Na osnovu člana 21 stav 2 Zakona o zaključivanju i izvršavanju međunarodnih ugovora („Službeni list CG“, broj 77/08), Vlada Crne Gore na sjednici od _____2018. godine, donijela je

ODLUKU
O OBJAVLJIVANJU SPORAZUMA IZMEĐU VLADE CRNE GORE I VLADE SAVEZNE REPUBLIKE NJEMAČKE O UZAJAMNOJ ZAŠTITI TAJNIH PODATAKA

Član 1

Objavljuje se Sporazum između Vlade Crne Gore i Vlade Savezne Republike Njemačke o uzajamnoj zaštiti tajnih podataka potpisan u Podgorici, 11. maja 2018. godine, u dva originala, svaki na crnogorskom, njemačkom i engleskom jeziku.

Član 2

Tekst Sporazuma iz člana 1 ove odluke, u originalu na crnogorskom i engleskom jeziku glasi:

Sporazum između
Vlade Crne Gore i
Vlade Savezne Republike Njemačke o
uzajamnoj zaštiti tajnih podataka

Vlada Crne Gore

i

Vlada Savezne Republike Njemačke,

u cilju obezbjeđivanja zaštite tajnih podataka koji se razmjenjuju između nadležnih organa Crne Gore i Savezne Republike Njemačke kao i sa izvršiocima posla na teritoriji druge ugovorne strane ili između izvršilaca posla dviju ugovornih strana,

želeći da postignu sporazum o uzajamnoj zaštiti tajnih podataka koji će se primjenjivati na sve sporazume o saradnji koji će se zaključivati između ugovornih strana i na ugovore koji podrazumijevaju razmjenu tajnih podataka,

sporazumjele su se o sljedećem:

Član 1

Definicije

(1) U smislu ovog Sporazuma

1. tajni podaci su:
   a) u Crnoj Gori

      podaci čijim bi otkrivanjem nepozvanom licu nastupile ili mogle nastupiti štetne posljedice za bezbjednost i odbranu, vanjsku, monetarnu i ekonomsku politiku Crne Gore;
   b) u Saveznoj Republici Njemačkoj

      činjenice, predmeti ili podaci koji, nezavisno od oblika u kojem se pojavljuju, u javnom interesu moraju ostati tajni. U skladu sa potrebom za njihovom zaštitom, njihov stepen tajnosti se određuje od strane ili na zahtjev službenog organa;
2. povjerljiv ugovor je

   ugovor između organa ili pravnog lica države jedne ugovorne strane (naručilac posla) i pravnog lica iz države druge ugovorne strane (izvršilac posla); po takvom ugovoru, tajni podaci iz države naručioca posla će biti ustupljeni izvršiocu posla, generisani od strane izvršioca posla ili učinjeni dostupnim licima zaposlenim kod izvršioca posla koji izvršavaju poslove u objektima naručioca posla.

(2) Stepeni tajnosti se definišu na sljedeći način:
1. U Saveznoj Republici Njemačkoj tajni podaci su
   a) GEHEIM ako otkrivanje tajnog podatka neovlašćenim licima može predstavljati prijetnju za bezbjednost Savezne Republike Njemačke ili jedne od njenih pokrajina ili nanijeti ozbiljnu štetu njihovim interesima;
   b) VS-VERTRAULICH ako otkrivanje tajnog podatka neovlašćenim licima može škoditi interesima Savezne Republike Njemačke ili jedne od njenih pokrajina;
   c) VS-NUR FÜR DEN DIENSTGEBRAUCH ako otkrivanje tajnog podatka neovlašćenim licima može biti smetnja interesima Savezne Republike Njemačke ili jedne od njenih pokrajina.
2. U Crnoj Gori
   a) stepen TAJNO se određuje za podatke čijim bi otkrivanjem mogle nastupiti teže štetne posljedice za bezbjednost i interese Crne Gore;
   b) stepen POVJERLJIVO se određuje za podatke čijim bi otkrivanjem mogle nastupiti štetne posljedice za bezbjednost i interese Crne Gore;
   c) stepen INTERNO se određuje za podatke čijim bi otkrivanjem mogle nastupiti štetne posljedice za ostvarivanje funkcije organa.

Član 2

Ekvivalentnost

Ugovorne strane određuju da su sljedeći stepeni tajnosti ekvivalentni:

Crna Gora	Engleski	Savezna Republika Njemačka
TAJNO	SECRET	GEHEIM
POVJERLJIVO	CONFIDENTIAL	VS-VERTRAULICH
INTERNO	RESTRICTED	VS-NUR FÜR DEN DIENSTGEBRAUCH

Član 3

Označavanje

(1) Proslijeđeni tajni podaci se označavaju ekvivalentnim nacionalnim stepenima tajnosti kao što je predviđeno u članu 2 od strane ili na zahtjev organa nadležnog za primaoca tih podataka.

