

PREDLOG

SPORAZUM IZMEĐU

VLADE CRNE GORE

I

VLADE REPUBLIKE FRANCUSKE

O RAZMJENI I UZAJAMNOJ ZAŠTITI TAJNIH PODATAKA

Vlada Crne Gore,

Vlada Republike Francuske,

U daljem tekstu „Strane”,

U želji da obezbijede zaštitu tajnih podataka i materijala koji se razmjenjuju ili nastaju između Strana ili između državnih organa i pravnih lica u skladu sa odgovarajućim nacionalnim zakonima i propisima,

Usaglasile su sljedeće uslove:

ČLAN 1

Definicije

U svrhu ovog Sporazuma:

- 1.1 Izraz **„Tajni podaci”** podrazumijeva informacije, dokumenta i materijale, bez obzira na formu, prirodu ili način njihovog dostavljanja, kao i na to da li su nastali ili su u procesu nastajanja, kojima je dodijeljen određeni stepen tajnosti i koji, u interesu nacionalne bezbjednosti i u skladu sa nacionalnim zakonima i propisima svake od Strana, zahtijevaju zaštitu od zloupotrebe, uništavanja, pronevjere, otkrivanja, gubljenja ili pristupa od strane neovlašćenog lica ili neke druge vrste odavanja.
- 1.2 Izraz **„Povjerljivi ugovor”** podrazumijeva ugovor, podugovor ili projekat čija priprema i izvršenje zahtijevaju pristup tajnim podacima ili korišćenje i stvaranje tajnih podataka.
- 1.3 Izrazi **„Ugovarač”** i **„Podugovarač”** označavaju svako fizičko ili pravno lice koje posjeduje pravnu sposobnost da pregovara i zaključuje povjerljive ugovore.
- 1.4 Izraz **„Nacionalni bezbjednosni organ” (NSA)** označava nacionalni organ koji je nadležan za opštu kontrolu i primjenu ovog sporazuma za svaku od Strana.

- 1.5 Izraz **„Nadležni bezbjednosni organi" (CSA)** označava svaki bezbjednosni organ ili svaki drugi nadležni organ, ovlašten u skladu sa nacionalnim zakonima i propisima Strana, određen kao odgovoran ili na koji je prenesena odgovornost za primjenu ovog sporazuma u cjelini ili njegovog dijela.
- 1.6 Izraz **„Strana Primaoc** označava Stranu, svako lice i organ u okviru njenih nacionalnih zakona i propisa, koja prima tajne podatke od Strane Pošiljaoca.
- 1.7 Izraz **„Strana Pošiljalac"** označava Stranu, svako lice i organ u okviru njenih nacionalnih zakona i propisa, koji šalju tajne podatke Strani Primaocu.
- 1.8 Izraz **„Potrebno je da zna"** označava potrebu za pristupom tajnim podacima u okviru datog službenog položaja i za potrebe izvršavanja konkretnog zadatka.
- 1.9 Izraz **„Dozvola za pristup tajnim podacima fizičkom licu" (PSC)** je pozitivna odluka kojom se, nakon sprovedenog postupka bezbjednosne provjere, u skladu sa nacionalnim zakonima i propisima jedne od Strana, određenom licu odobrava pristup tajnim podacima do određenog stepena tajnosti koji je definisan u dozvoli.
- 1.10 Izraz **„Treća strana"** označava svaku državu, uključujući pravna i fizička lica u njenoj nadležnosti, ili svaku međunarodnu organizaciju koja nije Strana ovog sporazuma.
- 1.11 Izraz **„Dozvola za pristup tajnim podacima pravnim licima" (FSC)** je pozitivna odluka kojom se, nakon sprovedenog postupka bezbjednosne provjere, u skladu sa nacionalnim zakonima i propisima jedne od Strana, potvrđuje da je ugovarač ovlašten za primanje, rukovanje, obradu i čuvanje tajnih podataka do određenog stepena tajnosti.
- 1.12 Izraz **„Strana domaćin"** je Strana na čijoj se teritoriji odvija posjeta.

ČLAN 2

Primjena i ciljevi

2.1 Ovaj sporazum predstavlja opšti bezbjednosni propis, primjenljiv na svaku razmjenu tajnih podataka između Strana ili između njihovih organa u skladu sa njihovim nacionalnim zakonima i propisima.

2.2 Ovaj sporazum se može koristiti kao okvir za razmjenu i zaštitu tajnih podataka dobijenih od neke međunarodne organizacije i razmjenjenih između Strana, ili između jedne Strane i međunarodne organizacije, po odobrenju oba Nacionalna bezbjednosna

organa i te međunarodne organizacije. Bezbjednosna zaštita reguliše se u pisanoj formi između Strana u okviru planirane razmjene.

ČLAN 3

Nacionalni bezbjednosni organi

Nacionalni bezbjednosni organ (NSA) za svaku od Strana je:

Za Crnu Goru:

Direkcija za zaštitu tajnih podataka

Ulica Jovana Tomaševića 29

81 000 Podgorica, Crna Gora

Za Republiku Francusku:

Generalni Sekretarijat za odbranu i nacionalnu bezbjednost (SGDSN)

51, Boulevard de La Tour-Maubourg

75700 PARIS 07 SP FRANCE

Strane će informisati jedna drugu ukoliko se za to ukaže potreba, o kontakt detaljima svog Nacionalnog bezbjednosnog organa (NSA) i Nadležnih bezbjednosnih organa (CSA) kao i o svim izmjenama koje se odnose na Nacionalni bezbjednosni organ (NSA) kao i Nadležne bezbjednosne organe (CSA).

ČLAN 4

Bezbjednosni principi

4.1 U skladu sa odgovarajućim nacionalnim zakonima i propisima, Strane preduzimaju sve odgovarajuće mjere za zaštitu tajnih podataka koji su razmijenjeni, primljeni ili su nastali u skladu sa odredbama ovog Sporazuma i obezbjeđuju tim podacima nivo zaštite koji je ekvivalentan nivou zaštite njihovih nacionalnih tajnih podataka kao što je definisano u članu 5 stavu 5.1.

4.2 Strana Primalac označava sve tajne podatke dobijene od Strane Pošiljaoca, svojim nacionalnim stepenom tajnosti u skladu sa ekvivalentnim stepenima definisanim u članu 5 stavu 5.1.

