Warszawa, dnia 26 lutego 2016 r.

Poz. 246

UMOWA

między Rządem Rzeczypospolitej Polskiej a Rządem Czarnogóry o wzajemnej ochronie informacji niejawnych,

podpisana w Warszawie dnia 18 listopada 2014 r.

W imieniu Rzeczypospolitej Polskiej

PREZYDENT RZECZYPOSPOLITEJ POLSKIEJ

podaje do powszechnej wiadomości:

Dnia 18 listopada 2014 r. w Warszawie została podpisana Umowa między Rządem Rzeczypospolitej Polskiej a Rządem Czarnogóry o wzajemnej ochronie informacji niejawnych, w następującym brzmieniu:

UMOWA
między Rządem Rzeczypospolitej Polskiej a Rządem Czarnogóry o wzajemnej ochronie informacji niejawnych

Rząd Rzeczypospolitej Polskiej i Rząd Czarnogóry,

zwane dalej „Stronami",

mając na uwadze konieczność zagwarantowania efektywnej ochrony informacji niejawnych wymienianych między Stronami lub wytwarzanych w wyniku współpracy,

kierując się zamiarem przyjęcia jednolitych dla obydwu Stron uregulowań prawnych w zakresie ochrony informacji niejawnych,

z zastrzeżeniem poszanowania obowiązujących norm prawa międzynarodowego i prawa wewnętrznego Stron,

uzgodniły, co następuje:

ARTYKUŁ 1
DEFINICJE

W rozumieniu niniejszej Umowy następujące definicje oznaczają:

1) **informacje niejawne** – wszelkie informacje niezależnie od formy, nośnika i sposobu ich utrwalenia oraz przedmioty lub dowolne ich części, także w trakcie ich opracowywania, które wymagają ochrony przed nieuprawnionym ujawnieniem, zgodnie z prawem wewnętrznym każdej ze Stron i niniejszą Umową;
2) **właściwe organy** – organy, o których mowa w artykule 3 niniejszej Umowy;
3) **upoważnione podmioty** – osoby fizyczne, osoby prawne lub inne jednostki organizacyjne właściwe do przetwarzania informacji niejawnych zgodnie z prawem wewnętrznym swojej Strony;
4) **kontrakt niejawny** – umowę, której realizacja wiąże się z dostępem do informacji niejawnych, bądź z wytworzeniem takich informacji;
5) **kontrahent** – osobę fizyczną, osobę prawną albo inną jednostkę organizacyjną, podlegającą prawodawstwu jednej ze Stron, która posiada zdolność do zawierania kontraktów niejawnych;
6) **zlecający** - osobę fizyczną, osobę prawną albo inną jednostkę organizacyjną, podlegającą prawodawstwu jednej ze Stron, która posiada zdolność do zlecania kontraktów niejawnych;
7) **strona trzecia** – organizację międzynarodową lub państwo, niebędące Stroną niniejszej umowy, osobę fizyczną albo inny podmiot podlegający prawodawstwu tego państwa.

ARTYKUŁ 2
KLAUZULE TAJNOŚCI

1. Informacjom niejawnym przyznaje się odpowiednią do ich treści klauzulę tajności zgodnie z prawem wewnętrznym Strony wytwarzającej informacje niejawne. Upoważniony podmiot otrzymujący informacje niejawne

gwarantuje co najmniej równorzędny poziom ochrony otrzymanych informacji niejawnych, zgodnie z postanowieniami ustępu 3.

2. Klauzula tajności może być zmieniona lub zniesiona wyłącznie przez upoważniony podmiot, który ją nadał. Upoważniony podmiot otrzymujący informacje niejawne jest pisemnie informowany o każdym przypadku zmiany lub zniesienia klauzuli tajności wcześniej otrzymanych informacji niejawnych.
3. Strony uzgadniają, że niżej wymienione klauzule tajności są równorzędne:

RZECZPOSPOLITA POLSKA	CZARNOGÓRA	ODPOWIEDNIK W JĘZYKU ANGIELSKIM
ŚCIŚLE TAJNE	STROGO TAJNO	TOP SECRET
TAJNE	TAJNO	SECRET
POUFNE	POVJERLJIVO	CONFIDENTIAL
ZASTRZEŻONE	INTERNO	RESTRICTED

ARTYKUŁ 3
WŁAŚCIWE ORGANY

1. W rozumieniu niniejszej Umowy właściwymi organami są:
   1) w Rzeczypospolitej Polskiej: Szef Agencji Bezpieczeństwa Wewnętrznego;
   2) w Czarnogórze: Zarząd do spraw ochrony informacji niejawnych (krajowa władza bezpieczeństwa).
2. Strony informują się drogą dyplomatyczną o zmianach właściwych organów, o których mowa w ustępie 1, lub zmianach ich właściwości.

