Crna Gora
Ministarstvo odbrane

PREDLOG OSNOVE

za vođenje pregovora i zaključivanje
Sporazuma o uzajamnoj razmjeni i zaštiti tajnih podataka između
Vlade Crne Gore i Vlade Republike Italije

Podgorica, 1. oktobar 2015. godine

PREDLOG OSNOVE

za vođenje pregovora i zaključivanje
Sporazuma o uzajamnoj razmjeni i zaštiti tajnih podataka između
Vlade Crne Gore i Vlade Republike Italije

I Ustavni osnov

Ustavni osnov za zaključivanje Sporazuma između Vlade Crne Gore i Vlade Republike Italije o uzajamnoj razmjeni i zaštiti tajnih podataka sadržan je u odredbama člana 15 stav 1 Ustava Crne Gore („Službeni list CG", broj 1/ 07), kojim je propisano da Crna Gora, na principima i pravilima međunarodnog prava, sarađuje i razvija prijateljske odnose sa drugim državama, regionalnim i međunarodnim organizacijama, kao i odredbama člana 100 tačke 1 i 4, kojima je propisano da Vlada vodi unutrašnju i vanjsku politiku i zaključuje međunarodne ugovore.

II Ocjena stanja odnosa između Crne Gore i Republike Italije

Odnosi između dvije zemlje su tradicionalno dobri i prijateljski. Kontinuirano se unapređuju kroz intenzivan politički dijalog i sadržajnu saradnju na svim poljima. U proteklom periodu realizovani su brojni zajednički projekti u oblastima ekonomije, odbrane, unutrašnjih poslova, prosvjete, nauke, kulture i razvoje saradnje.
Važna je i podrška koju Italija pruža Crnoj Gori u kontekstu ostvarenja njenog punopravnog članstva u EU i NATO.

III Razlozi za zaključivanje međunarodnog sporazuma

Ovaj Sporazum se zaključuje u cilju unapređenja saradnje u oblasti razmjene i zaštite tajnih podataka između dvije države. Zaključivanjem ovog sporazuma Crna Gora jača odnose sa državama članicama EU i NATO-a i intenzivira saradnju u primjeni standarda pomenutih međunarodnih organizacija.
Takođe, stvaraju se uslovi za zaključivanje drugih sporazuma o saradnji u oblasti bezbjednosti i odbrane i uslovi za zaključivanje povjerljivih ugovora. Najzad, stvaraju se uslovi za vršenje bezbjednosnih provjera crnogorskih državljana koji borave ili su boravili na teritoriji Republike Italije.

IV Osnovna pitanja o kojima će se voditi pregovori, odnosno bitni elementi koje ugovor treba da sadrži

Sporazumom se određuju nadležni bezbjednosni organi za primjenu ovog sporazuma, način zaštite tajnih podataka razmijenjenih ili nastalih između Strana ugovornica, rješavanje sporova koji mogu nastati u tumačenju ili primjeni, te način izmjene i otkaza Sporazuma.

Ugovorom se definiše pojam tajnog podatka, postupak označavanja stepena tajnosti, pristup tajnom podatku, korišćenje i ograničenje njegovog korišćenja, postupak prenosa, umnožavanja, prevoda i uništavanja tajnog podatka, kao i način priznavanja bezbjednosnih dozvola između Strana ugovornica.
Definisani su i pojam i uslovi za zaključivanje povjerljivih ugovora, zatim način postupanja organa odnosno Strana ugovornica u slučaju povrede bezbjednosti, te postupak realizacije posjeta predstavnika svake od Strana ugovornica koje uključuju pristup tajnim podacima. Sporazumom se predviđa da će svaka Strana snositi svoje troškove u vezi sa primjenom ovog sporazuma.

V Procjena potrebnih finansijskih sredstava za izvršavanje sporazuma i način njihovogobezbjeđenja

Za izvršavanje ovog sporazuma nije potrebno obezbijediti dodatna finansijska sredstva u Budžetu Crne Gore.

VII Potreba usaglašavanja propisa

Zaključivanje ovog sporazuma ne zahtijeva izmjenu važećih ili donošenje novih propisa.

VIII Predlog sastava delegacije

Tekst Sporazuma je usaglašen.