(2) Tajni podaci koji nastaju u državi primaocu u vezi sa povjerljivim ugovorima kao i kopije tajnih podataka koje se izrađuju u državi primaocu takođe moraju biti označeni.

(3) Na zahtjev nadležnog organa ugovorne strane porijekla, stepeni tajnosti će biti promijenjeni ili ukinuti od strane ili po nalogu organa nadležnog za primaoca predmetnog tajnog podatka. Nadležni organ ugovorne strane porijekla će šest nedjelja unaprijed obavijestiti nadležni organ druge ugovorne strane o svojoj namjeri da izmijeni ili ukine stepen tajnosti.

Član 4

Mjere na nacionalnom nivou

(1) U okviru svog nacionalnog zakonodavstva, ugovorne strane će preduzeti sve odgovarajuće mjere kako bi garantovale zaštitu tajnih podataka, koji nastaju, razmjenjuju se ili se čuvaju u skladu sa odredbama ovog Sporazuma. Ugovorne strane će takvim tajnim podacima obezbijediti stepen zaštite tajnosti bar jednak stepenu zaštite tajnosti koji ugovorna strana primalac zahtijeva za svoje podatke ekvivalentnog stepena tajnosti.

(2) Tajni podaci će se koristiti isključivo u svrhu za koju su namijenjeni. Ugovorna strana primalac ne smije ih otkrivati ili koristiti, ili dozvoliti njihovo otkrivanje ili korišćenje osim u svrhu i uz eventualna ograničenja naznačena od strane ili u ime ugovorne strane porijekla. Za svako drugo postupanje strana porijekla mora dostaviti pisanu saglasnost.

(3) Pristup tajnim podacima će se dozvoliti isključivo licima koja ispunjavaju princip "potrebno je da zna", u cilju ispunjavanja njihovih dužnosti, i koja - osim u slučaju tajnih podataka označenih stepenom tajnosti INTERNO / VS-NUR FÜR DEN DIENSTGEBRAUCH - imaju dozvolu za pristup tajnim podacima ekvivalentnog stepena tajnosti. Dozvola za pristup tajnim podacima će biti izdata tek po završetku bezbjednosne provjere koja se sprovodi po standardima ne nižim od onih koji se primjenjuju za pristup nacionalnim tajnim podacima ekvivalentnog stepena tajnosti.

(4) Pristup tajnim podacima stepena tajnosti POVJERLJIVO / VS-VERTRAULICH i više biće odobren bez prethodnog ovlašćenja ugovorne strane porijekla licu koje posjeduje isključivo državljanstvo jedne od ugovornih strana.

(5) Bezbjednosne provjere državljana jedne od ugovornih strana koji imaju prebivalište na teritoriji države te ugovorne strane i kojima je potreban pristup tajnim podacima u svojoj državi sprovodiće nadležna Nacionalna bezbjednosna agencija odnosno ovlašćeni bezbjednosni organi te države ili drugi nadležni nacionalni organi.

(6) Bezbjednosne provjere državljana jedne od ugovornih strana koji imaju legalno prebivalište na teritorijii države druge ugovorne strane najmanje pet godina i prijavljuju se za bezbjednosno osjetljiv posao u toj državi sprovodiće nadležni bezbjednosni organ te ugovorne strane koji će pri tom eventualno zatražiti bezbjednosne informacije u inostranstvu u skladu sa nacionalnim zakonima i propisima.

(7) Ugovorne strane će, svaka na svojoj teritoriji, obezbijediti sprovođenje potrebnih bezbjednosnih inspekcija i implementaciju odredbi ovog Sporazuma.

(8) Članovi 5 i 6 ovog Sporazuma se ne odnose na tajne podatke stepena INTERNO / VS-NUR FÜR DEN DIENSTGEBRAUCH.

Član 5

Zaključivanje povjerljivih ugovora

(1) Prije zaključivanja povjerljivog ugovora, naručilac posla će preko organa nadležnog za njega pribaviti bezbjednosnu dozvolu za pristup tajnim podacima od organa nadležnog za izvršioca posla kako bi se uvjerio da li potencijalni izvršilac posla podliježe bezbjednosnom nadzoru i provjeri od strane nadležnih organa te države i da li je preduzeo mjere zaštite tajnosti neophodne za izvršenje ovog ugovora. U slučaju da izvršilac posla još ne podliježe bezbjednosnom nadzoru i provjeri, može se podnijeti zahtjev u tu svrhu.

(2) Bezbjednosna dozvola za pristup tajnim podacima će se takođe pribaviti ako pravno lice treba da dostavi ponudu te će već, u okviru tendera, prije zaključivanja povjerljivog ugovora, tajni podaci biti ustupljeni.