4.3 Pristup tajnim podacima biće omogućen isključivo državljanima Strana koji imaju odgovarajuću dozvolu za pristup tajnim podacima fizičkim licima i čija potreba za obavljanjem službene dužnosti zahtijeva pristup tajnim podacima po principu „potrebno je da zna“.

4.4 Strana Primalac neće snižavati niti mijenjati stepen tajnosti podataka koje je primila, bez prethodne pisane saglasnosti Strane Pošiljaoca.

4.5 Strane će bez odlaganja informisati jedna drugu o svim promjenama u svojim nacionalnim zakonima i propisima koji utiču na zaštitu tajnih podataka ili bilo kojoj drugoj promjeni koja utiče na zaštitu tajnih podataka koji su razmijenjeni ili su nastali u skladu sa ovim sporazumom. U ovom slučaju, strane će se konsultovati u cilju razmatranja mogućih izmjena ovog sporazuma. U međuvremenu, tajni podaci će nastaviti da se štite u skladu sa uslovima iz ovog sporazuma.

4.6 Tajni podaci koji su ustupljeni mogu se koristiti isključivo u svrhu za koju su ustupljeni.

4.7 Nacionalni bezbjednosni organ (NSA) ili Nadležni bezbjednosni organi CSA će nadgledati, posebno putem inspeksijske kontrole, sve aspekte bezbjednosti u vezi sa realizacijom bilo koje aktivnosti, ugovora ili sporazuma između Strana koji uključuju razmjenu ili nastanak tajnih podataka.

ČLAN 5

Stepeni tajnosti i ekvivalenti

5.1 Strane preduzimaju mjere za zaštitu tajnih podataka koji su dostavljeni, primljeni ili sačinjeni u skladu sa ovim sporazumom i primjenjuju ekvivalentne bezbjednosne oznake stepena tajnosti podataka koji su definisani u navedenoj tabeli:

CRNA GORA	FRANCUSKA
STROGO TAJNO	TRÈS SECRET DÉFENSE
TAJNO	SECRET DÉFENSE
POVJERLJIVO	CONFIDENTIEL DÉFENSE
INTERNO	(član 5 st. 5.2 i 5.3)

5.2 Republika Francuska obrađuje i štiti tajne podatke označene „INTERNO“ koje je dostavila Crna Gora u skladu sa svojim važećim nacionalnim zakonima i propisima koji se odnose na zaštićene ali neklasifikovane podatke, kao što je „DIFFUSION RESTREINTE“.

5.3 Crna Gora obrađuje i štiti neklasifikovane podatke ali označene kao zaštićene, kao što je „DIFFUSION RESTREINTE“ koje je dostavila Republika Francuska u skladu sa svojim važećim nacionalnim zakonima i propisima koji se odnose na podatke stepena tajnosti „INTERNO“.

5.4 Iz posebnih bezbjednosnih razloga, kada Strana pošiljalac zahtijeva da se pristup tajnim podacima ograniči isključivo na državljane Strana, takvi podaci mogu biti označeni dodatnom ograničavajućom oznakom, kao što je „ISKLJUČIVO ZA DRŽAVLJANE CRNE GORE - FRANCUSKE“ i „SPECIAL FRANCE – MONTENEGRO“. U cilju održavanja ekvivalentnih bezbjednosnih standarda, na zahtjev bilo koje od Strana, druga Strana će dostaviti sve informacije koje su zatražene u vezi sa nacionalnim bezbjednosnim zakonima, propisima i procedurama koje se primjenjuju u cilju obezbjeđivanja zaštite tajnih podataka. Strane su saglasne da se omoguće lakši kontakti između njihovih Nacionalnih bezbjednosnih organa (NSA) i Nadležnih bezbjednosnih organa (CSA).

ČLAN 6

Postupak izdavanja dozvola za pristup tajnim podacima

6.1 Za pristup tajnim podacima označenim stepenom tajnosti „POVJERLJIVO“ ili „CONFIDENTIEL DÉFENSE“ ili višim stepenom, svaka Strana će sprovesti postupak izdavanja dozvole za pristup tajnim podacima fizičkim licima u skladu sa nacionalnim zakonima i propisima.

6.2 Za izdavanje dozvole za pristup tajnim podacima državljaninu jedne od Strana koji je boravio ili još uvijek boravi na teritoriji druge Strane, Nacionalni bezbjednosni organ (NSA) ili Nadležni bezbjednosni organi (CSA) svake od Strana će pomagati jedni drugima u skladu sa njihovim nacionalnim zakonima i propisima.

6.3 Na zahtjev Nacionalnog bezbjednosnog organa (NSA) ili Nadležnih bezbjednosnih organa (CSA) druge Strane, Nacionalni bezbjednosni organ (NSA) ili Nadležni bezbjednosni organi (CSA) svake od Strana će sprovoditi postupak izdavanja dozvole za pristup tajnim podacima fizičkim licima za svoje državljane, u skladu sa njihovim nacionalnim zakonima i propisima.

6.4 Strane obostrano priznaju dozvole za pristup tajnim podacima za fizička lica koje su izdate njihovim državljanima u okviru pristupa tajnim podacima razmijenjenim u skladu sa ovim sporazumom.

6.5 Nacionalni bezbjednosni organi (NSA) ili Nadležni bezbjednosni organi (CSA) odmah informišu jedni druge o promjenama koje se odnose na dozvole za pristup tajnim podacima za fizička lica svojih državljana u skladu sa ovim sporazumom, naročito, u slučaju povlačenja dozvole ili smanjivanja stepena tajnosti za koji je izdata.

ČLAN 7

Korišćenje tajnih podataka

7.1 Strana Primalac će koristiti tajne podatke jedino u svrhu u koju su ustupljeni i u okviru ograničenja postavljenih od strane Strane Pošiljaoca.

7.2 Strana Primalac neće otkriti trećoj strani tajne podatke koji su dostavljeni, primljeni ili su nastali u skladu ovim sporazumom, bez prethodne pisane saglasnosti Nacionalnog bezbjednosnog organa (NSA) ili Nadležnih bezbjednosnih organa (CSA) Strane Pošiljaoca.