Prilog: Predlog Sporazuma

SPORAZUM

IZMEĐU

VLADE CRNE GORE

I

VLADE REPUBLIKE ITALIJE

O

UZAJAMNOJ RAZMJENI I ZAŠTITI

TAJNIH PODATAKA

Vlada Crne Gore

i

Vlada Republike Italije

u daljem tekstu "Strane",

u cilju obezbjeđivanja zaštite tajnih podataka u skladu sa svojim nacionalnim zakonima i propisima koji se razmjenjuju između Strana ili pravnih i fizičkih lica pod njihovom nadležnošću, uzimajući u obzir nacionalne interese i bezbjednost, u skladu sa zakonima i propisima strana kao i preuzetim međunarodnim obavezama,

prepoznajući interes i zajedničku potrebu da obezbijede zaštitu svih tajnih podataka, takođe u vezi sa mogućnošću sprovođenja sporazuma o tehničkoj saradnji, razmijenjenih između ‘’Strana’’ kao i pravnih i fizičkih lica, u skladu sa zakonima i propisima ‘’Strana’’ kao i preuzetim međunarodnim obavezama i, za Italiju, onima koje proizilaze iz članstva u Evropskoj uniji,

složile su se o sljedećem:

ČLAN 1

CILJ

U skladu sa svojim nacionalnim zakonima i propisima i uzimajući u obzir svoje nacionalne interese i bezbjednost kao i aktivnosti u oblasti industrije obje Strane će preduzimati sve odgovarajuće mjere u cilju zaštite tajnih podataka, koji se prenose ili su nastali u skladu sa ovim Sporazumom.

ČLAN 2

DEFINICIJE

U smislu ovog Sporazuma sljedeći izrazi znače:

a) **tajni podatak**: svaka informacija, nezavisno od njene forme, koja se prenosi ili je nastala između Strana, koja je označena stepenom tajnosti u skladu sa nacionalnim zakonima i propisima Strana;

b) **nadležni bezbjednosni organ**: nadležni organ ovlašćen u skladu sa nacionalnim zakonima i propisima Strana koji je odgovoran za primjenu ovog Sporazuma;

c) **strana pošiljalac:** strana**,** uključujući pravno ili fizičko lice u njenoj nadležnosti, koja ustupa tajne podatke strani primaocu;

d) **strana primalac:** strana, uključujući pravno ili fizičko lice u njenoj nadležnosti, koja prima tajne podatke od strane pošiljaoca;

e) **potrebno je da zna**: princip u skladu sa kojim pristup tajnim podacima može biti omogućen samo licima u okviru svojih službenih dužnosti ili zadataka;

f) **dozvola za pristup tajnim podacima fizičkom licu:** pozitivna odluka donijeta na osnovu bezbjednosne provjere u skladu sa nacionalnim zakonima i propisima, na osnovu koje je lice ovlašćeno da ima pristup i da rukuje tajnim podacima do i uključujući stepen tajnosti određen odlukom;

g) **dozvola za pristup tajnim podacima pravnom licu:** pozitivna odluka donijeta na osnovu bezbjednosne provjere kojom se potvrđuje da ugovarač koji je pravno lice ispunjava uslove za rukovanje tajnim podacima u skladu sa nacionalnim zakonima i propisima jedne od Strana;

h) **ugovarač:** pravno ili fizičko lice koje ima pravnu sposobnost za zaključivanje ugovora ili podugovora;

i) **povjerljivi ugovor:** ugovor zaključen sa ugovaračem koji sadrži ili podrazumijeva pristup tajnim podacima;

j) **treća strana**: država, uključujući i sva pravna i fizička lica u njenoj nadležnosti, ili međunarodna organizacija koja nije jedna od Strana ovog Sporazuma;

k) **posjeta**: kontakt sa pravnim i fizičkim licima, u cilju ovog Sporazuma, koji uključuje pristup tajnim podacima.

ČLAN 3

NADLEŽNI BEZBJEDNOSNI ORGANI

(1) Nadležni bezbjednosni organi koje su Strane odredile kao odgovorne za opštu primjenu i odgovarajuće kontrole svih aspekata ovog Sporazuma su:

U Crnoj Gori :
- Direkcija za zaštitu tajnih podataka Crne Gore - (National Security Authority)

U Republici Italiji:
– Presidenza del Consiglio dei Ministri – Autorità di sicurezza competente- Dipartimento delle Informazioni per la Sicurezza (DIS) - UCSe.

(2) Nadležni bezbjednosni organi će obavijestiti jedni druge o svim drugim nadležnim bezbjednosnim organima koji su odgovorni za primjenu ovog Sporazuma.

(3) Strane će obavijestiti jedna drugu diplomatskim kanalima o svim budućim promjenama koje se odnose na Nadležne bezbjednosne organe.

(4) U cilju postizanja i održavanja uporednih standarda bezbjednosti, Nadležni bezbjednosni organi će, na zahtjev, obezbijediti jedan drugom informacije o svojim nacionalnim bezbjednosnim standardima, procedurama i praksama u oblasti zaštite tajnih podataka. U ovom cilju Nadležni bezbjednosni organi mogu posjetiti jedni druge.

(5) Nadležni bezbjednosni organi će obezbijediti potpunu i obavezujuću primjenu ovog Sporazuma od strane svih pravnih i fizičkih lica Strana u skladu sa svojim nacionalnim zakonima i propisima.

