na osnovu člana 68 stav 2 Zakona o tajnosti podataka ("Službeni list CG", br. 14/08, 76/09, 41/10, 38/12, 44/12, 14/13 i 18/14), Vlada Crne Gore, na sjednici od _____2015. godine, donijela je

U R E D B U

O BLIŽIM USLOVIMA I NAČINU SPROVOĐENJA ADMINISTRATIVNIH I FIZIČKIH MJERA ZAŠTITE TAJNIH PODATAKA

Član 1

Državni organi, organi državne uprave, organi jedinica lokalne samouprave i druga pravna lica kojima je povjereno vršenje javnih ovlašćenja (u daljem tekstu: organi), kao i pravna i fizička lica kad u vršenju zakonom utvrđenih poslova, odnosno izvršavanju ugovorenog posla saznaju za tajne podatke (u daljem tekstu: organizacije) dužni su da administrativne i fizičke mjere zaštite tajnih podataka, sprovode pod uslovima i na način propisan ovom uredbom.

Član 2

Izrazi koji se u ovoj uredbi koriste za fizička lica u muškom rodu podrazumijevaju iste izraze u ženskom rodu.

Član 3

Objekti, prostorije, odnosno prostori u kojima se čuvaju, koriste i obrađuju tajni podaci, moraju da imaju:

- bezbjednosnu procjenu ugroženosti;
- plan zaštite tajnih podataka;
- tehničku dokumentaciju.

Ažuriranje procjene, plana i dokumentacije iz stava 1 ovog člana, vrši se nakon svake promjene koja može da utiče na zaštitu tajnih podataka.

Član 4

Bezbjednosnu procjenu ugroženosti sačinjava organ nadležan za poslove nacionalne bezbjednosti (u daljem tekstu: Agencija), u skladu sa zakonom, a naročito u odnosu na: potencijalne prijetnje tajnim podacima sa osvrtom na poziciju, lokaciju i čuvanje objekata i bezbjednosnih zona, aktivnosti stranih obavještajnih službi, sabotera, terorista i kriminalnih grupa, kao i rizike koji mogu biti uzrokovani aktivnošću zaposlenih.

Zahtjev za bezbjednosnu procjenu ugroženosti organi, odnosno organizacije dostavljaju Agenciji, preko Direkcije za zaštitu tajnih podataka.

Bezbjednosnu procjenu ugroženosti za Ministarstvo odbrane i Vojsku Crne Gore sačinjava organizaciona jedinica Ministarstva odbrane nadležna za vojno obavještajne i bezbjednosne poslove, u saradnji sa Agencijom.

Član 5

Na osnovu bezbjednosne procjene ugroženosti, starješina organa, odnosno zakonski zastupnik organizacije procjenjuje stepen rizika prijetnje tajnim podacima (visoki, srednji ili niski), a naročito u odnosu na:

- stepen tajnosti podatka i broj tajnih podataka;
- broj lica koja rukuju tajnim podacima.

Zavisno od stepena rizika iz stava 1 ovog člana, starješina organa, odnosno zakonski zastupnik organizacije preduzima neophodne mjere zaštite tajnih podataka, u skladu sa ovom uredbom.

Član 6

Plan zaštite tajnih podataka sadrži:

1) lokaciju i opis objekta u kojem se nalaze bezbjednosne zone, posebno opis granica objekta, broj ulaza, opis okolnih objekata i drugo;
2) podatke o bezbjednosnim zonama, uključujući opis aktivnosti koje se u njima vrše,
3) lokaciju i opis bezbjednosnih zona (položaj, ulaz, debljina zida, dimenzije prozora, visina prozora iznad tla i drugo),
4) grafički prikaz objekta, granica objekta, bezbjednosnih zona i granica bezbjednosnih zona,
5) način vršenja fizičke zaštite objekata i bezbjednosnih zona, koji sadrži:
   - uputstva za vršenje fizičke zaštite;
   - broj lica koja vrše fizičku zaštitu;
   - način provjere lica i vozila prilikom ulaska i izlaska, u toku i van radnog vremena;
   - način obavljanja periodične kontrole;
   - način vršenja patrole;
   - način reagovanja na alarmne poruke tehničkih bezbjednosnih uređaja i sistema;
   - metode kontrole fizičke zaštite;
   - knjigu posjetilaca u koju se unose ime, prezime, jedinistveni matični broj lica ili broj javne isprave iz koje se može utvrditi identitet, kao i naziv institucije u kojoj je to lice zaposleno,
6) procedure zaštite tajnih podataka u kriznim situacijama, a naročito:
   - izbor rezervne lokacije;
   - prenos tajnih podataka;
   - komunikaciju sa drugim nadležnim organima (Uprava policije, drugi organi i službe);
   - određivanje mjera obezbjeđenja tajnih podataka.

Član 7

Tehnička dokumentacija obuhvata spisak i specifikaciju mehaničkih i tehničkih bezbjednosnih uređaja i sistema za zaštitu objekata i bezbjednosnih zona, pravila i uputstva za njihovu upotrebu i održavanje, evidencije i izveštaje o provjerama ispravnosti, kao i kopije sertifikata o ispunjenosti standarda mehaničkih i tehničkih bezbjednosnih uređaja i sistema.

Član 8

Prostor ili prostorija u objektu koji je određen kao administrativna, odnosno bezbjednosna zona treba da ima bezbjednosnu opremu u skladu sa propisanim standardima.

Član 9

Administrativnu i bezbjednosne zone određuje starješina organa, odnosno zakonski zastupnik organizacije, na osnovu bezbjednosne procjene ugroženosti.

Član 10

U administrativnoj zoni obrađuju se, čuvaju i koriste tajni podaci stepena tajnosti „INTERNO".

Za administrativnu zonu određuje se prostor ili prostorija koja se može nadzirati (ulaz, izlaz i kretanje lica i vozila).

Na ulazu u administrativnu zonu mora biti istaknuto obavještenje o nadzoru pristupa i kretanju u njoj.

Tajni podaci iz stava 1 ovog člana, čuvaju se u kancelarijskim ili metalnin ormarima koji se zaključavaju.

Član 11

Bezbjednosne zone mogu biti I ili II stepena.

Bezbjednosne zone moraju biti vidno označene natpisom "BEZBJEDNOSNA ZONA I", odnosno "BEZBJEDNOSNA ZONA II", uz dodatna obavještenja u vezi sa bezbjednosnim mjerama koje se sprovode u toj zoni.

Bezbjednosne zone moraju biti zaštićene na način da se onemogući pogled unutar zone.

Izuzetno, kad to zahtijevaju posebne okolnosti, starješina organa odnosno zakonski zastupnik organizacije, može odrediti da se bezbjednosne zone ne označavaju na način iz stava 2 ovog člana.

Član 12

Bezbjednosna zona I stepena je prostor ili prostorija u kojoj se obrađuju, čuvaju i koriste tajni podaci stepena tajnosti „STROGO TAJNO", „TAJNO" i „POVJERLJIVO", kao i tajni podaci stepena tajnosti „INTERNO" ukoliko je to potrebno, i sam ulazak u ovu zonu predstavlja pristup tajnim podacima.

U bezbjednosnoj zoni I stepena zabranjeno je unošenje mehaničkih, elektronskih i magnetno – optičkih sredstava i djelova sredstava, kojima bi se mogao neovlašćeno snimiti, odnijeti ili prenijeti tajni podatak.

Član 13

Bezbjednosna zona II stepena je prostor ili prostorija u kojoj se obrađuju i čuvaju tajni podaci stepena tajnosti „STROGO TAJNO”, „TAJNO” i „POVJERLJIVO”, kao i tajni podaci stepena tajnosti „INTERNO“ ukoliko je to potrebno, i ulazak i kretanje u toj zoni ne smatra se pristupom tajnim podacima.

U bezbjednosnoj zoni II stepena zabranjeno je unošenje mehaničkih, elektronskih i magnetno – optičkih sredstava i djelova sredstava, kojima bi se mogao neovlašćeno snimiti, odnijeti ili prenijeti tajni podatak, bez pisanog odobrenja ovlašćenog lica.

Član 14

Mjere fizičke zaštite u bezbjednosnim zonama utvrđuju se na osnovu stepena rizika prijetnje tajnim podacima iz člana 5 ove uredbe, na način što se vrši bodovanje mjera zaštite, u skladu sa prilogom koji čini sastavni dio ove uredbe (Prilog 1).

Ispunjenost mjera fizičke zaštite u bezbjednosnim zonama određuje se na osnovu broja bodova dobijenih u skladu sa stavom 1 ovog člana, i to za:

1) bezbjednosnu zonu I stepena:
- visok stepen rizika prijetnje tajnim podacima - najmanje 26 bodova;
- srednji stepen rizika prijetnje tajnim podacima - najmanje 24 boda; i
- nizak stepen rizika prijetnje tajnim podacima - najmanje 21 bod,

2) bezbjednosnu zonu II stepena:
- visok stepen rizika prijetnje tajnim podacima - najmanje 21 bod;
- srednji stepen rizika prijetnje tajnim podacima - najmanje 20 bodova; i
- nizak stepen rizika prijetnje tajnim podacima - najmanje 17 bodova.

Član 15

Prostori, odnosno prostorije u kojima se čuvaju, koriste, obrađuju ili uništavaju tajni podaci stepena tajnosti “POVJERLJIVO” ili većeg stepena tajnosti, kao i prilaz njima, obezbjeđuju se mehaničkim uređajima i tehničkim bezbjednosnim uređajima i sistemima.

Član 16

Mehaničke uređaje iz člana 15 ove uredbe čine:
- oprema za sigurno čuvanje predmeta i dokumenata (sefovi, kase i dr.);
- brave za opremu za sigurno čuvanje predmeta i dokumenata;
- vrata i njihove komponente;
- sistemi za zaključavanje vrata;
- protivprovalne rešetke ili barijere;
- bezbjednosne folije;
- prozori.

Član 17

Tehničke bezbjednosne uređaje i sisteme iz člana 15 ove uredbe, čine:

- sistemi za kontrolu ulaska i izlaska u prostorije sa elektronskom verifikacijom identiteta lica i njihovom autorizacijom (u daljem tekstu: kontrola pristupa);
- bezbjednosni sistemi za izvještavanje o povredama bezbjednosti (u daljem tekstu: alarmni sistemi);
- video nadzor (CCTV);
- uređaji za detekciju predmeta;
- uređaji za uništavanje tajnih podataka.

Član 18

Fizička zaštita objekta, prostora, odnosno prostorija u kojima se čuvaju, koriste i obrađuju tajni podaci stepena tajnosti "POVJERLJIVO" ili većeg stepena tajnosti vrše policijski službenici, službenici Agencije, pripadnici Vojske Crne Gore i fizička lica koja imaju dozvolu za vršenje poslova zaštite u skladu sa propisom kojim se uređuje zaštita lica i imovine (u daljem tekstu: fizičko obezbjeđenje).

Lica iz stava 1 ovog člana moraju imati dozvolu za pristup tajnim podacima najmanje stepena tajnosti podataka čiju zaštitu vrše.

Detaljne procedure postupanja fizičkog obezbjeđenja donose se na osnovu Plana zaštite tajnih podataka.

Član 19

Tehnički bezbjednosni uređaji i sistemi iz člana 15 ove uredbe moraju biti u funkciji bez prekida.

U slučaju aktiviranja tehničkih bezbjednosnih uređaja i sistema kojima se signalizira povreda bezbjednosti objekta, prostora odnosno prostorija u kojima se čuvaju, koriste i obrađuju tajni podaci, na mjestu gde je došlo do povrede, dužna su da reaguju najmanje dva lica fizičkog obezbjeđenja, na način da se zaštita ostalih djelova objekta, prostora odnosno prostorija ne smije oslabiti.

Starješina organa, odnosno zakonski zastupnik organizacije će odrediti vrijeme reakcije lica iz stava 1 ovog člana, tako da bude kraće od vremena potrebnog za prevazilaženje preduzetih mjera za zaštitu tajnih podataka i utvrditi intervale za provjeru vremena potrebnog za reakciju fizičkog obezbjeđenja.

Provjera iz stava 3 ovog člana sprovodi se najmanje jednom godišnje.

Član 20

Kontrola ulaska lica i vozila vrši se na svakom ulazu u objekat i bezbjednosne zone. Kontrola ulaska vrši se upotrebom mehaničkih uređaja i tehničkim bezbjednosnim uređajima i sistemima u kombinaciji sa fizičkim obezbjeđenjem iz člana 15 ove uredbe.

Za ulazak u bezbjednosne zone zaposleni koriste identifikacionu karticu sa mogućnošću elektronske verifikacije identiteta lica i njihove autorizacije.

Gubitak identifikacione kartice odmah se prijavljuje licu koga odredi starješina organa, odnosno zakonski zastupnik organizacije.

Za ulazak drugog lica u bezbjednosnu zonu izdaje se posebna bezbjednosna propusnica u pisanoj formi.

Lice iz stava 4 ovog člana, može ući u bezbjednosnu zonu samo u pratnji zaposlenog koji ga obavještava da se njegovo kretanje nadzire i evidentira i pri ulasku i kretanju u bezbjednosnoj zoni, mora imati na vidnom mjestu zakačenu bezbjednosnu propusnicu.

Identifikacione kartice i bezbjednosne propusnice izdaje lice određeno od strane starješine organa, odnosno zakonskog zastupnika organizacije.

O izdatim identifikacionim karticama i bezbjednosnim propusnicama vodi se evidencija.

Lica zadužena za održavanje čistoće, kao i lica zadužena za održavanje I popravke tehničkih uređaja mogu ući u bezbjednosnu zonu samo u pratnji zaposlenog koga odredi starješina organa, odnosno zakonski zastupnik organizacije, a koji je dužan da ih nadzire.

Član 21

Ključevi i pojedinačne kombinacije za otvaranje brava od opreme iz člana 16 stav 1 alineja 1 ove uredbe i ulaza u bezbjednosne zone predaju se zaposlenima uz potpis, o čemu se vodi posebna evidencija.

Rezervni ključevi i zapisi pojedinačnih kombinacija za otvaranje brava iz stava 1 ovog člana, deponuju se na način da samo fizičko obezbjeđenje ima pristup.

Izrada kopije ključeva dozvoljava se samo na osnovu pisane saglasnosti starješine organa, odnosno zakonskog zastupnika organizacije ili zaposlenog koga on odredi.

Izmjena pojedinačnih kombinacija za otvaranje brava vrši se prilikom instalacije mehaničkih ili tehničkih uređaja, poslije svake promjene zaposlenih koji su bili upoznati sa postojećim kombinacijama, u slučaju povrede ili postojanja sumnje da će se desiti povreda bezbjednosti tajnih podataka, a najmanje jednom u šest mjeseci.

Član 22

Označavanje opreme iz člana 16 stav 1 alineja 1 ove uredbe, vrši se na način što se na spoljnoj strani u gornjem lijevom uglu stavlja etiketa ili naljepnica prikladne veličine sa oznakom velikog štampanog slova, i to:

- „ST” za stepen tajnosti „STROGO TAJNO”;
- „T” za stepen tajnosti „TAJNO”;
- „P” za stepen tajnosti „POVJERLJIVO”;
- „I” za stepen tajnosti „INTERNO” .

Ako se u ormarima iz člana 10 stav 4 i opremi iz člana 16 stav 1 alineja 1 ove uredbe čuvaju tajni podaci različitog stepena tajnosti, oznaka tajnosti mora odgovarati najvišem stepenu tajnosti podatka koji se u njima čuvaju.

Član 23

U svim prostorima, odnosno prostorijama bezbjednosne zone I i II stepena mora biti obavljen pregled protiv prisluškivanja i to:

- prilikom određivanja bezbjednosne zone;
- kod svakog nasilnog upada ili neovlašćenog pristupa u zonu;
- kod promjene zaposlenih u bezbjednosnoj zoni I;
- nakon izvođenja bilo koje vrste građevinskih ili telekomunikacionih radova;
- jednom godišnje.

Zaštita od prisluškivanja drugih prostora, odnosno prostorija ili informacionih i telekomunikacionih veza putem kojih se prenose tajni podaci vrši se u skladu sa bezbjednosnom procjenom ugroženosti.

Pregled iz stava 1 ovog člana vrši Agencija.

Zahtjev za vršenje pregleda iz stava 1 ovog člana organi, odnosno organizacije dostavljaju Agenciji, preko Direkcije za zaštitu tajnih podataka.

Član 24

Tajni podaci, osim podataka stepena tajnosti „STROGO TAJNO”, mogu se obrađivati van bezbjednosnih zona, ako je prostor ili područje u kojem se obrađuju fizički ili tehnički obezbijeđen, a pristup do njega pod nadzorom. Lice koje obrađuje tajni podatak van bezbjednosnih zona mora imati tajni podatak cijelo vrijeme pod nadzorom. Po okončanoj obradi, tajni podatak se vraća u bezbjednosnu zonu.

Kad se tajni podatak stepena tajnosti „TAJNO” i „POVJERLJIVO” mora obrađivati van prostora, odnosno prostorija određenog organa radi izvođenja tačno određenog naloga, starješina organa utvrđuje mjere za zaštitu tajnog podatka koje moraju biti u skladu sa mjerama propisanim za odgovarajuću bezbjednosnu zonu.

Svako iznošenje ili unošenje tajnog podatka stepena tajnosti „TAJNO” i „POVJERLJIVO” van bezbjednosne zone se evidentira. Lice koje preuzima tajni podatak, potvrđuje to svojeručnim potpisom i preuzima odgovornost za zaštitu tajnog podatka.

Član 25

Ovlašćeno lice koje je odredilo stepen tajnosti podatka, dostavlja tajni podatak korisniku koji ima dozvolu za pristup tajnim podacima najmanje onog stepena tajnosti podatka koji se dostavlja, po principu „potrebno je da zna“.

Tajni podatak se dostavlja na korišćenje, u skladu sa stavom 1 ovog člana, preko lica kojem je izdata dozvola za pristup tajnim podacima odgovarajućeg stepena tajnosti (u daljem teksu: kurir).

Član 26

Tajni podatak označen stepenom tajnosti „STROGO TAJNO”, „TAJNO” i „POVJERLJIVO” unutar bezbjednosne zone, dostavlja se na korišćenje u zatvorenoj, neprovidnoj koverti na kojoj su naznačeni podaci o primaocu tog tajnog podatka.

Član 27

Tajni podatak sa oznakom stepena tajnosti „STROGO TAJNO”, van bezbjednosne zone, dostavlja se na korišćenje preko najmanje dva kurira, a dokument označen stepenom tajnosti „TAJNO” ili „POVJERLJIVO”, dostavlja jedan kurir.

Tajni podatak sa oznakom stepena tajnosti „INTERNO" može se dostavljati putem kurira ili putem pošte, preporučenom pošiljkom sa povratnicom.

Dostavljanje tajnih podataka stranoj državi ili međunarodnoj organizaciji može se vršiti i putem diplomatske pošte.

Član 28

Primopredaja tajnog podatka vrši se u posebnoj prostoriji koju odredi starješina organa, odnosno zakonski zastupnik organizacije kome se tajni podatak dostavlja na korišćenje.

Korisnik tajnog podatka potvrđuje prijem tog podatka potpisom na potvrdi, odnosno u dostavnoj knjizi.

Obrazac potvrde iz stava 2 ovog člana sastavni je dio ove uredbe (Prilog 2).

Član 29

Tajni podatak označen stepenom tajnosti „STROGO TAJNO”, dostavlja se na korišćenje van bezbjednosne zone u koverti koja mora biti u zatvorenom koferu, kutiji ili torbi, sa zatvaranjem na ključ ili sa šifrovanom kombinacijom.

Tajni podatak označen stepenom tajnosti „TAJNO” i „POVJERLJIVO” van bezbjednosne zone, dostavlja se, po pravilu, u dvije koverte.

Spoljna koverta je od tvrdog, neprovidnog, nepropusnog materijala, na kojoj je označen organ kojem se dostavlja tajni podatak.

Unutrašnja koverta iz st. 1 i 2 ovog člana, mora imati oznaku stepena tajnosti podatka, broj i datum akta i podatke o primaocu i pošiljaocu.

Član 30

Na zahtjev lica kome predaje ili od koga preuzima tajni podatak, kurir je dužan da pokaže kurirsko uvjerenje.

Obrazac uvjerenja iz stava 1 ovog člana sastavni je dio ove uredbe (Prilog 3.)

Član 31

Ukoliko se procijeni da može doći do narušavanja bezbjednosti dostave tajnog podatka, kuriru se može pružiti pomoć angažovanjem policijskog službenika ili pripadnika vojne policije, kako bi se spriječio neovlašćeni pristup, oštećenje ili uništenje tajnog podatka.

Član 32

Uz tajni podatak koji se dostavlja drugoj državi ili međunarodnoj organizaciji mora se priložiti sljedeća bezbjednosna klauzula:

„Ovaj dokument i svi sadržani prilozi smatraju se (navesti stepen tajnosti), vlasništvo su autora - (navesti nadležni organ u Crnoj Gori), i mogu se koristiti samo u svrhu za koju su dostavljeni. Primalac dokumenta vodiće brigu o zaštiti tajnosti podataka sadržanih u dokumentu u skladu sa propisima Crne Gore o zaštiti tajnih podataka. Ne smije se mijenjati stepen tajnosti označen na ovom dokumentu i nikome nije dozvoljen pristup podacima sadržanim u ovom dokumentu ako nema dozvolu za pristup tajnim podacima stepena tajnosti kojim je označen ovaj dokument. Dokument i njegov sadržaj ne smije se bez odobrenja Crne Gore objavljivati, umnožavati, davati na korišćenje drugom organu ili trećoj strani, odnosno koristiti u druge svrhe osim onih zbog kojih je dostavljen. Crna Gora zadržava pravo na informisanje o korišćenju dostavljenog dokumenta i podatka koje dokument sadrži, a primalac dokumenta se obavezuje da će o uništenju dokumenta obavijestiti Crnu Goru".

Akt iz stava 1 ovog člana ulaže se u unutrašnju kovertu**.**

Član 33

Korisnik tajnog podatka stepena tajnosti „INTERNO", „POVJERLJIVO" i „TAJNO" može umnožiti ili prevesti dokument ili sačiniti izvod iz dokumenta, ako na omotu nije naznačena zabrana umnožavanja.

Korisnik tajnog podatka stepena tajnosti „STROGO TAJNO„ može umnožiti ili prevesti dokument ili sačiniti izvod iz dokumenta, samo uz pisanu saglasnost ovlašćenog lica koje je odredilo stepen tajnosti podatka.

Broj umnoženih primjeraka, prevoda ili izvoda iz dokumenta koji sadrži tajni podatak iz st. 1 i 2 ovog člana, određuje se po principu „potrebno je da zna".

Odobrena elektronska oprema (kompjuteri, kopir/fax mašine i dr.) za obradu tajnih podataka štiti se fizičkim mjerama zaštite, na način da je mogu koristiti samo lica koja posjeduju dozvolu za pristup tajnim podacima odgovarajućeg stepena tajnosti.

Mjere zaštite određene za originalni dokument primjenjuju se i na umnožene primjerke, prevode ili izvode tog dokumenta.

Član 34

Kopije dokumenata**,** radni nacrti i bilješke koji sadrže tajne podatke, kao i dokumenti koji sadrže tajne podatke koji su fizički oštećeni i ne mogu se dalje koristiti, uništavaju se na način da se ne mogu raspoznati i obnoviti (spaljivanjem, drobljenjem i dr.).

Tajni podaci stranih država i međunarodnih organizacija, uključujući i originalni primjerak, uništavaju se na način da se ne mogu raspoznati i obnoviti (spaljivanjem, drobljenjem i dr.), u skladu sa međunarodnim ugovorima.

Originalni primjerak tajnog podatka arhivira se i čuva u skladu sa zakonom kojim se uređuje tajnost podataka.

Član 35

Starješina organa, odnosno zakonski zastupnik organizacije obrazuje komisiju za uništavanje tajnih podataka.

Komisiju iz stava 1 ovog člana, čine najmanje tri lica kojima je izdata dozvola za pristup tajnim podacima najmanje onog stepena tajnosti podataka koji se uništavaju.

O uništavanju podataka iz stava 1 ovog člana, vodi se zapisnik, koji potpisuju svi članovi komisije.

Zapisnik iz stava 3 ovog člana, sadrži podatke o broju i datumu akta kojim je određeno uništavanje tajnog podatka, broju, datumu i stepenu tajnog podatka koji se uništava i načinu njihovog uništavanja.

Zapisnik iz stava 3 ovog člana, za tajne podatke stepena tajnosti „STROGO TAJNO" čuva se deset godina, za podatke stepena tajnosti „TAJNO" pet godina, za podatke stepena tajnosti „POVJERLJIVO" tri godine, a za podatke stepena tajnosti „INTERNO" godinu dana od dana uništavanja.

O uništavanju tajnih podataka stepena tajnosti „STROGO TAJNO", „TAJNO" i „POVJERLJIVO", pisanim putem se obavještava ovlašćeno lice koje je odredilo stepen tajnosti podatka.

Član 36

Danom stupanja na snagu ove uredbe prestaje da važi Uredba o bližim uslovima i načinu sprovođenja mjera zaštite tajnih podataka (»Službeni list CG«, broj 72/08).

Član 37

Ova uredba stupa na snagu osmog dana od dana objavljivanja u »Službenom listu Crne Gore«.