(3) U slučajevima koji se odnose na stav (1) i (2) ovog člana primijeniće se sljedeća procedura:

1. Zahtjevi za izdavanje bezbjednosne dozvole za pristup tajnim podacima za izvršioce posla iz države druge ugovorne strane moraju sadržati informacije o projektu kao i o prirodi, obimu i stepenu tajnosti tajnih podataka za koje se očekuje da će biti ustupljeni izvršiocu posla ili koji će nastati kod njega.
2. Osim punog naziva pravnog lica i njegove adrese, imena njegovog službenika za bezbjednost, njegovog broja telefona i faksa i po potrebi email adrese, bezbjednosne dozvole za pristup tajnim podacima moraju prije svega sadržati informacije u kojem obimu

i do kojeg stepena tajnosti je pravno lice na osnovu nacionalnih bezbjednosnih propisa preduzelo mjere zaštite tajnosti.

3. Nadležni organi ugovornih strana će obavijestiti jedni druge o bilo kakvim promjenama činjenica na osnovu kojih su izdate bezbjednosne dozvole za pristup tajnim podacima.
4. Razmjena takvih informacija između nadležnih organa ugovornih strana će se vršiti na nacionalnom jeziku organa kojem se upućuje obavještenje ili na engleskom jeziku.
5. Bezbjednosne dozvole za pristup tajnim podacima i zahtjevi za izdavanje bezbjednosnih dozvola za pristup tajnim podacima, upućeni nadležnim organima ugovornih strana, biće predati u pisanoj formi.

Član 6

Realizacija povjerljivih ugovora

(1) Povjerljivi ugovori moraju sadržati klauzulu o zaštiti tajnosti po kojoj izvršilac posla ima obavezu da preduzme mjere potrebne za zaštitu tajnih podataka u skladu sa nacionalnim propisima o zaštiti tajnosti.

(2) Pored toga, klauzula o zaštiti tajnosti će sadržati sljedeće odredbe:

1. definiciju izraza "tajni podaci" i definiciju ekvivalentnih oznaka i stepena tajnosti dviju ugovornih strana u skladu sa odredbama ovoga Sporazuma;
2. nazive nadležnih organa ugovornih strana koji su ovlašćeni za odobrenje ustupanja tajnih podataka povezanih sa povjerljivim ugovorom kao i za koordinaciju njihove zaštite;
3. sredstva koja će se koristiti za prenos tajnih podataka između nadležnih organa i izvršilaca posla koji su u to uključeni;
4. procedure i mehanizme za obavještavanje o izmjenama koje mogu nastati u pogledu tajnih podataka, zbog promjene stepena tajnosti ili zato što zaštita više nije potrebna;
5. procedure za odobrenje posjeta ili pristupa od strane lica zaposlenih kod izvršilaca posla;
6. procedure za prenos tajnih podataka izvršiocima posla koji će takve podatke koristiti i čuvati;
7. zahtjev da izvršilac posla omogući pristup tajnim podacima isključivo licu koje ispunjava princip "potrebno je da zna" i koje je zaduženo za realizaciju povjerljivih ugovora ili učestvuje u tome i koje je – osim u slučaju tajnih podatka stepena tajnosti INTERNO / VS-NUR FÜR DEN DIENSTGEBRAUCH – unaprijed bezbjednosno provjereno do odgovarajućeg stepena tajnosti;
8. zahtjev da se tajni podatak ustupi licu, odnosno da se dozvoli njegovo ustupanje, jedino uz saglasnost ugovorne strane porijekla;
9. zahtjev da izvršilac posla bez odlaganja obavijesti organ nadležan za njega o svakom stvarnom gubitku, neovlašćenom ustupanju ili neovlašćenom otkrivanju tajnih podataka ili

sumnji na gubitak, neovlašćeno ustupanje ili neovlašćeno otkrivanje tajnih podataka koji su obuhvaćeni povjerljivim ugovorom.

(3) Organ koji je nadležan za naručioca posla će, na posebnoj listi (lista stepena tajnosti), dostaviti izvršiocu posla popis svih podataka za koje je potrebno odrediti stepen tajnosti, te će odrediti potreban stepen tajnosti i obezbijediti da se ova lista priloži kao prilog povjerljivom ugovoru. Organ koji je nadležan za naručioca posla će takođe poslati ili obezbijediti prenos ove liste organu koji je nadležan za izvršioca posla.

(4) Organ koji je nadležan za naručioca posla će obezbijediti da se izvršiocu posla omogući pristup tajnim podacima tek nakon prijema odgovarajuće bezbjednosne dozvole za pristup tajnim podacima od strane organa nadležnog za izvršioca posla.

Član 7

Prenos tajnih podataka

(1) Tajni podaci stepena tajnosti POVJERLJIVO / VS-VERTRAULICH i TAJNO / GEHEIM će se prenositi iz jedne države u drugu isključivo putem službenog kurira. Nacionalne bezbjednosne agencije odnosno ovlašćeni bezbjednosni organi ugovornih strana se mogu dogovoriti o alternativnim načinima prenosa. Prijem tajnih podataka se potvrđuje od strane, ili na zahtjev, nadležnog organa i takvi tajni podaci se prosljeđuju primaocu u skladu sa nacionalnim propisima o zaštiti tajnosti.