7.3 Tajnim podacima koji su zajednički nastali između Strana u skladu sa sporazumima, ugovorima ili bilo kojom drugom zajedničkom aktivnošću, ni jedna Strana ne može snižavati stepen tajnosti, niti ga može ukidati, niti ustupati tajne podatke trećoj strani bez prethodne pisane saglasnosti druge Strane.

ČLAN 8

Prevod, umnožavanje i uništavanje

8.1 Strana Primalac će umnožene tajne podatke i prevode koji su napravljeni označiti kao originale i obezbijediti im isti stepen zaštite.

8.2 Podatke označene stepenom tajnosti „STROGO TAJNO" ili „TRÈS SECRET DÉFENSE" Strana Primalac neće umnožavati niti prevoditi. Dodatni originalni dokumenti ili prevodi mogu biti dostavljeni na osnovu zahtjeva podnijetog Strani Pošiljaocu u pisanoj formi.

8.3 Podatke označene stepenom tajnosti „STROGO TAJNO" ili „TRÈS SECRET DÉFENSE" Strana Primalac ne smije uništavati. Takvi podaci se vraćaju Strani Pošiljaocu u skladu sa dolje navedenim članom 9 stav 9.1, nakon što se zaključi da više nisu potrebni ili nakon prestanka tajnosti.

8.4 Prevođenje i umnožavanje podataka označenih stepenom tajnosti „TAJNO" ili „SECRET DÉFENSE" će se odobriti isključivo uz pisanu saglasnost Nacionalnog bezbjednosnog organa (NSA) ili Nadležnih bezbjednosnih organa (CSA) Strane Pošiljaoca.

8.5 Podaci označeni stepenom tajnosti „TAJNO" ili „SECRET DEFENSE", „POVJERLJIVO" ili „CONFIDENTIEL DÉFENSE" uništavaće se u skladu sa nacionalnim zakonima i propisima Strane Primaoca i to na način da ih je nemoguće ponovo obnoviti u cjelini ili u djelovima.

8.6 U slučaju krizne situacije, koja onemogućava zaštitu ili vraćanje tajnih podataka koji su nastali ili su ustupljeni u skladu sa ovim sporazumom, tajni podaci će se uništiti bez odlaganja. Nacionalni bezbjednosni organ (NSA) Strane Primaoca će, bez odlaganja, obavjestiti Nacionalni bezbjednosni organ (NSA) Strane Pošiljaoca o uništavanju tajnih podataka.

ČLAN 9

Prenos podataka između Strana

9.1 Tajni podaci će se prenositi između Strana putem diplomatskih kanala u skladu sa nacionalnim zakonima i propisima Strane Pošiljaoca.

9.2 Nacionalni bezbjednosni organ (NSA) ili Nadležni bezbjednosni organi (CSA) mogu međusobnim sporazumom dogovoriti da se tajni podaci dostavljaju na drugačiji način.

9.3 Prenos veće količine tajnih podataka će organizovati nadležni Nacionalni bezbjednosni organi (NSA) ili Nadležni bezbjednosni organi (CSA) od slučaja do slučaja.

9.4 Tajni podaci i podaci označeni „DIFFUSION RESTREINTE" će se prenositi elektronski u kriptovanoj formi, korišćenjem kriptografskih metoda i uređaja odobrenih od strane oba Nacionalna bezbjednosna organa (NSA).

ČLAN 10

Povjerljivi ugovori

10.1 Nacionalni bezbjednosni organ (NSA) ili Nadležni bezbjednosni organi (CSA) Strane Pošiljaoca će obavjestiti Nacionalni bezbjednosni organ (NSA) ili Nadležne bezbjednosne organe (CSA) Strane Primaoca o svakom povjerljivom ugovoru prije bilo kakve razmjene tajnih podataka. Ovim obavještenjem se mora precizirati najviši stepen tajnosti podataka koje sadrži povjerljivi ugovor.

10.2 Strana koja namjerava da zaključi ili ovlasti nekog od svojih Ugovarača da zaključi povjerljivi ugovor stepena tajnosti „POVJERLJIVO“ ili „CONFIDENTIEL DÉFENSE“ ili višeg stepena sa Ugovaračem druge Strane, provjeriće sa Nacionalnim bezbjednosnim organom (NSA) ili Nadležnim bezbjednosnim organima (CSA) te Strane da li taj Ugovarač ima odgovarajuću dozvolu za pristup tajnim podacima pravnom licu neophodnu za izvršenje ugovora. Ukoliko takva dozvola za pristup tajnim podacima pravnom licu nije izdata, Nacionalni bezbjednosni organ (NSA) ili Nadležni bezbjednosni organi (CSA) Strane Primaoca će započeti proceduru izdavanja dozvole za pristup tajnim podacima pravnom licu zahtijevanog stepena tajnosti.

10.3 Za svaki povjerljivi ugovor, sačiniće se Aneks o bezbjednosti. U tom Aneksu, Nacionalni bezbjednosni organ (NSA) ili Nadležni bezbjednosni organi (CSA) Strane Pošiljaoca će precizirati šta Strana Primalac mora zaštititi, kao i odgovarajući stepen tajnosti. Samo Strana Pošiljalac može izmijeniti stepen tajnosti podataka koji je definisan Aneksom o bezbjednosti.

10.4 Nacionalni bezbjednosni organ (NSA) ili Nadležni bezbjednosni organi (CSA) Strane Pošiljaoca će poslati kopiju Aneksa o bezbjednosti Nacionalnom bezbjednosnom organu (NSA) ili Nadležnim bezbjednosnim organima (CSA) druge Strane.

10.5 Nacionalni bezbjednosni organ (NSA) ili Nadležni bezbjednosni organi (CSA) Strana na čijoj teritoriji će se izvoditi radovi, moraju obezbijediti primjenu mjera bezbjednosti, ekvivalentnih onima koje su potrebne za zaštitu njihovih tajnih podataka.

10.6 Prije potpisivanja povjerljivog ugovora sa Podugovaračem, Ugovarač mora imati prethodno odobrenje od strane svog Nacionalnog bezbjednosnog organa (NSA) ili svojih Nadležnih bezbjednosnih organa (CSA). Podugovarači moraju ispunjavati iste bezbjednosne uslove koji su propisani za Ugovarača.