Broj:_____
Podgorica, _____ 2015. godine

VLADA CRNE GORE

P r e d s j e d n i k,

Milo Đukanović

PRILOG 1

BODOVANJE MJERA FIZIČKE ZAŠTITE

1. OPREMA I BRAVE ZA SIGURNO ČUVANJE PREDMETA I DOKUMENATA – S1

1.1. Oprema za sigurno čuvanje predmeta i dokumenata (sefovi, kase i dr.) – SS1

1.1.1. Oprema za sigurno čuvanje predmeta i dokumenata - tip 4 SS1 = 4 boda

a) oprema namijenjena za deponovanje tajnih podataka svih stepena tajnosti pod uslovom da se nalaze u bezbjednosnoj zoni I ili II, koja ispunjava uslove bezbjednosti prema standardu MEST EN 1143-1 klase II ili više

b) oprema iz podtačke a) ove tačke mora biti opremljena najmanje sa bravom standarda MEST EN 1300 klase C

1.1.2. Oprema za sigurno čuvanje predmeta i dokumenata - tip 3 SS1 = 3 boda

a) oprema namijenjena za deponovanje tajnih podataka svih stepena tajnosti pod uslovom da se nalaze u bezbjednosnoj zoni I ili II, koja ispunjava uslove bezbjednosti prema standardu MEST EN 1143-1 klase I ili više

b) oprema iz podtačke a) ove tačke mora biti opremljena najmanje sa bravom standarda MEST EN 1300 klase B

1.1.3. Oprema za sigurno čuvanje predmeta i dokumenata - tip 2 SS1 = 2 boda

a) oprema namijenjena za deponovanje tajnih podataka stepena tajnosti do i uključujući „TAJNO“ pod uslovom da se nalaze u bezbjednosnoj zoni I ili II, koja ispunjava uslove bezbjednosti prema standardu MEST EN 1143-1 klase 0 ili više

b) oprema iz podtačke a) ove tačke mora biti opremljena najmanje sa bravom standarda MEST EN 1300 klase B

1.1.4. Oprema za sigurno čuvanje predmeta i dokumenata - tip 1 SS1 = 1 bod

a) oprema namijenjena za deponovanje tajnih podataka stepena tajnosti do i uključujući „POVJERLJIVO“ pod uslovom da se nalaze u bezbjednosnoj zoni I ili II

b) oprema iz podtačke a) ove tačke mora biti opremljena najmanje mehaničkom bravom sa ključem

1.2. Brave za opremu za sigurno čuvanje predmeta i dokumenata – SS2

1.2.1. Brave za opremu za sigurno čuvanje predmeta i dokumenata - tip 4 SS2 = 4 boda

Brave za opremu za sigurno čuvanje predmeta i dokumenata ispunjavaju uslov bezbjednosti prema standardu MEST EN 1300 klase C

1.2.2. Brave za opremu za sigurno čuvanje predmeta i dokumenata - tip 3 SS2 = 3 boda

Brave za opremu za sigurno čuvanje predmeta i dokumenata ispunjavaju uslov bezbjednosti prema standardu MEST EN 1300 klase B

1.2.3. Brave za opremu za sigurno čuvanje predmeta i dokumenata - tip 2 SS2 = 2 boda

Brave za opremu za sigurno čuvanje predmeta i dokumenata ispunjavaju uslov bezbjednosti prema standardu MEST EN 1300 klase A

1.2.4. Brave za opremu za sigurno čuvanje predmeta i dokumenata - tip 1 SS2 = 1 bod

Brave za opremu za sigurno čuvanje predmeta i dokumenata moraju biti mehaničke brave sa ključem

2. MJERE ZA ZAŠTITU BEZBJEDNOSNIH ZONA – S2

2.1. Bezbjednosna zona – SS3

2.1.1. Bezbjednosna zona - Tip 4 SS3 = 4 boda

a) zaštićeno područje pruža visok nivo otpornosti protiv provalnika koji koristi silu i koji je opremljen sa efikasnim prenosivim instrumenatima; granica zaštićenog područja pokazuje visok stepen otpornosti protiv prikrivenih upada

b) zidovi, podovi i plafoni u zaštićenom području, moraju biti od čvrstog materijala, tj. cigli minimalne debljine 300 mm ili od armiranog betona minimalne debljine 150 mm

c) vrata, kapije i sve njihove komponente ili rešetke ispunjavaju uslove najmanje prema standardu MEST EN 1627 klase 4

d) prozori i njihove komponente ispunjavanju uslove prema standardu MEST EN 1627 klase 4

e) ako je donja granica prozora ili ivica izlaza viša od 5,5 m iznad tla i ne može joj se pristupiti sa krova, gromobrana, drugih strukturnih elemenata, zemljanih nepravilnosti, drveća ili drugih konstrukcija, uslovi iz stava d) se ne primjenjuju

f) sistem zaključavanja mehaničkih uređaja mora da odgovara tipu 4 pod tačkom 2.2.1

2.1.2. Bezbjednosna zona - tip 3 SS3 = 3 boda

a) zaštićeno područje pruža visok nivo otpornosti protiv provalnika koji je opremljen sa efikasnim prenosnim instrumentima, zaštićeno područje granica pokazuje visok nivo otpora protiv prikrivenog upada

b) zidovi, podovi i plafoni u zaštićenom području, moraju biti od čvrstog materijala, tj. cigli minimalne debljine 150 mm ili od armiranog betona minimalne debljine 100 mm

c) vrata, kapije i sve njihove komponente ili rešetke ispunjavaju uslove najmanje prema standardu MEST EN 1627 klase 3

d) prozori i svi njihovi delovi ili rešetke ispunjavaju uslove prema standardu MEST EN 1627 klase 3

e) ako je donja granica prozora ili ivica izlaza viša od 5,5 m iznad tla i ne može joj se lako pristupiti sa krova, gromobrana, drugih strukturnih elemenata, zemljanih nepravilnosti, drveća ili drugih konstrukcija, uslovi iz podtačke d) ove tačke se ne primjenjuju

f) sistem zaključavanja mehaničkih uređaja mora da odgovara tipu 3 pod tačkom 2.2.2

2.1.3. Bezbjednosna zona - tip 2 SS3 = 2 boda

a) zaštićeno područje pruža otpor protiv nasilnog ulaska za koje se koriste ručni instrumenti, zaštićeno područje pokazuje visok stepen otpora protiv prikrivenog upada

b) zidovi, podovi i plafoni u zaštićenom području moraju biti od čvrstih materijala ili armiranog betona minimalne debljine 75 mm
c) vrata, kapije i sve njihove komponente ili rešetke moraju ispunjavati uslove najmanje prema standardu MEST EN 1627 klase 2

d) prozori i svi njihovi djelovi ili rešetke ispunjavaju uslove najmanje prema standardu MEST EN 1627 klase 2

e) ako je donja granica prozora ili ivica izlaza viša od 5,5 m iznad tla i ne može joj se lako pristupiti sa krova, gromobrana, drugih strukturnih elemenata, zemljanih nepravilnosti, drveća ili drugih konstrukcija, uslovi iz podtačke d) ove tačke se ne primjenjuju

f) sistem zaključavanja mehaničkih uređaja mora da odgovara tipu 2 pod tačkom 2.2.3

2.1.4. Bezbjednosna zona - tip 1 SS3 = 1 bod

a) zaštićeno područje mora biti zaključano tako da pruža otpor protiv fizičkog nasilja i protiv prikrivenog upada

b) zidovi, podovi i plafoni u zaštićenom području moraju biti od čvrstih materijala ili armiranog betona minimalne debljine 75 mm

c) vrata, kapije i sve njihove komponente ili rešetke moraju da obezbijede isti nivo otpora protiv nasilnika kao i preostali djelovi bezbjednosne zone

d) mehanički uređaji, koji mogu da se otvore, sa ugrađenim sistemom za zaključavanje maksimum tipa 3 pod tačkom 2.2.2

e) tajni podaci stepena tajnosti „STROGO TAJNO“ ne mogu da se deponuju u ovo zaštićeno područje

2.2. Sistemi za zaključavanje vrata – SS4

2.2.1. Sistem za zaključavanje vrata – tip 4 SS4 = 4 boda

a) sistem zaključavanja obezbjeđuje visok stepen otpornosti protiv profesionalnih i stručnih upada korišćenjem posebno razvijenih instrumenata i tehnologija koje nijesu komercijalno dostupne

b) sistem zaključavanja i njegove komponente ispunjavaju uslove minimuma otpornosti prema standardu MEST EN 1303 klasa 4

2.2.2. Sistem za zaključavanje vrata – tip 3 SS4 = 3 boda

a) sistem zaključavanja obezbeđuje visok stepen otpornosti protiv profesionalnih i stručnih upada korišćenjem posebno razvijenih instrumenata i tehnologija koje su komercijalno dostupne za profesionalne bravare

b) sistem zaključavanja i njegove komponente ispunjavaju uslove minimuma otpornosti prema standardu MEST EN 1303 klasa 3

2.2.3. Sistem za zaključavanje vrata - tip 2 SS4 = 2 boda

a) sistem zaključavanja pruža otpor protiv prekršioca koji posjeduje ograničen izbor instrumenta

b) sistem zaključavanja i njegove komponente ispunjavaju uslove minimuma otpornosti prema standardu MEST EN 1303 klasa 2

2.2.4. Sistem za zaključavanje vrata - tip 1 SS4 = 1 bod

a) sistem zaključavanja pruža otpor protiv slučajnog upada

b) specifikacija sistema zaključavanja i njegovih komponenti biće naznačena u bezbjednosnoj dokumentaciji fizičkog obezbjeđenja i bezbjednosti zgrade

3. MJERE ZA ZAŠTITU OBJEKATA – S3

Dio granice objekta koji ima najmanji otpor će biti od suštinskog značaja za određivanje otpornosti objekta

Mehanički uređaji koji se koriste za zaštitu objekta obuhvataju sisteme zaključavanja, vrata, rešetke, zaštitne folije, prozore i zastakljivanje

Ako kontrola ulaska u objekat nije obezbijeđena, **S3 = 0 bodova**

3.1. Objekat – SS5

3.1.1. Objekat - tip 4 SS5 = 5 bodova

a) obezbjeđuje visok stepen otpornosti protiv nasilnog ulaska u objekte koji imaju posebno jaku konstrukciju od armiranog betona minimalne debljine 300 mm ili drugog građevinskog materijala uporedivih karakteristika

b) mehanički uređaji pružaju isti nivo otpora protiv nasilnog ulaska, kao i drugi djelovi objekta

3.1.2. Objekat - tip 3 SS5 = 3 boda

a) obezbjeđuje viši nivo otpora protiv nasilnog ulaska, koji ima jaku konstrukciju od armiranog betona minimalne debljine 100 mm ili čvrstih cigli minimalne debljine 150 mm ili od drugih građevinskih materijala uporedivih karakteristika

b) mehanički uređaji pružaju isti nivo otpora protiv nasilnog ulaska, kao i drugi djelovi objekta

3.1.3. Objekat - tip 2 SS5 = 2 boda

a) pruža osnovni nivo otpora protiv nasilnog ulaska, koji ima jaku konstrukciju od armiranog betona minimalne debljine 75 mm ili od drugih građevinskih materijala uporedivih karakteristika

b) mehanički uređaji pružaju isti nivo otpora protiv nasilnog ulaska, kao drugi djelovi objekta

3.1.4. Objekat - tip 1 SS5 = 1 bod

a) obezbjeđuje minimalni nivo otpora protiv nasilnog ulaska, koji ima laku konstrukciju

b) mehanički uređaji pružaju isti nivo otpora protiv nasilnog ulaska, kao i drugi djelovi objekta

4. KONTROLA PRISTUPA, PERIODIČNE KONTROLE I REŽIM POSJETA – S4

4.1. Kontrola pristupa – SS6

4.1.1. Kontrola pristupa – tip 4 SS6 = 4 boda

a) kontrola pristupa odgovara sistemu za kontrolu ulaska i izlaska u prostorije sa elektronskom verifikacijom identiteta lica i njihovom autorizacijom koja zahtijeva minimum nadzora

b) sistem kontrole pristupa u kombinaciji sa jedinistvenim indentifikacionim brojem (PIN) ili biometrijskim indentifikacionim sitemom koji je u skladu sa zahtjevima kontrole pristupa klase B i prepoznavanju klase 3, u skladu sa standardom MEST EN 50133-1

c) signal u slučaju neovlašćenog pristupa do tačke gdje se nalazi fizičko obezbjeđenje, starješina organa, odnosno zakonski zastupnik organizacije ili lice određeno od njih

d) kontrola ulaska dopunjena pristupnim barijerama za prevenciju neovlašćenog ulaska koje trebaju da onemoguće ponavljanje pokušaja neovlašćenog pristupa i da omoguće režim "jedan prolaz – jedno lice"

4.1.2. Kontrola pristupa – tip 3 SS6 = 3 boda

a) električni sistem kontrole pristupa u kombinaciji sa jedinstvenim indetifikacionim brojem (PIN) ili biometrijskim indentifikacionim sistemom u skladu sa zahtjevima kontrole pristupa klase B I prepoznavanje klase 3, u skladu sa standardom MEST EN 50133-1

b) kontrola pristupa dopunjena odgovarajućim pristupnim barijerama uključujući nadzor

4.1.3. Kontrola pristupa – tip 2 SS6 = 2 boda

a) kontrola pristupa na osnovu indentifikacione dozvole za ulazak sa fotografijom, kontrolisana od strane fizičkog obezbjeđenja ili električni sistem kontrole pristupa u skladu sa zahtjevima kontrole pristupa klase B i prepoznavanja klase 2, u skladu sa standardom MEST EN 50133-1

b) kontrola pristupa koja se obezbjeđuje zaključavanjem i otključavanjem vrata od strane ovlašćenog lica koje koristi sistem kamera ili video interfona

4.1.4. Kontrola pristupa – tip 1 SS6 = 1 bod

a) kontrola pristupa koja se obezbjeđuje zaključavanjem vrata koristeći određeni ključ, šifru ili drugi sistem izdat određenim licima

b) kontrola pristupa se može primijeniti samo na ulaske u zaštićena područja gdje se obrađuju tajni podaci stepena "POVJERLJIVO" i niže

4.2. Periodične kontrole ulaska i izlaska – SS7

4.2.1. – Periodične kontrole ulaska i izlaska ako se obavljaju SS7 = 1 bod

Odnose se na periodične kontrole ulaska i izlaska koje su određene kao preventivne mjere protiv neovlašćenog pristupa tajnim podacima

4.2.2. – Periodične kontrole ulaska i izlaska ako se ne obavljaju SS7 = 0 bodova

4.3. Režim posjeta – SS8

4.3.1. – Posjete u pratnji tokom boravka u objektu i bezbjednosnim zonama SS8 = 2 boda

a) posjetioci imaju pratnju tokom boravka u objektu i bezbjednosnim zonama
b) posjetioci moraju biti vidno označeni tokom cijelog boravka u zgradi
c) vodi se evidencija o posjetama u koju se unose podaci o imenu, prezimenu, funkciji, broju indentifikacione kartice, lične karte, službene legitimacije ili putne isprave i vremenu posjete

4.3.2. – Posjete u pratnji tokom boravka u bezbjednosnim zonama SS8 = 1 bod

a) posjetioci imaju pratnju tokom boravka u bezbjednosnim zonama

b) posjetioci moraju biti vidno označen tokom cijelog boravka u zgradi

c) vodi se evidencija o posjetama u koju se unose podaci o imenu, prezimenu, funkciji, broju indentifikacione kartice, lične karte, službene legitimacije ili putne isprave i vremenu posjete

5. FIZIČKO OBEZBJEĐENJE I ELEKTRIČNI BEZBJEDNOSNI SISTEMI – S5

5.1. Fizičko obezbjeđenje – SS9

5.1.1. Fizičko obezbjeđenje – tip 5 SS9 = 5 bodova

a) fizičko obezbjeđenje se vrši od strane lica iz člana 18 ove uredbe

b) fizičko obezbjeđenje se vrši patrolno unutar zgrade, prvi obilazak se vrši odmah po završetku radnog vremena kad se vrši provjera da li su zatvoreni svi prozori i vrata i u isto vrijeme se vrši provjera lica koja se nalaze u bezbjednosnim zonama

c) stalno prisustvo najmanje jednog zaposlenog lica fizičkog obezbjeđenja zaštite mora biti obezbijeđeno na mjestima gdje je potrebno stalno izvršavanje poslova fizičke zaštite

5.1.2. Fizičko obezbjeđenje – tip 4 SS9 = 4 boda

a) fizičko obezbjeđenje se vrši od strane lica iz člana 18 ove uredbe

b) fizičko obezbjeđenje se vrši od strane patrola unutar zgrade

c) stalno prisustvo najmanje jednog zaposlenog lica fizičkog obezbjeđenja mora biti obezbijeđeno na mjestima gdje je potrebno stalno izvršavanje poslova fizičke zaštite

5.1.3. Fizičko obezbjeđenje – tip 3 SS9 = 3 boda

a) fizičko obezbjeđenje se vrši od strane lica iz člana 18 ove uredbe

b) fizičko obezbjeđenje se vrši od strane patrola van zgrade

c) stalno prisustvo najmanje jednog zaposlenog lica fizičkog obezbjeđenja mora biti obezbijeđeno na mjestima gdje je potrebno stalno izvršavanje poslova fizičke zaštite

5.1.4. Fizičko obezbjeđenje – tip 2 SS9 = 2 boda

a) fizičko obezbjeđenje ne zahtijeva patrole i sprovodi se kroz metode unutrašnje zaštite, koristeći stalno prisutna lica

b) u slučaju potrebe, fizičko obezbjeđenje će tražiti pomoć, npr. Uprave policije, Vojne policije, lica koja imaju dozvolu za vršenje poslova zaštite u skladu sa propisom kojim se uređuje zaštita lica i imovine ili zaposlenih koji su obučeni za takve poslove

5.1.5. Fizičko obezbjeđenje – tip 1 SS9 = 1 bod

Fizičko obezbjeđenje se vrši kontrolom granica objekta, van radnog vremena

5.2. Električni bezbjednosni sistemi – SS10

5.2.1. Alarmni sistemi – SS10.1

Tehnički standardi alarmnih sistema su određeni u odnosu na najniži tip alarmnih sistema tehničkih uređaja koji se primjenjuju

5.2.1.1. Tehnički standardi alarmnih sistema – tip 4 SS10.1 = 4 boda

Komponente alarmnih sistema moraju biti u skladu sa zahtjevima bezbjednosnog nivoa 4 u skladu sa standardom MEST EN 50131

5.2.1.2. Tehnički standardi alarmnih sistema – tip 3 SS10.1 = 3 boda

Komponente alarmnih sistema moraju biti u skladu sa zahtjevima bezbjednosnog nivoa 3 u skladu sa standardom MEST EN 50131

5.2.1.3. Tehnički standardi alarmnih sistema – tip 2 SS10.1 = 2 boda

Komponente alarmnih sistema moraju biti u skladu sa zahtjevima bezbjednosnog nivoa 2 u skladu sa standardom MEST EN 50131

5.2.1.4. Tehnički standardi alarmnih sistema – tip 2 SS10.1 = 1 bod

Komponente alarmnih sistema moraju biti u skladu sa zahtjevima bezbjednosnog nivoa 1 u skladu sa standardom MEST EN 50131

5.2.2. Video nadzor (CCTV) – SS10.2

Sistem video nadzora koji se koristi za zaštitu objekta ili bezbjednosnih zona mora biti u skladu sa standardima MEST EN 50132

Video nadzor ulaska u bezbjednosne zone služi kao dodatna mjera i instaliran je na način da se omogući identifikacija lica

U prostorijama unutar bezbjednosnih zona u kojima se obrađuju, nastaju i čuvaju tajni podaci ne instalira se video nadzor

5.2.2.1. CCTV - tip 4 SS10.2 = 4 boda

a) CCTV instaliran na način da se vrši nadzor okoline i unutrašnjosti objekta
b) izlazni signal video kamera mora biti povezan sa kontrolnom tačkom na kojoj se nalaze lica iz člana 18 ove uredbe
c) izlazni signal se snima i arhivira na period od najmanje 15 kalendarskih dana

5.2.2.2. CCTV – tip 3 SS10.2 = 3 boda

a) CCTV instaliran na način da se vrši nadzor unutrašnjosti objekta
b) izlazni signal se snima i arhivira na period od najmanje 15 kalendarskih dana

5.2.2.3. CCTV – tip 2 SS10.2 = 2 boda

a) CCTV instaliran na način da se vrši nadzor bezbjednosnih zona
b) izlazni signal se snima i arhivira na period od najmanje 15 kalendarskih dana

6. MJERE SPOLJAŠNJE ZAŠTITE – S6

Spoljašnja zaštita objekta se vrši kao kompleksan sistem mjera za zaštitu granica objekta, ulaza u objekat, izlaza i uređaja za zatvaranje

6.1. Barijere – SS11

6.1.1. Barijere – tip 5 SS11 = 5 bodova

a) minimalan prelaz visine granice je 2500 mm
b) barijera sa sistemom za detekciju perimetra i instaliranim CCTV
c) kontrolisani prostor od 20 m koji je ostavljen između barijera i granice objekta

6.1.2. Barijera – tip 4 SS11 = 4 boda

a) minimalan prelaz visine granice je 2300 mm
b) barijera sa instaliranim sistemom CCTV
c) kontrolisani prostor od 10 m koji je ostavljen između barijera i granice objekta

6.1.3. Barjera – tip 3 SS11 = 3 boda

a) minimalan prelaz visine granice je 2150 mm
b) barijera sa instaliranim sistemom CCTV
c) kontrolisani prostor je ostavljen između barijera i granice objekta

6.1.4. Barijera – tipe 2 SS11 = 2 boda

a) minimalan prelaz visine granice je 1800 mm
b) kontrolisani prostor je ostavljen između barijera i granice objekta

6.2. Kontrola pristupa na ulazima u barijere – SS12

6.2.1. Kontrola pristupa koja se vrši na svim ulazima SS12 = 1 bod

Kontrola pristupa na ulazima u barijere u skladu sa potpoglavljem 4.1. Metod koji obezbjeđuje kontrolu pristupa će se naznačiti u bezbjednosnoj dokumentaciji i elaboratu obezbjeđenja objekta

6.2.2. Kontrola ulaska koja se ne vrši na svakom ulazu SS12 = 0 bodova

6.3. Sistem za perimetarsku zaštitu – SS13

Sistem za perimetarsku zaštitu primjenjuje se u cilju da se poveća spoljašnja bezbijednost objekta, instalira se skriven ili vidljiv, kao komponenta za preventivno dejstvo

6.3.1. Sistem za perimetarsku zaštitu implementiran SS13 = 1 bod

Izlazni signal sistema mora biti povezan sa kontrolnom tačkom na kojoj se nalaze lica iz člana 18 ove uredbe, kod starješine organa, odnosno zakonskog zastupnika organizacije ili lica kojeg oni odrede

6.3.2. Sistem za perimetarsku zaštitu nije implementiran SS13 = 0 bodova

6.4. Sigurnosno osvjetljenje – SS14

6.4.1. Sigurnosno osvjetljenje instalirano SS14 = 1 bod

Sigurnosno osvjetljenje je instalirano kao dopuna spoljnoj zaštiti kao komponenta za preventivno dejstvo

6.4.2. Sigurnosno osvjetljenje nije instalirano SS14 = 0 bodova

6.5. Spoljašnji CCTV – SS15

6.5.1. CCTV instaliran SS15 = 1 bod

CCTV je instaliran u cilju indentifikacije lica prema standardu MEST EN 50132

6.5.2. CCTV nije instaliran SS15 = 0 bodova

7. UREĐAJI ZA DETEKCIJU PREDMETA

Uređaji za detekciju predmeta nalaze se na ulaznim tačkama u objektu ili bezbjednosnim zonama i oni obezbjeđuju prepoznavanje predmeta koji nijesu dozvoljeni u zaštićenim područjima
Uređaji za detekciju predmeta moraju biti pod direktnim nadzorom ovlašćenih lica

8. UREĐAJI ZA UNIŠTAVANJE TAJNIH PODATAKA

Za fizičko uništavanje tajnih podataka, kao što su dokumenta, diskete, kompakt diskovi, magnetne trake, memorijske kartice, hard diskovi i dr. mogu se koristitit sljedeći uređaji:

8.1. Uređaji za fizičko uništavanje tajnih podataka - tip 4 bez evaluacije

Uređaji za fizičko uništavanje tajnih podataka svih stepena tajnosti dimenzija ostatka 0.8 mm x 11 mm

8.2. Uređaj za fizičko uništenje tajnih podataka (medija) - tip 3 bez evaluacije

Uređaji za fizičko uništavanje tajnih podataka stepena tajnosti “TAJNO” i niže dimenzija ostatka 1.9 mm x 15 mm

8.3. Uređaj za fizičko uništenje tajnih podataka (medija) - tip 2 bez evaluacije

Uređaji za fizičko uništavanje tajnih podataka stepena tajnosti “POVJERLJIVO” i niže dimenzija ostatka 3.9 mm x 30-50 mm

8.4. Uređaj za fizičko uništenje tajnih podataka (medija) - tip 1 bez evaluacije

Uređaji za fizičko uništavanje tajnih podataka stepena tajnosti “INTERNO” dimenzija ostatka 7.5 mm x 40-80 mm

8.5. Uređaji za demagnetizaciju - bez evaluacije

Uređaji za trajno brisanje tajnih podatka pohranjenih na elektronskim medijima za stepen tajnosti “TAJNO” i niže stepene tajnosti

9. EVALUACIJA BEZBJEDNOSNIH MJERA I ZAŠTIĆENIH PODRUČJA

9.1. OPREMA I BRAVE ZA SIGURNO ČUVANJE PREDMETA I DOKUMENATA - S1

Oprema za sigurno čuvanje predmeta i dokumenata (sefovi, kase i dr.) i njihova evaluacija - SS1 (potpoglavlje 1.1.)