(2) Za posebno određeni projekat, nadležni organi se mogu dogovoriti – uopšteno ili uz ograničenja – da se tajni podaci stepena tajnosti POVJERLJIVO / VS-VERTRAULICH i TAJNO / GEHEIM mogu prenositi i na drugi način, a ne službenim kurirom, ukoliko bi prenos putem službenog kurira mogao proizvesti neprihvatljive poteškoće za prenos ili realizaciju povjerljivog ugovora. U tim slučajevima

1. nosilac mora biti ovlašćen za pristup tajnim podacima ekvivalentnog stepena tajnosti;
2. listu tajnih podataka koji se prenose zadržava pošiljalac; kopija ove liste će se predati primaocu za prosljeđivanje nadležnom organu;
3. tajni podaci moraju se pakovati u skladu sa propisima kojima se uređuje prenos podataka unutar državnih granica;
4. dostava tajnih podataka se vrši uz potvrdu o prijemu;
5. nosilac mora posjedovati kurirsko uvjerenje izdato od strane nadležnog organa pošiljaoca ili primaoca.

(3) Kada se vrši prenos većeg broja tajnih podataka sredstva transporta, ruta i pratnja će se odrediti za svaki pojedinačni slučaj i na osnovu detaljnog plana o prenosu podataka od strane nadležnih organa.

(4) Elektronski prenos tajnih podataka stepena tajnosti POVJERLJIVO / VS-VERTRAULICH i višeg se ne vrši u nekriptovanoj formi. Tajni podaci ovih stepena tajnosti će se kriptovati isključivo

sredstvima kriptovanja koja su odobrena međusobnim sporazumom između nadležnih bezbjednosnih organa ugovornih strana.

(5) Tajni podaci stepena tajnosti INTERNO / VS-NUR FÜR DEN DIENSTGEBRAUCH mogu se prenositi poštom ili drugim dostavnim službama primaocima na teritoriji druge ugovorne strane, vodeći računa o nacionalnim propisima zaštite tajnosti.

(6) Tajni podaci stepena tajnosti INTERNO / VS-NUR FÜR DEN DIENSTGEBRAUCH se mogu prenositi ili ustupiti elektronskim putem komercijalnim sredstvima kriptovanja koja su odobrena od strane jednog od nadležnih nacionalnih organa ugovornih strana. Tajni podaci ovog stepena tajnosti se mogu slati u nekriptovanoj formi jedino ukoliko to nije u protivurječnosti sa nacionalnim propisima zaštite tajnosti, ukoliko nijedno odobreno sredstvo kriptovanja nije dostupno, ukoliko se prenos obavlja samo u okviru mreža fiksne telefonije i ukoliko su pošiljalac i primalac prethodno postigli dogovor o predloženom prenosu.

Član 8

Posjete

(1) Posjetiocima sa teritorije jedne ugovorne strane će se na teritoriji druge ugovorne strane odobriti pristup tajnim podacima i objektima u kojima se rukuje sa tajnim podacima jedino uz prethodnu dozvolu nadležnog organa ugovorne strane zemlje koja se posjećuje. Takva dozvola će se dati samo licima koja ispunjavaju princip "potrebno je da zna" i koja – osim u slučaju tajnog podatka stepena tajnosti INTERNO / VS-NUR FÜR DEN DIENSTGEBRAUCH –posjeduju dozvolu za pristup tajnim podacima.

(2) Zahtjevi za posjete se podnose nadležnom organu države čiju teritoriju posjetioci žele da posjete blagovremeno i u skladu sa propisima te države. Nadležni organi će obavijestiti jedni druge o detaljima koji se tiču posjeta i obezbijediti zaštitu ličnih podataka.

(3) Zahtjevi za posjete se podnose na jeziku zemlje koja se posjećuje ili na engleskom jeziku i sadrže sljedeće informacije:

1. ime i prezime posjetioca, datum i mjesto rođenja i broj lične karte ili pasoša;
2. državljanstvo posjetioca;
3. funkciju posjetioca i naziv organa ili institucije čiji je on predstavnik;
4. stepen tajnosti za koji je izdata dozvola za pristup tajnim podacima posjetiocu;
5. svrhu posjete i predloženi datum posjete;
6. organe, kontakt osobe i objekte koji će se posjetiti;

Član 9

Konsultacije

(1) Nadležni organi ugovornih strana će voditi računa o odredbama koje se tiču zaštite tajnih podataka a koje se primjenjuju na teritoriji druge ugovorne strane.

(2) Da bi obezbijedili blisku saradnju tokom implementacije ovog Sporazuma, nadležni organi će konsultovati jedni druge na zahtjev jednog od ovih organa.