ČLAN 4

STEPENI TAJNOSTI

(1) Tajni podaci ustupljeni u skladu sa ovim Sporazumom biće označeni odgovarajućim stepenom tajnosti u skladu sa nacionalnim zakonima i propisima Strana.

(2) Sljedeće oznake stepena tajnosti su ekvivalentne:

Crna Gora	Republika Italija	Engleski prevod
STROGO TAJNO	SEGRETISSIMO	TOP SECRET
TAJNO	SEGRETO	SECRET
POVJERLJIVO	RISERVATISSIMO	CONFIDENTIAL
INTERNO	RISERVATO	RESTRICTED

ČLAN 5

PRINCIPI ZAŠTITE TAJNIH PODATAKA

(1) Strane će pružiti tajnim podacima koji proizilaze iz ovog Sporazuma istu zaštitu kao i svojim tajnim podacima označenim istim stepenom tajnosti.

(2) Nadležni bezbjednosni organ strane pošiljaoca će:

a) obezbijediti da su tajni podaci označeni odgovarajućim stepenom tajnosti u skladu sa svojim zakonima i propisima, i
b) obavijestiti stranu primaoca o svim uslovima ustupanja ili ograničenjima u pogledu upotrebe tajnih podataka kao i o budućim promjenama stepena tajnosti.

(3) Nadležni bezbjednosni organ strane primaoca:

a) će obezbijediti da su tajni podaci označeni ekvivalentnim stepenom tajnosti u skladu sa stavom 2 člana 4, i
b) će obezbijediti da se oznaka stepena tajnosti ne mijenja osim ukoliko strana pošiljalac to ne odobri u pisanoj formi,
c) će koristiti tajne podatke isključivo u svrhu u koju su ustupljeni i u skladu sa ograničenjima određenim od strane pošiljaoca,
d) neće ustupiti tajne podatke trećoj strani bez prethodno pisane saglasnosti strane pošiljaoca.

ČLAN 6

PRISTUP TAJNIM PODACIMA I DOZVOLE ZA PRISTUP TAJNIM PODACIMA FIZIČKIM LICIMA

(1) Pristup tajnim podacima označenim stepenom tajnosti POVJERLJIVO/RISERVATISSIMO /CONFIDENTIAL i više biće dozvoljen isključivo licima koja imaju potrebu da znaju i koja imaju dozvolu za pristup tajnim podacima fizičkom licu i koja se redovno informišu.

(2) Pristup tajnim podacima označenim stepenom tajnosti INTERNO/RISERVATO/ RESTRICTED biće ograničen na lica koja imaju potrebu da znaju i koja se, u skladu sa tim informišu.

(3) Strane će uzajamno priznavati dozvole za pristup tajnim podacima fizičkim licima. U skladu sa tim primjenjivaće se stav 2 člana 4.

(4) Na zahtjev, Nadležni bezbjednosni organi će sarađivati i pružati pomoć jedni drugima tokom procedure bezbjednosne provjere za izdavanje dozvole za pristup tajnim podacima.

(5) Nadležni bezbjednosni organi će bez odlaganja obavijestiti jedan drugog o bilo kojoj promjeni koja se odnosi na međusobno priznate dozvole za pristup tajnim podacima fizičkim licima.

ČLAN 7

ZAŠTITA TAJNIH PODATAKA U KOMUNIKACIONIM I INFORMACIONIM SISTEMIMA

(1) Nadležni bezbjednosni organi će, u skladu sa odgovarajućim zakonima i propisima, obezbijediti primjenu odgovarajućih mjera za zaštitu tajnih podataka koji se obrađuju, čuvaju ili se prenose putem komunikacionih i informacionih sistema. Takve mjere će obezbijediti tajnost, integritet, dostupnost i, gdje je primjenljivo, načelo neodbijanja i vjerodostojnosti tajnih podataka kao i odgovarajući stepen odgovornosti i praćenja preduzetih mjera vezanih za tajne podatke.

(2) U tu svrhu, Nadležni bezbjednosni organi će obezbijediti da se na taj način razmijenjeni tajni podaci čuvaju, da se njima rukuje, da se prenose i štite u skladu sa njihovim odgovarajućim nacionalnim pravilima i propisima.

(3) Nadležni bezbjednosni organi će međusobno priznavati svaki zvanični dokument koji se odnosi na odobrenje, opremu i mehanizme koji su u vezi sa komunikacionim i informacionim sistemima, izdat od strane drugog Nadležnog bezbjednosnog organa.

(4) Kada je neophodno, ažurirani spisak odobrene opreme i mehanizama biće razmijenjen između Nadležnih bezbjednosnih organa.

ČLAN 8

PRENOS TAJNIH PODATAKA

(1) Tajni podaci će se prenositi između Strana putem diplomatskih kanala ili drugih zaštićenih kanala zajednički odobrenih od strane Nadležnih bezbjednosnih organa u skladu sa njihovim zakonima i propisima.