Klasifikacija opreme za sigurno čuvanje predmeta i dokumenata i njihova evaluacija SS1:

tip 4 – 4 boda
tip 3 – 3 boda
tip 2 – 2 boda
tip 1 – 1 bod

Brave za opremu za sigurno čuvanje predmeta i dokumenata – SS2 (potpoglavlje 1.2.)

Klasifikacija brava za opremu za sigurno čuvanje predmeta i dokumenata i njihova evaluacija SS2:

tip 4 – 4 boda
tip 3 – 3 boda
tip 2 – 2 boda
tip 1 – 1 bod

Ukupna evaluacija opreme za sigurno čuvanje predmeta i dokumenata i njihovih brava S1 = SS1 x SS2

9.2. MJERE ZA ZAŠTITU BEZBJEDNOSNIH ZONA – S2

Bezbjednosne zone – SS3 (potpoglavlje 2.1.)

Klasifikacija bezbjednosnih zona i njihova evaluacija SS3:

tip 4 – 4 boda
tip 3 – 3 boda
tip 2 – 2 boda
tip 1 – 1 bod

Sistemi za zaključavanje vrata – SS4 (potpoglavlje 2.2.)

Klasifikacija sistema za zaključavanje i njihova evaluacija SS4:

tip 4 – 4 boda
tip 3 – 3 boda
tip 2 – 2 boda
tip 1 – 1 bod

Ukupna evaluacija mjera zaštite zaštićenih područja S2 = SS3 + SS4

9.3. MJERE ZA ZAŠTITU OBJEKATA – S3

Objekti – SS5 (potpoglavlje 3.1.)

Klasifikacija objekata i njihova evaluacija SS5:

tip 4 – 5 bodova
tip 3 – 3 boda
tip 2 – 2 boda
tip 1 – 1 bod

Ukupna evaluacija objekata S3 = SS5 (5,3,2 ili 1)

9.4. KONTROLA PRISTUPA, PERIODIČNE KONTROLE I REŽIM POSJETA – S4

Kontrola pristupa – SS6 (potpoglavlje 4.1.)

Klasifikacija kontrole pristupa i njihova evaluacija SS6:

tip 4 – 4 boda
tip 3 – 3 boda
tip 2 – 2 boda
tip 1 – 1 bod

Periodične kontrole ulazaka i izlazaka – SS7 (potpoglavlje 4.2.)

Klasifikacija periodičnih kontrola ulazaka i izlazaka i njihova evaluacija SS7:

obavljaju se – 1 bod
ne obavljaju se – 0 bodova

Režim posjeta – SS8 (potpoglavlje 4.3.)

Klasifikacija režima posjeta i njihova evaluacija SS8:

posjete u pratnji tokom boravka u objektu i bezbjednosnim zonama – 2 boda
posjete u pratnji tokom boravka u bezbjednosnim zonama – 1 bod
posjete bez pratnje – 0 bodova

Ukupna evaluacija kontrole pristupa i režima posjeta S4 = SS6 + SS8

9.5. FIZIČKO OBEZBJEĐENJE I ELEKTRIČNI BEZBJEDNOSNI SISTEMI – S5

Fizičko obezbjeđenje – SS9 (potpoglavlje 5.1.)

Klasifikacija fizičkog obezbjeđenja i evaluacija SS9:

tip 5 – 5 bodova
tip 4 – 4 boda
tip 3 – 3 boda
tip 2 – 2 boda
tip 1 – 1 bod

Električni bezbjednosni sistemi – SS10 (potpoglavlje 5.2.)

Alarmni sitemi – SS10.1 (tačka 5.2.1.)

Klasifikacija tehničkih standarda alarmnih sistema i njihova evaluacija SS10.1:

tip 4 – 4 boda
tip 3 – 3 boda
tip 2 – 2 boda
tip 1 – 1 bod

Video nadzor – SS10.2 (tačka 5.2.2.)

Klasifikacija sistema video nadzora i njihova evaluacija SS10.2:

tip 4 – 4 boda

tip 3 – 3 boda
tip 2 – 2 boda

SS10 = (SS10.1 + SS10.2) x K/2, gdje je:

K instalacioni koeficijent koji treba odrediti formulom **K = SS10.2/CHP** u kojoj je **CHP** bodovan prema kategoriji bezbjednosne zone odnosno:

bezbjednosna zona I stepena - 4 boda
bezbjednosna zona II stepena - 3 boda

Srednji rezultat SS10 treba da bude zaokružen na cijeli broj. Najveća vrijednost SS10 ne može preći 4 boda.

Ukupna evaluacija fizičkog obezbjeđenja i električnih bezbjednosnih sistema S5 = SS9 + SS10

9.6. MJERE ZA SPOLJAŠNJU ZAŠTITU – S6

Barijere – SS11 (potpoglavlje 6.1.)

Klasifikacija barijera i njihova evaluacija SS11:

tip 5 – 5 bodova
tip 4 – 4 boda
tip 3 – 3 boda
tip 2 – 2 boda

Kontrola pristupa na ulazima u barijere – SS12 (potpoglavlje 6.2.)

Klasifikacija kontrole ulaska kroz ulaze barijera i njihova evaluacija SS12:

vrši se na svim ulazima – 1 bod
ne vrši se na svim ulazima – 0 bodova

Sistemi za perimetarsku zaštitu – SS13 (potpoglavlje 6.3.)

Klasifikacija sistema za detekciju perimetra i njihova evaluacija SS13:

implementiran – 1 bod
nije implementiran – 0 bodova

Sigurnosno osvjetljenje – SS14 (potpoglavlje 6.4.)

Klasifikacija sigurnosnog osvjetljenja i njihova evaluacija SS14:

instalirano – 1 bod
nije instalirano – 0 bodova

Spoljašnji CCTV – SS15 (potpoglavlje 6.5.)

Klasifikacija CCTV-a i njegova evaluacija SS15:

instaliran – 1 bod
nije instaliran – 0 bodova

Ukupna evaluacija mjera za spoljašnju zaštitu S6 = (SS11 x SS12) + SS7 + SS13 + SS14 + SS15

10. MINIMALNO ZAHTIJEVANE VRIJEDNOSTI EVALUACIJE MJERA FIZIČKE ZAŠTITE BEZBJEDNOSNIH ZONA I OBJEKATA

10.1. Mininalno zahtijevane vrijednosti evaluacije mjera fizičke zaštite bezbjednosne zone I stepena i objekta u kojoj se ona nalazi u skladu sa rizikom ugroženosti:

Nizak stepen ugroženosti:

obavezno: (S1) + (S2) + (S3) = 10 bodova
obavezno: (S4) + (S5)* = 6 bodova
neobavezno: (S6) = 5 bodova
UKUPNO = 21 bod
*Vrijednost S5 mora dostići vrijednost od minimalno 4 boda

Srednji stepen ugroženosti:

obavezno: (S1) + (S2) + (S3) = 11 bodova
obavezno: (S4) + (S5)* = 7 bodova
neobavezno: (S6) = 6 bodova
UKUPNO = 24 boda
*Vrijednost S5 mora dostići vrijednost od minimalno 4 boda

Visok stepen ugroženosti:

obavezno: (S1) + (S2) + (S3) = 13 bodova
obavezno: (S4) + (S5)* = 7 bodova
neobavezno: (S6) = 6 bodova
UKUPNO = 26 bodova
*Vrijednost S5 mora dostići vrijednost od minimalno 4 boda

10.2. Mininalno zahtijevane vrijednosti evaluacije mjera fizičke zaštite bezbjednosne zone II stepena i objekta u kojoj se ona nalazi u skladu sa rizikom ugrozenosti:

Nizak stepen ugroženosti:

obavezno: (S1) + (S2) + (S3) = 8 bodova
obavezno: (S4) + (S5)** = 4 boda
neobavezno: (S6) = 5 bodova
UKUPNO = 17 bodova
****** Vrijednost S5 mora dostići vrijednost od minimalno 3 boda

Srednji stepen ugroženosti:

obavezno: (S1) + (S2) + (S3) = 9 bodova
obavezno: (S4) + (S5)** = 5 bodova
neobavezno: (S6) = 6 bodova
UKUPNO = 20 bodova
****** Vrijednost S5 mora dostići vrijednost od minimalno 3 boda

Visok stepen ugroženosti:

obavezno: (S1) + (S2) + (S3) = 10 bodova
obavezno: (S4) + (S5)** = 5 bodova
neobavezno: (S6) = 6 bodova
UKUPNO = 21 bod
****** Vrijednost S5 mora dostići vrijednost od minimalno 3 boda

PRILOG 2

Datum: **Potvrda broj:**
Date: **Receipt N^{o}:**

Primalac: **Molimo potpišite i odmah vratite:**
Addressee: **Please sing and return immediately to:**

Redni broj Item	Oznaka dokumenta Document Identification	Datum Date	Jezik Lang	Stepen tajn. Class.	Izdato kopija Copy Nos.	Br. kopije Nbr of Copies
1						
2						
3						
4						
5						

Ime (odštampano) NAME (Printed)	Potpis SIGNATURE	Datum i vrijeme prijema DATE & TIME RECEIVED

PRILOG 3

Broj:_____
Mjesto i datum,_____

Na osnovu člana 30 Uredbe o bližim uslovima i načinu sprovođenja administrativnih i fizičkih mjera zaštite tajnih podataka („Službeni list CG“, broj _____), _____, i z d a j e

KURIRSKO UVJERENJE

Da je _____, JMB_____

zaposlen u _____ ovlašćen

da vrši dostavu pošiljki označenih stepenom tajnosti.

Ovo uvjerenje važi do _____ .

_____

M.P.

O B R A Z L O Ž E NJ E

Pravni osnov za donošenje ove uredbe sadržan je u odredbi člana 68 stav 2 Zakona o tajnosti podataka ("Službeni list CG", br. 14/08, 76/09, 41/10, 38/12, 44/12, 14/13 i 18/14), kojom je propisano da bliže uslove i način sprovođenja administrativnih, fizičkih, informatičkih i industrijskih mjera zaštite tajnih podataka, kao i uslove i način obezbjeđivanja kripto zaštite tajnih podataka propisuje Vlada.

Uredbu o bližim uslovima i načinu sprovođenja mjera zaštite tajnih podataka (,,Službeni list CG“, broj 72/08), donijela je Vlada Crne Gore na sjednici od od 6. novembra 2008. godine.

Razlog za donošenje nove Uredbe je njeno usaglašavanje sa propisima i standardima EU, te uvođenje sistema bodovanja objekata, prostorija i prostora u kojima se čuvaju, koriste i obrađuju tajni podaci, sa ciljem da se postignu standardi a istovremeno obezbjedi ušteda sredstava za stvaranje uslova za rad sa tajnim podacima.

Uslovi za rad sa tajnim podacima odnose se na sačinjavanje bezbjednosne procjene ugroženosti objekta, prostorija i prostora u kojima se čuvaju, koriste i obrađuju tajni podaci, izradu plana zaštite tajnih podataka, te posjedovanje tehničke dokumentacije o specifikaciji mehaničkih i tehničkih bezbjednosnih uređaja i sistema za zaštitu objekata i bezbjednosnih zona i posjedovanje kopije sertifikata o ispunjenosti standarda ovih uređaja i sistema.

Tajni podatak se čuva, koristi i obrađuje u prostoriji, odnosno prostoru koji je određen kao administrativna, odnosno bezbjednosna zona, koja ima bezbjednosnu opremu u skladu sa propisanim standardima.

Mjere fizičke zaštite u bezbjednosnim zonama utvrđuju se na osnovu stepena rizika prijetnje tajnim podacima, na način što se vrši bodovanje mjera zaštite koje se odnose na: opremu i brave za sigurno čuvanje predmeta i dokumenata koji su određeni kao tajni podaci, mjere za zaštitu bezbjednosnih zona i zaštitu objekata u kojima se čuvaju, koriste i obrađuju tajni podaci, kontrolu pristupa, periodične kontrole i režim posjeta, fizičko obezbjeđenje i električne bezbjednosne sisteme, mjere spoljašnje zaštite, uređaje za detekciju predmeta i uređaje za uništavanje tajnih podataka. Nakon implementiranja mjera zaštite tajnih podataka vrši se evaluacija bezbjednosnih mjera i zaštićenih područja, kao u Prilogu 1 ove uredbe.

Crna Gora
Ministarstvo vanjskih poslova i evropskih integracija

Broj: 03/1/2-2/85/2

Podgorica, 22. VII 2015.

MINISTARSTVO ODBRANE

Dopisom broj 813-3039/15-6 od 22. jula 2015. godine tražili ste mišljenje o usklađenosti **Predloga uredbe o bližim uslovima i načinu sprovođenja administrativnih i fizičkih mjera zaštite tajnih podataka** s pravnom tekovinom Evropske unije, saglasno **članu 40 stav 1 alineja 2 Poslovnika Vlade**.

Nakon upoznavanja sa sadržinom propisa, Ministarstvo vanjskih poslova i evropskih integracija je saglasno s navedenim u ocjeni usklađenosti propisa s pravnim propisima Evropske unije.

MINISTAR

Prof. dr Igor Lukšić

IZJAVA O USKLAĐENOSTI NACRTA/PREDLOGA PROPISA CRNE GORE S PRAVNOM TEKOVINOM EVROPSKE UNIJE

	Identifikacioni broj Izjave	**MO-IU/PA/15/06**
1. Naziv nacrta/predloga propisa		
- na crnogorskom jeziku	Predlog uredbe o bližim uslovima i načinu sprovođenja administrativnih i fizičkih mjera zaštite tajnih podataka	
- na engleskom jeziku	Proposal for the Decree on closer conditions and procedures for implementing administrative and physical measures for protection of classified information	
2. Podaci o obrađivaču propisa		
a) Organ državne uprave koji priprema propis		
Organ državne uprave	Ministarstvo odbrane	
- Sektor/odsjek	Odjeljenje za normativnu djelatnost i evropske integracije	
- odgovorno lice (ime, prezime, telefon, e-mail)	Nada Ulićević, sekretar Ministarstva, tel. 020 224 627	
- kontakt osoblja (ime, prezime, telefon, e-mail)	Relja Radonjić tel. 020 483 698	
b) Pravno lice s javnim ovlašćenjem za pripremu i sprovođenje propisa		
- Naziv pravnog lica	/	
- odgovorno lice (ime, prezime, telefon, e-mail)	/	
- kontakt osoblja (ime, prezime, telefon, e-mail)	/	
3. Organi državne uprave koji primjenjuju/sssprovode propis		
- Organ državne uprave	Državni organi, organi državne uprave, organi jedinica lokalne samouprave i druga pravna lica kojima je povjereno vršenje javnih ovlašćenja (organi), kao i pravna i fizička lica kada u vršenju zakonom utvrđenih poslova, odnosno izvršavanju ugovorenog posla saznaju za tajne podatke (organizacije)	
4. Usklađenost nacrta/predloga propisa s odredbama Sporazuma o stabilizaciji i pridruživanju između Evropske unije i njenih država članica, s jedne strane i Crne Gore, s druge strane (SSP)		
a) Odredbe SSPa s kojima se usklađuje propis		
Sporazum ne sadrži odredbu koja se odnosi na normativni sadržaj predlog propisa.		
b) Stepen ispunjenosti obaveza koje proizilaze iz navedenih odredbi SSPa		
☐	ispunjava u potpunosti	
☐	djelimično ispunjava	
☐	ne ispunjava	
c) Razlozi za djelimično ispunjenje, odnosno neispunjenje obaveza koje proizilaze iz navedenih odredbi SSPa		
5. Veza nacrta/predloga propisa s Programom pristepena Crne Gore Evropskoj uniji (PPCG)		
- PPCG za period	2015-2018	
- Poglavlje, potpoglavlje	Poglavlje 31 – Vanjska, bezbjednosna i odbrambena politika, 2 Planovi i potrebe, 2.2 Zakonodavni okvir, A.1) Kontrola naoružanja, neproliferacija i EBOP	
- Rok za donošenje propisa	2015/III	
- Napomena	/	
6. Usklađenost nacrta/predloga propisa s pravnom tekovinom Evropske unije		
a) Usklađenost s primarnim izvorima prava Evropske unije		
Ne postoji odredba primarnih izvora prava EU s kojom bi se predlog propisa mogao uporediti radi dobijanja stepena njegove usklađenosti.		
b) Usklađenost sa sekundarnim izvorima prava Evropske unije		

32013D0488 Odluka Savjeta od 23. septembra 2013. o bezbjednosnim pravilima za zaštitu tajnih podataka EU / Council Decision of 23 September 2013 on the security rules for protecting EU classified information *(OJ L 274, 15.10.2013)* **Potpuno usklađeno/fully harmonized**
c) Usklađenost s ostalim izvorima prava Evropske unije
EU upravljanje procesima procjene rizika za fizičku zaštitu od 19. novembra 2007 / EU risk-management process for physical security, 19 November 2007 **Potpuno usklađeno/Fully harmonized**
6.1. Razlozi za djelimičnu usklađenost ili neusklađenost nacrta/predloga propisa Crne Gore s pravnom tekovinom Evropske unije i rok u kojem je predviđeno postizanje potpune usklađenosti
/
7. Ukoliko ne postoje odgovarajući propisi Evropske unije s kojima je potrebno obezbijediti usklađenost konstatovati tu činjenicu
/
8. Navesti pravne akte Savjeta Evrope i ostale izvore međunarodnog prava korišćene pri izradi nacrta/predloga propisa

Ne postoje izvori međunarodnog prava s kojima je potrebno uskladiti predlog propisa.	/

9. Navesti da li su navedeni izvori prava Evropske unije, Savjeta Evrope i ostali izvori međunarodnog prava prevedeni na crnogorski jezik (prevode dostaviti u prilogu)
Navedeni izvor prava EU je preveden na hrvatski jezik.
10. Navesti da li je nacrt/predlog propisa iz tačke 1 Izjave o usklađenosti preveden na engleski jezik (prevod dostaviti u prilogu)
Predlog uredbe o bližim uslovima i načinu sprovođenja administrativnih i fizičkih mjera zaštite tajnih podataka je preveden na engleski jezik.
11.Učešće konsultanata u izradi nacrta/predloga propisa i njihovo mišljenje o usklađenosti
U izradi Predloga uredbe o bližim uslovima i načinu sprovođenja administrativnih i fizičkih mjera zaštite tajnih podataka nije bilo učešća konsultanata.

Potpis / ovlašćeno lice obrađivača propisa	**Potpis** / ministar vanjskih poslova i evropskih integracija
Datum: 22.7.2015. godine	Datum:

Prilog obrasca:

1. Prevodi propisa Evropske unije
2. Prevod nacrta/predloga propisa na engleskom jeziku (ukoliko postoji)

TABELA USKLAĐENOSTI

1. Identifikacioni broj (IB) nacrta/predloga propisa	**1.1. Identifikacioni broj izjave o usklađenosti i datum utvrđivanja nacrta/predloga propisa na Vladi**
MO-TU/PA/15/06	**MO-IU/PA/15/06**
2. Naziv izvora prava Evropske unije i CELEX oznaka	
Odluka Savjeta od 23. septembra 2013. o bezbjednosnim pravilima za zaštitu tajnih podataka EU - **32013D0488**	
3. Naziv nacrta/predloga propisa Crne Gore	
Na crnogorskom jeziku	Na engleskom jeziku
Predlog uredbe o bližim uslovima i načinu sprovođenja administrativnih i fizičkih mjera zaštite tajnih podataka	Proposal for the Decree on closer conditions and procedures for implementing administrative and physical measures for protection of classified information

4. Usklađenost nacrta/predloga propisa s izvorima prava Evropske unije				
a)	b)	c)	d)	e)
Odredba i tekst odredbe izvora prava Evropske unije (član, stav, tačka)	Odredba i tekst odredbe nacrta/predloga propisa Crne Gore (član, stav, tačka)	Usklađenost odredbe nacrta/ predloga propisa Crne Gore s odredbom izvora prava Evropske unije	Razlog za djelimičnu usklađenost ili neusklađenost	Rok za postizanje potpune usklađenosti
Odluka 2013/488/EU				
Član 1. **Svrha, područje primjene i definicije** 1. Ovom se Odlukom utvrđuju osnovna načela i minimalni standardi bezbjednosti za zaštitu tajnih podataka EU-a (EUCI). 2. Navedeni minimalni standardi i osnovna načela primjenjuju se na Savjet i GSC, a države članice ih poštuju u skladu s njihovim nacionalnim zakonima i propisima kako bi svi bili sigurni da je za tajne podatke EU-a osigurana jednak nivo zaštite. 3. Za potrebe ove Odluke primjenjuju se definicije navedene u Dodatku A.	Nema odgovarajuće odredbe		Materija je regulisana čl. 1, 2 i 8. Zakona o tajnosti podataka ("Sl. list CG", br. 14/08, 76/09, 41/10, 38/12, 44/12, 14/13 i 18/14).	
Član 2. **Definicija tajnih podataka EU-a, stepena tajnosti i oznaka** 1. „Tajni podatak EU-a" (EUCI) znači svaki podatak ili materijal koji je označen stepenom tajnosti EU-u i čije neovlašćeno otkrivanje može uzrokovati različite stepene prijetnje nanošenjem štete interesima	Nema odgovarajuće odredbe		Materija je regulisana čl. 3, 8, 12 i 22 Zakona o tajnosti podataka ("Sl. list CG", br. 14/08, 76/09, 41/10, 38/12,	

Europske unije ili jedne ili više država članica. 2. Tajni podaci EU-a označavaju se prema sljedećim stepenima tajnosti: (a) TRÈS SECRET UE/EU TOP SECRET podaci i materijali čije neovlašteno otkrivanje može nanijeti izuzetno teške posljedice bitnim interesima Europske unije ili jedne ili više država članica; (b) SECRET UE/EU SECRET podaci i materijali čije neovlašteno otkrivanje može nanijeti teške štetne posljedice interesima Europske unije ili jedne ili više država članica; (c) CONFIDENTIEL UE/EU CONFIDENTIAL podaci i materijali čije neovlašteno otkrivanje može nanijeti štetu bitnim interesima Europske unije ili jedne ili više država članica; (d) RESTREINT UE/EU RESTRICTED podaci i materijali čije neovlašteno otkrivanje može dovesti u nepovoljan položaj interese Europske unije ili jedne ili više država članica. 3. Tajni podaci EU-a moraju biti označeni stepenom tajnosti u skladu sa stavom 2. Mogu nositi i dodatne oznake kojima se utvrđuje područje djelatnosti na koje se odnose, određuje onog od kojeg potiču, ograničava distribucija, ograničava upotreba ili naznačava mogućnost objavljivanja.			44/12, 14/13 i 18/14) i uredbom o načinu i postupku označavanja tajnosti podataka ("Sl. list CG", broj 67/08).	
Član 3. **Upravljanje stepenima tajnosti** 1. Nadležna tijela osiguravaju da su tajni podaci EU-a tajni na odgovarajući način, da su jasno određeni kao tajni podaci i da zadrže svoj stepen tajnosti samo onoliko dugo koliko je to potrebno. 2. Bez prethodne pisane saglasnosti onog od kojeg potiču, ne smije se smanjiti stepen tajnosti tajnih podataka EU- a, tajni se podaci EU-a ne smiju ukinuti niti se smije promijeniti ili ukloniti ijedna oznaka iz člana 2. stava 3. 3. Savjet odobrava bezbjednosnu politiku za stvaranje tajnih podataka EU-a koja mora obuhvatati i praktični vodič za označavanje stepena tajnosti .	Nema odgovarajuće odredbe		Materija je regulisana čl. 10, 14, 15, 16, 17, 18, 19b i 21 Zakona o tajnosti podataka ("Sl. list CG", br. 14/08, 76/09, 41/10, 38/12, 44/12, 14/13 i 18/14).	
Član 4. **Zaštita tajnih podataka** 1. Tajni podaci EU-a štite se u skladu s ovom Odlukom. 2. Vlasnik tajnog podatka EU-a odgovoran je za njegovom zaštitu u skladu s ovom Odlukom. 3. Ako države članice uvedu tajne podatke s oznakom nacionalnog stepena tajnosti u strukture ili mreže Unije, Savjet i GSC štite navedene podatke u skladu sa zahtjevima primjenljivima na tajne	Nema odgovarajuće odredbe		Materija je regulisana čl. 7, 8 stav 1 tačka 3, član 10 stav 4, član 17 stav 2 i član 19 Zakona o tajnosti podataka ("Sl. list CG", br. 14/08, 76/09, 41/10, 38/12, 44/12, 14/13 i 18/14) i	

podatke EU-a na jednakom nivou kako je utvrđeno u tabeli ekvivalentnosti stepena tajnosti sadržanoj u Dodatku B. 4. Skup tajnih podataka EU-a može nalagati stepen zaštite koji odgovara višem stepenu tajnosti od njegovih pojedinačnih dijelova.			članom 6 Uredbe o načinu i postupku označavanja tajnosti podataka ("Sl. list CG", broj 67/08).	
Član 5. **Upravljanje bezbjednosnim rizicima** 1. Rizikom za tajne podatke EU-a upravlja se kao procesom. Cilj je tog procesa utvrđivanje poznatih bezbjednosnih rizika, definisanje bezbjednosnih mjera za smanjenje takvih rizika na prihvatljiv nivo u skladu s osnovnim načelima i minimalnim standardima navedenim u ovoj Odluci te primjena navedenih mjera u skladu s konceptom dubinske odbrane kako je određeno u Dodatku A. Efikasnost takvih mjera stalno se ocjenjuje. 2. Bezbjednosne mjere za zaštitu tajnih podataka EU-a moraju tokom njihovog životnog ciklusa biti primjerene njihovom stepenu tajnosti, obliku i obimu podataka ili materijala, mjestu i konstrukciji objekata u kojima su smješteni tajni podaci EU-a i lokalno procijenjenoj prijetnji zlonamjernih i/ili kriminalnih aktivnosti, uključujući špijunažu, sabotažu i terorizam. 3. U kriznim se planovima mora imati na umu potreba zaštite tajnih podataka EU-a u vanrednim situacijama kako bi se spriječio neovlašćeni pristup, otkrivanje ili gubitak cjelovitosti ili dostupnosti. 4. U planove neprekidnosti poslovanja moraju se uključiti preventivne mjere i mjere oporavka kako bi se na najmanju moguću mjeru sveli veliki propusti ili nezgode u postepenu s tajnim podacima EU-a i njihovu čuvanju.	**Član 4** Bezbjednosnu procjenu ugroženosti sačinjava organ nadležan za poslove nacionalne bezbjednosti (u daljem tekstu: Agencija), u skladu sa zakonom, a naročito u odnosu na: potencijalne prijetnje tajnim podacima sa osvrtom na poziciju, lokaciju i čuvanje objekata i bezbjednosnih zona, aktivnosti stranih obavještajnih službi, sabotera, terorista i kriminalnih grupa, kao i rizike koji mogu biti uzrokovani aktivnošću zaposlenih. Zahtjev za bezbjednosnu procjenu ugroženosti organi, odnosno organizacije dostavljaju Agenciji, preko Direkcije za zaštitu tajnih podataka. Bezbjednosnu procjenu ugroženosti za Ministarstvo odbrane i Vojsku Crne Gore sačinjava organizaciona jedinica Ministarstva odbrane nadležna za vojno obavještajne i bezbjednosne poslove, u saradnji sa Agencijom. **Član 5** Na osnovu bezbjednosne procjene ugroženosti, starješina organa, odnosno zakonski zastupnik organizacije procjenjuje stepen rizika prijetnje tajnim podacima (visoki, srednji ili niski), a naročito u odnosu na: – stepen tajnosti podatka i broj tajnih podataka; – broj lica koja rukuju tajnim podacima. Zavisno od stepena rizika iz stava 1 ovog člana, starješina organa, odnosno zakonski zastupnik organizacije preduzima neophodne mjere zaštite tajnih podataka, u skladu sa ovom Uredbom. **Član 6** Plan zaštite tajnih podataka sadrži:	Potpuno usklađeno	Dodatkom A Odluke EU je propisana definicija odbrane po dubini, a čitav koncept ove Uredbe zasniva se na tom principu uvodeći višeslojne nivoe zaštite.	