ARTYKUŁ 4
ZASADY OCHRONY INFORMACJI NIEJAWNYCH

1. Strony podejmują wszelkie określone w niniejszej Umowie oraz zgodne ze swoim prawem wewnętrznym działania w celu ochrony informacji niejawnych przekazywanych lub wytwarzanych w wyniku wspólnej działalności Stron lub upoważnionych podmiotów, w tym także wytworzonych w związku z realizacją kontraktów niejawnych.
2. Upoważniony podmiot otrzymujący wykorzystuje informacje niejawne wyłącznie w celach, dla których zostały one przekazane.
3. Informacje niejawne mogą być udostępniane tylko tym osobom, których zadania wymagają zapoznania się z nimi i które zgodnie z prawem wewnętrznym Strony otrzymującej zostały upoważnione do dostępu do nich.
4. Upoważniony podmiot otrzymujący nie udostępnia informacji, o których mowa w ustępie 1, stronie trzeciej, bez uprzedniej pisemnej zgody upoważnionego podmiotu wytwarzającego.

ARTYKUŁ 5
POŚWIADCZENIA BEZPIECZEŃSTWA ORAZ ŚWIADECTWA BEZPIECZEŃSTWA PRZEMYSŁOWEGO

W zakresie niniejszej Umowy, Strony uznają poświadczenia bezpieczeństwa i świadectwa bezpieczeństwa przemysłowego wydane zgodnie z prawem wewnętrznym drugiej Strony.

ARTYKUŁ 6
KONTRAKTY NIEJAWNE

1. Przed zawarciem kontraktu niejawnego, związanego z dostępem do informacji niejawnych o klauzuli POUFNE/POVJERLJIVO/CONFIDENTIAL lub wyższej, zlecający składa wniosek do właściwego organu swojej Strony,

o wystąpienie do właściwego organu drugiej Strony, z prośbą o pisemne potwierdzenie, że kontrahent posiada ważne świadectwo bezpieczeństwa przemysłowego odpowiednie do klauzuli informacji niejawnych, do których będzie miał dostęp.

2. Pisemne potwierdzenie, o którym mowa w ustępie 1, jest równoznaczne z gwarancją, że zostały przeprowadzone czynności niezbędne do stwierdzenia, że kontrahent spełnia warunki w zakresie ochrony informacji niejawnych określone w prawie wewnętrznym Strony, na terytorium której posiada siedzibę.
3. Informacje niejawne nie są udostępniane kontrahentowi do czasu uzyskania pisemnego potwierdzenia, o którym mowa w ustępie 1.
4. Zlecający przekazuje kontrahentowi instrukcję bezpieczeństwa przemysłowego niezbędną do realizacji kontraktu niejawnego, która stanowi integralną część każdego kontraktu niejawnego. Instrukcja bezpieczeństwa przemysłowego zawiera postanowienia dotyczące wymogów bezpieczeństwa, w szczególności:
   1) wykaz rodzajów informacji niejawnych odnoszących się do danego kontraktu niejawnego, z uwzględnieniem ich klauzul tajności;
   2) zasady przyznawania klauzul tajności informacjom wytworzonym podczas realizacji danego kontraktu niejawnego.
5. Zlecający przekazuje kopię instrukcji bezpieczeństwa przemysłowego właściwemu organowi swojej Strony, który przesyła ją właściwemu organowi Strony kontrahenta.
6. Realizacja kontraktu niejawnego w części związanej z dostępem do informacji niejawnych, będzie możliwa po spełnieniu przez kontrahenta warunków niezbędnych do ochrony informacji niejawnych, zgodnie z instrukcją bezpieczeństwa przemysłowego.
7. Każdy podwykonawca podlega tym samym obowiązkom ochrony informacji niejawnych, jakie nałożono na kontrahenta.

ARTYKUŁ 7
PRZEKAZYWANIE INFORMACJI NIEJAWNYCH

1. Informacje niejawne są przekazywane drogą dyplomatyczną.
2. Informacje niejawne o klauzuli ZASTRZEŻONE/INTERNO/RECTRICTED oraz POUFNE/POVJERLJIVO/CONFIDENTIAL mogą być przekazywane również za pośrednictwem uprawnionych do tego przewoźników, zgodnie z prawem wewnętrznym Strony przekazującej.
3. W pilnych przypadkach, o ile nie można skorzystać z innej formy przekazania, jeżeli spełnione są wymogi bezpieczeństwa określone prawem wewnętrznym Strony przekazującej, dopuszczalny jest przewóz osobisty informacji niejawnych o klauzuli ZASTRZEŻONE /INTERNO/ RESTRICTED oraz POUFNE /POVJERLJIVO/CONFIDENTIAL.
4. Właściwe organy Stron mogą ustalić inne sposoby przekazywania informacji niejawnych zapewniające ochronę przed ich nieuprawnionym ujawnieniem.
5. Upoważniony podmiot otrzymujący pisemnie potwierdza odbiór informacji niejawnych.