(3) Svaka ugovorna strana će, pored toga, dozvoliti Nacionalnoj bezbjednosnoj agenciji ili nadležnom bezbjednosnom organu druge ugovorne strane ili bilo kojem drugom organu određenim međusobnim sporazumom, da posjeti njenu teritoriju kako bi sa njenim bezbjednosnim organima ocijenio procedure i objekte za zaštitu tajnih podataka koje je ustupila druga ugovorna strana. Svaka ugovorna strana će pomagati tom organu u vršenju provjere da li su tajni podaci koja je ustupila druga ugovorna strana adekvatno zaštićeni. Detalji posjeta će biti utvrđeni od strane nadležnih organa.

Član 10

Kršenje odredbi o uzajamnoj zaštiti tajnih podataka

(1) Kada se ne može isključiti neovlašćeno otkrivanje tajnih podataka ili kada se takvo otkrivanje utvrdi ili se na njega sumnja, druga ugovorna strana će odmah biti obaviještena o tome.

(2) Istragu i gonjenje kršenja odredbi o zaštiti tajnih podataka vrše nadležni organi i sudovi ugovorne strane u čijoj je to nadležnosti, a u skladu sa zakonom te ugovorne strane. Druga ugovorna strana će, na zahtjev, pružiti pomoć u tim istragama i biće obaviještena o njihovom ishodu.

Član 11

Troškovi

Svaka ugovorna strana snosi svoje troškove koji nastaju implementacijom ovog Sporazuma.

Član 12

Nadležni organi

Ugovorne strane će obavijestiti jedna drugu o organima odgovornim za implementaciju ovog Sporazuma.

Član 13

Odnos prema drugim sporazumima, ugovorima i dogovorima

Ovaj sporazum ne utiče na bilo koji postojeći sporazum, ugovor i dogovor o zaštiti tajnih podataka između ugovornih strana ili nadležnih organa ukoliko nisu u protivurječnosti sa odredbama ovog Sporazuma.

Član 14

Završne odredbe

(1) Ovaj Sporazum stupa na snagu danom potpisivanja.

(2) Ovaj Sporazum se zaključuje na neodređeni vremenski period.

(3) Ovaj Sporazum se može izmijeniti i dopuniti pisanim putem međusobnim sporazumom između ugovornih strana. Svaka ugovorna strana može, u bilo koje vrijeme, podnijeti pisani zahtjev za izmjene i dopune ovog Sporazuma. Ukoliko jedna od ugovornih strana podnese takav zahtjev, ugovorne strane će inicirati pregovore o izmjenama i dopunama ovog Sporazuma.

(4) Svaka ugovorna strana može, podnoseći obavještenje u pisanoj formi šest mjeseci unaprijed, diplomatskim putem, otkazati ovaj Sporazum. U slučaju otkaza Sporazuma, tajni podaci koji su ustupljeni ili su nastali kod izvršioca posla i dalje će biti tretirani u skladu sa odredbama člana 4 ovog Sporazuma dok god to zahtijeva postojeći stepen tajnosti.

(5) Registraciju ovog Sporazuma u Sekretarijatu Ujedinjenih nacija u skladu sa članom 102 Povelje Ujedinjenih nacija će, odmah po njegovom stupanju na snagu, pokrenuti ugovorna strana na čijoj teritoriji je ovaj Sporazum zaključen. Druga ugovorna strana će biti obaviještena o registraciji i registarskom broju UN čim se registracija potvrdi od strane Sekretarijata Ujedinjenih nacija.

Sačinjeno u Podgorici, dana11.maja 2018.godine u dva originala, svaki na crnogorskom, njemačkom i engleskom jeziku, pri čemu su sva tri teksta jednako vjerodostojna. U slučaju različitih tumačenja tekstova na crnogorskom i njemačkom jeziku, mjerodavan je tekst na engleskom jeziku.

Za Vladu	Za Vladu
Crne Gore	Savezne Republike Njemačke
Savo Vučinić, s.r.	Hans Gunther Mattern, s.r.

Agreement between
the Government of Montenegro and
the Government of the Federal Republic of Germany
on the
Mutual Protection of Classified Information

The Government of Montenegro
and
the Government of the Federal Republic of Germany,

Intending to ensure the protection of classified information that is exchanged between the competent authorities of Montenegro and the Federal Republic of Germany as well as with contractors in the territory of the other Contracting Party or between contractors of the two Contracting Parties,

Desirous of laying down an arrangement on the mutual protection of classified information that shall apply to all agreements on cooperation to be concluded between the Contracting Parties and to contracts involving an exchange of classified information,

Have agreed as follows:

Article 1
Definitions

(1) For the purposes of this Agreement

1. "classified information" is

a) in the Federal Republic of Germany
facts, items or intelligence which, regardless of how they are presented, are to be kept secret in the public interest. They shall be classified by, or at the instance of, an official agency in accordance with their need for protection;

b) in Montenegro
information the disclosure of which to unauthorized persons has or may have adverse effects on the security and defence of Montenegro or its foreign, monetary and economic affairs;

2. a “classified contract” is

a contract between an authority or a legal entity from the country of one Contracting Party (contract owner) and a legal entity from the country of the other Contracting Party (contractor); under such contract, classified information from the country of the contract owner is to be released to the contractor, is to be generated by the contractor or is to be made accessible to members of the contractor’s staff who are to perform tasks in facilities of the contract owner.