	1. lokaciju i opis objekta u kojem se nalaze bezbjednosne zone, posebno opis granica objekta, broj ulaza, opis okolnih objekata i drugo; 2. podatke o bezbjednosnim zonama, uključujući opis aktivnosti koje se u njima vrše, 3. lokaciju i opis bezbjednosnih zona (položaj, ulaz, debljina zida, dimenzije prozora, visina prozora iznad tla i drugo), 4. grafički prikaz objekta, granica objekta, bezbjednosnih zona i granica bezbjednosnih zona, 5. način vršenja fizičke zaštite objekata i bezbjednosnih zona, koji sadrži: - uputstva za vršenje fizičke zaštite; - broj lica koja vrše fizičku zaštitu; - način provjere lica i vozila prilikom ulaska i izlaska, u toku i van radnog vremena; - način obavljanja periodične kontrole; - način vršenja patrole; - način reagovanja na alarmne poruke tehničkih bezbjednosnih uređaja i sistema; - metode kontrole fizičke zaštite; - knjigu posjetilaca u koju se unose ime, prezime, jedinistveni matični broj lica ili broj javne isprave iz koje se može utvrditi identitet, kao i naziv institucije u kojoj je to lice zaposleno, 6. procedure zaštite tajnih podataka u kriznim situacijama, a naročito: - izbor rezervne lokacije; - prenos tajnih podataka; - komunikaciju sa drugim nadležnim organima (Uprava policije, drugi organi i službe); - određivanje mjera obezbjeđenja tajnih podataka.			
Član 6. **Sprovođenje ove Odluke** 1. Savjet prema potrebi, na preporuku Bezbjednosnog odbora, odobrava bezbjednosne politike u kojima su navedene mjere za	Nema odgovarajuće odredbe	Neprenosivo		

sprovođenje ove Odluke. 2. Bezbjednosni odbor se na svom nivou može dogovoriti o bezbjednosnim smjernicama kojima će dopuniti ili potkrijepiti ovu Odluku te sve bezbjednosne politike koje odobri Savjet.				
Član 7. **Bezbjednost osoblja** 1. Bezbjednost osoblja je primjena mjera kojima se osigurava odobravanje pristupa tajnim podacima EU-a samo pojedincima: — kojima je nužan pristup podacima, — koji su, prema potrebi, prošli bezbjednosnu provjeru za odgovarajući stepen, i — koji su upoznati sa svojim odgovornostima. 2. Postupci za bezbjednosnu provjeru lica oblikovani su tako da se njima utvrđuje može li se pojedinac, s obzirom na njegovom lojalnost, vjerodostojnost i pouzdanost, ovlastiti za pristup tajnim podacima EU-a. 3. Svi pojedinci u GSC-u koji zbog svojih dužnosti moraju imati pristup ili moraju postupati s tajnim podacima EU-a sa stepenom tajnosti CONFIDENTIEL UE/EU CONFIDENTIAL ili višim moraju proći bezbjednosnu provjeru za odgovarajući stepen prije nego što im se omogući pristup takvim tajnim podacima EU-a. Te pojedince mora ovlastiti tijelo za imenovanja GSC-a za pristup tajnim podacima EU-a do određenog nivoa i do određenog datuma. 4. Osoblje država članica iz člana 15. stava 3., koje zbog svojih dužnosti može zatrebati pristup tajnim podacima EU-a sa stepenom tajnosti CONFIDENTIEL UE/EU CONFIDENTIAL ili višim mora proći bezbjednosnu provjeru za odgovarajući stepen ili mora biti na neki drugi način propisno ovlašteno na osnovu svojih funkcija, u skladu s nacionalnim zakonima i propisima, prije nego što mu se odobri pristup takvim tajnim podacima EU-a. 5. Prije nego što im se odobri pristup tajnim podacima EU-a te u pravilnim vremenskim razmacima nakon toga, svi se pojedinci upoznaju sa svojim odgovornostima povezanim sa zaštitom tajnih podataka EU-a u skladu s ovom Odlukom te ih moraju prihvatiti. 6. Odredbe za sprovođenje ovog člana navedene su u Prilogu I.	Nema odgovarajuće odredbe		Materija je regulisana čl. 25-54 Zakona o tajnosti podataka ("Sl. list Crne Gore", br. 14/08, 76/09, 41/10, 38/12, 44/12, 14/13 i 18/14)	
Član 8. **Fizička bezbjednost** 1. Fizička bezbjednost je primjena fizičkih i tehničkih zaštitnih mjera za sprečavanje neovlaštenog pristupa tajnim podacima EU-a. 2. Cilj mjera fizičke bezbjednosti je sprečavanje tajnog ili nasilnog	**Član 3** Objekti, prostorije, odnosno prostori u kojima se čuvaju, koriste i obrađuju tajni podaci, moraju da imaju: – bezbjednosnu procjenu ugroženosti,	Potpuno usklađeno	Materija je regulisana i čl. 64 i 68 Zakona o tajnosti podataka ("Sl. list CG", br. 14/08, 76/09, 41/10, 38/12,	

ulaska neovlašćenog osoblja, odvraćanje od neovlašćenih radnji, sprječavanje ili otkrivanje neovlašćenih radnji te omogućavanje razdvajanja osoblja koje pristupa tajnim podacima EU-a zbog nužnosti pristupa. Takve se mjere određuju na osnovu procesa upravljanja rizicima. 3. Mjere fizičke bezbjednosti uspostavljaju se za sve prostorije, zgrade, kancelarije, sobe i druga područja u kojima se postupa s tajnim podacima EU-a ili se ondje čuvaju, uključujući područja u kojima su smješteni komunikacioni i informacioni sistemi kako je određeno u članu 10. stavu 2. 4. Područja u kojima se čuvaju tajni podaci EU-a sa stepenom tajnosti CONFIDENTIEL UE/EU CONFIDENTIAL ili više utvrđuju se kao bezbjednosne zone u skladu s Prilogom II., a odobrava ih nadležno bezbjednosno tijelo. 5. Za zaštitu tajnih podataka EU-a sa stepenom tajnosti CONFIDENTIEL UE/EU CONFIDENTIAL ili više koristi se samo odobrena oprema ili uređaji. 6. Odredbe za sprovođenje ovog člana navedene su u Prilogu II.	– plan zaštite tajnih podataka, – tehničku dokumentaciju. Ažuriranje procjene, plana i dokumentacije iz stava 1 ovog člana, vrši se nakon svake promjene koja može da utiče na zaštitu tajnih podataka. **Član 8** Prostor ili prostorija u objektu koji je određen kao administrativna, odnosno bezbjednosna zona treba da ima bezbjednosnu opremu u skladu sa propisanim standardima.		44/12, 14/13 i 18/14), Uredbom o bližim uslovima i načinu sprovođenja informatičkih mjera zaštite tajnih podataka ("Sl. list CG", br. 57/10) i Uredbom o evidenciji tajnih podataka("Sl. list CG", br. 67/08, 49/10).	
Član 9. **Upravljanje tajnim podacima** 1. Upravljanje tajnim podacima primjena je administrativnih mjera za kontrolu tajnih podataka EU-a tokom njihovog životnog ciklusa kojima se dopunjuju mjere iz člana 7., 8. i 10. i pri tome pomaže pri odvraćanju i otkrivanju namjernog ili slučajnog ugrožavanja ili gubitka takvih podataka. Takve se mjere posebno odnose na stvaranje, evidenciju, umnožavanje, prevođenje, smanjenje stepena tajnosti, ukidanje, prenos i uništavanje tajnih podataka EU-a. 2. Podaci označeni kao CONFIDENTIEL UE/EU CONFIDENTIAL ili više evidentiraju se iz bezbjednosnih razloga prije distribucije i po prijemu U tu svrhu nadležna tijela u GSC-u i državama članicama uspostavljaju sistem registara. Podaci označeni kao TRÈS SECRET UE/EU TOP SECRET evidentiraju se u predviđene registre. 3. Službe i prostorije u kojima se postupa s tajnim podacima EU-a ili se ondje čuvaju podliježu redovnim inspekcijama koje sprovodi nadležno bezbjednosno tijelo. 4. Tajni podaci EU-a prosljeđuju se između službi i prostorija izvan fizički zaštićenih područja na sljedeći način: (a) u pravilu, tajni podaci EU-a prenose se elektronskim sredstvima koja su zaštićena kriptografskim proizvodima odobrenima u skladu s članom 10. stavom 6.;	**Član 1** Državni organi, organi državne uprave, organi jedinica lokalne samouprave i druga pravna lica kojima je povjereno vršenje javnih ovlašćenja (u daljem tekstu: organi), kao i pravna i fizička lica kad u vršenju zakonom utvrđenih poslova, odnosno izvršavanju ugovorenog posla saznaju za tajne podatke (u daljem tekstu: organizacije) dužni su da administrativne i fizičke mjere zaštite tajnih podataka, sprovode pod uslovima i na način propisan ovom Uredbom. **Član 25** Ovlašćeno lice koje je odredilo stepen tajnosti podatka, dostavlja tajni podatak korisniku koji ima dozvolu za pristup tajnim podacima najmanje onog stepena tajnosti podatka koji se dostavlja, po principu „potrebno je da zna“. Tajni podatak se dostavlja na korišćenje, u skladu sa stavom 1 ovog člana, preko lica kojem je izdata dozvola za pristup tajnim podacima odgovarajućeg stepena tajnosti (u daljem teksu: kurir).	Potpuno usklađeno	Materija je regulisana i Zakonom o tajnosti podataka u čl. 10, 21, 18, 19a, 19b, 63 stav 1 tačka 4, 64 stav 1 tač. 6 i 7, član 66 stav 1 tačka 2 i član 72, ("Sl. list CG", br. 14/08, 76/09, 41/10, 38/12, 44/12, 14/13 i 18/14), Uredbom o bližim uslovima i načinu sprovođenja informatičkih mjera zaštite tajnih podataka ("Sl. list CG", br. 57/10) i Uredbom o evidenciji tajnih podataka ("Sl. list CG", br. 67/08, 49/10)	

(b) ako se ne koriste sredstva iz tačke (a), tajni podaci EU-a prenose se: i. na elektronskim medijima (npr. USB-u, CD-u, tvrdom disku) koji su zaštićeni kriptografskim proizvodima odobrenima u skladu s članom 10. stavom 6.; ili ii. u svim drugim slučajevima na način koji je propisalo nadležno bezbjednosno tijelo u skladu s odgovarajućim zaštitnim mjerama utvrđenima u Prilogu III. 5. Odredbe za sprovođenje ovog člana navedene su u prilozima III. i IV.	**Član 26** Tajni podatak označen stepenom tajnosti „STROGO TAJNO", „TAJNO" i „POVJERLJIVO" unutar bezbjednosne zone, dostavlja se na korišćenje u zatvorenoj, neprovidnoj koverti na kojoj su naznačeni podaci o primaocu tog tajnog podatka. **Član 27** Tajni podatak sa oznakom stepena tajnosti „STROGO TAJNO", van bezbjednosne zone, dostavlja se na korišćenje preko najmanje dva kurira, a dokument označen stepenom tajnosti „TAJNO" ili „POVJERLJIVO", dostavlja jedan kurir. Tajni podatak sa oznakom stepena tajnosti „INTERNO" može se dostavljati putem kurira ili putem pošte, preporučenom pošiljkom sa povratnicom. Dostavljanje tajnih podataka stranoj državi ili međunarodnoj organizaciji može se vršiti i putem diplomatske pošte. **Član 28** Primopredaja tajnog podatka vrši se u posebnoj prostoriji koju odredi starješina organa, odnosno zakonski zastupnik organizacije kome se tajni podatak dostavlja na korišćenje. Korisnik tajnog podatka potvrđuje prijem tog podatka potpisom na potvrdi, odnosno u dostavnoj knjizi. Obrazac potvrde iz stava 2 ovog člana sastavni je dio ove Uredbe (Prilog 2). **Član 29** Tajni podatak označen stepenom tajnosti „STROGO TAJNO", dostavlja se na korišćenje van bezbjednosne zone u koverti koja mora biti u zatvorenom koferu, kutiji ili torbi, sa zatvaranjem na ključ ili sa šifrovanom kombinacijom. Tajni podatak označen stepenom tajnosti „TAJNO" i „POVJERLJIVO" van bezbjednosne zone, dostavlja se, po pravilu, u dvije koverte.			

	Spoljna koverta je od tvrdog, neprovidnog, nepropusnog materijala, na kojoj je označen organ kojem se dostavlja tajni podatak. Unutrašnja koverta iz st. 1 i 2 ovog člana, mora imati oznaku stepena tajnosti podatka, broj i datum akta i podatke o primaocu i pošiljaocu. **Član 30** Na zahtjev lica kome predaje ili od koga preuzima tajni podatak, kurir je dužan da pokaže kurirsko uvjerenje. Obrazac uvjerenja iz stava 1 ovog člana sastavni je dio ove Uredbe (Prilog 3.) **Član 31** Ukoliko se procijeni da može doći do narušavanja bezbjednosti dostave tajnog podatka, kuriru se može pružiti pomoć angažovanjem policijskog službenika ili pripadnika vojne policije, kako bi se spriječio neovlašćeni pristup, oštećenje ili uništenje tajnog podatka. **Član 32** Uz tajni podatak koji se dostavlja drugoj državi ili međunarodnoj organizaciji mora se priložiti sljedeća bezbjednosna klauzula: „Ovaj dokument i svi sadržani prilozi smatraju se (navesti stepen tajnosti), vlasništvo su autora - (navesti nadležni organ u Crnoj Gori), i mogu se koristiti samo u svrhu za koju su dostavljeni. Primalac dokumenta vodiće brigu o zaštiti tajnosti podataka sadržanih u dokumentu u skladu sa propisima Crne Gore o zaštiti tajnih podataka. Ne smije se mijenjati stepen tajnosti označen na ovom dokumentu i nikome nije dozvoljen pristup podacima sadržanim u ovom dokumentu ako nema dozvolu za pristup tajnim podacima stepena tajnosti kojim je označen ovaj dokument. Dokument i njegov sadržaj ne smije se bez odobrenja Crne Gore objavljivati, umnožavati, davati na korišćenje drugom organu ili trećoj strani, odnosno koristiti u druge svrhe osim onih zbog kojih je dostavljen. Crna Gora zadržava pravo			

	na informisanje o korišćenju dostavljenog dokumenta i podatka koje dokument sadrži, a primalac dokumenta se obavezuje da će o uništenju dokumenta obavijestiti Crnu Goru". Akt iz stava 1 ovog člana ulaže se u unutrašnju kovertu**.** **Član 33** Korisnik tajnog podatka stepena tajnosti „INTERNO", „POVJERLJIVO" i „TAJNO" može umnožiti ili prevesti dokument ili sačiniti izvod iz dokumenta, ako na omotu nije naznačena zabrana umnožavanja. Korisnik tajnog podatka stepena tajnosti „STROGO TAJNO„ može umnožiti ili prevesti dokument ili sačiniti izvod iz dokumenta, samo uz pisanu saglasnost ovlašćenog lica koje je odredilo stepen tajnosti podatka. Broj umnoženih primjeraka, prevoda ili izvoda iz dokumenta koji sadrži tajni podatak iz st. 1 i 2 ovog člana, određuje se po principu „potrebno je da zna". Odobrena elektronska oprema (kompjuteri, kopir/fax mašine i dr.) za obradu tajnih podataka štiti se fizičkim mjerama zaštite, na način da je mogu koristiti samo lica koja posjeduju dozvolu za pristup tajnim podacima odgovarajućeg stepena tajnosti. Mjere zaštite određene za originalni dokument primjenjuju se i na umnožene primjerke, prevode ili izvode tog dokumenta. **Član 34** Kopije dokumenata**,** radni nacrti i bilješke koji sadrže tajne podatke, kao i dokumenti koji sadrže tajne podatke koji su fizički oštećeni i ne mogu se dalje koristiti, uništavaju se na način da se ne mogu raspoznati i obnoviti (spaljivanjem, drobljenjem i dr.). Tajni podaci stranih država i međunarodnih organizacija, uključujući i originalni primjerak, uništavaju se na način da se ne mogu			

	raspoznati i obnoviti (spaljivanjem, drobljenjem i dr.), u skladu sa međunarodnim ugovorima. Originalni primjerak tajnog podatka arhivira se i čuva u skladu sa zakonom kojim se uređuje tajnost podataka. **Član 35** Starješina organa, odnosno zakonski zastupnik organizacije obrazuje komisiju za uništavanje tajnih podataka. Komisiju iz stava 1 ovog člana, čine najmanje tri lica kojima je izdata dozvola za pristup tajnim podacima najmanje onog stepena tajnosti podataka koji se uništavaju. O uništavanju podataka iz stava 1 ovog člana, vodi se zapisnik, koji potpisuju svi članovi komisije. Zapisnik iz stava 3 ovog člana, sadrži podatke o broju i datumu akta kojim je određeno uništavanje tajnog podatka, broju, datumu i stepenu tajnog podatka koji se uništava i načinu njihovog uništavanja. Zapisnik iz stava 3 ovog člana, za tajne podatke stepena tajnosti „STROGO TAJNO" čuva se deset godina, za podatke stepena tajnosti „TAJNO" pet godina, za podatke stepena tajnosti „POVJERLJIVO" tri godine, a za podatke stepena tajnosti „INTERNO" godinu dana od dana uništavanja. O uništavanju tajnih podataka stepena tajnosti „STROGO TAJNO", „TAJNO" i „POVJERLJIVO", pisanim putem se obavještava ovlašćeno lice koje je odredilo stepen tajnosti podatka.			
Član 10. **Zaštita tajnih podataka EU-a koji se obrađuju u komunikacionim i informacionim sistemima** 1. Informatička bezbjednost (IA) u području komunikacionih i informacionih sistema garantuje da će takvi sistemi štititi podatke koji se obrađuju i da će funkcionisati kada je to potrebno i u skladu sa potrebama ovlašćenih korisnika. Efikasni IA osigurava	Nema odgovarajuće odredbe		Materija je regulisana Zakonom o tajnosti podataka, čl. 66, 68 stav 2, ("Sl. list Crne Gore", br. 14/08, 76/09, 41/10,	

odgovarajući nivo tajnosti, cjelovitosti, dostupnosti, nepobitnosti i autentičnosti. IA se temelji na procesu upravljanja rizicima. 2. „Komunikacioni i informacioni sistem" (CIS) znači svaki sistem koji omogućava postepene s podacima u elektronskom obliku. CIS obuhvata sva sredstva potrebna za njegov rad, uključujući infrastrukturu, organizaciju, osoblje i informacijske resurse. Ova se Odluka primjenjuje na CIS za postepene s tajnim podacima EU-a (CIS). 3. CIS postupa s tajnim podacima EU-a u skladu s konceptom IA-a. 4. Svaki CIS mora proći proces akreditacije. Cilj je akreditacije pribavljanje potvrde da su sve odgovarajuće bezbjednosne mjere sprovedene i da je ostvaren potreban nivo zaštite tajnih podataka EU-a i CIS-a u skladu s ovom Odlukom. U izjavi o akreditaciji određuje se najviši stepen tajnosti podataka s kojima se može postupati u CIS-u i odgovarajući uslovi. 5. Sprovode se bezbjednosne mjere za zaštitu CIS-a, u kojem se postupa s podacima sa stepenom tajnosti CONFIDENTIEL UE/EU CONFIDENTIAL i višim, od ugrožavanja takvih podataka nenamjernim elektromagnetnim zračenjem („bezbjednosne mjere TEMPEST"). Takve bezbjednosne mjere srazmjerne su riziku iskorišćavanja i stepenu tajnosti tih podataka. 6. Ako su tajni podaci EU-a zaštićeni kriptografskim proizvodima, takvi proizvodi odobravaju se kako slijedi: (a) tajnost podataka označenih kao SECRET UE/EU SECRET i više zaštićena je kriptografskim proizvodima koje je odobrilo Savjet u ulozi tijela za odobravanje kriptomaterijala (CAA) na preporuku Bezbjednosnog odbora; (b) tajnost podataka označenih kao CONFIDENTIEL UE/EU CONFIDENTIAL ili RESTREINT UE/EU RESTRICTED zaštićena je kriptografskim proizvodima koje je odobrio glavni sekretar Savjeta („glavni sekretar") u ulozi CAA-a na preporuku Bezbjednosnog odbora. Nezavisno od tačke (b), unutar nacionalnih sistema država članica povjerljivost tajnih podataka EU-a sa stepenom tajnosti CONFIDENTIEL UE/EU CONFIDENTIAL ili RESTREINT UE/EU RESTRICTED može se zaštititi kriptografskim proizvodima koje je odobrio CAA države članice. 7. Tokom prenosa tajnih podataka EU-a elektronskim sredstvima koriste se odobreni kriptografski proizvodi. Nezavisnoo tom zahtjevu, u vanrednim se okolnostima ili posebnim tehničkim			38/12, 44/12, 14/13 i 18/14), i Uredbom o bližim uslovima i načinu sprovođenja informatičkih mjera zaštite tajnih podataka ("Sl. list CG", br. 57/10)	

konfiguracijama navedenima u Prilogu IV. mogu primjenjivati posebni postupci. 8. Nadležna tijela GSC-a, odnosno država članica uspostavljaju sljedeće funkcije IA-a: (a) tijelo za IA (IAA); (b) tijelo za TEMPEST (TA); (c) tijelo za odobravanje kriptomaterijala (CAA); (d) tijelo za distribuciju kriptomaterijala (CDA). 9. Nadležna tijela GSC-a, odnosno država članica uspostavljaju za svaki sistem: (a) tijelo za bezbjednosnu akreditaciju (SAA); (b) operativno tijelo za IA. 10. Odredbe za sprovođenje ovog člana navedene su u Prilogu IV.				
Član 11. **Industrijska bezbjednost** 1. Industrijska bezbjednost je primjena mjera kojima se osigurava da ugovarači i podugovarači štite tajne podatke EU-a u pregovorima prije sklapanja ugovora i tokom životnog ciklusa tajnih ugovora. Takvi ugovori ne smiju uključivati pristup podacima koji su tajni kao TRÈS SECRET UE/EU TOP SECRET. 2. GSC može na osnovu ugovora povjeriti zadatke koji obuhvataju ili uključuju pristup ili postepene s tajnim podacima EU-a ili njihovo čuvanje industrijskim ili drugim subjektima registrovanim u državi članici ili trećoj državi koja je sklopila sporazum ili administrativni dogovor u skladu s članom 13. stavom 2. tačkama (a) ili (b). 3. GSC, kao tijelo za ugovaranje, osigurava poštovanje minimalnih standarda o industrijskoj bezbjednosti navedenih u ovoj Odluci, i iz ugovora, prilikom sklapanja tajnih ugovora s industrijskim ili drugim subjektima. 4. Nacionalno bezbjednosno tijelo (NSA) ili zaduženo bezbjednosno tijelo (DSA) ili bilo koje drugo nadležno tijelo svake države članice osigurava, u mjeri u kojoj je to moguće prema nacionalnim zakonima i propisima, da ugovarači i podugovarači registrovani na njenom državnom području preduzmu sve odgovarajuće mjere za zaštitu tajnih podataka EU-a tokom pregovora prije sklapanja ugovora i prilikom izvršenja tajnog ugovora. 5. NSA, DSA ili bilo koje drugo nadležno bezbjednosno tijelo svake države članice osigurava, u skladu s nacionalnim zakonima i propisima, da ugovarači ili podugovarači koji su registrovani u državi članici i koji učestvuju u tajnim ugovorima ili podugovorima koji	Nema odgovarajuće odredbe		Materija je regulisana čl. 8 stav 1 tačka 4 i čl. 28, 30, 30a, 31, 62, 67 Zakona o tajnosti podataka ("Sl. list Crne Gore", br. 14/08, 76/09, 41/10, 38/12, 44/12, 14/13 i 18/14) i čl. 1, 2, 4, 6 i 8 Uredbe o bližim uslovima i načinu sprovođenja industrijskih mjera zaštite tajnih podataka ("Sl. list CG", broj 08/11).	