10.7 Prije nego se neki tajni podatak dobijen od Strane Pošiljaoca dostavi Ugovaračima, Nacionalni bezbjednosni organ (NSA) ili Nadležni bezbjednosni organi (CSA) Strane Primaoca će:

- a) obezbijediti da Ugovarači i njihovi objekti zadovoljavaju uslove za pružanje odgovarajuće zaštite tajnim podacima;
- b) izdati odgovarajuću dozvolu za pristup tajnim podacima potrebnog stepena pravnom licu za objekte datog Ugovarača;
- c) izdati odgovarajuću dozvolu za pristup tajnim podacima fizičkim licima potrebnog stepena u skladu sa principom „potrebno je da zna“;

d) obezbijediti da sva lica koja imaju pristup tajnim podacima budu obaviještena o njihovim dužnostima i odgovornostima koje proističu iz važećih nacionalnih zakona i propisa;

e) vršiti bezbjednosne kontrole datih objekata u skladu sa nacionalnim zakonima i propisima.

10.8 Ukoliko neka od Strana ili jedan od njenih Ugovarača namjerava da, za povjerljivi ugovor, koristi pravno lice druge Strane, a to pravno lice je u vlasništvu ili pod kontrolom treće strane, Nacionalni bezbjednosni organ (NSA) ili Nadležni bezbjednosni organi (CSA) zainteresovane Strane će biti obaviješteni o tome.

ČLAN 11

Posjete

11.1 Kada posjete podrazumijevaju pristup tajnim podacima označenim stepenom tajnosti „STROGO TAJNO“ ili „TRÈS SECRET DÉFENSE“, zahtjev za posjete će se slati diplomatskim kanalima Nacionalnom bezbjednosnom organu (NSA) Strane domaćina. Zahtjevi za posjete će se slati najkasnije tri (3) nedjelje prije datuma za koji se posjeta zahtjeva.

11.2 Posjete pravnim licima jedne Strane, koje uključuju pristup tajnim podacima od strane predstavnika druge Strane stepena tajnosti „TAJNO“ ili „SECRET DÉFENSE“ i „POVJERLJIVO“ ili „CONFIDENTIEL DÉFENSE“, ili mjestima gdje je moguć direktan pristup pomenutim tajnim podacima, biće predmet zahtjeva za posjetu i prethodnog pisanog odobrenja Nacionalnog bezbjednosnog organa (NSA) ili Nadležnih bezbjednosnih organa (CSA) Strane domaćina.

11.3 Posjete treće strane pravnim licima jedne od Strana, koje uključuju pristup tajnim podacima stepena „POVJERLJIVO“ ili „CONFIDENTIEL DÉFENSE“ ili iznad tog stepena razmijenjenim ili nastalim između Strana, ili mjestima gdje je moguć direktan pristup takvim podacima, biće predmet prethodnog odobrenja u pisanoj formi od strane Nacionalnog bezbjednosnog organa (NSA) ili Nadležnih bezbjednosnih organa (CSA) druge Strane.

11.4 Posjete navedene u st. 11.1, 11.2, 11.3 ovog člana zahtijevaju da svi posjetioци posjeduju odgovarajuću dozvolu za pristup tajnim podacima fizičkim licima u skladu sa principom „potrebno je da zna“.

11.5 Zahtjev za posjetu mora sadržati sljedeće informacije:

- a) ime i prezime posjetioca, datum i mjesto rođenja, državljanstvo i broj pasoša ili lične karte;
- b) zvanje i radno mjesto posjetioca, naziv organa ili institucije u kojem je zaposlen/a;
- c) stepen tajnosti za koji je izdata dozvola posjetioca, potvrđen bezbjednosnim sertifikatom izdatim od strane Nacionalnog bezbjednosnog organa (NSA) ili Nadležnih bezbjednosnih organa (CSA) Strane koja podnosi zahtjev;
- d) predloženi datum posjete i planirano trajanje;
- e) svrha posjete i sve neophodne informacije kojima se preciziraju teme koje uključuju tajne podatke uključujući i njihov stepen tajnosti;
- f) nazivi organa, institucija ili prostorija koji će se posjetiti;
- g) datum, potpis i zvanični pečat ili zvanično priznati elektronski potpis Nacionalnog bezbjednosnog organa (NSA) ili Nadležnog bezbjednosnog organa (CSA) Strane koja podnosi zahtjev.

11.6 Svaka od Strana može tražiti odobrenje za posjetu za maksimalni period od dvanaest (12) mjeseci. Ukoliko se određena posjeta ne obavi u vremenskom roku datom u odobrenju za posjetu, ili ukoliko je potrebno produženje tog perioda, Strana koja podnosi zahtjev može zatražiti novo odobrenje za posjetu, pod uslovom da taj zahtjev podnese najmanje tri (3) nedjelje prije isteka postojećeg odobrenja.

11.7 Posjetioci će se pridržavati bezbjednosnih propisa i instrukcija Strane domaćina.

11.8 Strane mogu sačiniti spisak osoblja kojem se odobrava više posjeta u vezi svakog projekta, programa ili konkretnog ugovora u skladu sa uslovima dogovorenim od strane Nacionalnog bezbjednosnog organa (NSA) ili Nadležnih bezbjednosnih organa (CSA) obje Strane.

11.9 Svaka Strana će garantovati zaštitu ličnih podataka posjetilaca u skladu sa svojim zakonima i propisima.

ČLAN 12

Povrede bezbjednosti

12.1 Svaka povreda bezbjednosti, vezano za zaštitu tajnih podataka dobijenih ili nastalih kao rezultat zajedničke saradnje, biće istražena u skladu sa nacionalnim zakonima i propisima Strane na čijoj se teritoriji povreda bezbjednosti dogodila. Druga Strana će, ukoliko je potrebno, sarađivati u istrazi.

12.2 U slučaju okolnosti iz stava 12.1 ovog člana, Nacionalni bezbjednosni organ (NSA) ili Nadležni bezbjednosni organi (CSA) na čijoj teritoriji se povreda dogodila informisaće Nacionalni bezbjednosni organ (NSA) ili Nadležne bezbjednosne organe (CSA) druge Strane u najkraćem mogućem roku.

12.3 Druga Strana će biti obaviještena o rezultatima istrage navedene u stavu 12.1 ovog člana i dobiće konačni izvještaj o razlozima i obimu narušavanja bezbjednosti.