(2) The levels of security classification are defined as follows:

1. In the Federal Republic of Germany, classified information is
   a) GEHEIM if knowledge of it by unauthorized persons may pose a threat to the security of the Federal Republic of Germany or one of its states (*Länder*), or may cause severe damage to their interest;
   b) VS-VERTRAULICH if knowledge of it by unauthorized persons may be damaging to the interests of the Federal Republic of Germany or one of its states (*Länder*);
   c) VS-NUR FÜR DEN DIENSTGEBRAUCH if knowledge of it by unauthorized persons may be disadvantageous to the interests of the Federal Republic of Germany or one of its states (*Länder*).
2. In Montenegro
   a) TAJNO classification shall be applied to classified information the disclosure of which could seriously harm the security or interests of Montenegro;
   b) POVJERLJIVO classification shall be applied to classified information the disclosure of which could harm the security or interests of Montenegro;
   c) INTERNO classification shall be applied to classified information the disclosure of which could harm the performance of tasks of an entity.

Article 2

Comparability

The Contracting Parties stipulate that the following security classifications shall be comparable:

Montenegro	**English**	**Federal Republic of Germany**
TAJNO	SECRET	GEHEIM
POVJERLJIVO	CONFIDENTIAL	VS-VERTRAULICH
INTERNO	RESTRICTED	VS-NUR FÜR DEN DIENSTGEBRAUCH

Article 3

Marking

(1) Transmitted classified information shall be marked with the comparable national security classification as provided under Article 2 by, or at the instance of, the competent authority of the recipient.

(2) Classified information which is generated in the receiving country in connection with classified contracts as well as copies of the classified information which are made in the receiving country shall also be marked.

(3) Security classifications shall, at the request of the competent authority of the originating Contracting Party, be amended or revoked by, or at the instance of, the competent authority of the recipient of the given classified information. The competent authority of the originating Contracting Party shall, six weeks in advance, inform the competent authority of the other Contracting Party of its intention to amend or revoke a security classification.

Article 4

Measures at the National Level

(1) Within the scope of their national legislation, the Contracting Parties shall take all appropriate measures to guarantee the security protection of classified information generated, exchanged or held under the terms of this Agreement. They shall afford such classified information a degree of security protection at least equal to that required by the receiving Contracting Party for its own classified information of the comparable level of security classification.

(2) The classified information shall be used solely for the designated purpose. The receiving Contracting Party shall not disclose or use, or permit the disclosure or use of, any classified information except for the purposes and within any limitations stated by or on behalf of the originating Contracting Party. The originator of the classified information must have given its written consent to any arrangement to the contrary.

(3) Access to classified information may be granted only to persons having a need-to-know on account of their duties and – except in the case of classified information at the INTERNO / VS-NUR FÜR DEN DIENSTGEBRAUCH level – having been authorized to have access to classified information of the comparable level of security classification. A security clearance shall be granted only after completion of a security screening under standards no less stringent than those applied for access to national classified information of the comparable level of the security classification.

(4) Access to classified information at the POVJERLJIVO / VS-VERTRAULICH level or higher by a person having sole nationality of a Contracting Party shall be granted without prior authorization of the originating Contracting Party.

(5) Personal Security Clearances for nationals of one Contracting Party residing, and requiring access to classified information, in the territory of the country of that Contracting Party shall be

undertaken by their National Security Authority (NSA) / Designated Security Authorities (DSAs) or other competent national authorities.

(6) However, Personal Security Clearances for nationals of one Contracting Party who have been legally resident in the territory of the country of the other Contracting Party for at least five years and apply for a security-sensitive job in that country shall be undertaken by the competent security authority of that Contracting Party, conducting overseas checks as appropriate in accordance with its national laws and regulations.

(7) The Contracting Parties shall, each within its territory, ensure that the necessary security inspections are carried out and that this Agreement is complied with.

(8) Article 5 and Article 6 of this Agreement shall not apply to classified information at the INTERNO / VS-NUR FÜR DEN DIENSTGEBRAUCH level.

Article 5

Award of Classified Contracts

(1) Prior to the award of a classified contract, the contract owner shall, through its competent authority, obtain a Facility Security Clearance from the competent authority of the contractor in order to obtain assurance as to whether the prospective contractor is subject to security oversight by the competent authority of this country and whether it has taken the security precautions required for discharging the performance of the contract. Where a contractor is not yet subject to security oversight, an application may be made to that end.

(2) A Facility Security Clearance shall also be obtained if a legal entity has been requested to submit a bid and if classified information will have to be released prior to the award of a contract under the bid procedure.