(2) Podaci označeni stepenom tajnosti “STROGO TAJNO/SEGRETISSIMO/TOP SECRET” prenosiće se isključivo putem diplomatskih ili vojnih kanala u skladu sa nacionalnim zakonima i propisima.

(3) Podaci označeni stepenom tajnosti “INTERNO/RISERVATO/RESTRICTED mogu se prenositi i poštom ili drugom službom dostavljanja u skladu sa nacionalnim zakonima i propisima.

(4) U slučaju prenosa velike pošiljke koja sadrži tajne podatke, procedure prevoza biće zajednički usaglašene i procijenjene, od slučaja do slučaja, od strane Nadležnih bezbjednosnih organa Strana.

ČLAN 9

UMNOŽAVANJE, PREVOD I UNIŠTAVANJE TAJNIH PODATAKA

(1) Sve kopije i prevodi biće označeni odgovarajućom oznakom stepena tajnosti i biće zaštićeni kao i original tajnog podatka. Prevodi i broj kopija biće ograničeni na minimum potreban za službenu upotrebu.

(2) Svi prevodi će biti označeni stepenom tajnosti kao i original i sadržaće odgovarajuću napomenu, na jeziku prevoda, koja ukazuje da sadrže tajne podatke strane pošiljaoca.

(3) Tajni podaci označeni stepenom tajnosti STROGO TAJNO/SEGRETISSIMO/TOP SECRET, i originali i prevodi, umnožavaće se uz prethodnu pisanu saglasnost strane pošiljaoca.

(4) Tajni podaci označeni stepenom tajnosti STROGO TAJNO/SEGRETISSIMO/TOP SECRET se ne uništavaju. Takvi podaci se vraćaju strani pošiljaocu ukoliko više nisu potrebni strani primaocu.

(5) Tajni podaci označeni stepenom tajnosti TAJNO/SEGRETO/SECRET i niže biće uništeni u skladu sa odgovarajućim nacionalnim zakonima i propisima ukoliko se više ne budu smatrali potrebnim od strane strane primaoca. Strana primalac će obavijestiti stranu pošiljaoca o takvom uništavanju.

(6) U kriznim situacijama u kojima je nemoguće zaštiti ili vratiti tajne podatke razmijenjene ili nastale u skladu sa ovim Sporazumom, tajni podaci će biti uništeni bez odlaganja. Strana primalac će obavijestiti Nadležni bezbjednosni organ strane pošiljaoca o tom uništenju bez odlaganja.

ČLAN 10

POVJERLJIVI UGOVORI I DOZVOLE ZA PRISTUP TAJNIM PODACIMA PRAVNIM LICIMA

(1) Prije ustupanja tajnih podataka koji su u vezi sa povjerljivim ugovorom ugovaraču ili potencijalnom ugovaraču, strana primalac će obezbijediti da:

a) ugovarači ili potencijalni ugovarači i njihove prostorije ispunjavaju uslove za odgovarajuću zaštitu tajnih podataka i da imaju dozvolu za pristup tajnim podacima pravnim licima u skladu sa njihovim nacionalnim zakonima i propisima;

b) ugovarači ili potencijalni ugovarači i njihove prostorije posjeduju dozvolu za pristup tajnim podacima pravnim licima odgovarajućeg stepena tajnosti prije izvršenja ugovora;

c) lica koja obavljaju poslove koji zahtijevaju pristup tajnim podacima imaju odgovarajuću dozvolu za pristup tajnim podacima fizičkim licima;

d) sva lica koja imaju pristup tajnim podacima su upoznata sa svojim odgovornostima i obavezama u pogledu zaštite tajnih podataka u skladu sa odgovarajućim zakonima i propisima strane primaoca.

(2) Povjerljivi ugovor će sadržati odredbe o bezbjednosnim zahtjevima, stepenu tajnosti svih djelova ili elemenata povjerljivog ugovora i izričito pozivanje na ovaj Sporazum. Kopija tog dokumenta će biti proslijeđena Nadležnim bezbejdnosnim organima Strana.

(3) Strane će međusobno priznavati dozvole za pristup tajnim podacima pravnim licima.

(4) Nadležni bezbjednosni organi će, bez odlaganja, obavijestiti jedan drugog o svakom ukidanju međusobno priznatih dozvola za pristup tajnim podacima pravnim licima.

ČLAN 11

POSJETE

(1) Posjete koje obuhvataju pristup tajnim podacima biće predmet prethodne saglasnosti Nadležnog bezbjednosnog organa Strane domaćina.