zahtijevaju pristup podacima tajnima kao CONFIDENTIEL UE/EU CONFIDENTIAL ili SECRET UE/EU SECRET unutar svojih prostorija, bilo tokom izvršenja takvih ugovora ili u fazi prije sklapanja ugovora, posjeduju uvjerenje o bezbjednosnoj provjeri pravne osobe (FSC) za odgovarajući stepen tajnosti. 6. Osoblju ugovarača ili podugovarača kojem za izvršenje tajnog ugovora treba pristup podacima tajnima kao CONFIDENTIEL UE/EU CONFIDENTIAL ili SECRET UE/EU SECRET odgovarajući NSA, DSA ili bilo koje drugo nadležno bezbjednosno tijelo odobrava uvjerenje o bezbjednosnoj provjeri osobe (PSC) u skladu s nacionalnim zakonima i propisima te minimalnim standardima utvrđenima u Prilogu I. 7. Odredbe za sprovođenje ovog člana navedene su u Prilogu V.				
Član 12. **Razmjena tajnih podataka EU-a** 1. Savjet određuje uslove prema kojima ono može razmjenjivati tajne podatke EU-a u njegovom vlasništvu s drugim institucijama, tijelima, Kancelarijama, ili agencijama Unije. U tu svrhu može se uspostaviti odgovarajući okvir, uključujući sklapanje međuinstitucionalnih sporazuma ili drugih dogovora, ako je to potrebno. 2. Takvim okvirom garantuje se da su tajni podaci EU-a zaštićeni na odgovarajući način u skladu sa stepenom tajnosti te u skladu sa osnovnim načelima i minimalnim standardima koji su jednaki onim utvrđenim u ovoj Odluci.	Nema odgovarajuće odredbe		Materija je regulisana članom 76. Zakona o tajnosti podataka ("Sl. list Crne Gore", br. 14/08, 76/09, 41/10, 38/12, 44/12, 14/13 i 18/14)	
Član 13. **Razmjena tajnih podataka s trećim državama i međunarodnim organizacijama** 1. Ako Savjet utvrdi da postoji potreba za razmjenom tajnih podataka EU-a s trećim državama ili međunarodnim organizacijama, u tu se svrhu uspostavlja odgovarajući okvir. 2. Za uspostavljanje takvog okvira i definisanje uzajamnih pravila o zaštiti razmijenjenih tajnih podataka: (a) Unija sklapa sporazume s trećim državama ili međunarodnim organizacijama o bezbjednosnim postupcima za razmjenu i zaštitu tajnih podataka („sporazumi o bezbjednosti podataka”); ili (b) glavni sekretar može sklapati administrativne dogovore u ime GSC-a u skladu sa stavom 17. Priloga VI. ako stepen tajnosti tajnih podataka EU-a koji se treba objaviti u pravilu nije viši od RESTREINT UE/EU RESTRICTED. 3. Sporazumi o bezbjednosti podataka ili administrativni dogovori iz	Nema odgovarajuće odredbe		Materija je regulisana čl. 6, 8 stav 1 tačka 3, čl. 76, 76a stav 1 tačka 1, čl. 77, 77a i 78 Zakona o tajnosti podataka("Sl. list CG", br. 14/08, 76/09, 41/10, 38/12, 44/12, 14/13 i 18/14), i Sporazumom između Crne Gore i Evropske unije o bezbjedonosnim procedurama za razmjenu i zaštitu tajnih podataka (Sl. list CG - Međunarodni ugovori, broj 13/2010	

stava 2. sadrže odredbe kojima se osigurava odgovarajuća zaštita podataka koje prime treće države ili međunarodne organizacije u skladu s njihovim stepenom tajnosti i minimalnim standardima koji nisu ništa manje strogi od minimalnih standarda utvrđenih ovom Odlukom. 4. Odluku o objavljivanju tajnih podataka EU-a koji potiču od Savjeta trećoj državi ili međunarodnoj organizaciji donosi Savjet od slučaja do slučaja, u skladu s prirodom i sadržajem takvih podataka, nužnosti prkorisnika za pristupom podacima i koristi koju će imati Unija. Ako onaj od kojeg potiču tajni podaci koji se žele objaviti nije Savjet, GSC najprije mora zatražiti pisanu saglasnost za objavljivanje od onog od koga podaci potiču. Ako se taj ne može utvrditi, Savjet preuzima odgovornost onog od koga podaci potiču. 5. Organizuju se posjete za procjenu stanja, kako bi se utvrdila efikasnost uspostavljenih bezbjednosnih mjera u trećoj državi ili međunarodnoj organizaciji za zaštitu dostavljenih ili razmijenjenih tajnih podataka EU-a. 6. Odredbe za sprovođenje ovog člana navedene su u Prilogu VI.				
Član 14. **Povrede bezbjednosti i ugrožavanje tajnih podataka EU-a** 1. Povreda bezbjednosti posljedica je radnje ili propusta pojedinca koji su u suprotnosti sa bezbjednosnim propisima utvrđenima ovom Odlukom. 2. Do ugrožavanja tajnih podataka EU-a dolazi kada su ti podaci djelimično ili u potpunosti otkriveni neovlašćenim osobama kao rezultat povrede bezbjednosti. 3. Svaka povreda ili sumnja u povredu bezbjednosti odmah se prijavljuje nadležnom bezbjednosnom tijelu. 4. Ako je poznato ili ako postoje opravdani razlozi na osnovu kojih se može pretpostaviti da su tajni podaci EU-a ugroženi ili izgubljeni, NSA ili drugo nadležno tijelo preduzima sve odgovarajuće mjere u skladu s mjerodavnim zakonima i propisima, kako bi: (a) obavijestilo onog od koga podaci potiču; (b) osiguralo da istragu predmeta sprovede osoblje koje nije neposredno povezano s povredom s ciljem utvrđivanja činjenica; (c) procijenilo moguću štetu nanesenu interesima Unije ili država članica; (d) preduzelo odgovarajuće mjere za sprečavanje ponovne povrede; i (e) obavijestilo nadležna tijela o preduzetim mjerama.	Nema odgovarajuće odredbe		Materija je regulisana Zakonom o tajnosti podataka ("Sl. list Crne Gore", br. 14/08, 76/09, 41/10, 38/12, 44/12, 14/13 i 18/14), i Krivičnim zakonikom Crne Gore (Sl. RCG", br. 70/2003, 13/2004, 47/2006 i "Sl. list CG", br. 40/2008, 25/2010, 32/2011, 40/2013 i 56/2013 i Sporazumom između Crne Gore i Evropske unije o bezbjedonosnim procedurama za razmjenu i zaštitu tajnih podataka (Sl. list CG - Međunarodni ugovori, broj 13/2010)	

5. Protiv svakog pojedinca odgovornog za povredu bezbjednosnih propisa utvrđenih ovom Odlukom može se pokrenuti disciplinski postupak u skladu s mjerodavnim pravilima i propisima. Protiv svakog pojedinca odgovornog za ugrožavanje ili gubitak tajnih podataka EU-a pokreće se disciplinski i/ili pravni postupak u skladu s važećim zakonima, pravilima i propisima				
Član 15. **Odgovornost za sprovođenje** 1. Savjet preduzima sve potrebne mjere, kako bi osiguralo cjelokupnu dosljednost u primjeni ove Odluke. 2. Glavni sekretar preduzima sve potrebne mjere kako bi osigurao da, prilikom postepena s tajnim podacima EU-a ili bilo kojim drugim tajnim podacima ili prilikom njihovog čuvanja, zvaničnici GSC-a i drugi službenici, osoblje upućeno GSC-u i ugovarači GSC-a primjenjuju ovu Odluku u prostorijama kojima se koristi Savjet i unutar GSC-a.	Nema odgovarajuće odredbe	Neprenosivo		
3. Države članice preduzimaju sve odgovarajuće mjere u skladu sa svojim nacionalnim zakonima i propisima kako bi osigurale da prilikom postupanja s tajnim podacima EU-a i njihovog čuvanja ovu Odluku poštuju: (a) osoblje stalnih predstavništava država članica u Europskoj uniji i nacionalni predstavnici koji prisustvuju sastancima Savjeta ili njegovih pripremnih tijela ili učestvuju u drugim aktivnostima Savjeta; (b) ostalo osoblje u nacionalnim administracijama država članica, uključujući osoblje upućeno tim administracijama, bez obzira na to obavlja li ono svoju službu na državnom području države članice ili u inostranstvu; (c) ostale osobe u državama članicama koje su, u skladu sa svojim funkcijama, propisno ovlaštene za pristup tajnim podacima EU-a; i (d) ugovarači država članica, bez obzira na to jesu li na području države članice ili u inostranstvu.	Nema odgovarajuće odredbe		Materija je regulisana Zakonom o tajnosti podataka ("Sl. list Crne Gore", br. 14/08, 76/09, 41/10, 38/12, 44/12, 14/13 i 18/14). i Sporazumom između Crne Gore i Evropske unije o bezbjedonosnim procedurama za razmjenu i zaštitu tajnih podataka (Sl. list CG - Međunarodni ugovori, broj 13/2010)	
Član 16. **Organizacija bezbjednosti u Savjetu** 1. U okviru svoje uloge u osiguravanju cjelokupne dosljednosti u primjeni ove Odluke Savjet odobrava: (a) sporazume iz člana 13. stava 2. tačke (a); (b) odluke kojima se odobrava ili daje saglasnost za objavu tajnih podataka EU-a koji potiču od Savjeta ili su njegovom posjedu trećim državama i međunarodnim organizacijama, u skladu s načelom	Nema odgovarajuće odredbe	Neprenosivo		

pristanka izvora; (c) godišnji program posjeta radi procjene stanja na preporuku Bezbjednosnog odbora za posjete radi procjene službi i prostorija država članica, tijela, agencija i subjekata Unije koji primjenjuju ovu Odluku ili njezina načela te za posjete radi procjene stanja trećim državama i međunarodnim organizacijama, kako bi se utvrdila efikasnost provedenih mjera za zaštitu tajnih podataka EU-a; i (d) bezbjednosne politike predviđene članom 6. stavom 1. 2. Glavni sekretar bezbjednosno je tijelo GSC-a. U tom svojstvu glavni sekretar: (a) sprovodi i preispituje bezbjednosnu politiku Savjeta; (b) koordinira s NSA-ima država članica sva pitanja bezbjednosti povezana sa zaštitom tajnih podataka koji se odnose na aktivnosti Savjeta; (c) izdaje zvaničnicima GSC-a, drugim službenicima i upućenim nacionalnim stručnjacimaovlašćenjei za pristup podacima sa stepenom tajnosti CONFIDENTIEL UE/EU CONFIDENTIAL ili višim, u skladu s članom 7. stavom 3.; (d) prema potrebi, nalaže istrage svake stvarne ugrožavanja ili gubitka ili ako postoji sumnja u ugrožavanje ili gubitak tajnih podataka koji su u posjedu ili potiču od Savjeta te zahtijeva pomoć od nadležnih bezbjednosnih tijela u takvim istragama; (e) preduzima periodične inspekcije bezbjednosnih mjera za zaštitu tajnih podataka u prostorijama GSC-a; (f) preduzima periodične posjete radi procjene bezbjednosnih mjera za zaštitu tajnih podataka EU-a u tijelima, agencijama i subjektima Unije koji primjenjuju ovu Odluku ili njezina načela; (g) zajedno i u dogovoru s predmetnim NSA-om preduzima periodične procjene bezbjednosnih mjera za zaštitu tajnih podataka EU-a u službama i prostorijama država članica; (h) osigurava da se bezbjednosne mjere koordiniraju prema potrebi s nadležnim tijelima država članica koja su odgovorna za zaštitu tajnih podataka i, prema potrebi, trećim državama ili međunarodnim organizacijama, također i u pogledu prirode prijetnji bezbjednosti tajnih podataka EU-u i sredstava za zaštitu od njih; i (i) sklapa administrativne dogovore iz člana 13. stava 2. tačke (b). Kancelarija za bezbjednost GSC-a na raspolaganju je glavnom sekretaru i pruža mu pomoć u pogledu navedenih odgovornosti. 3. Za potrebe sprovođeja člana 15. stava 3. države članice trebale bi: (a) odrediti NSA, kako je navedeno u Dodatku C, odgovoran za				

bezbjednosne mjere za zaštitu tajnih podataka EU-a, kako bi: i. tajni podaci u posjedu bilo kojeg nacionalnog odjela, tijela ili agencije, bilo javne ili privatne, kod kuće ili u inostranstvu, bili zaštićeni u skladu s ovom Odlukom; ii. se bezbjednosne mjere za zaštitu tajnih podataka EU-a povremeno pregledale ili procijenile; iii. svi pojedinci zaposleni u nacionalnoj administraciji ili pri ugovaratelju kojem se može odobriti pristup podacima tajnim kao CONFIDENTIEL UE/EU CONFIDENTIAL ili više prošli odgovarajuću bezbjednosnu provjeru ili bili na neki drugi način propisno ovlašćeni na osnovu svojih funkcija u skladu s nacionalnim zakonima i propisima; iv. se prema potrebi uspostavili bezbjednosni programi radi smanjivanja opasnosti od ugrožavanja ili gubitka tajnih podataka EU-a; v. pitanja bezbjednosti koja se odnose na zaštitu tajnih podataka EU-a bila usklađena s drugim nadležnim nacionalnim tijelima, uključujući tijela iz ove Odluke; vi. se odgovorilo na odgovarajuće zahtjeve za bezbjednosnu provjeru, a posebno na one koje su podnijele bilo koja tijela, agencije, subjekti i operacije Unije, uspostavljeni na osnovu glave V. poglavlja 2. UEU-a, te posebni predstavnici EU-a (PPEU-i) i njihovi timovi koji primjenjuju ovu Odluku ili njezina načela; (b) osigurati da njihovog nadležna tijela dostave podatke i savjete svojim vladama, a putem njih i Savjetu, o prirodi prijetnji bezbjednosti tajnih podataka EU-a i sredstvima zaštite od njih.				
Čl. 17-19	Nema odgovarajuće odredbe	Neprenosivo		
PRILOG I. **BEZBJEDNOST LICA** I. UVOD II. ODOBRAVANJE PRISTUPA TAJNIM PODACIMA EU-a 2. Pojedincu se odobrava pristup tajnim podacima samo nakon što: (a) je za njega utvrđena nužnost pristupa podacima; (b) je upoznat sa bezbjednosnim propisima i postupcima za zaštitu tajnih podataka EU- i nakon što je potvrdio svoje odgovornosti povezane sa zaštitom takvih podataka; i (c) u slučaju podataka sa stupnjem tajnosti CONFIDENTIEL UE/EU CONFIDENTIAL ili višim: — nakon što mu je odobren PSC za relevantni stepen tajnosti ili nakon što je na neki drugi način propisno ovlašten na	Nema odgovarajuće odredbe		Materija je regulisana čl. 25-54 Zakona o tajnosti podataka ("Sl. list Crne Gore", br. 14/08, 76/09, 41/10, 38/12, 44/12, 14/13 i 18/14)	

temelju svojih funkcija u skladu s nacionalnim zakonima i propisima, ili — u slučaju dužnosnika GSC-a, drugih službenika ili upućenih nacionalnih stručnjaka, njima tijelo za imenovanja GSC-a mora dati ovlaštenje za pristup tajnim podacima EU-a do određenog stepena tajnosti i do određenog datuma, u skladu sa stavcima od 16. do 25. u sljedećem tekstu. 3. Svaka država članica i GSC utvrđuju položaje u svojim strukturama za koje je potreban pristup podacima sa stupnjem tajnosti CONFIDENTIEL UE/EU CONFIDENTIAL ili višim i stoga zahtijevaju uvjerenje o bezbjednosnoj provjeri za odgovarajući stepen tajnosti. III. ZAHTJEVI POVEZANI S UVJERENJEM O BEZBJEDNOSNOJ PROVJERI OSOBA IV. OBRAZOVANJE I PODIZANJE SVIJESTI O BEZBJEDNOST V. POSEBNE OKOLNOSTI VI. UČEŠĆE NA SASTANCIMA SAVJETA VII. MOGUĆI PRISTUP TAJNIM PODACIMA EU-a				
PRILOG II. **FIZIČKA BEZBJEDNOST** I. UVOD 1. U ovom se Prilogu određuju odredbe za provedbu članka 8. U njemu se utvrđuju minimalni zahtjevi za fizičku zaštitu prostorija, zgrada, kancelarija, soba i drugih područja u kojima se postupa s tajnim podacima EU-a ili se čuvaju, uključujući područja u kojima je smješten CIS. 2. Mjere fizičke bezbjednosti namijenjene su sprečavanju neovlaštenog pristupa tajnim podacima EU-a tako da se: (a) osigura pravilno postupanje s tajnim podacima EU-a i njihovo čuvanje; (b) omogući razdvajanje osoblja u smislu pristupa tajnim podacima EU-a na temelju nužnosti pristupa podacima za obavljanje poslova iz djelokruga te, prema potrebi, s obzirom na njihovu bezbjednosnu provjeru; (c) odvraćaju, sprečavaju otkrivaju neovlaštene radnje; i (d) onemogući ili odgodi tajni ili nasilni ulazak neovlaštenih osoba.	**Član 1** Državni organi, organi državne uprave, organi jedinica lokalne samouprave i druga pravna lica kojima je povjereno vršenje javnih ovlašćenja (u daljem tekstu: organi), kao i pravna i fizička lica kad u vršenju zakonom utvrđenih poslova, odnosno izvršavanju ugovorenog posla saznaju za tajne podatke (u daljem tekstu: organizacije) dužni su da administrativne i fizičke mjere zaštite tajnih podataka, sprovode pod uslovima i na način propisan ovom Uredbom.	Potpuno usklađeno	Materija je regulisana i čl. 64 i 68 Zakona o tajnosti podataka ("Sl. list CG", br. 14/08, 76/09, 41/10, 38/12, 44/12, 14/13 i 18/14),	
PRILOG II. **FIZIČKA BEZBJEDNOST** II. ZAHTJEVI I MJERE POVEZANE S FIZIČKOM BEZBJEDNOŠĆU 3. Mjere fizičke bezbjednosti biraju se na osnovu procjene prijetnje	**Član 4** Bezbjednosnu procjenu ugroženosti sačinjava organ nadležan za poslove nacionalne bezbjednosti (u daljem tekstu: Agencija), u skladu	Potpuno usklađeno		

koju sprovode nadležna tijela. GSC i države članice primjenjuju proces upravljanja rizicima za zaštitu tajnih podataka EU-a u svojim prostorijama kako bi osigurali nivo fizičke zaštite srazmjernu procijenjenim rizicima. U procesu upravljanja rizicima u obzir se uzimaju svi važni činioci, a posebno: (a) stepen tajnosti tajnih podataka EU-a; (b) oblik i obim tajnih podataka EU-a, imajući na umu da velike količine ili zbirka tajnih podataka EU- a mogu zahtijevati primjenu strožih mjera zaštite; (c) okruženje i struktura zgrada ili područja u kojima su smješteni tajni podaci EU-a; i (d) procijenjena prijetnja od obavještajnih službi, čiji su cilj Unija ili države članice te od sabotaže, terorista, subverzivnih ili drugih kriminalnih aktivnosti.	sa zakonom, a naročito u odnosu na: potencijalne prijetnje tajnim podacima sa osvrtom na poziciju, lokaciju i čuvanje objekata i bezbjednosnih zona, aktivnosti stranih obavještajnih službi, sabotera, terorista i kriminalnih grupa, kao i rizike koji mogu biti uzrokovani aktivnošću zaposlenih. Zahtjev za bezbjednosnu procjenu ugroženosti organi, odnosno organizacije dostavljaju Agenciji, preko Direkcije za zaštitu tajnih podataka. Bezbjednosnu procjenu ugroženosti za Ministarstvo odbrane i Vojsku Crne Gore sačinjava organizaciona jedinica Ministarstva odbrane nadležna za vojno obavještajne i bezbjednosne poslove, u saradnji sa Agencijom. **Član 5** Na osnovu bezbjednosne procjene ugroženosti, starješina organa, odnosno zakonski zastupnik organizacije procjenjuje stepen rizika prijetnje tajnim podacima (visoki, srednji ili niski), a naročito u odnosu na: stepen tajnosti podatka i broj tajnih podataka; broj lica koja rukuju tajnim podacima. Zavisno od stepena rizika iz stava 1 ovog člana, starješina organa, odnosno zakonski zastupnik organizacije preduzima neophodne mjere zaštite tajnih podataka, u skladu sa ovom Uredbom.			
4. Primjenjujući koncept dubinske odbrane, nadležno bezbjednosno tijelo određuje odgovarajuću kombinaciju mjera fizičke zaštite koje će se provesti. One mogu obuhvatati jednu ili više sljedećih mjera: (a) rubna prepreka: fizička prepreka kojom se brani granica nekog područja za koje je potrebna zaštita; (b) sistemi za otkrivanje neovlaštenog ulaska (IDS): IDS se može upotrebljavatiza poboljšanje razine zaštite koju osigurava rubna prepreka ili u sobama i zgradama umjesto fizičkog obezbjeđenja ili kao pomoć njemu; (c) kontrola pristupa: kontrola pristupa može se provoditi na lokaciji, u zgradi ili zgradama na lokaciji ili u područjima ili sobama unutar zgrade. Kontrolu može provoditi fizičko obezbjeđenje i/ili recepcionar pomoću elektroničkih ili	**Član 15** Prostori, odnosno prostorije u kojima se čuvaju, koriste, obrađuju ili uništavaju tajni podaci stepena tajnosti “POVJERLJIVO” ili većeg stepena tajnosti, kao i prilaz njima, obezbjeđuju se mehaničkim uređajima i tehničkim bezbjednosnim uređajima i sistemima. **Član 16** Mehaničke uređaje iz člana 15 ove Uredbe čine: • oprema za sigurno čuvanje predmeta i dokumenata (sefovi, kase i dr.); • brave za opremu za sigurno čuvanje predmeta i dokumenata; • vrata i njihove komponente;	Potpuno usklađeno		