ČLAN 13

Troškovi

13.1 Primjena odredbi ovog sporazuma neće, po pravilu, iziskivati bilo kakve posebne troškove.

13.2 Ukoliko nastanu određeni troškovi, svaka Strana će snositi svoje troškove.

ČLAN 14

Rješavanje sporova

14.1 Svaki spor u vezi sa tumačenjem ili primjenom ovog sporazuma će se rješavati isključivo putem konsultacija između Strana, bez uključivanja bilo koje treće strane ili međunarodnog ili nacionalnog suda.

14.2 Tokom trajanja spora, Strane se obavezuju da će poštovati obaveze predviđene ovim sporazumom.

ČLAN 15

Završne odredbe

15.1 Ovaj sporazum se zaključuje ne neodređeno vrijeme. Svaka Strana će obavijestiti drugu Stranu o okončanju unutrašnjih procedura neophodnih za stupanje na snagu ovog sporazuma. On će stupiti na snagu prvog dana drugog mjeseca nakon prijema zadnjeg obavještenja.

15.2 Ukoliko je potrebno, Nacionalni bezbjednosni organ (NSA) ili Nadležni bezbjednosni organi (CSA) Strana mogu imati međusobne konsultacije o posebnim tehničkim aspektima

vezano za primjenu ovog sporazuma i zaključiti neophodne aranžmane za njegovu primjenu.

15.3 Odredbe ovog sporazuma se mogu izmijeniti zajedničkim dogovorom Strana u pisanoj formi. Te izmjene će stupiti na snagu u skladu sa rokovima i uslovima predviđenim u stavu 15.1 ovog člana.

15.4 Ovaj sporazum se može otkazati zajedničkim dogovorom ili jednostrano. Obavještenje o otkazu sporazuma će stupiti na snagu šest (6) mjeseci nakon prijema pisanog obavještenja. Obavještenje o otkazu neće imati uticaja na prava i obaveze Strana u vezi sa podacima koji su dostavljeni, primljeni ili su nastali u skladu sa ovim sporazumom.

U POTVRDU ČEGA su, predstavnici obje Strane, propisno ovlašćeni u tom smislu, potpisali ovaj sporazum i stavili svoje pečate.

Potpisano u dana u dva originalna primjerka, na crnogorskom i francuskom jeziku, pri čemu su oba teksta jednako vjerodostojna.

Za Vladu Crne Gore

Za Vladu Republike Francuske

Accord entre

le Gouvernement du Monténégro

et

le Gouvernement de la République française

relatif à l'échange et à la protection réciproque d'informations
classifiées

Le Gouvernement du Monténégro,

Le Gouvernement de la République française,

Ci-après dénommés les « Parties »,

Désireux de garantir la protection des informations et matériels classifiés échangés entre les deux Parties ou des organismes publics ou privés régis par leurs lois et règlements nationaux respectifs, ou produits par eux,

Sont convenus des dispositions suivantes :

ARTICLE 1^{er}

Définitions

Aux fins du présent Accord :

- 1.1 L'expression « **informations classifiées** » désigne les informations, documents et matériels, quels qu'en soient la forme, la nature ou le mode de transmission, qu'ils soient élaborés ou en cours d'élaboration, auxquels un degré de classification a été attribué et qui, dans l'intérêt de la sécurité nationale et conformément aux lois et règlements nationaux de chacune des Parties, nécessitent une protection contre toute violation, toute destruction, tout détournement, toute divulgation, toute perte ou tout accès par toute personne non autorisée ou tout autre type de compromission.
- 1.2 L'expression « **contrat classifié** » désigne un contrat, un contrat de sous-traitance ou un projet dont l'élaboration et l'exécution nécessitent l'accès à des informations classifiées ou l'utilisation et la production d'informations classifiées.
- 1.3 Les expressions « **contractant** » et « sous-traitant » désignent toute personne physique ou morale ayant la capacité juridique de négocier et de conclure des contrats classifiés.
- 1.4 L'expression « **Autorité nationale de sécurité** » (ANS) désigne l'autorité nationale responsable du contrôle général et de l'application du présent Accord pour chacune des Parties.
- 1.5 L'expression « **Autorités de sécurité compétentes** » (ASC) désigne toute autorité de sécurité désignée ou toute autre entité compétente autorisée conformément aux lois et règlements nationaux des Parties, qui a été désignée comme responsable ou à qui a été déléguée la responsabilité de l'application de tout ou partie du présent Accord.
- 1.6 L'expression « **Partie destinataire** » désigne la Partie, et notamment toute personne ou entité régie par ses lois et règlements nationaux, qui reçoit les informations classifiées de la Partie d'origine.
- 1.7 L'expression « **Partie d'origine** » désigne la Partie, et notamment toute personne ou entité régie par ses lois et règlements nationaux, qui communique des informations classifiées à la Partie destinataire.
- 1.8 L'expression « **besoin d'en connaître** » désigne la nécessité d'avoir accès à des informations classifiées dans le cadre d'une fonction officielle et en vue d'exécuter une tâche spécifique.
- 1.9 L'expression « **habilitation de sécurité individuelle** » désigne une décision positive faisant suite à une procédure d'examen conforme aux lois et règlements nationaux de l'une des Parties, établissant qu'une personne est autorisée à avoir accès à des

informations classifiées jusqu'à un certain niveau de classification défini dans l'habilitation.

- 1.10** L'expression « **tierce partie** » désigne tout État, y compris les personnes physiques ou morales placées sous sa juridiction, ou toute organisation internationale non partie au présent Accord.
- 1.11** L'expression « **habilitation de sécurité des établissements** » désigne une décision positive faisant suite à une procédure d'examen conforme aux lois et règlements nationaux de l'une des Parties, établissant qu'un contractant est autorisé à recevoir, à manipuler, à traiter et à stocker des informations classifiées jusqu'à un certain niveau de classification.
- 1.12** L'expression « **Partie d'accueil** » désigne la Partie sur le territoire de laquelle une visite a lieu.

ARTICLE 2

Applicabilité et objectifs

2.1 Le présent Accord constitue le règlement commun de sécurité applicable à tout échange d'informations classifiées entre les Parties ou entre leurs organismes régis par leurs lois et règlements nationaux.