(2) Zahtjev za posjetu će se podnijeti Nadležnom bezbjednosnom organu najkasnije 30 dana prije datuma posjete. Zahtjev za posjetu će sadržati sledeće podatke koji će se koristiti isključivo u svrhu posjete:

a) ime posjetioca, datum i mjesto rođenja, državljanstvo i broj lične karte/pasoša;

b) radno mjesto na koje je posjetilac raspoređen, sa naznakom poslodavca koga posjetilac predstavlja;

c) detalje projekta u kome posjetilac učestvuje;

d) trajanje i stepen tajnosti dozvole za pristup tajnim podacima za fizičko lice posjetioca, ukoliko se zahtijeva;

e) ime, adresa, broj telefona/faksa, e-mail i kontakt osoba organa koji se posjećuje;

f) cilj posjete, uključujući i najviši stepen tajnosti podataka koji će biti uključeni;

g) datum i trajanje posjete. U slučaju ponovnih posjeta cio period koji obuhvata posjete će biti naznačen;

h) datum i potpis Nadležnog bezbjednosnog organa koji šalje zahtjev.

(3) U hitnim slučajevima, Nadležni bezbjednosni organi mogu se složiti o kraćem vremenskom periodu podnošenja zahtjeva.

(4) Nadležni bezbjednosni organi mogu dogovoriti listu posjetilaca za posjete koje se ponavljaju. Lista će važiti ne duže od 12 mjeseci i važenje se može produžiti na određeni period ne duži od 12 mjeseci. Zahtjev za ponovne posjete će se podnositi u skladu sa stavom 2 ovog člana. Kada se lista odobri, posjete mogu biti dogovorene direktno između organa koji se posjećuju.

(5) Svaka Strana će garantovati zaštitu ličnih podataka posjetilaca u skladu sa nacionalnim zakonima i propisima.

ČLAN 12

POVREDA BEZBJEDNOSTI

(1) U slučaju povrede bezbjednosti koja obuhvata neovlašćeno otkrivanje, pronevjeru ili gubitak tajnih podatka ili sumnje da je došlo do takve povrede bezbjednosti, Nadležni bezbjednosni organ strane primaoca će bez odlaganja obavijestiti o tome Nadležni bezbjednosni organ strane pošiljaoca u pisanoj formi.

(2) Nadležna Strana će preduzeti sve mjere u skladu sa svojim nacionalnim zakonima i propisima kako bi umanjila posledice povrede iz stava 1 ovog člana i kako bi spriječila dalje povrede bezbjednosti. Na zahtjev, druga Strana će obezbijediti odgovarajuću pomoć; biće obaviještena o rezultatima postupka i mjerama koje su preduzete u vezi sa povredom.

(3) Kada povreda bezbjednosti nastane u trećoj strani, Nadležni bezbjednosni organ strane pošiljaoca će preduzeti mjere iz stava 2 ovog člana bez odlaganja.

(4) Nadležni bezbjednosni organi će obavijesiti jedan drugog o posebnim bezbjednosnim rizicima koji mogu ugroziti ustupljene tajne podatke.

ČLAN 13

TROŠKOVI

(1) Primjena ovog Sporazuma ne iziskuje nikakve troškove.

(2) U slučaju da, u toku sprovođenja ovog Sporazuma, nastanu neočekivani troškovi za bilo koju Stranu, svaka Strana će snositi svoje troškove.

ČLAN 14

RJEŠAVANJE SPOROVA

Svaki spor koji se odnosi na primjenu ovog Sporazuma će biti riješen konsultacijama i pregovorima između Strana. U međuvremenu, Strane će nastaviti ispunjavanje odredaba ovog Sporazuma.

ČLAN 15

ZAVRŠNE ODREDBE

(1) Ovaj Sporazum stupa na snagu prvog dana drugog mjeseca nakon prijema poslednjeg pisanog obavještenja u kojem Strane obavještavaju jedna drugu, putem diplomatskih kanala, da su njihove unutrašnje pravne procedure neophodne za stupanje na snagu ovog Sporazuma ispunjene.

(2) Ovaj Sporazum može biti dopunjen na osnovu zajedničke pisane saglasnosti Strana. Takve izmjene i dopune stupaju na snagu u skladu sa stavom 1 ovog člana.

(3) Sporazum se zaključuje na neodređeno vrijeme. Sporazum može biti raskinut od strane svake ugovorne Strane slanjem pisanog obavještenja drugoj Strani putem diplomatskih kanala. U tom slučaju Sporazum prestaje da važi šest mjeseci nakon pisanog obavještenja o otkazu.

(4) U slučaju otkaza, tajni podaci razmijenjeni u skladu sa ovim Sporazumom će se čuvati u skladu sa navedenim odredbama i na zahtjev biti vraćeni strani pošiljaocu.

(5) U svrhu primjene ovog Sporazuma mogu se zaključivati aranžmani.

U prisustvu svjedoka, dolje imenovani, propisno ovlašćeni u tom smislu, potpisali su ovaj Sporazum.

Sačinjeno u …….. dana …… u tri originalna primjerka na crnogorskom, italijanskom i engleskom jeziku, pri čemu su svi tekstovi jednako vjerodostojni. U slučaju razlika u tumačenju mjerodavan je tekst na engleskom jeziku.