ARTYKUŁ 8
POWIELANIE LUB TŁUMACZENIE INFORMACJI NIEJAWNYCH

1. Powielanie lub tłumaczenie informacji niejawnych odbywa się w sposób zgodny z prawem wewnętrznym każdej ze Stron. Powielone lub przetłumaczone informacje podlegają takiej samej ochronie jak oryginały. Liczba kopii i tłumaczeń będzie ograniczona do liczby wymaganej dla celów służbowych.
2. Informacje niejawne o klauzuli ŚCIŚLE TAJNE/STROGO TAJNO/TOP SECRET są powielane lub tłumaczone tylko po uprzednim uzyskaniu pisemnego zezwolenia wydanego przez upoważniony podmiot wytwarzający.

ARTYKUŁ 9
NISZCZENIE INFORMACJI NIEJAWNYCH

1. Z zastrzeżeniem ustępu 2, informacje niejawne są niszczone zgodnie z prawem wewnętrznym Strony otrzymującej w sposób uniemożliwiający ich częściowe lub całkowite odtworzenie.
2. Informacje niejawne o klauzuli ŚCIŚLE TAJNE/STROGO TAJNO/TOP SECRET nie są niszczone; są one zwracane upoważnionemu podmiotowi wytwarzającemu.

ARTYKUŁ 10
WIZYTY

1. Z zastrzeżeniem ustępów 5 i 6, osobom przybywającym z wizytą na terytorium państwa drugiej Strony zezwala się na dostęp do informacji niejawnych, tylko po uprzednim uzyskaniu pisemnego zezwolenia wydanego przez właściwy organ drugiej Strony.
2. Właściwy organ Strony wysyłającej zwraca się do właściwego organu Strony przyjmującej z wnioskiem o wyrażenie zgody na wizytę co najmniej trzydzieści dni przed planowanym terminem wizyty.
3. Wniosek, o którym mowa w ustępie 2, powinien zawierać:
   1) cel, termin i program wizyty;
   2) imię i nazwisko, datę i miejsce urodzenia, obywatelstwo i numer paszportu lub innego dokumentu tożsamości osoby przybywającej z wizytą;
   3) stanowisko służbowe osoby przybywającej z wizytą wraz z nazwą podmiotu, który reprezentuje;
   4) poziom i datę ważności poświadczenia bezpieczeństwa posiadanego przez osobę przybywającą z wizytą;

5) nazwę i adres odwiedzanego podmiotu;

6) imię i nazwisko oraz stanowisko służbowe osoby przyjmującej;

7) datę, podpis oraz oficjalną pieczęć właściwego organu.

4. Do ochrony danych osobowych, o których mowa w ustępie 3, przekazywanych w związku z postanowieniami ustępu 1, 5 oraz 6, stosuje się, z uwzględnieniem prawa wewnętrznego każdej ze Stron, następujące postanowienia:

1) otrzymane przez Stronę przyjmującą wizytę dane osobowe będą wykorzystane wyłącznie w celu i na warunkach określonych przez Stronę je przekazującą;

2) Strona przyjmująca wizytę nie przechowuje danych osobowych dłużej, aniżeli jest to niezbędne dla osiągnięcia celu przetwarzania;

3) w przypadku przekazania danych, których nie wolno było przekazać zgodnie z jej prawem wewnętrznym, Strona przekazująca dane osobowe zawiadamia o tym Stronę przyjmującą wizytę, która jest zobowiązana do usunięcia tych danych w sposób uniemożliwiający ich częściowe lub całkowite odtworzenie;

4) Strona przekazująca dane osobowe odpowiada za ich merytoryczną poprawność i jeśli okaże się, że przekazane zostały dane nieprawdziwe lub niekompletne, zawiadamia o tym Stronę przyjmującą wizytę, która jest zobowiązana do sprostowania lub usunięcia tych danych;

5) Strona przyjmująca wizytę oraz Strona przekazująca dane osobowe są zobowiązane do rejestrowania ich przekazywania, otrzymywania i usuwania;

6) Strona przekazująca dane osobowe oraz Strona przyjmująca wizytę są zobowiązane do skutecznego zabezpieczania przetwarzanych danych przed ich udostępnieniem osobom nieupoważnionym, nieuprawnionym dokonywaniem zmian tych danych, ich utratą, uszkodzeniem lub zniszczeniem.