2.2 Le présent Accord peut être utilisé pour encadrer l'échange et la protection d'informations classifiées fournies par une organisation internationale et échangées entre les Parties, ou entre une Partie et cette organisation internationale, sur autorisation des deux Autorités nationales de sécurité et de l'organisation internationale concernée. Une assurance de sécurité serait rédigée par les Parties dans le cadre de l'échange prévu.

ARTICLE 3

Autorités nationales de sécurité

L'Autorité nationale de sécurité pour chacune des Parties est :

Pour le Monténégro :

Direkcija za zaštitu tajnih podataka
Ulica Jovana Tomaševića 29
81000 Podgorica, CRNA GORA

Pour la République française :

Secrétariat général de la défense et de la sécurité nationale (S.G.D.S.N.)
51, bl de La Tour-Maubourg
75700 PARIS 07 SP FRANCE

Les Parties se tiennent mutuellement informées, s'il y a lieu, des coordonnées de leur ANS et de leurs ASC et de tout changement concernant l'ANS et les ASC.

ARTICLE 4

Principes de sécurité

4.1 Conformément à leurs lois et règlements nationaux respectifs, les Parties prennent toutes les mesures propres à assurer la protection des informations classifiées transmises, reçues ou générées en vertu des dispositions du présent Accord et leur accordent un niveau de protection équivalent à celui appliqué à leurs propres informations classifiées nationales, tel que défini au paragraphe 1 de l'article 5.

- 4.2 La Partie destinataire appose sur les informations classifiées reçues de la Partie d'origine son propre marquage de classification nationale conformément aux équivalences définies au paragraphe 1 de l'article 5.
- 4.3 L'accès aux informations classifiées est strictement réservé aux ressortissants des Parties qui ont obtenu l'habilitation de sécurité individuelle appropriée et dont les fonctions rendent essentiel l'accès à ces informations, sur la base du besoin d'en connaître.
- 4.4 La Partie destinataire ne déclassifie ni ne déclassifie des informations classifiées reçues, sans le consentement écrit préalable de la Partie d'origine.
- 4.5 Les Parties se tiennent mutuellement informées immédiatement de tout changement dans leurs lois et règlements nationaux ayant un effet sur la protection des informations classifiées ou de tout changement affectant la protection des informations classifiées échangées ou produites en vertu du présent Accord. Dans ce cas, les Parties se consultent afin d'étudier les modifications éventuelles à apporter au présent Accord. Dans l'intervalle, les informations classifiées continuent d'être protégées conformément aux présentes dispositions.
- 4.6 Les informations classifiées transmises ne peuvent être utilisées à des fins autres que celles pour lesquelles elles ont été transmises.
- 4.7 L'ANS ou les ASC supervisent, notamment par des inspections, tous les aspects de la sécurité relatifs à l'exécution de toute activité, tout contrat ou accord entre les Parties donnant lieu à l'échange ou la création d'informations classifiées.

ARTICLE 5

Classifications de sécurité et équivalences

- 5.1 Les Parties s'engagent à assurer la protection des informations classifiées transmises, reçues ou créées en vertu du présent Accord et adoptent les équivalences de niveaux de classification de sécurité définies dans le tableau ci-dessous :

MONTÉNÉGRO	FRANCE
STROGO TAJNO	TRÈS SECRET DÉFENSE
TAJNO	SECRET DÉFENSE
POVJERLJIVO NSE	CONFIDENTIEL DÉFE
INTERNO	(voir ci-dessous paragraphes 2 et 3 de l'article 5)

- 5.2 La République française traite et protège les informations portant la mention « INTERNO », transmises par le Monténégro, conformément à ses lois et règlements nationaux en vigueur relatifs aux informations protégées mais non classifiées portant une mention telle que « DIFFUSION RESTREINTE ».
- 5.3 Le Monténégro traite et protège les informations non classifiées portant une mention indiquant qu'elles sont protégées telle que « DIFFUSION RESTREINTE », transmises par la République française, conformément à ses lois et règlements nationaux en vigueur relatifs à la protection des informations portant la mention «INTERNO ».
- 5.4 Pour des raisons de sécurité particulières, lorsque la Partie d'origine exige que l'accès à des informations classifiées soit limité aux personnes ayant exclusivement la nationalité des Parties, ces informations pourraient porter un avertissement de limitation supplémentaire, tel que « ISKLJUČIVO ZA DRŽAVLJANE CRNE GORE - FRANCUSKE » et « SPÉCIAL FRANCE - MONTÉNÉGRO ». Pour maintenir des normes de sécurité

comparables, chaque Partie fournit, à la demande de l'autre Partie, toutes les informations requises relatives aux lois, règlements et procédures nationaux en matière de sécurité qui sont appliqués pour assurer la sécurité des informations classifiées. Les Parties conviennent de faciliter les contacts entre leurs ANS et ASC respectives.

ARTICLE 6

Procédure d'habilitation de sécurité

- 6.1 En vue de l'accès aux informations classifiées au niveau « POVJERLJIVO » ou « CONFIDENTIEL DÉFENSE » ou à un niveau plus élevé, chaque Partie applique une procédure d'habilitation de sécurité individuelle conformément à ses lois et règlements nationaux.
- 6.2 L'ANS ou les ASC de chacune des Parties se prêtent mutuellement assistance, conformément à leurs lois et règlements nationaux, en vue de l'attribution d'une habilitation de sécurité individuelle à un ressortissant de l'une des Parties qui a séjourné ou se trouve encore sur le territoire de l'autre Partie.
- 6.3 L'ANS ou les ASC de chaque Partie appliquent à ses ressortissants, à la demande de l'ANS ou des ASC de l'autre Partie, une procédure d'habilitation de sécurité individuelle conformément à ses lois et règlements nationaux.
- 6.4 Les Parties reconnaissent mutuellement les habilitations de sécurité individuelles délivrées à leurs ressortissants dans le cadre de l'accès à des informations classifiées échangées en vertu du présent Accord.
- 6.5 Les ANS ou ASC se tiennent mutuellement informées immédiatement des changements qui affectent les habilitations de sécurité individuelles de leurs ressortissants relevant du présent Accord, en particulier en cas de retrait ou de déclassément d'une habilitation.