elektromehaničkih sredstava ili bilo kojih drugih fizičkih sredstava; (d) fizičko obezbjeđenje: može se zaposliti fizičko obezbjeđenje koje je obučeno pod nadzorom i koje je, prema potrebi, prošlo odgovarajuću bezbjednosnu provjeru, kako bi se, *inter alia*, odvratili pojedinci koji planiraju tajni neovlašteni ulazak; (e) televizija zatvorenog kruga (CCTV): fizičko obezbjeđenje može upotrebljavatiCCV za provjeru incidenata i dojava IDS-a na velikim lokacijama ili unutar perimetara; (f) bezbjednosna rasvjeta: bezbjednosna se rasvjeta može upotrebljavati za odvraćanje mogućih neovlaštenih osoba te za osvjetljavanje potrebno za efikasan nadzor koji direktno provodi fizičko obezbjeđenje ili koji se posredno provodi putem CCTV sistema; i (g) sve druge odgovarajuće mjere fizičke zaštite namijenjene odvraćanju od ili otkrivanju neovlaštenog pristupa ili sprečavanju gubitka ili oštećivanja tajnih podatak EU-a. 5. Nadležno tijelo može biti ovlašteno za provođenje pretrage prilikom ulaska i izlaska s ciljem odvraćanja od neovlaštenog unosa materijala ili neovlaštenog odnošenja tajnih podataka EU-a iz prostorija ili zgrada. 6. Ako postoji opasnost od uvida u tajne podatke EU-a, čak i slučajno, poduzimaju se odgovarajuće mjere za suzbijanje opasnosti. 7. Za nove se objekte zahtjevi u pogledu fizičke bezbjednosti i njihove funkcionalne specifikacije definišuu okviru planiranja i projektiranja objekata. U postojećim se objektima zahtjevi u pogledu fizičke bezbjednosti provode u najvećoj mogućoj mjeri. **III. OPREMA ZA FIZIČKU ZAŠTITU TAJNIH PODATAKA EU-a** 8. Pri nabavi opreme (kao što su sigurnosni spremnici, uništavači papira, brave za vrata, elektronički sistemi za kontrolu pristupa, IDS, sistemi uzbunjivanja) za fizičku zaštitu tajnih podataka EU-a, nadležno bezbjednosno tijelo osigurava da oprema ispunjava odobrene tehničke norme i minimalne zahtjeve. 9. Tehničke specifikacije opreme koja služi za fizičku zaštitu tajnih podataka EU-a navedene su u bezbjednosnim smjernicama koje odobrava Sigurnosni odbor. 10. Sigurnosni se sistemi pregledavaju u pravilnim vremenskim razmacima, a oprema se redovito održava. Radovi održavanja u skladu su s ishodom insekcija kako bi se osigurao daljnji	• sistemi za zaključavanje vrata; • protivprovalne rešetke ili barijere; • bezbjednosne folije; • prozori. **Član 17** Tehničke bezbjednosn*e* uređaje i sisteme iz člana 15 ove Uredbe, čine: • sistemi za kontrolu ulaska i izlaska u prostorije sa elektronskom verifikacijom identiteta lica i njihovom autorizacijom (u daljem tekstu: kontrola pristupa); • bezbjednosni sistemi za izvještavanje o povredama bezbjednosti (u daljem tekstu: alarmni sistemi); • video nadzor (CCTV); • uređaji za detekciju predmeta; • uređaji za uništavanje tajnih podataka. **PRILOG 1** **BODOVANJE MJERA FIZIČKE ZAŠTITE** 1. OPREMA I BRAVE ZA SIGURNO ČUVANJE PREDMETA I DOKUMENATA –S1 1.1. Oprema za sigurno čuvanje predmeta i dokumenata (sefovi, kase i dr.) – SS1 1.1.1. Oprema za sigurno čuvanje predmeta i dokumenata - tip 4 SS1 = 4 boda a) oprema namijenjena za deponovanje tajnih podataka svih stepena tajnosti pod uslovom da se nalaze u bezbjednosnoj zoni I ili II, koja ispunjava uslove bezbjednosti prema standardu MEST EN 1143-1 klase II ili više b) oprema iz podtačke a) ove tačke mora biti opremljena najmanje sa bravom standarda MEST EN 1300 klase C 1.1.2. Oprema za sigurno čuvanje predmeta i dokumenata - tip 3 SS1 = 3 boda a) oprema namijenjena za deponovanje tajnih podataka svih stepena tajnosti pod uslovom da se			

optimalni rad opreme. 11. Efikasnost pojedinačnih bezbjednosnim mjera i cjelokupnog bezbjednosnog sistema ponovno se ocjenjuje tokom svake inspekcije.	nalaze u bezbjednosnoj zoni I ili II, koja ispunjava uslove bezbjednosti prema standardu MEST EN 1143-1 klase I ili više b) oprema iz podtačke a) ove tačke mora biti opremljena najmanje sa bravom standarda MEST EN 1300 klase B 1.1.3. Oprema za sigurno čuvanje predmeta i dokumenata - tip 2 SS1 = 2 boda a) oprema namijenjena za deponovanje tajnih podataka stepena tajnosti do i uključujući „TAJNO“ pod uslovom da se nalaze u bezbjednosnoj zoni I ili II, koja ispunjava uslove bezbjednosti prema standardu MEST EN 1143-1 klase 0 ili više b) oprema iz podtačke a) ove tačke mora biti opremljena najmanje sa bravom standarda MEST EN 1300 klase B 1.1.4. Oprema za sigurno čuvanje predmeta i dokumenata - tip 1 SS1 = 1 bod a) oprema namijenjena za deponovanje tajnih podataka stepena tajnosti do i uključujući „POVJERLJIVO“ pod uslovom da se nalaze u bezbjednosnoj zoni I ili II b) oprema iz podtačke a) ove tačke mora biti opremljena najmanje mehaničkom bravom sa ključem 1.2. Brave za opremu za sigurno čuvanje predmeta i dokumenata – SS2 1.2.1. Brave za opremu za sigurno čuvanje predmeta i dokumenata - tip 4 SS2 = 4 boda Brave za opremu za sigurno čuvanje predmeta i dokumenata ispunjavaju uslov bezbjednosti prema standardu MEST EN 1300 klase C 1.2.2. Brave za opremu za sigurno čuvanje predmeta i dokumenata - tip 3 SS2 = 3 boda Brave za opremu za sigurno čuvanje predmeta i dokumenata ispunjavaju uslov bezbjednosti prema			

	standardu MEST EN 1300 klase B 1.2.3. Brave za opremu za sigurno čuvanje predmeta i dokumenata - tip 2 SS2 = 2 boda Brave za opremu za sigurno čuvanje predmeta i dokumenata ispunjavaju uslov bezbjednosti prema standardu MEST EN 1300 klase A 1.2.4. Brave za opremu za sigurno čuvanje predmeta i dokumenata - tip 1 SS2 = 1 bod Brave za opremu za sigurno čuvanje predmeta i dokumenata moraju biti mehaničke brave sa ključem 2. MJERE ZA ZAŠTITU BEZBJEDNOSNIH ZONA – S2 2.1. Bezbjednosna zona – SS3 2.1.1. Bezbjednosna zona - Tip 4 SS3 = 4 boda a) zaštićeno područje pruža visok nivo otpornosti protiv provalnika koji koristi silu i koji je opremljen sa efikasnim prenosivim instrumenatima; granica zaštićenog područja pokazuje visok stepen otpornosti protiv prikrivenih upada b) zidovi, podovi i plafoni u zaštićenom području, moraju biti od čvrstog materijala, tj. cigli minimalne debljine 300 mm ili od armiranog betona minimalne debljine 150 mm c) vrata, kapije i sve njihove komponente ili rešetke ispunjavaju uslove najmanje prema standardu MEST EN 1627 klase 4 d) prozori i njihove komponente ispunjavanju uslove prema standardu MEST EN 1627 klase 4 e) ako je donja granica prozora ili ivica izlaza viša od 5,5 m iznad tla i ne može joj se pristupiti sa krova, gromobrana, drugih strukturnih elemenata, zemljanih nepravilnosti, drveća ili drugih konstrukcija, uslovi iz stava d) se ne primjenjuju f) sistem zaključavanja mehaničkih uređaja mora da odgovara tipu 4 pod tačkom 2.2.1			

	2.1.2. Bezbjednosna zona - tip 3 SS3 = 3 boda a) zaštićeno područje pruža visok nivo otpornosti protiv provalnika koji je opremljen sa efikasnim prenosnim instrumentima, zaštićeno područje granica pokazuje visok nivo otpora protiv prikrivenog upada b) zidovi, podovi i plafoni u zaštićenom području, moraju biti od čvrstog materijala, tj. cigli minimalne debljine 150 mm ili od armiranog betona minimalne debljine 100 mm c) vrata, kapije i sve njihove komponente ili rešetke ispunjavaju uslove najmanje prema standardu MEST EN 1627 klase 3 d) prozori i svi njihovi delovi ili rešetke ispunjavaju uslove prema standardu MEST EN 1627 klase 3 e) ako je donja granica prozora ili ivica izlaza viša od 5,5 m iznad tla i ne može joj se lako pristupiti sa krova, gromobrana, drugih strukturnih elemenata, zemljanih nepravilnosti, drveća ili drugih konstrukcija, uslovi iz podtačke d) ove tačke se ne primjenjuju f) sistem zaključavanja mehaničkih uređaja mora da odgovara tipu 3 pod tačkom 2.2.2 2.1.3. Bezbjednosna zona - tip 2 SS3 = 2 boda a) zaštićeno područje pruža otpor protiv nasilnog ulaska za koje se koriste ručni instrumenti, zaštićeno područje pokazuje visok stepen otpora protiv prikrivenog upada b) zidovi, podovi i plafoni u zaštićenom području moraju biti od čvrstih materijala ili armiranog betona minimalne debljine 75 mm c) vrata, kapije i sve njihove komponente ili rešetke moraju ispunjavati uslove najmanje prema standardu MEST EN 1627 klase 2 d) prozori i svi njihovi djelovi ili rešetke ispunjavaju uslove najmanje prema standardu MEST EN 1627 klase 2 e) ako je donja granica prozora ili ivica izlaza			

	viša od 5,5 m iznad tla i ne može joj se lako pristupiti sa krova, gromobrana, drugih strukturnih elemenata, zemljanih nepravilnosti, drveća ili drugih konstrukcija, uslovi iz podtačke d) ove tačke se ne primjenjuju f) sistem zaključavanja mehaničkih uređaja mora da odgovara tipu 2 pod tačkom 2.2.3 2.1.4. Bezbjednosna zona - tip 1 SS3 = 1 bod a) zaštićeno područje mora biti zaključano tako da pruža otpor protiv fizičkog nasilja i protiv prikrivenog upada b) zidovi, podovi i plafoni u zaštićenom području moraju biti od čvrstih materijala ili armiranog betona minimalne debljine 75 mm c) vrata, kapije i sve njihove komponente ili rešetke moraju da obezbijede isti nivo otpora protiv nasilnika kao i preostali djelovi bezbjednosne zone d) mehanički uređaji, koji mogu da se otvore, sa ugrađenim sistemom za zaključavanje maksimum tipa 3 pod tačkom 2.2.2 e) tajni podaci stepena tajnosti „STROGO TAJNO“ ne mogu da se deponuju u ovo zaštićeno područje 2.2. Sistemi za zaključavanje vrata – SS4 2.2.1. Sistem za zaključavanje vrata – tip 4 SS4 = 4 boda a) sistem zaključavanja obezbjeđuje visok stepen otpornosti protiv profesionalnih i stručnih upada korišćenjem posebno razvijenih instrumenata i tehnologija koje nijesu komercijalno dostupne b) sistem zaključavanja i njegove komponente ispunjavaju uslove minimuma otpornosti prema standardu MEST EN 1303 klasa 4 2.2.2. Sistem za zaključavanje vrata – tip 3 SS4 = 3 boda			

	a) sistem zaključavanja obezbeđuje visok stepen otpornosti protiv profesionalnih i stručnih upada korišćenjem posebno razvijenih instrumenata i tehnologija koje su komercijalno dostupne za profesionalne bravare b) sistem zaključavanja i njegove komponente ispunjavaju uslove minimuma otpornosti prema standardu MEST EN 1303 klasa 3 2.2.3. Sistem za zaključavanje vrata - tip 2 SS4 = 2 boda a) sistem zaključavanja pruža otpor protiv prekršioca koji posjeduje ograničen izbor instrumenta b) sistem zaključavanja i njegove komponente ispunjavaju uslove minimuma otpornosti prema standardu MEST EN 1303 klasa 2 2.2.4. Sistem za zaključavanje vrata - tip 1 SS4 = 1 bod a) sistem zaključavanja pruža otpor protiv slučajnog upada b) specifikacija sistema zaključavanja i njegovih komponenti biće naznačena u bezbjednosnoj dokumentaciji fizičkog obezbjeđenja i bezbjednosti zgrade 3. MJERE ZA ZAŠTITU OBJEKATA – S3 Dio granice objekta koji ima najmanji otpor će biti od suštinskog značaja za određivanje otpornosti objekta Mehanički uređaji koji se koriste za zaštitu objekta obuhvataju sisteme zaključavanja, vrata, rešetke, zaštitne folije, prozore i zastakljivanje Ako kontrola ulaska u objekat nije obezbijeđena, S3 = 0 bodova 3.1. Objekat – SS5 3.1.1. Objekat - tip 4 SS5 = 5 bodova a) obezbjeđuje visok stepen otpornosti protiv nasilnog ulaska u objekte koji imaju			

	posebno jaku konstrukciju od armiranog betona minimalne debljine 300 mm ili drugog građevinskog materijala uporedivih karakteristika b) mehanički uređaji pružaju isti nivo otpora protiv nasilnog ulaska, kao i drugi djelovi objekta 3.1.2. Objekat - tip 3 SS5 = 3 boda a) obezbjeđuje viši nivo otpora protiv nasilnog ulaska, koji ima jaku konstrukciju od armiranog betona minimalne debljine 100 mm ili čvrstih cigli minimalne debljine 150 mm ili od drugih građevinskih materijala uporedivih karakteristika b) mehanički uređaji pružaju isti nivo otpora protiv nasilnog ulaska, kao i drugi djelovi objekta 3.1.3. Objekat - tip 2 SS5 = 2 boda a) pruža osnovni nivo otpora protiv nasilnog ulaska, koji ima jaku konstrukciju od armiranog betona minimalne debljine 75 mm ili od drugih građevinskih materijala uporedivih karakteristika b) mehanički uređaji pružaju isti nivo otpora protiv nasilnog ulaska, kao drugi djelovi objekta 3.1.4. Objekat - tip 1 SS5 = 1 bod a) obezbjeđuje minimalni nivo otpora protiv nasilnog ulaska, koji ima laku konstrukciju b) mehanički uređaji pružaju isti nivo otpora protiv nasilnog ulaska, kao i drugi djelovi objekta 4. KONTROLA PRISTUPA, PERIODIČNE KONTROLE I REŽIM POSJETA – S4 4.1. Kontrola pristupa – SS6 4.1.1. Kontrola pristupa – tip 4 SS6 = 4 boda a) kontrola pristupa odgovara sistemu za kontrolu ulaska i izlaska u prostorije sa elektronskom verifikacijom identiteta lica i njihovom autorizacijom koja zahtijeva minimum nadzora b) sistem kontrole pristupa u kombinaciji sa			

	jedinistvenim indentifikacionim brojem (PIN) ili biometrijskim indentifikacionim sitemom koji je u skladu sa zahtjevima kontrole pristupa klase B i prepoznavanju klase 3, u skladu sa standardom MEST EN 50133-1 c) signal u slučaju neovlašćenog pristupa do tačke gdje se nalazi fizičko obezbjeđenje, starješina organa, odnosno zakonski zastupnik organizacije ili lice određeno od njih d) kontrola ulaska dopunjena pristupnim barijerama za prevenciju neovlašćenog ulaska koje trebaju da onemoguće ponavljanje pokušaja neovlašćenog pristupa i da omoguće režim "jedan prolaz – jedno lice" 4.1.2. Kontrola pristupa – tip 3 SS6 = 3 boda a) električni sistem kontrole pristupa u kombinaciji sa jedinstvenim indetifikacionim brojem (PIN) ili biometrijskim indentifikacionim sistemom u skladu sa zahtjevima kontrole pristupa klase B I prepoznavanje klase 3, u skladu sa standardom MEST EN 50133-1 b) kontrola pristupa dopunjena odgovarajućim pristupnim barijerama uključujući nadzor 4.1.3. Kontrola pristupa – tip 2 SS6 = 2 boda a) kontrola pristupa na osnovu indentifikacione dozvole za ulazak sa fotografijom, kontrolisana od strane fizičkog obezbjeđenja ili električni sistem kontrole pristupa u skladu sa zahtjevima kontrole pristupa klase B i prepoznavanja klase 2, u skladu sa standardom MEST EN 50133-1 b) kontrola pristupa koja se obezbjeđuje zaključavanjem i otključavanjem vrata od strane ovlašćenog lica koje koristi sistem kamera ili video interfona 4.1.4. Kontrola pristupa – tip 1 SS6 = 1 bod			

	a) kontrola pristupa koja se obezbjeđuje zaključavanjem vrata koristeći određeni ključ, šifru ili drugi sistem izdat određenim licima b) kontrola pristupa se može primijeniti samo na ulaske u zaštićena područja gdje se obrađuju tajni podaci stepena "POVJERLJIVO" i niže 4.2. Periodične kontrole ulaska i izlaska – SS7 4.2.1. – Periodične kontrole ulaska i izlaska ako se obavljaju SS7 = 1 bod Odnose se na periodične kontrole ulaska i izlaska koje su određene kao preventivne mjere protiv neovlašćenog pristupa tajnim podacima 4.2.2. – Periodične kontrole ulaska i izlaska ako se ne obavljaju SS7 = 0 bodova 4.3. Režim posjeta – SS8 4.3.1. – Posjete u pratnji tokom boravka u objektu i bezbjednosnim zonama SS8 = 2 boda a) posjetioci imaju pratnju tokom boravka u objektu i bezbjednosnim zonama b) posjetioci moraju biti vidno označeni tokom cijelog boravka u zgradi c) vodi se evidencija o posjetama u koju se unose podaci o imenu, prezimenu, funkciji, broju indentifikacione kartice, lične karte, službene legitimacije ili putne isprave i vremenu posjete 4.3.2. – Posjete u pratnji tokom boravka u bezbjednosnim zonama SS8 = 1 bod a) posjetioci imaju pratnju tokom boravka u bezbjednosnim zonama b) posjetioci moraju biti vidno označen tokom cijelog boravka u zgradi c) vodi se evidencija o posjetama u koju se unose podaci o imenu, prezimenu, funkciji, broju indentifikacione kartice, lične karte, službene legitimacije ili putne isprave i vremenu posjete			

	5. FIZIČKO OBEZBJEĐENJE I ELEKTRIČNI BEZBJEDNOSNI SISTEMI – S5 5.1. Fizičko obezbjeđenje – SS9 5.1.1. Fizičko obezbjeđenje – tip 5 SS9 = 5 bodova a) fizičko obezbjeđenje se vrši od strane lica iz člana 18 ove Uredbe b) fizičko obezbjeđenje se vrši patrolno unutar zgrade, prvi obilazak se vrši odmah po završetku radnog vremena kad se vrši provjera da li su zatvoreni svi prozori i vrata i u isto vrijeme se vrši provjera lica koja se nalaze u bezbjednosnim zonama c) stalno prisustvo najmanje jednog zaposlenog lica fizičkog obezbjeđenja zaštite mora biti obezbijeđeno na mjestima gdje je potrebno stalno izvršavanje poslova fizičke zaštite 5.1.2. Fizičko obezbjeđenje – tip 4 SS9 = 4 boda a) fizičko obezbjeđenje se vrši od strane lica iz člana 18 ove Uredbe b) fizičko obezbjeđenje se vrši od strane patrola unutar zgrade c) stalno prisustvo najmanje jednog zaposlenog lica fizičkog obezbjeđenja mora biti obezbijeđeno na mjestima gdje je potrebno stalno izvršavanje poslova fizičke zaštite 5.1.3. Fizičko obezbjeđenje – tip 3 SS9 = 3 boda a) fizičko obezbjeđenje se vrši od strane lica iz člana 18 ove Uredbe b) fizičko obezbjeđenje se vrši od strane patrola van zgrade c) stalno prisustvo najmanje jednog zaposlenog lica fizičkog obezbjeđenja mora biti obezbijeđeno na mjestima gdje je potrebno stalno izvršavanje poslova fizičke zaštite 5.1.4. Fizičko obezbjeđenje – tip 2 SS9 = 2 boda			

	a) fizičko obezbjeđenje ne zahtijeva patrole i sprovodi se kroz metode unutrašnje zaštite, koristeći stalno prisutna lica b) u slučaju potrebe, fizičko obezbjeđenje će tražiti pomoć, npr. Uprave policije, Vojne policije, lica koja imaju dozvolu za vršenje poslova zaštite u skladu sa propisom kojim se uređuje zaštita lica i imovine ili zaposlenih koji su obučeni za takve poslove 5.1.5. Fizičko obezbjeđenje – tip 1 SS9 = 1 bod Fizičko obezbjeđenje se vrši kontrolom granica objekta, van radnog vremena 5.2. Električni bezbjednosni sistemi – SS10 5.2.1. Alarmni sistemi – SS10.1 Tehnički standardi alarmnih sistema su određeni u odnosu na najniži tip alarmnih sistema tehničkih uređaja koji se primjenjuju 5.2.1.1. Tehnički standardi alarmnih sistema – tip 4 SS10.1 = 4 boda Komponente alarmnih sistema moraju biti u skladu sa zahtjevima bezbjednosnog nivoa 4 u skladu sa standardom MEST EN 50131 5.2.1.2. Tehnički standardi alarmnih sistema – tip 3 SS10.1 = 3 boda Komponente alarmnih sistema moraju biti u skladu sa zahtjevima bezbjednosnog nivoa 3 u skladu sa standardom MEST EN 50131 5.2.1.3. Tehnički standardi alarmnih sistema – tip 2 SS10.1 = 2 boda Komponente alarmnih sistema moraju biti u skladu sa zahtjevima bezbjednosnog nivoa 2 u skladu sa standardom MEST EN 50131 5.2.1.4. Tehnički standardi alarmnih sistema – tip 2 SS10.1 = 1 bod Komponente alarmnih sistema moraju biti u skladu sa zahtjevima bezbjednosnog nivoa 1 u skladu sa standardom MEST EN 50131			

	5.2.2. Video nadzor (CCTV) – SS10.2 Sistem video nadzora koji se koristi za zaštitu objekta ili bezbjednosnih zona mora biti u skladu sa standardima MEST EN 50132 Video nadzor ulaska u bezbjednosne zone služi kao dodatna mjera i instaliran je na način da se omogući identifikacija lica U prostorijama unutar bezbjednosnih zona u kojima se obrađuju, nastaju i čuvaju tajni podaci ne instalira se video nadzor 5.2.2.1. CCTV - tip 4 SS10.2 = 4 boda a) CCTV instaliran na način da se vrši nadzor okoline i unutrašnjosti objekta b) izlazni signal video kamera mora biti povezan sa kontrolnom tačkom na kojoj se nalaze lica iz člana 18 ove Uredbe c) izlazni signal se snima i arhivira na period od najmanje 15 kalendarskih dana 5.2.2.2. CCTV – tip 3 SS10.2 = 3 boda a) CCTV instaliran na način da se vrši nadzor unutrašnjosti objekta b) izlazni signal se snima i arhivira na period od najmanje 15 kalendarskih dana 5.2.2.3. CCTV – tip 2 SS10.2 = 2 boda a) CCTV instaliran na način da se vrši nadzor bezbjednosnih zona b) izlazni signal se snima i arhivira na period od najmanje 15 kalendarskih dana 6. MJERE SPOLJAŠNJE ZAŠTITE – S6 Spoljašnja zaštita objekta se vrši kao kompleksan sistem mjera za zaštitu granica objekta, ulaza u objekat, izlaza i uređaja za zatvaranje 6.1. Barijere – SS11 6.1.1. Barijere – tip 5 SS11 = 5 bodova a) minimalan prelaz visine granice je 2500 mm			

	b) barijera sa sistemom za detekciju perimetra i instaliranim CCTV c) kontrolisani prostor od 20 m koji je ostavljen između barijera i granice objekta 6.1.2. Barijera – tip 4 SS11 = 4 boda a) minimalan prelaz visine granice je 2300 mm b) barijera sa instaliranim sistemom CCTV c) kontrolisani prostor od 10 m koji je ostavljen između barijera i granice objekta 6.1.3. Barjera – tip 3 SS11 = 3 boda a) minimalan prelaz visine granice je 2150 mm b) barijera sa instaliranim sistemom CCTV c) kontrolisani prostor je ostavljen između barijera i granice objekta 6.1.4. Barijera – tipe 2 SS11 = 2 boda a) minimalan prelaz visine granice je 1800 mm b) kontrolisani prostor je ostavljen između barijera i granice objekta 6.2. Kontrola pristupa na ulazima u barijere – SS12 6.2.1. Kontrola pristupa koja se vrši na svim ulazima SS12 = 1 bod Kontrola pristupa na ulazima u barijere u skladu sa potpoglavljem 4.1. Metod koji obezbjeđuje kontrolu pristupa će se naznačiti u bezbjednosnoj dokumentaciji i elaboratu obezbjeđenja objekta 6.2.2. Kontrola ulaska koja se ne vrši na svakom ulazu SS12 = 0 bodova 6.3. Sistem za perimetarsku zaštitu – SS13 Sistem za perimetarsku zaštitu primjenjuje se u cilju da se poveća spoljašnja bezbijednost objekta, instalira se skriven ili vidljiv, kao komponenta za preventivno dejstvo 6.3.1. Sistem za perimetarsku zaštitu implementiran SS13 = 1 bod Izlazni signal sistema mora biti povezan sa			

	kontrolnom tačkom na kojoj se nalaze lica iz člana 18 ove Uredbe, kod starješine organa, odnosno zakonskog zastupnika organizacije ili lica kojeg oni odrede 6.3.2. Sistem za perimetarsku zaštitu nije implementiran SS13 = 0 bodova 6.4. Bezbjednosno osvjetljenje – SS14 6.4.1. Bezbjednosno osvjetljenje instalirano SS14 = 1 bod Bezbjednosno osvjetljenje je instalirano kao dopuna spoljnoj zaštiti kao komponenta za preventivno dejstvo 6.4.2. Bezbjednosno osvjetljenje nije instalirano SS14 = 0 bodova 6.5. Spoljašnji CCTV – SS15 6.5.1. CCTV instaliran SS15 = 1 bod CCTV je instaliran u cilju indentifikacije lica prema standardu MEST EN 50132 6.5.2. CCTV nije instaliran SS15 = 0 bodova 7. UREĐAJI ZA DETEKCIJU PREDMETA Uređaji za detekciju predmeta nalaze se na ulaznim tačkama u objektu ili bezbjednosnim zonama i oni obezbjeđuju prepoznavanje predmeta koji nijesu dozvoljeni u zaštićenim područjima Uređaji za detekciju predmeta moraju biti pod direktnim nadzorom ovlašćenih lica 8. UREĐAJI ZA UNIŠTAVANJE TAJNIH PODATAKA Za fizičko uništavanje tajnih podataka, kao što su dokumenta, diskete, kompakt diskovi, magnetne trake, memorijske kartice, hard diskovi i dr. mogu se koristitit sljedeći uređaji: 8.1. Uređaji za fizičko uništavanje tajnih podataka - tip 4 bez evaluacije Uređaji za fizičko uništavanje tajnih podataka svih stepena tajnosti dimenzija ostatka 0.8 mm x 11 mm			