5. Właściwe organy mogą wyrazić zgodę na ustalenie list osób upoważnionych do składania wielokrotnych wizyt związanych z realizacją konkretnego projektu, programu lub kontraktu niejawnego. Listy te zawierają dane określone w ustępie 3 i są ważne przez okres dwunastu miesięcy. Po zatwierdzeniu takich list przez właściwe organy, terminy wizyt uzgadniane są bezpośrednio między jednostką wysyłającą a jednostką przyjmującą wizytę.
6. Wizyty związane z dostępem do informacji niejawnych o klauzuli ZASTRZEŻONE/INTERNO/RESTRICTED są uzgadniane bezpośrednio między jednostką wysyłającą a jednostką przyjmującą wizytę.

ARTYKUŁ 11
NARUSZENIE REGULACJI DOTYCZĄCYCH OCHRONY INFORMACJI NIEJAWNYCH

1. Naruszeniem regulacji dotyczących ochrony informacji niejawnych jest działanie lub zaniechanie sprzeczne z niniejszą Umową lub prawem wewnętrznym Stron, dotyczącym ochrony informacji niejawnych.
2. Informacja o każdym przypadku naruszenia lub o podejrzeniu naruszenia regulacji dotyczących ochrony informacji niejawnych przekazanych przez upoważniony podmiot, który je wytworzył lub informacji niejawnych wytworzonych w wyniku wspólnego działania upoważnionych podmiotów Stron będzie niezwłocznie przekazywana właściwemu organowi Strony, na terytorium której miało miejsce lub zaistniało podejrzenie takiego naruszenia.
3. Każdy przypadek naruszenia lub podejrzenia naruszenia regulacji dotyczących ochrony informacji niejawnych będzie wyjaśniany zgodnie z prawem wewnętrznym Strony, na terytorium której zdarzenie miało miejsce.

4. W przypadku naruszenia regulacji dotyczących ochrony informacji niejawnych, o których mowa w ustępie 1, właściwy organ Strony, na terytorium której naruszenie miało miejsce, niezwłocznie pisemnie informuje właściwy organ drugiej Strony o fakcie, okolicznościach naruszenia oraz wyniku czynności, o których mowa w ustępie 3.
5. Właściwe organy Stron współpracują przy czynnościach, o których mowa w ustępie 3, na wniosek jednego z nich.

ARTYKUŁ 12
JĘZYKI

W zakresie stosowania postanowień niniejszej Umowy, Strony używają języka angielskiego lub swoich języków urzędowych, dołączając – w przypadku użycia języka urzędowego jednej ze Stron – tłumaczenie na język urzędowy drugiej Strony lub na język angielski.

ARTYKUŁ 13
KOSZTY

Każda ze Stron pokrywa koszty własne, poniesione w związku z realizacją postanowień niniejszej Umowy.

ARTYKUŁ 14
KONSULTACJE

1. Właściwe organy informują się wzajemnie o wszelkich zmianach w prawie wewnętrznym swoich państw, dotyczących ochrony informacji niejawnych, w zakresie niezbędnym do wykonywania postanowień niniejszej Umowy.
2. W celu zapewnienia ścisłej współpracy przy realizacji postanowień niniejszej Umowy właściwe organy konsultują się, na wniosek jednego z tych organów.

3. Każda ze Stron zezwoli przedstawicielom właściwego organu drugiej Strony na składanie wizyt na swoim terytorium w celu omówienia procedur służących ochronie informacji niejawnych, które zostały jej przekazane przez drugą Stronę.
4. W celu zapewnienia skutecznej współpracy, będącej przedmiotem niniejszej Umowy, i w zakresie kompetencji przyznanych im prawem wewnętrznym swoich Stron, właściwe organy mogą, w razie potrzeby, zawierać pisemne szczegółowe uzgodnienia techniczne lub organizacyjne.

ARTYKUŁ 15
ROZSTRZYGANIE SPORÓW

1. Wszelkie sporne kwestie dotyczące stosowania niniejszej Umowy będą rozstrzygane w drodze bezpośrednich konsultacji między właściwymi organami.
2. Jeśli nie jest możliwe rozwiązanie sporu w sposób, o którym mowa w ustępie 1, będzie on rozstrzygany drogą dyplomatyczną.

ARTYKUŁ 16
POSTANOWIENIA KOŃCOWE

1. Niniejsza Umowa podlega przyjęciu zgodnie z prawem wewnętrznym każdej ze Stron, co zostanie stwierdzone w drodze wymiany not. Umowa wejdzie w życie w pierwszym dniu drugiego miesiąca, który nastąpi po dniu otrzymania noty późniejszej.
2. Niniejsza Umowa może zostać zmieniona na podstawie wspólnej pisemnej zgody obu Stron. Takie zmiany wejdą w życie zgodnie z postanowieniami ustępu 1.