ARTICLE 7

Utilisation des informations classifiées

- 7.1 La Partie destinataire utilise les informations classifiées uniquement aux fins pour lesquelles elles ont été communiquées et dans les limites établies par la Partie d'origine.
- 7.2 La Partie destinataire ne divulgue à une tierce partie aucune information classifiée transmise, reçue ou créée en vertu du présent Accord, sans le consentement écrit préalable de l'ANS ou des ASC de la Partie d'origine.
- 7.3 Les informations classifiées élaborées conjointement par les Parties en vertu d'accords, de contrats ou dans le cadre de toute autre activité commune ne peuvent être déclassées, déclassifiées ou transférées par une Partie à une tierce partie sans le consentement écrit préalable de l'autre Partie.

ARTICLE 8

Traduction, reproduction et destruction

- 8.1 La Partie destinataire procède au marquage des reproductions et des traductions élaborées de manière identique aux informations classifiées d'origine et leur accorde la même protection.
- 8.2 Les informations classifiées « STROGO TAJNO » ou « TRÈS SECRET DÉFENSE » ne sont ni reproduites ni traduites par la Partie destinataire. Des documents originaux et des traductions supplémentaires peuvent être fournis sur demande écrite à la Partie d'origine.
- 8.3 Les informations classifiées « STROGO TAJNO » ou « TRÈS SECRET DÉFENSE » ne doivent pas être détruites par la Partie destinataire. Elles sont restituées à la Partie d'origine

conformément aux dispositions du paragraphe 1 de l'article 9 ci-dessous, lorsqu'il a été reconnu qu'elles ne sont plus nécessaires ou après la venue à expiration de leur validité.

- 8.4 La traduction et la reproduction d'informations classifiées « TAJNO » ou « SECRET DÉFENSE » sont autorisées uniquement avec le consentement écrit de l'ANS ou des ASC de la Partie d'origine.
- 8.5 Les informations classifiées « TAJNO » ou « SECRET DÉFENSE », « POVJERLJIVO » ou « CONFIDENTIEL DÉFENSE » sont détruites conformément aux lois et règlements nationaux de la Partie destinataire et de telle manière que leur reconstitution totale ou partielle soit impossible.
- 8.6 En cas de situation de crise rendant impossibles la protection et la restitution d'informations classifiées générées ou communiquées en vertu du présent Accord, les informations classifiées sont détruites immédiatement. L'ANS de la Partie destinataire informe immédiatement l'ANS de la Partie d'origine de la destruction des informations classifiées.

ARTICLE 9

Transmission d'informations entre les Parties

- 9.1 Les informations classifiées sont transmises par une Partie à l'autre Partie par la voie diplomatique, conformément aux lois et règlements nationaux de la Partie d'origine.
- 9.2 L'ANS ou les ASC peuvent, d'un commun accord, convenir de la transmission des informations classifiées par d'autres moyens.
- 9.3 La transmission d'une quantité significative d'informations classifiées est organisée entre les ANS ou les ASC des Parties au cas par cas.
- 9.4 La transmission électronique d'informations classifiées ou d'informations protégées de niveau « DIFFUSION RESTREINTE » s'effectue sous forme chiffrée au moyen des méthodes et dispositifs cryptographiques approuvés d'un commun accord par les ANS des Parties.

ARTICLE 10

Contrats classifiés

- 10.1 L'ANS ou les ASC de la Partie d'origine informent l'ANS ou les ASC de la Partie destinataire de tout contrat classifié avant tout échange d'informations classifiées. Cette notification doit préciser le niveau de classification le plus élevé des informations mises en œuvre dans le contrat classifié.
- 10.2 Une Partie désireuse de conclure, ou d'autoriser l'un de ses contractants à conclure, un contrat classifié de niveau « POVJERLJIVO » ou « CONFIDENTIEL DÉFENSE » ou de niveau plus élevé avec un contractant de l'autre Partie s'assure auprès de l'ANS ou des ASC de cette Partie que ledit contractant a reçu l'habilitation de sécurité des établissements au niveau requis en vue d'exécuter le contrat. À défaut d'une telle habilitation de sécurité, l'ANS ou les ASC de la Partie destinataire engagent une procédure visant à émettre l'habilitation au niveau requis.
- 10.3 Tout contrat classifié comprend une annexe de sécurité. Dans cette annexe de sécurité, l'ANS ou les ASC de la Partie d'origine précise les éléments nécessitant une protection de la part de la Partie destinataire, ainsi que le niveau de classification qu'il convient d'appliquer. Seule la Partie d'origine peut modifier le niveau de classification défini dans l'annexe de sécurité.
- 10.4 L'ANS ou les ASC de la Partie d'origine transmettent une copie de l'annexe de sécurité à l'ANS ou aux ASC de l'autre Partie.

- 10.5 L'ANS ou les ASC des Parties sur le territoire desquelles le travail doit être réalisé doivent faire en sorte que soit appliqué et maintenu un niveau de sécurité équivalent au niveau requis pour assurer la protection de leurs propres informations classifiées.
- 10.6 Avant de signer un contrat classifié avec un sous-traitant, le contractant reçoit l'autorisation de son ANS ou de ses ASC. Les sous-traitants se conforment aux mêmes exigences de sécurité que celles établies pour le contractant.
- 10.7 Avant de transmettre à des contractants des informations classifiées reçues de la Partie d'origine, l'ANS ou les ASC de la Partie destinataire :
- a) s'assurent que les contractants et leurs établissements sont en mesure de protéger comme il convient les informations classifiées ;
 - b) accordent le niveau d'habilitation requis aux établissements du contractant considéré ;
 - c) accordent le niveau d'habilitation individuelle requis aux personnes ayant « besoin d'en connaître » ;
 - d) s'assurent que toutes les personnes qui ont accès à des informations classifiées ont été informées de leurs devoirs et de leurs responsabilités résultant des lois et règlements nationaux applicables ;
 - e) effectuent les contrôles de la sécurité des établissements concernés conformément aux lois et règlements nationaux.
- 10.8 Si une Partie ou l'un de ses contractants souhaite recourir à un établissement de l'autre Partie pour un contrat classifié et si cet établissement est détenu ou contrôlé par une tierce partie, l'ANS ou les ASC de la Partie concernée en sont informées.