	8.2. Uređaj za fizičko uništenje tajnih podataka (medija) - tip 3 bez evaluacije Uređaji za fizičko uništavanje tajnih podataka stepena tajnosti “TAJNO” i niže dimenzija ostatka 1.9 mm x 15 mm 8.3. Uređaj za fizičko uništenje tajnih podataka (medija) - tip 2 bez evaluacije Uređaji za fizičko uništavanje tajnih podataka stepena tajnosti “POVJERLJIVO” i niže dimenzija ostatka 3.9 mm x 30-50 mm 8.4. Uređaj za fizičko uništenje tajnih podataka (medija) - tip 1 bez evaluacije Uređaji za fizičko uništavanje tajnih podataka stepena tajnosti “INTERNO” dimenzija ostatka 7.5 mm x 40-80 mm 8.5. Uređaji za demagnetizaciju - bez evaluacije Uređaji za trajno brisanje tajnih podatka pohranjenih na elektronskim medijima za stepen tajnosti “TAJNO” i niže stepene tajnosti			
PRILOG II. **FIZIČKA BEZBJEDNOST** IV. FIZIČKI ZAŠTIĆENA PODRUČJA 12. Za fizičku zaštitu tajnih podataka EU-a utvrđene su dvije vrste fizički zaštićenih područja ili njihovih nacionalnih ekvivalenata: (a) administrativne zone; i (b) bezbjednosne zone (uključujući tehnički zaštićene bezbjednosne zone). U ovoj se Odluci svako upućivanje na administrativne zone i bezbjednosne zone, uključujući tehnički zaštićene bezbjednosne zone, smatra i upućivanjem na njihove nacionalne ekvivalente. 13. Nadležno bezbjednosno tijelo određuje da određeno područje ispunjava zahtjeve te ga se stoga može odrediti kao administrativnu zonu, bezbjednosnu zonu ili tehnički zaštićenu bezbjednosnu zonu. 14. Za administrativne zone: (a) uspostavlja se vidljivo utvrđeni perimetar koji omogućava	**Član 8** Prostor ili prostorija u objektu koji je određen kao administrativna, odnosno bezbjednosna zona treba da ima bezbjednosnu opremu u skladu sa propisanim standardima. **Član 9** Administrativnu i bezbjednosne zone određuje starješina organa, odnosno zakonski zastupnik organizacije, na osnovu bezbjednosne procjene ugroženosti. **Član 10** U administrativnoj zoni obrađuju se, čuvaju i koriste tajni podaci stepena tajnosti „INTERNO". Za administrativnu zonu određuje se prostor ili prostorija koja se može nadzirati (ulaz, izlaz i kretanje lica i vozila). Na ulazu u administrativnu zonu mora biti	Potpuno usklađeno		

provjeru pojedinaca i, ako je moguće, vozila; (b) pristup bez pratnje odobrava se samo pojedincima koje je propisno ovlastilo nadležno tijelo; i (c) svi drugi pojedinci stalno imaju pratnju ili podliježu jednakim kontrolama. 15. Za bezbjednosne zone: (a) uspostavlja se vidljivo utvrđen i zaštićen perimetar kroz koji se nadziru svi ulasci i izlasci pomoću propusnice ili sistema prepoznavanja osoba; (b) pristup bez pratnje odobrava se samo pojedincima koji su prošli bezbjednosnu provjeru i koji su posebno ovlašćeni za ulazak u područje na osnovu nužnosti pristupa podacima; i (c) svi drugi pojedinci stalno imaju pratnju ili podliježu jednakim kontrolama. 16. Ako ulazak u bezbjednosnu zonu praktično predstavlja direktan pristup tajnim podacima sadržanima u toj zoni, primjenjuju se dodatni zahtjevi: (a) mora biti jasno naveden najviši stepen tajnosti podataka koji se uobičajeno čuvaju u zoni; (b) svi posjetioci moraju zatražiti posebno ovlašćenje i za ulazak u zonu, moraju stalno imati pratnju i moraju proći odgovarajuću bezbjednosnu provjeru, osim ako su preduzeti koraci kojima se onemogućava svaki pristup tajnim podacima EU-a. 17. Bezbjednosne zone zaštićene od prisluškivanja označene su kao tehnički zaštićene bezbjednosne zone. Primjenjuju se sljedeći dodatni zahtjevi: (a) takve zone opremljene su IDS-om, zaključane su kada u njima nema nikog i pod zaštitom kada je netko u njima. Svi se ključevi nadziru u skladu s odjeljkom VI.; (b) nadziru se svi materijali i osobe koji ulaze u takve zone; (c) u takvim se zonama redovno sprovode fizičke i/ili tehničke inspekcije na zahtjev nadležnog bezbjednosnog tijela. Takve se inspekcije također sprovode nakon svakog neovlaštenog ulaska ili sumnje u takav ulazak; i (d) u takvim zonama ne smije biti neovlašćenih komunikacijskih linija, neovlašćenih telefona ili drugih neovlašćenih komunikacijskih uređaja i električne ili elektroničke opreme. 18. Nezavisnood tačke(d) stava 17., prije upotrebe u zonama u kojima se održavaju sastanci ili obavlja posao koji obuhvata podatke	istaknuto obavještenje o nadzoru pristupa i kretanju u njoj. Tajni podaci iz stava 1 ovog člana, čuvaju se u kancelarijskim ili metalnin ormarima koji se zaključavaju. **Član 11** Bezbjednosne zone mogu biti I ili II stepena. Bezbjednosne zone moraju biti vidno označene natpisom "BEZBJEDNOSNA ZONA I", odnosno "BEZBJEDNOSNA ZONA II", uz dodatna obavještenja u vezi sa bezbjednosnim mjerama koje se sprovode u toj zoni. Bezbjednosne zone moraju biti zaštićene na način da se onemogući pogled unutar zone. Izuzetno, kad to zahtijevaju posebne okolnosti, starješina organa odnosno zakonski zastupnik organizacije, može odrediti da se bezbjednosne zone ne označavaju na način iz stava 2 ovog člana. **Član 12** Bezbjednosna zona I stepena je prostor ili prostorija u kojoj se obrađuju, čuvaju i koriste tajni podaci stepena tajnosti „STROGO TAJNO”, „TAJNO” i „POVJERLJIVO”, kao i tajni podaci stepena tajnosti „INTERNO“ ukoliko je to potrebno, i sam ulazak u ovu zonu predstavlja pristup tajnim podacima. U bezbjednosnoj zoni I stepena zabranjeno je unošenje mehaničkih, elektronskih i magnetno – optičkih sredstava i djelova sredstava, kojima bi se mogao neovlašćeno snimiti, odnijeti ili prenijeti tajni podatak. **Član 13** Bezbjednosna zona II stepena je prostor ili prostorija u kojoj se obrađuju i čuvaju tajni podaci stepena tajnosti „STROGO TAJNO”, „TAJNO” i „POVJERLJIVO”, kao i tajni podaci stepena tajnosti „INTERNO“ ukoliko je to potrebno, i ulazak i kretanje u toj zoni ne smatra se pristupom tajnim			

tajne kao SECRET UE/EU SECRET ili više i u kojima je prijetnja tajnim podacima EU- a ocijenjena kao visoka, sve komunikacijske uređaje i električnu ili elektronsku opremu najprije ispituje nadležno bezbjednosno tijelo s ciljem sprečavanja slučajnog ili nedopuštenog prenosa razumljivih podataka pomoću takve opreme izvan perimetra bezbjednosne zone. 19. Bezbjednosne zone u kojima nema osoblja na dužnosti 24 sata dnevno pregledaju se, prema potrebi, na kraju redovnog radnog vremena i u nasumičnim vremenskim razmacima izvan redovnog radnog vremena, osim ako je postavljen IDS. 20. Bezbjednosne zone i tehnički zaštićene bezbjednosne zone mogu se uspostaviti privremeno unutar administrativne zone za tajne sastanke ili u druge slične svrhe. 21. Za svaku se bezbjednosnu zonu sastavljaju bezbjednosno-operativni postupci kojima se određuju: (a) stepen tajnosti tajnih podataka EU-a s kojima se može postupati i koji se mogu čuvati u zoni; (b) mjere nadzora i zaštitne mjere koje je potrebno održavati; (c) pojedinci ovlašćeni za pristup zoni bez pratnje, na osnovu nužnosti pristupa podacima i bezbjednosne provjere; (d) prema potrebi, postupci za pratnju ili zaštitu tajnih podataka EU-a ako se ovlašćuju bilo koji drugi pojedinci za pristup zoni; i (e) sve druge odgovarajuće mjere i postupci. 22. Unutar sigurnosnih zona moraju biti izgrađeni trezori. Nadležno bezbjednosno tijelo odobrava zidove, podove, stropove, prozore i vrata koja se mogu zaključati, koji osiguravaju zaštitu jednaku bezbjednosnom kasi odobrenom za čuvanje tajnih podataka EU-a istog stepena tajnosti. V. FIZIČKE MJERE ZAŠTITE ZA POSTUPANJE S TAJNIM PODACIMA EU-a I NJIHOVO ČUVANJE 23. S tajnim podacima EU-a sa stepenom tajnosti RESTREINT UE/EU RESTRICTED može se postupati: (a) u bezbjednosnoj zoni; (b) u administrativnoj zoni uz uslov da su tajni podaci EU-a zaštićeni od pristupa neovlašćenih pojedinaca; ili (c) izvan bezbjednosne ili administrativne zone uz uslov da korisnik prenosi tajne podatke EU-a u skladu sa stavovima od 28. do 41. Priloga III. i da se obvezao poštovati kompenzacijske mjere utvrđene u bezbjednosnim uputstvima koje izdaje nadležno bezbjednosno tijelo s ciljem zaštite tajnih podataka EU-a od pristupa neovlašćenih	podacima. U bezbjednosnoj zoni II stepena zabranjeno je unošenje mehaničkih, elektronskih i magnetno – optičkih sredstava i djelova sredstava, kojima bi se mogao neovlašćeno snimiti, odnijeti ili prenijeti tajni podatak, bez pisanog odobrenja ovlašćenog lica. **Član 15** Prostori, odnosno prostorije u kojima se čuvaju, koriste, obrađuju ili uništavaju tajni podaci stepena tajnosti "POVJERLJIVO" ili većeg stepena tajnosti, kao i prilaz njima, obezbjeđuju se mehaničkim uređajima i tehničkim bezbjednosnim uređajima i sistemima. **Član 16** Mehaničke uređaje iz člana 15 ove Uredbe čine: - oprema za sigurno čuvanje predmeta i dokumenata (sefovi, kase i dr.); - brave za opremu za sigurno čuvanje predmeta i dokumenata; - vrata i njihove komponente; - sistemi za zaključavanje vrata; - protivprovalne rešetke ili barijere; - bezbjednosne folije; - prozori. **Član 17** Tehničke bezbjednosne uređaje i sisteme iz člana 15 ove Uredbe, čine: – sistemi za kontrolu ulaska i izlaska u prostorije sa elektronskom verifikacijom identiteta lica i njihovom autorizacijom (u daljem tekstu: kontrola pristupa); – bezbjednosni sistemi za izvještavanje o povredama bezbjednosti (u daljem tekstu: alarmni sistemi); – video nadzor (CCTV); – uređaji za detekciju predmeta; – uređaji za uništavanje tajnih podataka.			

osoba. 24. Tajni podaci EU-a sa stepenom tajnosti RESTREINT UE/EU RESTRICTED čuvaju se u primjerenom zaključanom kancelarijskom namještaju u administrativnoj ili bezbjednosnoj zoni. Privremeno se mogu čuvati izvan bezbjednosne ili administrativne zone uz uslov da se korisnik obvezao poštovati kompenzacijske mjere utvrđene u bezbjednosnim uputstvima koje izdaje nadležno bezbjednosno tijelo. 25. S tajnim podacima EU-a sa stepenom tajnosti CONFIDENTIEL UE/EU CONFIDENTIAL ili SECRET UE/EU SECRET može se postupati: (a) u bezbjednosnoj zoni; (b) u administrativnoj zoni uz uslov da su tajni podaci EU-a zaštićeni od pristupa neovlašćenih pojedinaca; ili (c) izvan bezbjednosne ili administrativne zone uz uslov da korisnik: i. prenosi tajne podatke EU-a u skladu sa stavovima od 28. do 41. Priloga III.; ii. obavezao se poštovati kompenzacijske mjere utvrđene u bezbjednosnim uputstvima koje izdaje nadležno bezbjednosno tijelo s ciljem zaštite tajnih podataka EU-a od pristupa neovlašćenih osoba; iii. stalno drži tajne podatke EU-a pod ličnom kontrolom; i iv. ako su dokumenti u papirnom obliku, obavijestio je o tome nadležni registar. 26. Tajni podaci EU-a sa stepenom tajnosti CONFIDENTIEL UE/EU CONFIDENTIAL ili SECRET UE/EU SECRET čuvaju se u bezbjednosnoj zoni ili u bezbjednosnoj kasi ili u trezoru. 27. S tajnim podacima EU-a sa stepenom tajnosti TRÈS SECRET UE/EU TOP SECRET postupa se u bezbjednosnoj zoni. 28. Tajni podaci EU-a sa stepenom tajnosti TRÈS SECRET UE/EU TOP SECRET čuvaju se u bezbjednosnoj zoni uz jedan od sljedećih uslova: (a) u bezbjednosnom kasi u skladu sa stavom 8. uz najmanje jednu od sljedećih dodatnih kontrola: i. stalnu zaštitu ili provjeru koju sprovodi fizičko obezbjeđenje ili osoblje na dužnosti koje je prošlo bezbjednosnu provjeru; ii. odobren IDS u kombinaciji sa fizičkim obezbjeđenjem za odziv; (b) u trezoru opremljenom IDS-om u kombinaciji sa fizičkim obezbjeđenjem za odziv. 29. Pravila kojima se uređuje prenos tajnih podataka EU-a izvan fizički zaštićenih područja određena su u Prilogu III. VI. KONTROLA KLJUČEVA I KOMBINACIJA ZA ZAŠTITU TAJNIH PODATAKA EU-a	**Član 18** Fizička zaštita objekta, prostora, odnosno prostorija u kojima se čuvaju, koriste i obrađuju tajni podaci stepena tajnosti "POVJERLJIVO" ili većeg stepena tajnosti vrše policijski službenici, službenici Agencije, pripadnici Vojske Crne Gore i fizička lica koja imaju dozvolu za vršenje poslova zaštite u skladu sa propisom kojim se uređuje zaštita lica i imovine (u daljem tekstu: fizičko obezbjeđenje). Lica iz stava 1 ovog člana moraju imati dozvolu za pristup tajnim podacima najmanje stepena tajnosti podataka čiju zaštitu vrše. Detaljne procedure postupanja fizičkog obezbjeđenja donose se na osnovu Plana zaštite tajnih podataka. **Član 19** Tehnički bezbjednosni uređaji i sistemi iz člana 15 ove Uredbe moraju biti u funkciji bez prekida. U slučaju aktiviranja tehničkih bezbjednosnih uređaja i sistema kojima se signalizira povreda bezbjednosti objekta, prostora odnosno prostorija u kojima se čuvaju, koriste i obrađuju tajni podaci, na mjestu gde je došlo do povrede, dužna su da reaguju najmanje dva lica fizičkog obezbjeđenja, na način da se zaštita ostalih djelova objekta, prostora odnosno prostorija ne smije oslabiti. Starješina organa, odnosno zakonski zastupnik organizacije će odrediti vrijeme reakcije lica iz stava 1 ovog člana, tako da bude kraće od vremena potrebnog za prevazilaženje preduzetih mjera za zaštitu tajnih podataka i utvrditi intervale za provjeru vremena potrebnog za reakciju fizičkog obezbjeđenja. Provjera iz stava 3 ovog člana sprovodi se najmanje jednom godišnje. **Član 20** Kontrola ulaska lica i vozila vrši se na			

30. Nadležno bezbjednosno tijelo određuje postupke za upravljanje ključevima i postavama kombinacija za kancelarije, sobe, trezore i bezbjednosne kase. Takvi postupci predstavljaju zaštitu od neovlaštenog pristupa. 31. Postavke kombinacija pamti najmanji mogući broj pojedinaca koji ih moraju znati. Postavke kombinacija za bezbjednosne kase i trezore u kojima se čuvaju tajni podaci EU-a mijenjaju se: (a) prilikom prijema nove kase; (b) pri svakoj promjeni osoblja koje zna kombinaciju; (c) pri svakoj pojavi ugrožavanja ili sumnje u ugrožavanje; (d) u slučaju popravka ili održavanja brave i (e) najmanje svakih 12 mjeseci.	svakom ulazu u objekat i bezbjednosne zone. Kontrola ulaska vrši se upotrebom mehaničkih uređaja i tehničkim bezbjednosnim uređajima i sistemima u kombinaciji sa fizičkim obezbjeđenjem iz člana 15 ove Uredbe. Za ulazak u bezbjednosne zone zaposleni koriste identifikacionu karticu sa mogućnošću elektronske verifikacije identiteta lica i njihove autorizacije. Gubitak identifikacione kartice odmah se prijavljuje licu koga odredi starješina organa, odnosno zakonski zastupnik organizacije. Za ulazak drugog lica u bezbjednosnu zonu izdaje se posebna bezbjednosna propusnica u pisanoj formi. Lice iz stava 4 ovog člana, može ući u bezbjednosnu zonu samo u pratnji zaposlenog koji ga obavještava da se njegovo kretanje nadzire i evidentira i pri ulasku i kretanju u bezbjednosnoj zoni, mora imati na vidnom mjestu zakačenu bezbjednosnu propusnicu. Identifikacione kartice i bezbjednosne propusnice izdaje lice određeno od strane starješine organa, odnosno zakonskog zastupnika organizacije. O izdatim identifikacionim karticama i bezbjednosnim propusnicama vodi se evidencija. Lica zadužena za održavanje čistoće, kao i lica zadužena za održavanje I popravke tehničkih uređaja mogu ući u bezbjednosnu zonu samo u pratnji zaposlenog koga odredi starješina organa, odnosno zakonski zastupnik organizacije, a koji je dužan da ih nadzire. **Član 21** Ključevi i pojedinačne kombinacije za otvaranje brava od opreme iz člana 15 stav 1 ove Uredbe i ulaza u bezbjednosne zone se predaju zaposlenima uz potpis, o čemu se vodi posebna evidencija. Rezervni ključevi i zapisi pojedinačnih			

	kombinacija za otvaranje brava iz stava 1 ovog člana, deponuju se na način da samo fizičko obezbjeđenje ima pristup. Izrada kopije ključeva dozvoljava se samo na osnovu pisane saglasnosti starješine organa, odnosno zakonskog zastupnika organizacije ili zaposlenog koga on odredi. Izmjena pojedinačnih kombinacija za otvaranje bravavrši se prilikom instalacije mehaničkih ili tehničkih uređaja, poslije svake promjene zaposlenih koji su bili upoznati sa postojećim kombinacijama, u slučaju povrede ili postojanja sumnje da će se desiti povreda bezbjednosti tajnih podataka, a najmanje jednom u šest mjeseci. **Član 23** U svim prostorima, odnosno prostorijama bezbjednosne zone I i II stepena mora biti obavljen pregled protiv prisluškivanja i to: – prilikom određivanja bezbjednosne zone; – kod svakog nasilnog upada ili neovlašćenog pristupa u zonu; – kod promjene zaposlenih u bezbjednosnoj zoni I; – nakon izvođenja bilo koje vrste građevinskih ili telekomunikacionih radova; – jednom godišnje. Zaštita od prisluškivanja drugih prostora, odnosno prostorija ili informacionih i telekomunikacionih veza putem kojih se prenose tajni podaci vrši se u skladu sa bezbjednosnom procjenom ugroženosti. Pregled iz stava 1 ovog člana vrši Agencija. Zahtjev za vršenje pregleda iz stava 1 ovog člana organi, odnosno organizacije dostavljaju Agenciji, preko Direkcije za zaštitu tajnih podataka. **Član 24** Tajni podaci, osim podataka stepena tajnosti „STROGO TAJNO”, mogu se obrađivati van			

	bezbjednosnih zona, ako je prostor ili područje u kojem se obrađuju fizički ili tehnički obezbijeđen, a pristup do njega pod nadzorom. Lice koje obrađuje tajni podatak van bezbjednosnih zona mora imati tajni podatak cijelo vrijeme pod nadzorom. Po okončanoj obradi, tajni podatak se vraća u bezbjednosnu zonu. Kad se tajni podatak stepena tajnosti „TAJNO" i „POVJERLJIVO" mora obrađivati van prostora, odnosno prostorija određenog organa radi izvođenja tačno određenog naloga, starješina organa utvrđuje mjere za zaštitu tajnog podatka koje moraju biti u skladu sa mjerama propisanim za odgovarajuću bezbjednosnu zonu. Svako iznošenje ili unošenje tajnog podatka stepena tajnosti „TAJNO" i „POVJERLJIVO" van bezbjednosne zone se evidentira. Lice koje preuzima tajni podatak, potvrđuje to svojeručnim potpisom i preuzima odgovornost za zaštitu tajnog podatka. **Član 26** Tajni podatak označen stepenom tajnosti „STROGO TAJNO", „TAJNO" i „POVJERLJIVO" unutar bezbjednosne zone, dostavlja se na korišćenje u zatvorenoj, neprovidnoj koverti na kojoj su naznačeni podaci o primaocu tog tajnog podatka. **Prilog I** **BODOVANJE MJERA FIZIČKE ZAŠTITE** **4. KONTROLA PRISTUPA, PERIODIČNE KONTROLE I REŽIM POSJETA – S4** **5. FIZIČKO OBEZBJEĐENJE I ELEKTRIČNI BEZBJEDNOSNI SISTEMI – S5**			
PRILOG III. **UPRAVLJANJE TAJNIM PODACIMA** I. UVOD 1. U ovom se Prilogu određuju odredbe za provedbu članka 9. U njemu se utvrđuju upravne mjere za kontrolu tajnih podataka EU-a tokomnjihova životnog ciklusa, radi lakšeg odvraćanja i otkrivanja namjerne ili slučajne ugroze ili gubitka takvih podataka.	Nema odgovarajuće odredbe		Materija je regulisana čl. 10, 14, 15, 16, 17, 18, 19b i 21 Zakona o tajnosti podataka ("Sl. list CG", br. 14/08, 76/09, 41/10, 38/12, 44/12, 14/13 i 18/14).	

II. UPRAVLJANJE OZNAKAMA TAJNOSTI **Stepeni tajnosti i oznake** 2. Podaci se označavaju ako je potrebna zaštita u pogledu njihove tajnosti. 3. Onaj od kojeg potiču tajni podaci EU-a odgovoran je za utvrđivanje stepena tajnosti u skladu s odgovarajućim smjernicama za označavanje te za početno širenje podataka. 4. Stepen tajnosti tajnih podataka EU-a određuje se u skladu s članom 2. stavom 2. i pozivom na bezbjednosnu politiku koja se odobrava u skladu s članom 3. stavom 3. 5. Stepen tajnosti mora biti jasno i pravilno naveden, bez obzira na to jesu li tajni podaci EU-a u papirnatom, usmenom, elektroničkom ili nekom drugom obliku. 6. Pojedinačni dijelovi određenog dokumenta (npr. stranice, stavci, odjeljci, prilozi, dodaci i privici) mogu zahtijevati drugačiju oznaku te stoga moraju biti označeni na odgovarajući način, uključujući dijelove pohranjene u elektroničkom obliku. 7. Cjelokupni stepen tajnosti dokumenta ili spisa mora biti najmanje jednako visok kao njegova komponenta s najvišim stupnjem tajnosti. Ako se uređuju podaci iz različitih izvora, konačni se proizvod pregledava kako bi se utvrdio njegov cjelokupni stepen tajnosti jer mu se može odrediti viši stepen tajnosti od onog koji imaju njegovi sastavni dijelovi. 8. Ako je to moguće, dokumenti koji sadržavaju dijelove s različitim stupnjevima tajnosti strukturiraju se tako da se dijelovi s različitim stupnjevima tajnosti mogu lako utvrditi i prema potrebi odvojiti. 9. Stepen tajnosti pisma ili napomene koji obuhvaćaju privitke mora biti jednak najvišem stupnju tajnosti njihovih privitaka. Onaj od kojeg podaci potiču jasno navodi koji je stepen tajnosti pisma ili napomene kada se odvoji od privitaka koristeći odgovarajuće oznake, npr.: CONFIDENTIEL UE/EU CONFIDENTIAL Bez privitka(-taka) RESTREINT UE/EU RESTRICTED				
Oznake 10. Uz jednu od oznaka stepena tajnosti navedenih u članku 2. stavku 2. tajni podaci EU-a mogu nositi dodatne oznake kao što su: (a) oznaka kojom se određuje onaj od kojeg podaci potiču;			Materija je regulisana čl. 10, 14, 15, 16, 17, 18, 19b, 21, 58,63, 72, 74,77,77a Zakona o tajnosti podataka ("Sl.	