3. Niniejsza Umowa zawarta jest na czas nieokreślony. Może być ona wypowiedziana w drodze pisemnej notyfikacji przez każdą ze Stron. W takim przypadku utraci moc po upływie sześciu miesięcy od dnia otrzymania noty informującej o wypowiedzeniu.
4. W przypadku wypowiedzenia, informacje niejawne przekazane lub wytworzone na podstawie niniejszej Umowy będą nadal chronione zgodnie z jej postanowieniami.

Sporządzono w WARSZAWIE dnia 18 listopada 2014 roku w dwóch jednobrzmiących egzemplarzach, każdy w językach polskim, czarnogórskimi i angielskim, przy czym wszystkie teksty posiadają jednakową moc. W przypadku rozbieżności przy ich interpretacji, tekst w języku angielskim uważany będzie za rozstrzygający.

Z UPOWAŻNIENIA RZĄDU RZECZYPOSPOLITEJ POLSKIEJ

Z UPOWAŻNIENIA RZĄDU CZARNOGÓRY

SPORAZUM

IZMEĐU

VLADE REPUBLIKE POLJSKE I VLADE CRNE GORE

O

UZAJAMNOJ ZAŠTITI TAJNIH PODATAKA

Vlada Republike Poljske i Vlada Crne Gore, u daljem tekstu "Strane",

Uvažavajući potrebu da se obezbijedi efikasna zaštita tajnih podataka

razmijenjenih ili nastalih u toku saradnje između Strana,

Vodeći se namjerom da usvoje jedinstvene propise za obije Strane u oblasti

zaštite tajnih podataka,

Poštujući obavezujuća pravila međunarodnog prava i domaćih propisa svake od

Strana,

Saglasne su u sljedećem:

ČLAN 1
DEFINICIJE

U smislu ovog Sporazuma, sljedeće definicije imaju značenja:

1. **tajni podatak:** svaka informacija, nezavisno od oblika, načina prenosa i evidentiranja, kao i predmet ili bilo koji njegov dio, koji u procesu prikupljanja zahtijevaju zaštitu od neovlašćenog otkrivanja u skladu sa unutrašnjim pravom Strana i ovim sporazumom;

2. **nadležni organ:** organi iz člana 3 ovog Sporazuma;

3. **ovlašćena tijela:** fizička lica, pravna lica ili druga udruženja, nadležna za rukovanje tajnim podacima u skladu sa unutrašnjim pravom njihove Strane;

4. **povjerljivi ugovori:** ugovor, djelatnost koja podrazumijeva pristup tajnim podacima ili od koga nastaju tajni podaci;

5. **ugovarač:** fizičko lice, pravno lice ili druga udruženja osnovana u skladu sa domaćim zakonom jedne od Strana, koja imaju poslovnu sposobnost za zaključivanje povjerljivih ugovora;

6. **naručilac:** fizičko lice, pravno lice ili druga organizacija osnovana u skladu sa domaćim pravom jedne od Strana, koji ima poslovnu sposobnost da bude naručilac u povjerljivom ugovoru;

7. **treća strana:** svaka država, pravno lice ili druga organizacija osnovana u skladu sa domaćim propisima, ili međunarodna organizacija koja nija Strana u ovom sporazumu.

ČLAN 2
STEPENI TAJNOSTI

1. Tajnim podacima se određuju stepen tajnosti saglasno njihovom sadržaju, u skladu sa domaćim pravom Strane porijekla. Nadležni organ prijema će garantovati najmanje jednak nivo zaštite primljenog tajnog podatka, u skladu sa stavom 3 ovog člana.

2. Stepen tajnosti može biti promijenjen ili ukinut samo od strane nadležnog organa koji ga je odredio. Nadležni organ prijema će biti pisanim putem obaviješten o svakoj promjeni ili ukidanju stepena tajnosti primljenih tajnih podataka.

3. Strane su saglasne da su sljedeći stepeni tajnosti podataka ekvivalentni:

REPUBLIKA POLJSKA	CRNA GORA	EKVIVALENTI NA ENGLESKOM JEZIKU
ŚCIŚLE TAJNE	STROGO TAJNO	TOP SECRET
TAJNE	TAJNO	SECRET
POUFNE	POVJERLJIVO	CONFIDENTIAL
ZASTRZEŻONE	INTERNO	RESTRICTED

ČLAN 3
NADLEŽNI ORGANI

1. Za primjenu ovog Sporazuma, nadležni organi su:

1) Za Republiku Poljsku: Direktorat za unutrašnju bezbjednost;

2) Za Crnu Goru: Direkcija za zaštitu tajnih podataka;

2. Strane treba da informišu jedna drugu diplomatskim putem o svim promjenama nadležnog organa određenog u stavu 1 ovog člana, ili o izmjenama i dopunama svojih nadležnosti.