U ime Vlade Crne Gore **U ime Vlade Republike Italije**

AGREEMENT

BETWEEN

THE GOVERNMENT OF THE ITALIAN REPUBLIC

AND

THE GOVERNMENT OF MONTENEGRO

ON THE

EXCHANGE AND MUTUAL PROTECTION

OF CLASSIFIED INFORMATION

The Government of the Italian Republic

and

The Government of Montenegro

hereinafter referred to as the "Parties",

wishing to ensure the protection of Classified Information in accordance with their national laws and regulations exchanged between the Parties or between public and private entities under their jurisdiction, in respect of national interests and security, in accordance with the laws and regulations of the parties as well as their international commitments,

recognizing the interest and the common necessity to ensure the protection of any Classified Information, also in relation to the possibility of implementing technical cooperation agreements, exchanged between the Parties and through public and private entities, in accordance with the laws and regulations of the Parties as well as their international commitments and, for Italy, with those deriving from EU membership.

have agreed on the following:

ARTICLE 1

OBJECTIVE

In accordance with their national laws and regulations and in respect of national interests and security as well as of industrial activities both Parties shall take all appropriate measures to ensure the protection of Classified Information, which is transmitted or generated according to this Agreement.

ARTICLE 2

DEFINITIONS

For the purposes of this Agreement these terms mean the following:

a) **Classified Information**: Any information, regardless of its form, transmitted or generated between the Parties, to which a security classification has been assigned in accordance with the national laws and regulations of the Parties.

b) **Competent Security Authority**: A competent entity authorised according to the national laws and regulations of the Parties that is responsible for the implementation of this Agreement.

c) **Originating Party:** The Party, including any public or private entity under its jurisdiction, which releases Classified Information to the Recipient Party.

d) **Recipient Party:** The Party, including any public or private entity under its jurisdiction, which receives Classified Information from the Originating Party.

e) **Need-to-Know**: A principle by which access to Classified Information may be granted to an individual only in connection with his official duties or tasks.

f) **Personnel Security Clearance:** A positive decision following a vetting procedure in accordance with the national laws and regulations, on the basis of which an individual is authorised to have access to and to handle Classified Information up to the level defined in the decision.

g) **Facility Security Clearance:** A positive decision following a vetting procedure certifying that a contractor which is a legal entity fulfils the conditions of handling Classified Information in accordance with the national laws and regulations of one of the Parties.

h) **Contractor:** A public or private entity possessing the legal capacity to conclude contracts or subcontracts.

i) **Classified Contract:** A contract with a Contractor which contains or implies the knowledge of Classified Information.

j) **Third Party**: A state, including any public or private entity under its jurisdiction, or an international organisation that is not a Party to this Agreement.

k) **Visit**: Access to public or private entities, for the purpose of this Agreement, which includes access to Classified Information**.**

ARTICLE 3

COMPETENT SECURITY AUTHORITIES

(1) The Competent Security Authorities designated by the Parties as responsible for the general implementation and the relevant controls of all aspects of this Agreement are:

In the Italian Republic:
– Presidenza del Consiglio dei Ministri – Autorità di sicurezza competente- Dipartimento delle Informazioni per la Sicurezza (DIS) - UCSe.

In Montenegro :
- Direkcija za zaštitu tajnih podataka Crne Gore - (National Security Authority)

(2) The Competent Security Authorities shall notify each other of any other Competent Security Authorities that are responsible for the implementation of this Agreement.

(3) The Parties shall inform each other through diplomatic channels of any subsequent changes of the Competent Security Authorities.

(4) In order to achieve and maintain comparable standards of security, the Competent Security Authorities shall, on request, provide each other with information about their national security standards, procedures and practices for the protection of Classified Information. To this aim the Competent Security Authorities may visit each other.

(5) The Competent Security Authorities shall ensure a strict and binding observance of this agreement by any public and private entity of the Parties in accordance with their national laws and regulations.

ARTICLE 4

SECURITY CLASSIFICATIONS

(1) Classified Information released under this Agreement shall be marked with the appropriate security classification level in accordance with the national laws and regulations of the Parties.

(2) The following national security classification markings are equivalent:

Italian Republic	Montenegro	English translation
SEGRETISSIMO	STROGO TAJNO	TOP SECRET
SEGRETO	TAJNO	SECRET
RISERVATISSIMO	POVJERLJIVO	CONFIDENTIAL
RISERVATO	INTERNO	RESTRICTED

ARTICLE 5

PRINCIPLES FOR THE PROTECTION OF CLASSIFIED INFORMATION

(1) The Parties shall afford to Classified Information referred to in this Agreement the same protection as to their own Classified Information of the corresponding security classification level.