ARTICLE 11

Visites

- 11.1 Lorsqu'une visite permet d'accéder à des informations classifiées de niveau « STROGO TAJNO » ou « TRÈS SECRET DÉFENSE », les demandes de visite sont transmises par la voie diplomatique à l'ANS de la Partie d'accueil. Les demandes de visite sont adressées au moins trois (3) semaines avant la date de visite requise.
- 11.2 Les visites des établissements de l'une des Parties qui impliquent l'accès d'un représentant de l'autre Partie à des informations classifiées de niveau « TAJNO » ou « SECRET DÉFENSE » et « POVJERLJIVO » ou « CONFIDENTIEL DÉFENSE », ou les visites de sites dans le cadre desquelles un accès direct aux informations classifiées évoquées ci-dessus est possible, sont soumises à une demande de visite et à une autorisation écrite préalable de l'ANS ou des ASC de la Partie d'accueil.
- 11.3 Les visites des établissements de l'une des Parties par une tierce partie qui impliquent l'accès à des informations classifiées de niveau « POVJERLJIVO » ou « CONFIDENTIEL DÉFENSE » ou de niveau plus élevé, échangées entre les Parties ou produites par celles-ci, ou les visites de sites dans le cadre desquelles un accès direct à ce type d'informations est possible, sont soumises à l'autorisation écrite préalable de l'ANS ou des ASC de l'autre Partie.
- 11.4 Les visites mentionnées aux paragraphes 1 à 3 de l'article 11 nécessitent que tous les visiteurs justifient d'un niveau approprié d'habilitation de sécurité individuelle et du besoin d'en connaître.
- 11.5 Toute demande de visite doit comporter les renseignements suivants :
- a) le prénom, le nom, la date et le lieu de naissance, la nationalité et le numéro du passeport ou de la carte d'identité du visiteur ;

- b) le titre et la fonction du visiteur et le nom de l'organisme ou de l'institution qui l'emploie ;
- c) le niveau d'habilitation de sécurité du visiteur, authentifié par un certificat de sécurité fourni par l'ANS ou les ASC de la Partie requérante ;
- d) la date envisagée pour la visite et sa durée prévue ;
- e) l'objet de la visite et tous renseignements nécessaires précisant les sujets à traiter mettant en jeu des informations classifiées et le niveau de classification de celles-ci ;
- f) les noms des organismes, des établissements et des locaux qui font l'objet de la visite ;
- g) la date, la signature et le timbre officiel ou la signature électronique officiellement reconnue de l'ANS ou des ASC de la Partie requérante.

11.6 Chaque Partie peut demander une autorisation de visite pour une durée maximale de douze (12) mois. Si une visite n'a pas eu lieu dans les délais prévus par l'autorisation de visite, ou si une prorogation de la durée est nécessaire, la Partie requérante peut demander une nouvelle autorisation de visite, sous réserve que cette demande soit présentée au moins trois (3) semaines avant l'expiration de l'autorisation en cours.

11.7 Les visiteurs se conforment aux règlements de sécurité et aux instructions de la Partie d'accueil.

11.8 Les Parties peuvent établir une liste des personnels autorisés à effectuer plusieurs visites en rapport avec tout projet, programme ou contrat spécifique conformément aux modalités convenues par l'ANS ou les ASC des Parties.

11.9 Chaque Partie garantit la protection des données à caractère personnel des visiteurs conformément à ses lois et règlements nationaux.

ARTICLE 12

Atteintes à la sécurité

- 12.1 Toute atteinte à la sécurité relative à la protection d'informations classifiées transmises ou générées à la suite d'une coopération mutuelle fait l'objet d'une enquête conformément aux lois et règlements nationaux de la Partie sur le territoire de laquelle l'atteinte à la sécurité a eu lieu. L'autre Partie coopère à l'enquête, sur demande.
- 12.2 Sous réserve du paragraphe 1 de l'article 12, l'ANS ou les ASC sur le territoire desquelles l'atteinte à la sécurité a eu lieu informe dès que possible l'ANS ou les ASC de l'autre Partie.
- 12.3 L'autre Partie est informée des résultats de l'enquête mentionnée au paragraphe 1 de l'article 12 et reçoit un compte rendu final des raisons et de l'ampleur de l'atteinte à la sécurité.

ARTICLE 13

Dépenses

- 13.1 L'application des dispositions du présent Accord n'entraîne en principe aucune dépense spécifique.
- 13.2 Dans le cas contraire, chaque Partie prend en charge ses propres dépenses.

ARTICLE 14

Règlement des différends

- 14.1 Tout différend relatif à l'interprétation ou à l'application du présent Accord est réglé exclusivement par voie de consultations entre les Parties, en excluant tout recours à une tierce partie ou à une juridiction nationale ou internationale.

14.2 Pendant la durée du différend, les Parties s'engagent à respecter les obligations énoncées dans le présent Accord.

ARTICLE 15
Dispositions finales

15.1 Le présent Accord est conclu pour une durée indéterminée. Chacune des Parties notifie à l'autre Partie l'accomplissement des procédures internes requises en ce qui la concerne pour l'entrée en vigueur du présent Accord. Le présent Accord prend effet le premier jour du deuxième mois suivant la réception de la dernière des notifications.

15.2 L'ANS ou les ASC des Parties peuvent se consulter en tant que de besoin au sujet des aspects techniques spécifiques relatifs à l'application du présent Accord et conclure les arrangements de mise en œuvre nécessaires.

15.3 Les dispositions du présent Accord peuvent être modifiées par accord écrit entre les Parties. Les modifications prennent effet selon les modalités prévues au paragraphe 1 de l'article 15.

15.4 Le présent Accord peut être dénoncé soit d'un commun accord soit unilatéralement. La notification de dénonciation prend effet six (6) mois après réception de la notification écrite. La notification de dénonciation n'a aucun effet sur les droits et obligations des Parties relatifs aux informations transmises, reçues ou générées en vertu du présent Accord.

EN FOI DE QUOI, les représentants des deux Parties dûment autorisés à cet effet ont signé le présent Accord et y ont apposé leur sceau.

Signé à, le, en deux exemplaires originaux, en langues monténégrine et française, les deux textes faisant également foi.

Pour le Gouvernement du Monténégro

**Pour le Gouvernement de
la République française**