ČLAN 4
PRINCIPI ZAŠTITE TAJNIH PODATAKA

1. Strane treba da prihvate sve mjere propisane ovim sporazumom i njihovim domaćim pravom radi zaštite ustupljenih tajnih podataka, ili tajnih podataka nastalih kao rezultat saradnje između Strana ili njihovih nadležnih organa, uključujući i tajne podatke koji su nastali u izvršavanju povjerljivih ugovora.

2. Strana primalac koristiće tajne podatke isključivo u svrhu za koju su dostavljeni.

3. Pristup tajnim podacima će biti odobren samo onim licima koja imaju opravdanu potrebu da znaju i koja su ovlašćena za pristup u skladu sa domaćim pravom Strane primaoca.

4. Strana primalac neće dostavljati tajne podatke iz stava 1 ovog člana trećoj strani bez prethodnog pisanog odobrenja Strane porijekla.

ČLAN 5
BEZBJEDNOSNA DOZVOLA

U okviru ovog sporazuma, Strane će priznati bezbjednosne dozvole za fizička i pravna lica, izdate u skladu sa unutrašnjim pravom druge Strane.

ČLAN 6
POVJERLJIVI UGOVORI

1. Prije zaključivanja povjerljivog ugovora koji podrazumijeva pristup tajnim podacima stepena tajnosti POUFNE/POVJERLJIVO/CONFIDENTIAL ili više, naručilac će podnijeti zahtjev kod svog nadležnog organa da zatraži od nadležnog organa druge Strane potvrdu u pisanoj formi da ugovarač posjeduje bezbjednosnu dozvolu za pravno lice, za pristup tajnim podacima odgovarajućeg stepena tajnosti.

2. Izdavanje potvrde u pisanoj formi iz stava 1 ovog člana će se smatrati garancijom da su preduzete sve potrebne radnje kako bi se utvrdilo da ugovarač ispunjava sve kriterijume za zaštitu tajnih podataka definisanih domaćim pravom Strane na čijoj teritoriji se nalazi.

3. Tajni podaci se neće dostavljati ugovaraču prije prijema potvrde iz stava 1 ovog člana.

4. Naručilac će dostaviti ugovaraču Upustvo o mjerama zaštite, koje je sastavni dio svakog povjerljivog ugovora, a koje je neophodno za njegovo izvršenje. Uputstvo o mjerama zaštite obuhvata bezbjednosne zahtjeve, naročito:

1) spisak tajnih podataka povezanih sa povjerljivim ugovorom, uključujući njihov stepen tajnosti;

2) pravila za određivanje stepena tajnosti podataka nastalih u izvršavanju povjerljivog ugovora.

5. Naručilac će dostaviti kopiju Uputstva o mjerama zaštite nadležnom organu na njegovoj teritoriji, koji će ga proslijediti nadležnom organu Strane ugovarača

6. Izvršenje povjerljivog ugovora u dijelu koji se odnosi na pristup tajnim podacima će biti moguće pod uslovom da ugovarač ispunjava kriterijume neophodne za zaštitu tajnih podataka, sadržanih u Uputstvu o mjerama zaštite.

7. Svaki podugovarač treba da ispunjava iste uslove za zaštitu tajnih podataka kao i ugovarač.

ČLAN 7
PRENOŠENJE TAJNIH PODATAKA

1. Prenošenje tajnih podataka će se vršiti diplomatskim putem.

2. Podaci stepena tajnosti ZASTRZEŽONE/INTERNO/RESTRICTED ili POUFNE/POVJERLJIVO/CONFIDENTIAL mogu se prenositi i preko ovlašćenih kurira, u skladu sa domaćim pravom Strane pošiljaoca.

3. U hitnim slučajevima, ukoliko nije moguće koristiti druge načine prenošenja, a bezbjednosni uslovi propisani domaćim pravom Strane pošiljaoca su ispunjeni, prenos tajnih podataka stepena tajnosti ZASTRZEŽONE /INTERNO/RESTRICTED ili POUFNE/POVJERLJIVO/CONFIDENTIAL, može se izvršiti i preko drugih lica.

4. Nadležni organi se mogu sporazumjeti i u vezi drugih načina prenošenja tajnih podataka koji obezbjeđuju njihovu zaštitu od neovlašćenog otkrivanja.