(2) The Competent Security Authority of the Originating Party shall:

a) ensure that the Classified Information is marked with an appropriate security classification marking in accordance with its national laws and regulations, and
b) inform the Recipient Party of any conditions of release or limitations on the use of the Classified Information and of any subsequent changes in the security classification.

(3) The Competent Security Authority of the Recipient Party shall:

a) ensure that the Classified Information is marked with an equivalent security classification marking in accordance with Paragraph 2 of Article 4, and
b) ensure that the security classification level is not changed unless authorized in writing by the Originating Party.
c) use Classified Information only for the purpose for which it has been released and within the limitations stated by the Originating Party.
d) not release Classified Information to a Third Party without a prior written consent of the Originating Party.

ARTICLE 6

ACCESS TO CLASSIFIED INFORMATION AND PERSONNEL SECURITY CLEARANCES

(1) Access to Classified Information classified as RISERVATISSIMO/POVJERLJIVO/ CONFIDENTIAL and above shall be allowed only to those individuals with a Need-to-Know who hold appropriate Personnel Security Clearance and are regularly briefed.

(2) Access to Classified Information classified as RISERVATO/INTERNO/RESTRICTED shall be limited to persons who have a Need-to-Know and who have been briefed accordingly.

(3) The Parties shall mutually recognise their Personnel Security Clearances. Paragraph 2 of Article 4 shall apply accordingly.

(4) On request, the Competent Security Authorities shall cooperate and give mutual assistance during the vetting procedures for the release of Personnel Security Clearances.

(5) The Competent Security Authorities shall promptly inform each other of any changes in mutually recognised Personnel Security Clearances.

ARTICLE 7

PROTECTION OF CLASSIFIED INFORMATION IN COMMUNICATION AND INFORMATION SYSTEMS

(1) The Competent Security Authorities shall ensure according to their relevant laws and regulations, that appropriate measures are implemented for the protection of Classified Information processed, stored or transmitted in communication and information systems. Such measures shall ensure the confidentiality, integrity, availability and, where applicable, non-repudiation and authenticity of Classified Information as well as an appropriate level of accountability and traceability of actions in relation to that Classified Information.

(2) To this end, the Competent Security Authorities shall ensure that such Classified Information exchanged will be stored, handled, transmitted and safeguarded in accordance with their respective national rules and regulations.

(3) Both Competent Security Authorities mutually recognize each formal act of approval, referring to equipment and mechanisms related to communication and information systems, issued by the relevant Competent Security Authority.

(4) When necessary, the updated list of such approved equipment and mechanism shall be exchanged between the Competent Security Authorities.

ARTICLE 8

TRANSMISSION OF CLASSIFIED INFORMATION

(1) Classified Information shall be transmitted between the Parties through diplomatic channels or through other secure channels mutually approved by their Competent Security Authorities in accordance with the national laws and regulations.

(2) Information classified “SEGRETISSIMO/ STROGO TAJNO/TOP SECRET” shall be sent only through diplomatic or military channels in accordance with national laws and regulations.

(3) Information classified as “RISERVATO/INTERNO/RESTRICTED may be transmitted also by post or another delivery service in accordance with national laws and regulations.

(4) In case of transmitting a large consignment containing Classified Information, procedures for transport shall be jointly agreed and evaluated, on a case-by-case basis, by the Competent Security Authorities of the Parties.

ARTICLE 9

REPRODUCTION, TRANSLATION AND DESTRUCTION OF CLASSIFIED INFORMATION

(1) All reproductions and translations shall bear appropriate security classification markings and shall be protected as the original Classified Information. The translations and the number of reproductions shall be limited to the minimum required for an official purpose.

(2) All translations shall be marked with the original security classification marking and shall contain a suitable annotation, in the language of translation, indicating that they contain Classified Information of the Originating Party.

(3) Classified Information marked SEGRETISSIMO/STROGO TAJNO/TOP SECRET both original and translation, shall be reproduced only upon prior written permission of the Originating Party.

(4) Classified Information marked SEGRETISSIMO/ STROGO TAJNO /TOP SECRET shall not be destroyed. It shall be returned to the Originating Party after it is no longer considered necessary by the Recipient Party.

(5) Information classified as SEGRETO/TAJNO /SECRET or below shall be destroyed in accordance with relevant national laws and regulations after it is no longer considered necessary by the Recipient Party. The Recipient Party shall inform the Originating Party of such destruction.

(6) In a crisis situation in which it is impossible to protect or return Classified Information transmitted or generated under this Agreement, the Classified Information shall be destroyed immediately. The Recipient Party shall inform the Competent Security Authority of the Originating Party about this destruction as soon as possible.