(b) sva upozorenja, šifre ili akronimi kojima se navodi područje djelovanja na koje se dokument odnosi, posebna distribucija prema nužnosti pristupa podacima ili ograničenja uporabe; (c) oznake o mogućnosti objavljivanja; ili (d) ako je primjenjivo, datum ili posebni događaj nakon kojeg se stepen tajnosti može smanjiti ili se može ukinuti tajnost. **Skraćene oznake stepena tajnosti** 11. Mogu se upotrebljavatistandardizirane skraćene oznake stepena tajnosti kojima se navodi stepen tajnosti pojedinačnih stavaka u tekstu. Skraćenice ne zamjenjuju potpunu oznaku stepena tajnosti. 12. U tajnim podacima EU-a mogu se koristiti sljedeće standardne skraćenice kojima se označava stepen tajnosti odjeljaka ili dijelova teksta kraćih od jedne stranice: **Stvaranje tajnih podataka EU-a** 13. Prilikom stvaranja tajnog podatka EU-a: (a) svaka stranica mora biti jasno označena stupnjem tajnosti; (b) svaka stranica mora biti označena; (c) dokument mora imati referentni broj i predmet koji sam za sebe nije tajni podatak, osim ako je označen kao takav; (d) dokument mora biti označen datumom; i (e) dokumenti tajni kao SECRET UE/EU SECRET ili iznad moraju imati broj kopija na svakoj stranici ako se distribuiraju u nekoliko primjeraka. 14. Ako se stavak 13. ne može primijeniti na tajne podatke EU-a, poduzimaju se druge odgovarajuće mjere u skladu sa bezbjednosnim smjernicama koje se utvrđuju u skladu s članom 6. stavom 2. **Smanjivanje stepena tajnosti i ukidanje stepena tajnosti tajnih podataka EU-a** 15. U trenutku njihova stvaranja onaj od kojeg podaci navodi, ako je to moguće, a posebno za podatke tajne kao RESTREINT UE/EU RESTRICTED, može li se stepen tajnosti tajnih podataka EU-a smanjiti, odnosno mogu li se oni ukinuti na određeni datum ili nakon određenog događaja. 16. GSC redovito pregledava tajne podatke EU-a u svojem posjedu kako bi utvrdio primjenjuje li se još uvijek stepen tajnosti. GSC uspostavlja sustav za pregled stepena tajnosti tajnih podataka EU-a koji potiču od njega najmanje svakih pet godina. Takav pregled nije neophodan ako je onaj od kojeg podaci potiču na	Nema odgovarajuće odredbe		list CG", br. 14/08, 76/09, 41/10, 38/12, 44/12, 14/13 i 18/14) i Uredbom o načinu i postupku označavanja tajnosti podataka ("Sl. list CG", broj 67/08).	

početku naveo da će se stepen tajnosti podataka automatski smanjiti ili da će se podaci ukinuti te ako su podaci u skladu s tim označeni.				
III. UPIS TAJNIH PODATAKA EU-a U BEZBJEDNOSNE SVRHE 17. Za svaki se organizacioni subjekt u sklopu GSC-a i nacionalnih administracija država članica u kojem se postupa s tajnim podacima EU-a određuje odgovorni registar, kako bi se osiguralo postupanje s tajnim podacima EU-a u skladu s ovom Odlukom. Registri se uspostavljaju kao bezbjednosne zone kako je određeno u Prilogu II. 18. Za potrebe ove Odluke, upis u bezbjednosne svrhe („upis") znači primjenu postupaka za bilježenje životnog ciklusa materijala, uključujući njegovo širenje i uništavanje. 19. Svi materijali tajni kao CONFIDENTIEL UE/EU CONFIDENTIAL i više upisuju se u određene registre kada stignu u organizacionisubjekt ili iz njega odlaze. 20. Središnji registar u sklopu GSC-a čuva evidenciju o svim tajnim podacima koje su Savjet i GSC objavili trećim državama i međunarodnim organizacijama, te o svim tajnim podacima primljenim od trećih zemalja ili međunarodnih organizacija. 21. U slučaju CIS-a, postupak upisa provodi se kroz procese unutar samog CIS-a. 22. Savjet odobrava bezbjednosnu politiku o upisu tajnih podataka EU-a u bezbjednosne svrhe. **Registri za podatke tajne kao TRÈS SECRET UE/EU TOP SECRET** 23. U državama članicama i GSC-u određuje se registar koji djeluje kao središnje tijelo za primanje i slanje podataka tajnih kao TRÈS SECRET UE/EU TOP SECRET. Prema potrebi, mogu se odrediti podregistri za postupanje s takvim podacima u svrhu njihova upisa. 24. Takvi podregistri ne smiju direktno prenositi dokumente tajne kao TRÈS SECRET UE/EU TOP SECRET u druge podregistre istog središnjeg registra za podatke tajne kao TRÈS SECRET UE/EU TOP SECRET ili izvan njega bez izričitog pisanog odobrenja.	Nema odgovarajuće odredbe		Materija je regulisana čl. 74, stav 1 tačka 7, članom 77 i 77a Zakona o tajnosti podataka ("Sl. list CG", br. 14/08, 76/09, 41/10, 38/12, 44/12, 14/13 i 18/14) i Uredbom o evidenciji tajnih podataka ("Sl. list CG", br. 67/08, 49/10)	
Iz Unije na državno područje treće države 37. Tajni podaci koji se iz Unije prenose na državno područje treće države zapakovani su tako da su zaštićeni od neovlaštenog otkrivanja. 38. Podaci tajni kao CONFIDENTIEL UE/EU CONFIDENTIAL i SECRET	**Član 28** Primopredaja tajnog podatka vrši se u posebnoj prostoriji koju odredi starješina organa, odnosno zakonski zastupnik organizacije kome se tajni podatak dostavlja na korišćenje.	Potpuno usklađeno		

UE/EU SECRET prenose se iz Unije na državno područje treće države na jedan od sljedećih načina: (a) po vojnom ili diplomatskom kuriru; (b) ručno, uz sljedeće uslove: i. da je na paketu službeni pečat ili da je zapakovan na način kojim se naznačuje kako je riječ o službenoj pošiljci koja ne prolazi carinsku ili bezbjednosnu provjeru; ii. da pojedinci nose kurirsku potvrdu kojom se identifikuje paket i koja pojedince ovlašćuje za nošenje paketa; iii. da su tajni podaci EU-a stalno u posjedu kurira, osim ako su pohranjeni u skladu sa zahtjevima navedenim u Prilogu II.; iv. da se tajni podaci EU-a putem ne otvaraju i da se ne čitaju na javnim mjestima; i v. da su pojedinci upoznati sa svojim odgovornostima u pogledu bezbjednosti. 39. Prijenos podataka sa stupnjem tajnosti CONFIDENTIEL UE/EU CONFIDENTIAL i SECRET UE/EU SECRET koje je Unija objavila trećoj državi ili međunarodnoj organizaciji udovoljava odgovarajućim odredbama sporazuma o bezbjednosti podataka ili administrativnog dogovora u skladu s članom 13. stavom 2. tačkama (a) ili (b). 40. Podaci tajni kao RESTREINT UE/EU RESTRICTED mogu se također prenositi poštanskom službom ili komercijalnom kurirskom službom. 41. Podaci tajni kao TRÈS SECRET UE/EU TOP SECRET prenose se iz Unije na državno područje treće države po vojnom ili diplomatskom kuriru. **VI. UNIŠTAVANJE TAJNIH PODATAKA EU-a** 42. Tajni dokumenti EU-a koji više nisu potrebni mogu se uništiti ne dovodeći u pitanje mjerodavna pravila i propise o arhiviranju. 43. Dokumente koji podliježu upisu u skladu s članom 9. stavom 2. uništava odgovorni registar prema uputi korisnika ili nadležnog tijela. Očevidnici i drugi podaci o upisu ažuriraju se u skladu s tim. 44. Dokumenti tajni kao SECRET UE/EU SECRET ili TRÈS SECRET UE/EU TOP SECRET uništavaju se u prisutnosti svjedoka koji je prošao bezbjednosnu provjeru najmanje za stepen tajnosti dokumenta koji se uništava. 45. Službenik i svjedok, ako je potrebna prisutnost potonjeg,	Korisnik tajnog podatka potvrđuje prijem tog podatka potpisom na potvrdi, odnosno u dostavnoj knjizi. Obrazac potvrde iz stava 2 ovog člana sastavni je dio ove Uredbe (Prilog 2). **Član 25** Ovlašćeno lice koje je odredilo stepen tajnosti podatka, dostavlja tajni podatak korisniku koji ima dozvolu za pristup tajnim podacima najmanje onog stepena tajnosti podatka koji se dostavlja, po principu „potrebno je da zna“. Tajni podatak se dostavlja na korišćenje, u skladu sa stavom 1 ovog člana, preko lica kojem je izdata dozvola za pristup tajnim podacima odgovarajućeg stepena tajnosti (u daljem teksu: kurir). **Član 29** Tajni podatak označen stepenom tajnosti „STROGO TAJNO”, dostavlja se na korišćenje van bezbjednosne zone u koverti koja mora biti u zatvorenom koferu, kutiji ili torbi, sa zatvaranjem na ključ ili sa šifrovanom kombinacijom. Tajni podatak označen stepenom tajnosti „TAJNO” i „POVJERLJIVO” van bezbjednosne zone, dostavlja se, po pravilu, u dvije koverte. Spoljna koverta je od tvrdog, neprovidnog, nepropusnog materijala, na kojoj je označen organ kojem se dostavlja tajni podatak. Unutrašnja koverta iz st. 1 i 2 ovog člana, mora imati oznaku stepena tajnosti podatka, broj i datum akta i podatke o primaocu i pošiljaocu. **Član 30** Na zahtjev lica kome predaje ili od koga preuzima tajni podatak, kurir je dužan da pokaže kurirsko uvjerenje. Obrazac uvjerenja iz stava 1 ovog člana sastavni je dio ove Uredbe (Prilog 3.) **Član 33** Korisnik tajnog podatka stepena tajnosti „INTERNO“, „POVJERLJIVO” i „TAJNO” može			

potpisuju potvrdu o uništavanju koja se pohranjuje u registru. Registar čuva potvrde o uništavanju dokumenata tajnih kao TRÈS SECRET UE/EU TOP SECRET najmanje 10 godina, a dokumenata tajnih kao CONFIDENTIEL UE/EU CONFIDENTIAL i SECRET UE/EU SECRET najmanje pet godina. 46. Tajni dokumenti, uključujući dokumente tajne kao RESTREINT UE/EU RESTRICTED, uništavaju se na načine koji ispunjavaju odgovarajuće standarde EU-a ili jednake standarde ili koje su odobrile države članice u skladu s nacionalnim tehničkim normama radi sprečavanja rekonstrukcije u cijelosti ili djelimično. 47. Računarski nosači podataka koji su se koristili za tajne podatke EU-a uništavaju se u skladu sa stavom 37. Priloga IV. 48. U hitnim slučajevima, ako postoji neposredna opasnost od neovlaštenog otkrivanja, korisnik uništava tajne podatke EU-a tako da se ne mogu djelimično ili u cijelosti rekonstruirati. O vanrednom uništenju upisanih tajnih podataka EU-a obavještava se onaj od kojeg potiču ti podaci i izvorni registar.	umnožiti ili prevesti dokument ili sačiniti izvod iz dokumenta, ako na omotu nije naznačena zabrana umnožavanja. Korisnik tajnog podatka stepena tajnosti „STROGO TAJNO„ može umnožiti ili prevesti dokument ili sačiniti izvod iz dokumenta, samo uz pisanu saglasnost ovlašćenog lica koje je odredilo stepen tajnosti podatka. Broj umnoženih primjeraka, prevoda ili izvoda iz dokumenta koji sadrži tajni podatak iz st. 1 i 2 ovog člana, određuje se po principu „potrebno je da zna". Odobrena elektronska oprema (kompjuteri, kopir/fax mašine i dr.) za obradu tajnih podataka štiti se fizičkim mjerama zaštite, na način da je mogu koristiti samo lica koja posjeduju dozvolu za pristup tajnim podacima odgovarajućeg stepena tajnosti. Mjere zaštite određene za originalni dokument primjenjuju se i na umnožene primjerke, prevode ili izvode tog dokumenta. **Član 34** Kopije dokumenata**,** radni nacrti i bilješke koji sadrže tajne podatke, kao i dokumenti koji sadrže tajne podatke koji su fizički oštećeni i ne mogu se dalje koristiti, uništavaju se na način da se ne mogu raspoznati i obnoviti (spaljivanjem, drobljenjem i dr.). Tajni podaci stranih država i međunarodnih organizacija, uključujući i originalni primjerak, uništavaju se na način da se ne mogu raspoznati i obnoviti (spaljivanjem, drobljenjem i dr.), u skladu sa međunarodnim ugovorima. Originalni primjerak tajnog podatka arhivira se i čuva u skladu sa zakonom kojim se uređuje tajnost podataka. **Član 35** Starješina organa, odnosno zakonski zastupnik organizacije obrazuje komisiju za uništavanje tajnih podataka.			

	Komisiju iz stava 1 ovog člana, čine najmanje tri lica kojima je izdata dozvola za pristup tajnim podacima najmanje onog stepena tajnosti podataka koji se uništavaju. O uništavanju podataka iz stava 1 ovog člana, vodi se zapisnik, koji potpisuju svi članovi komisije. Zapisnik iz stava 3 ovog člana, sadrži podatke o broju i datumu akta kojim je određeno uništavanje tajnog podatka, broju, datumu i stepenu tajnog podatka koji se uništava i načinu njihovog uništavanja. Zapisnik iz stava 3 ovog člana, za tajne podatke stepena tajnosti „STROGO TAJNO" čuva se deset godina, za podatke stepena tajnosti „TAJNO" pet godina, za podatke stepena tajnosti „POVJERLJIVO" tri godine, a za podatke stepena tajnosti „INTERNO" godinu dana od dana uništavanja. O uništavanju tajnih podataka stepena tajnosti „STROGO TAJNO", „TAJNO" i „POVJERLJIVO", pisanim putem se obavještava ovlašćeno lice koje je odredilo stepen tajnosti podatka.			
VII. POSJETE RADI PROCJENE STANJA 49. Pojam „posjeta radi procjene stanja" rabi se dalje u tekstu te podrazumijeva: (a) inspekcije ili posjete radi procjene stanja u skladu s članom 9. stavom 3. i članom 16. stavom 2. tačkama (e), (f) i (g); ili (b) posjet radi procjene stanja u skladu s članom 13. stavom 5., s ciljem ocjenjivanja učinkovitosti provedenih mjera za zaštitu tajnih podataka EU-a. 50. Posjete radi procjene stanja se sprovode kako bi se, *inter alia*: (a) osiguralo poštovanje potrebnih minimalnih standarda za zaštitu tajnih podataka EU-a utvrđenih ovom Odlukom; (b) naglasila važnost bezbjednosti i efikasnog upravljanja rizicima unutar subjekata u kojima se provodi inspekcija; (c) preporučile protumjere za ublažavanje specifičnog učinka gubitka tajnosti, cjelovitosti ili dostupnosti tajnih podataka; i (d) ojačali tekući obrazovni programi i programi za podizanje	Nema odgovarajuće odredbe		Materija je regulisana čl. 71,80,81 i 82 Zakona o tajnosti podataka ("Sl. list CG", br. 14/08, 76/09, 41/10, 38/12, 44/12, 14/13 i 18/14) i Uredbom o načinu vršenja i sadržaju unutrašnje kontrole nad sprovođenjem mjera zaštite tajnih podataka ("Sl. list CG", br. 48/09)	

svijesti o bezbjednosti koje provode bezbjednosna tijela. 51. Prije završetka svake kalendarske godine Savjet za sljedeću godinu donosi program posjeta radi procjene stanja predviđen članom 16. stavom 1. točkom (c). Stvarni datumi svakog posjeta radi procjene stanja određuju se u dogovoru s predmetnim tijelom ili agencijom Unije, državom članicom, trećom državom ili međunarodnom organizacijom.				
Posjeti radi procjene stanja 52. Posjeti radi procjene stanja provode se s ciljem provjere mjerodavnih pravila, propisa i postupaka u subjektu koji se posjećuje te kako bi se provjerilo jesu li prakse subjekta u skladu s osnovnim načelima i minimalnim standardima utvrđenima ovom Odlukom i odredbama kojima se uređuje razmjena tajnih podataka s tim subjektom. 53. Posjeti radi procjene stanja provode se u dvije faze. Prije samog posjeta organizira se, prema potrebi, pripremni sastanak s predmetnim subjektom. Nakon pripremnog sastanka tim za procjenu, u dogovoru s predmetnim subjektom, utvrđuje podrobni program posjeta radi procjene stanja kojim su obuhvaćena sva područja bezbjednosti. Tim za procjenu stanja trebao bi imati pristup svim lokacijama na kojima se postupa s tajnim podacima EU-a, a posebno registrima i tačkama pristupa CIS-u. 54. Posjeti radi procjene stanja nacionalnim administracijama, trećim državama i međunarodnim organizacijama provode se u potpunoj saradnji s zaposlenima subjekta, treće države ili međunarodne organizacije koja se posjećuje. 55. Posjete radi procjene stanja tijelima, agencijama i subjektima Unije koji primjenjuju ovu Odluku ili njezina načela sprovode se uz pomoć stručnjaka NSA-a na čijem se državnom području nalazi tijelo ili agencija. 56. Za posjete radi procjene stanja tijelima, agencijama i subjektima Unije koji primjenjuju ovu Odluku ili njezina načela te trećim državama i međunarodnim organizacijama može se tražiti pomoć i doprinos stručnjaka NSA-a u skladu s detaljnim rješenjima koje treba dogovoriti Bezbjednosni odbor.	Nema odgovarajuće odredbe		Materija je regulisana čl. 71,80,81 i 82 Zakona o tajnosti podataka ("Sl. list CG", br. 14/08, 76/09, 41/10, 38/12, 44/12, 14/13 i 18/14) i Uredbom o načinu vršenja i sadržaju unutrašnje kontrole nad sprovođenjem mjera zaštite tajnih podataka ("Sl. list CG", br. 48/09)	
Izvještaji 57. Na kraju posjeta radi procjene stanja posjećenom subjektu predstavljaju se glavni zaključci i preporuke. Nakon toga sastavlja se izvještaj o posjeti radi procjene stanja. Ako su			Materija je regulisana čl. 71,80,81 i 82 Zakona o tajnosti podataka ("Sl. list CG", br. 14/08,	

predložene korektivne mjere i preporuke, doneseni se zaključci moraju dovoljno podrobno potkrijepiti u izvješću. Izvještaj se prosljeđuje odgovarajućem tijelu posjećenog subjekta. 58. Za posjete radi procjene stanja provedene u nacionalnim administracijama država članica: (a) nacrt izvještaja o procjeni prosljeđuje se predmetnom NSA-u koji provjerava tačnost činjenica te sadrži li izvještaj podatke sa stupnjem tajnosti višim od RESTREINT UE/EU RESTRICTED; i (b) osim ako predmetni NSA države članice zabrani opću distribuciju, izvještaja o procjeni prosljeđuju se Bezbjednosnom odboru. Izvještaj je označen kao RESTREINT UE/EU RESTRICTED. Bezbjednosno tijelo GSC-a (Kancelarija za bezbjednost) odgovorno je za pripremu redovitog izvještaja u kojem se ističu lekcije naučene iz posjeta radi procjene stanja provedenih u državama članicama u određenom razdoblju i pregledanih od strane Bezbjednosnog odbora. 59. Izvještaj o posjetima trećim državama i međunarodnim organizacijama radi procjene stanja dostavlja se Bezbjednosnom odboru. Izvještaj je označen najmanje kao RESTREINT UE/EU RESTRICTED. Sve korektivne radnje provjeravaju se tokomsljedećeg posjeta te se o njima izvještava Sigurnosni odbor. 60. Za posjete radi procjene stanja bilo kojim tijelima, agencijama, i subjektima Unije koji primjenjuju ovu Odluku ili njezina načela, izvještaja o posjetima radi procjene stanja dostavljaju se Bezbjednosnom odboru. Nacrt izvještaja o posjetu radi procjene stanja prosljeđuje se predmetnoj agenciji ili tijelu koje provjerava tačnost činjenica te sadrži li izvještaj podatke sa stupnjem tajnosti višim od RESTREINT UE/EU RESTRICTED. Sve korektivne radnje provjeravaju se tokomsljedećeg posjeta te se o njima izvještava Bezbjednosni odbor. 61. Bezbjednosno tijelo GSC-a provodi redovne inspekcije organizacijskih subjekata GSC-a u svrhe utvrđene u stavku 50. Kontrolna lista 62. Bezbjednosno tijelo GSC-a (Kancelarija za bezbjednost) sastavlja i ažurira kontrolnu listu stavki koje se provjeravaju tokomposjeta radi procjene stanja. Ta se kontrolna lista prosljeđuje Bezbjednosnom odboru.	Nema odgovarajuće odredbe		76/09, 41/10, 38/12, 44/12, 14/13 i 18/14) i Uredbom o načinu vršenja i sadržaju unutrašnje kontrole nad sprovođenjem mjera zaštite tajnih podataka ("Sl. list CG", br. 48/09) i Zakon o inspekcijskom nadzoru("Sl. list CG", br. 39/03,76/09,57/11,18/14 i 11/15)	

63. Podaci za popunjavanje kontrolne liste dobijaju se posebno tokom posjeta od rukovodstva za bezbjednost subjekta koji se pregleda. Nakon što je popunjena odgovarajućim odgovorima, kontrolna se lista označava stepenom tajnosti u dogovoru s pregledanim subjektom. Ona ne čini dio izvještaja o inspekciji.				
PRILOG IV. **ZAŠTITA TAJNIH PODATAKA EU-a S KOJIMA SE POSTUPA U CIS-u**	Nema odgovarajuće odredbe		Materija je regulisana Zakonom o tajnosti podataka, čl. 66, 68 stav 2, ("Sl. list Crne Gore", br. 14/08, 76/09, 41/10, 38/12, 44/12, 14/13 i 18/14), i Uredbom o bližim uslovima i načinu sprovođenja informatičkih mjera zaštite tajnih podataka ("Sl. list CG", br. 57/10)	
PRILOG V. **INDUSTRIJSKA ZAŠTITA**	Nema odgovarajuće odredbe		Materija je regulisana čl. 8 stav 1 tačka 4 i čl. 28, 30, 30a, 31, 62, 67 Zakona o tajnosti podataka ("Sl. list Crne Gore", br. 14/08, 76/09, 41/10, 38/12, 44/12, 14/13 i 18/14) i čl. 1, 2, 4, 6 i 8 Uredbe o bližim uslovima i načinu sprovođenja industrijskih mjera zaštite tajnih podataka ("Sl. list CG", broj 08/11).	
PRILOG VI. **RAZMJENA TAJNIH PODATAKA S TREĆIM DRŽAVAMA I MEĐUNARODNIM ORGANIZACIJAMA**	Nema odgovarajuće odredbe		Materija je regulisana čl. 6, 8 stav 1 tačka 3, čl. 76, 76a stav 1 tačka 1, čl. 77, 77a i 78 Zakona o tajnosti podataka("Sl. list CG", br. 14/08, 76/09, 41/10, 38/12,	

			44/12, 14/13 i 18/14), i Sporazumom između Crne Gore i Evropske unije o bezbjedonosnim procedurama za razmjenu i zaštitu tajnih podataka (Sl. list CG - Međunarodni ugovori, broj 13/2010	
Dodatak A **DEFINICIJE**	Nema odgovarajuće odredbe		Materija je regulisana čl. 8 Zakona o tajnosti podataka("Sl. list CG", br. 14/08, 76/09, 41/10, 38/12, 44/12, 14/13 i 18/14) i podzakonskim aktima za sprovođenje zakona	
Dodatak B **EKVIVALENTNOST STUPNJEVA TAJNOSTI** **Dodatak C** **POPIS NACIONALNIH SIGURNOSNIH TIJELA (NSA)** **Dodatak D** **Popis skraćenica**	Nema odgovarajuće odredbe	Neprenosivo		
EU UPRAVLJANJE PROCESIMA PROCJENE RIZIKA ZA FIZIČKU ZAŠTITU	PRILOG 1 BODOVANJE MJERA FIZIČKE ZAŠTITE	Potpuno usklađeno		