5. Strana primalac će pisanim putem potvrditi prijem tajnog podatka.

ČLAN 8
UMNOŽAVANJE ILI PREVOD TAJNIH PODATAKA

1. Umnožavanje ili prevod tajnih podataka će se izvršiti u skladu sa domaćim pravom svake od Strana. Umnoženi ili prevedeni tajni podaci će se zaštititi kao i originalni podaci. Broj kopija i prevoda će se ograničiti na broj potreban za službene svrhe.

2. Tajni podaci stepena tajnosti ŚCIŚLE TAJNE/STROGO TAJNO/TOP SECRET će se umnožavati ili prevoditi samo nakon pribavljene pisane saglasnosti Strane porijekla.

ČLAN 9
UNIŠTAVANJE TAJNIH PODATAKA

1. Tajni podaci će se uništavati u skladu sa domaćim pravom Strane primaoca na način što će se onemogućiti njegova djelimična ili potpuna rekonstrukcija, izuzev tajnih podataka iz stava 2 ovog člana.

2. Tajni podaci stepena tajnosti ŚCIŚLE TAJNE/STROGO TAJNO/TOP SECRET se neće uništavati, već će biti vraćeni nadležnom organu Strane porijekla.

ČLAN 10
POSJETE

1. Licima koja odlaze u posjetu na teritoriju druge Strane će biti dozvoljen pristup tajnim podacima jedino uz pisanu saglasnost nadležnog organa te Strane, izuzev u slučajevima iz stava 5 i 6 ovog člana.

2. Nadležni organ Strane koja vrši posjetu će uputiti zahtjev nadležnom organu Strane domaćina najmanje 30 dana prije planiranog datuma posjete.

3. Zahtjev iz Stava 2 ovog člana treba da sadrži:

1) svrhu, datum i program posjete;

2) ime i prezime posjetioca, datum i mjesto rođenja, nacionalnost i broj pasoša ili

3) drugog identifikacionog dokumenta;

4) zvanje posjetioca kao i naziv organa koji on/ona predstavlja;

5) stepen tajnosti i datum trajanja bezbjednosne dozvole koju posjeduje;

6) naziv i adresu organa koji se posjećuje;

7) ime, prezime i zvanje lica koja se posjećuju;

8) datum, potpis i zvanični pečat nadležnog organa Strane koja vrši posjetu.

4. U cilju zaštite ličnih podataka iz stava 3 ovog člana, a koji se odnose na lica iz stava 1, 5 i 6, primjenjivaće se sljedeće odredbe koje su predmet domaćeg prava svake od Strana ugovornica:

1) lični podaci koje primi Strana primalac će se koristiti isključivo u svrhu i pod uslovima koje odredi Strana pošiljalac;

2) lični podaci koje primi Strana primalac će se čuvati ne duže nego što je potrebno da se postigne svrha za koju su prikupljeni;

3) u slučaju prenosa ličnih podataka suprotno pravilima domaćeg prava, Strana pošiljalac će obavijestiti Stranu primaoca, koja će biti obavezna da uništi podatke na način što će se onemogućiti njihova djelimična ili potpuna rekonstrukcija;

4) Strana pošiljalac će preuzeti odgovornost za tačnost ličnih podataka i u slučaju da se utvrdi da su lični podaci netačni ili nekompletni, obavijestiće Stranu primaoca koja će biti obavezna da ispravi ili uništi podatke;

5) Strana primalac i Strana pošiljalac biće dužne da evidentiraju slanje, prijem i uništavanje ličnih podataka;

6) Strana pošiljalac i Strana primalac će biti obavezne da obrađene lične podatke efikasno štite od neovlašćenog otkrivanja, neovlašćenih izmjena podataka, gubitka, oštećenja ili uništenja.

5. Nadležni organi Strana se mogu sporazumjeti da ustanove listu lica ovlašćenih za vršenje posjeta u vezi sa implementacijom posebnih projekata, programa ili povjerljivih ugovora. Lista će sadržati podatke određene u stavu 3 ovog člana, za period od 12 mjeseci. Kada ovakva lista bude odobrena od strane nadležnih organa, datumi posjeta će se ugovarati direktno između subjekata koji učestvuju u posjeti.

6. Posjete koje uključuju pristup tajnim podacima stepena tajnosti INTERNO biće dogovorene direktno između subjekata koji učestvuju u posjeti.

ČLAN 11
POVREDE BEZBIJEDNOSTI

1. Povreda bezbjednosti je činjenje ili nečinjenje koje je suprotno odredbama Sporazuma ili domaćeg prava Strana ugovornica, a koja se tiče zaštite tajnih podataka.