ARTICLE 10

CLASSIFIED CONTRACTS AND FACILITY SECURITY CLEARANCES

(1) Before providing Classified Information related to a Classified Contract to Contractors or prospective Contractors, the Recipient Party shall ensure that:

a) such Contractors or prospective Contractors and their facilities have the capability to protect Classified Information adequately and have a Facility Security Clearance in accordance with national laws and regulations;

b) Contractors or prospective Contractors and their facilities hold an appropriate Facility Security Clearance at the adequate level before the execution of the Contract;

c) persons who perform functions which require access to Classified Information hold an appropriate Personnel Security Clearance;

d) all persons having access to the Classified Information are informed of their responsibilities and obligation to protect the information in accordance with the appropriate laws and regulations of the Recipient Party.

(2) A Classified Contract shall contain provisions on the security requirements, classification of each aspect or element of the Classified Contract and specific reference to this agreement. A copy of such document shall be submitted to the Competent Security Authorities of the Parties.

(3) The Parties shall mutually recognise their Facility Security Clearances.

(4) The Competent security authorities shall promptly inform each other about any withdrawal regarding mutually recognized Facility Security Clearances.

ARTICLE 11

VISITS

(1) Visits involving access to Classified Information shall be subject to prior permission of the Competent Security Authority of the host Party.

(2) A request for visit shall be submitted to the relevant Competent Security Authority at least 30 days prior to the commencement of the visit. The request for visit shall include the following data that shall be used for the purpose of the visit only:

a) the visitor's name, date and place of birth, citizenship and identification card/passport number;

b) the visitor's position, with a specification of the employer which the visitor represents;

c) a specification of the project in which the visitor participates;

d) the validity and level of the visitor's Personnel Security Clearance, if required;

e) the name, address, phone/fax number, e-mail and point of contact of the facility to be visited;

f) the purpose of the visit, including the highest security classification level of Classified Information to be involved;

g) the date and duration of the visit. In case of recurring visits the total period covered by the visits shall be stated;

h) the date and signature of the sending Competent Security Authority.

(3) In urgent cases, the Competent Security Authorities can agree on a shorter period for the submission of the request for visit.

(4) The Competent Security Authorities may agree on a list of visitors entitled to recurring visits. The list shall be valid for an initial period not exceeding 12 months and may be extended for a further period of time not exceeding 12 months. A request for recurring visits shall be submitted in accordance with Paragraph 2 of this Article. Once the list has been approved, visits may be arranged directly between the facilities involved.

(5) Each Party shall guarantee the protection of personal data of the visitors in accordance with the national laws and regulations.

ARTICLE 12

BREACH OF SECURITY

(1) In case of a security breach resulting in unauthorised disclosure, misappropriation or loss of Classified Information or suspicion of such a breach, the Competent Security Authority of the Recipient Party shall immediately inform the Competent Security Authority of the Originating Party thereof in writing.

(2) The competent Party shall undertake all measures in accordance with the national laws and regulations so as to limit the consequences of the breach referred to in Paragraph 1 of this Article and to prevent further breaches. On request, the other Party shall provide appropriate assistance; it shall be informed of the outcome of the proceedings and the measures undertaken due to the breach.

(3) When the breach of security has occurred in a Third Party, the Competent Security Authority of the sending Party shall take the actions referred to in Paragraph 2 of this Article without delay.

(4) The Competent Security Authorities shall inform each other of exceptional security risks that may endanger the released Classified Information.

ARTICLE 13

EXPENSES

(1) The implementation of this Agreement does not include any cost.

(2) In case that, in the course of the implementation of this Agreement, there are unexpected costs for any of the Parties, each Party shall bear its own expenses.

ARTICLE 14

SETTLEMENT OF DISPUTES

Any dispute regarding the interpretation or application of this Agreement shall be settled by consultations and negotiations between the Parties. Meanwhile the Parties will continue to fulfil the provisions set forth in this agreement.

ARTICLE 15

FINAL PROVISIONS

(1) This Agreement shall enter into force on the first day of the second month from the date of receipt of the latest written notification by which the Parties have informed each other, through diplomatic channels, that their internal legal requirements necessary for its entry into force have been fulfilled.

(2) This Agreement may be amended by mutual written consent of the Parties. Amendments shall enter into force in accordance with paragraph 1 of this Article.

(3) This Agreement is concluded for an indefinite period of time. Either Party may denounce this Agreement by giving the other Party notice in writing through diplomatic channels. In that case, this Agreement shall terminate six months from the date on which the other Party has received the denunciation notice.

(4) In case of termination of this Agreement, all Classified Information transferred pursuant to this Agreement shall continue to be protected in accordance with the provisions set forth herein and, upon request, returned to the Originating Party.

(5) Implementing arrangements may be concluded for the implementation of this Agreement.

In witness whereof the undersigned, being duly authorised thereto, have signed this Agreement.

Done in……..on……in [three] originals in the Italian, Montenegrin and English languages, all texts being equally authentic. In case of any divergence of interpretation, the English text shall prevail.

On behalf of the Government of the Italian Republic	**On behalf of Government of Montenegro**