(3) In the cases referred to in paragraphs (1) and (2) above, the following procedure shall be applied:

1. Requests for the issuance of a Facility Security Clearance for contractors from the country of the other Contracting Party shall contain information on the project as well as the nature, the scope and the level of security classification of the classified information expected to be released to the contractor or to be generated by it.
2. In addition to the full name of the legal entity, its postal address and the name, telephone and fax number and, if applicable, e-mail address of its security official, Facility Security Clearances must include information in particular on the extent to which, and the level of security classification up to which, security measures have been taken by the respective legal entity on the basis of national security regulations.
3. The competent authorities of the Contracting Parties shall inform each other of any changes in the facts forming the basis of the issued Facility Security Clearances.

4. The exchange of such information between the competent authorities of the Contracting Parties shall be effected either in the national language of the authority to be informed or in English.
5. Facility Security Clearances and requests addressed to the respective competent authorities of the Contracting Parties for the issuance of Facility Security Clearances shall be transmitted in writing.

Article 6

Performance of Classified Contracts

(1) Classified contracts must contain a security requirement clause under which the contractor is under an obligation to make the arrangements required for the protection of classified information pursuant to the national security regulations of its country.

(2) In addition, the security requirement clause shall contain the following provisions:

1. the definition of the term "classified information" and of the comparable levels of protective markings and security classifications of the two Contracting Parties in accordance with the provisions of this Agreement;
2. the names of the competent authority of each of the two Contracting Parties empowered to authorize the release and to coordinate the safeguarding of classified information related to the contract;
3. the channels to be used for the transfer of classified information between the competent authorities and contractors involved;
4. the procedures and mechanisms for communicating changes that may arise in respect of classified information either because of changes in its protective markings or because protection is no longer necessary;
5. the procedures for the approval of visits, or access, by personnel of the contractors;
6. the procedures for transmitting classified information to contractors where such information is to be used and held;
7. the requirement that the contractor shall grant access to classified information only to a person who has a need-to-know and has been charged with, or contributes to, the performance of the contracts and – except in the case of classified information at the INTERNO / VS-NUR FÜR DEN DIENSTGEBRAUCH level – has been security-cleared to the appropriate level in advance;
8. the requirement that classified information shall only be disclosed to a person, or that such disclosure shall only be permitted, if this has been approved by the originating Contracting Party;

9. the requirement that the contractor shall immediately notify its competent authority of any actual or suspected loss, leak or unauthorized disclosure of the classified information covered by the contract.

(3) The competent authority of the contract owner shall provide the contractor with a separate list (classification guide) of all documentary records requiring security classification, shall determine the required level of security classification and shall arrange for this list to be enclosed as an appendix to the classified contract. The competent authority of the contract owner shall also transmit, or arrange for the transmission of, the list to the competent authority of the contractor.

(4) The competent authority of the contract owner shall ensure that the contractor will be given access to classified information only after the pertinent Facility Security Clearance has been received from the competent authority of the contractor.

Article 7

Transmission of Classified Information

(1) As a matter of principle, classified information at the POVJERLJIVO / VS-VERTRAULICH and TAJNO / GEHEIM levels shall be transmitted from one country to another by official courier. The National Security Authorities / Designated Security Authorities of the Contracting Parties may agree on alternative channels of transmission. Receipt of classified information shall be confirmed by, or at the instance of, the competent authority and the classified information shall be forwarded to the recipient in accordance with national security regulations.

(2) For a specifically designated project, the competent authorities may agree – generally or subject to restrictions – that classified information at the POVJERLJIVO / VS-VERTRAULICH and TAJNO / GEHEIM levels may be transmitted through channels other than official courier if reliance on the official courier service would cause undue difficulties for such transportation or for the execution of a contract. In such cases

1. the bearer must be authorized to have access to classified information of the comparable level of security classification;
2. a list of the items of classified information transmitted must be retained by the dispatching agency; a copy of this list shall be handed over to the recipient for forwarding to the competent authority;
3. items of classified information must be packed in accordance with the regulations governing transportation within national boundaries;
4. items of classified information must be delivered against receipt;
5. the bearer must carry a courier certificate issued by the competent authority of the dispatching or the receiving agency.

(3) Where large volumes of classified information are to be transmitted, the means of transportation, the route, and the escort shall be determined on a case-by-case basis by the competent authorities on the basis of a detailed transport plan.

(4) The electronic transmission of classified information at the POVJERLJIVO / VS-VERTRAULICH level and higher must not take place in an unencrypted form. Classified information of these levels of security classification may only be encrypted by encryption means approved by mutual agreement by the competent security authorities of the Contracting Parties.

(5) Classified information at the INTERNO / VS-NUR FÜR DEN DIENSTGEBRAUCH level may be transmitted by post or other delivery services to recipients within the territory of the other Contracting Party, taking into account national security regulations.

(6) Classified information at the INTERNO / VS-NUR FÜR DEN DIENSTGEBRAUCH level may be electronically transmitted or made available by means of commercial encryption devices approved by a competent national authority of the Contracting Parties. Classified information of this level of security classification may only be transmitted in an unencrypted form provided that this does not conflict with national security regulations, no approved encryption means are available, transmission is effected within fixed networks only and the sender and the recipient have reached agreement on the proposed transmission in advance.

Article 8

Visits

(1) As a matter of principle, it is only with the prior permission of the competent authority of the Contracting Party whose country is to be visited that visitors from the territory of one Contracting Party will, in the territory of the other Contracting Party, be granted access to classified information and to facilities in which classified information is being handled. Such permission shall be given only to persons having a need-to-know and – except in the case of classified information at the INTERNO / VS-NUR FÜR DEN DIENSTGEBRAUCH level – having been authorized to have access to classified information.

(2) Requests for visits shall be submitted, on a timely basis and in accordance with the regulations of the country whose territory such visitors wish to enter, to the competent authority of that country. The competent authorities shall inform each other of the details regarding such requests and shall ensure that personal data are protected.

(3) Requests for visits shall be submitted in the language of the country to be visited or in English and shall contain the following information:

1. the visitor's first name and surname, date and place of birth, and his/her passport or identity card number;
2. the visitor's nationality;
3. the visitor's service designation, and the name of his/her parent authority or agency;

4. the level of the visitor's security clearance for access to classified information;
5. the purpose of the visit, and the proposed date of the visit;
6. the designation of the agencies, the contact persons and the installations to be visited.

Article 9

Consultations

(1) The competent authorities of the Contracting Parties shall take note of the provisions governing the protection of classified information that apply within the territory of the other Contracting Party.

(2) To ensure close cooperation in the implementation of this Agreement, the competent authorities shall consult each other at the request of one of these authorities.

(3) Each Contracting Party shall, in addition, allow the National or Designated Security Authority of the other Contracting Party or any other authority designated by mutual agreement to visit its territory in order to discuss, with its security authorities, its procedures and facilities for the protection of classified information received from the other Contracting Party. Each Contracting Party shall assist that authority in ascertaining whether such classified information which has been made available by the other Contracting Party is adequately protected. The details of the visits shall be laid down by the competent authorities.

Article 10

Violations of Provisions Governing the Mutual Protection of Classified Information

(1) Whenever unauthorized disclosure of classified information cannot be ruled out or if such disclosure is suspected or ascertained, the other Contracting Party shall immediately be informed.

(2) Violations of provisions governing the protection of classified information shall be investigated, and pertinent legal action shall be taken, by the competent authorities and courts of the Contracting Party having jurisdiction, according to that Contracting Party's law. The other Contracting Party should, if so requested, support such investigations and shall be informed of the outcome.

Article 11

Costs

Each Contracting Party shall pay the expenses incurred by it in implementing the provisions of this Agreement.

Article 12

Competent Authorities

The Contracting Party shall inform each other of the authorities to be responsible for the implementation of this Agreement.

Article 13

Relationship with Other Agreements, Memoranda of Understanding and Arrangements

Any existing Agreements, Memoranda of Understanding and Arrangements between the Contracting Parties or the competent authorities on the protection of classified information shall be unaffected by the present Agreement in so far as they do not conflict with its provisions.

Article 14

Final Provisions

(1) This Agreement shall enter into force on the date of signature thereof.

(2) This Agreement is concluded for an indefinite period of time.

(3) This Agreement may be amended in writing by mutual agreement between the Contracting Parties. Either Contracting Party may at any time submit a written request for the amendment of this Agreement. If such a request is submitted by one of the Contracting Parties, the Contracting Parties shall initiate negotiations on the amendment of the Agreement.

(4) Either Contracting Party may, through diplomatic channels, denounce this Agreement by giving six months' written notice. In the event of denunciation, classified information transmitted, or generated by the contractor, on the basis of this Agreement shall continue to be treated in accordance with the provisions of Article 4 above for as long as is justified by the existence of the security classification.

(5) Registration of this Agreement with the Secretariat of the United Nations, in accordance with Article 102 of the United Nations Charter, shall be initiated by the Contracting Party on whose national territory the Agreement is concluded immediately following its entry into force. The other Contracting Party shall be informed of the registration, and of the UN registration number, as soon as this has been confirmed by the Secretariat of the United Nations.

Done at Podgorica, on 11 May 2018 in duplicate in the Montenegrin, German and English languages, all three texts being authentic. In the case of divergent interpretations of the German and Montenegrin texts, the English text shall prevail.

For the Government
of Montenegro
Savo Vučinić

For the Government
of the Federal Republic of Germany
Hans Gunther Mattern

Član 3

Ova odluka stupa na snagu osmog dana od dana objavljivanja u „Službenom listu Crne Gore-Međunarodni ugovori“.

Broj: _____
Podgorica, _____ 2018. godine

Vlada Crne Gore

Predsjednik,

Duško Marković