2. Informacije o svakoj povredi bezbjednosti ili postojanju sumnji o takvoj povredi koja se odnosi na tajne podatke nadležnog organa od koga potiču ili su nastali kao rezultat saradnje nadležnih organa Strana ugovornica, biće odmah prijavljene nadležnom organu Strane na čijoj teritoriji se povreda desila, ili postoji sumnja da se desila.

3. Svaka povreda ili sumnja da postoji povreda bezbjednosti biće ispitana u skladu sa domaćim pravom Strane na čijoj teritoriji se to dogodilo.

4. U slučaju povrede bezbjednosti iz stava 1 ovog člana, nadležni organ Strane na čijoj teritoriji je nastupila povreda bezbjednosti će pisanim putem obavijestiti drugu Stranu o činjenicama, okolnostima povrede i o ishodu preduzetih radnji iz stava 3 ovog člana.

5. Nadležni organi će sarađivati u primjeni radnji iz stava 3 ovog člana, na zahtjev svake od njih.

ČLAN 12
JEZICI

U cilju primjene odredaba ovog Sporazuma, Strane će koristiti engleski ili svoj jezik koji je u zvaničnoj upotrebi, dok će prevod Sporazuma na jeziku druge Strane ili na engleskom jeziku biti u prilogu.

ČLAN 13
TROŠKOVI

Svaka Strana će snositi svoje troškove nastale primjenom odredaba ovog Sporazuma.

ČLAN 14
KONSULTACIJE

1. Nadležni organi Strana će se međusobno obavještavati o svim izmjenama u domaćem pravu iz oblasti zaštite tajnih podataka, a koje su u vezi sa primjenom ovog sporazuma.

2. Nadležni organi Strana će se konsultovati na osnovu zahtjeva jednog od njih kako bi osigurali bližu saradnju u primjeni odredbi ovog sporazuma.

3. Svaka Strana će omogućiti predstavnicima nadležnog organa druge Strane da vrše posjete na njenoj teritoriji radi razmatranja procedura za zaštitu tajnih podataka dobijenih od druge Strane.

4. U cilju obezbjeđivanja efikasne saradnje, koja je predmet ovog sporazuma, i u cilju uzajamnog razumijevanja domaćih propisa Strana ugovornica, nadležni organi Strana mogu, ukoliko je to potrebno, da zaključe detaljni tehnički ili organizacioni sporazum.

ČLAN 15

RJEŠAVANJE SPOROVA

1. Svaki spor koji se odnosi na primjenu ovog sporazuma će biti riješen direktnim pregovorima između nadležnih organa Strana.

2. Ukoliko rješavanje sporova nije moguće postići na način predviđen u stavu 1 ovog člana, takvi sporovi će biti rješavani diplomatskim putem.

ČLAN 16

ZAVRŠNE ODREDBE

1. Sporazum će stupiti na snagu u skladu sa domaćim pravom svake od Strana, što će biti potvrđeno razmjenom pisanih obavještenja. Sporazum će stupiti na snagu prvog dana drugog mjeseca nakon prijema posljednjeg pisanog obavještenja.

2. Sporazum može biti dopunjen na osnovu zajedničke pisane saglasnosti obje Strane. Takve izmjene i dopune će stupiti na snagu u skladu sa odredbama iz stava 1 ovog člana.

3. Sporazum se zaključuje na neodređeno vrijeme. Može biti raskinut od strane svake ugovorne Strane slanjem pisanog obavještenja drugoj Strani. U tom slučaju, Sporazum će prestati da važi šest mjeseci nakon pisanog obavještenja o otkazu.

4. U slučaju otkaza, tajni podaci razmijenjeni ili nastali na osnovu ovog sporazuma će se čuvati u skladu sa navedenim odredbama.

Sačinjeno u VARŠAVI dana 18. NOVEMBAR 2014 u dva originalna primjerka na poljskom, crnogorskom i engleskom jeziku, pri čemu su svi tekstovi jednako vjerodostojni. U slučaju razlika u tumačenju, mjerodavan je tekst na engleskom jeziku.

ZA VLADU
REPUBLIKE POLJSKE

ZA VLADU
CRNE GORE

AGREEMENT

between the Government of the Republic of Poland

and the Government of Montenegro

on the mutual protection of classified information

The Government of the Republic of Poland and the Government of Montenegro, hereinafter referred to as the "Parties",

having due regard for the necessity of guaranteeing the effective protection of classified information exchanged between the Parties or originated during cooperation course,

being guided by the intention to adopt uniform regulations for both Parties in the scope of the protection of classified information,

subject to respect binding rules of the international law and the internal law of the Parties,

have agreed as follows:

ARTICLE 1
DEFINITIONS

For the purpose of this Agreement, the following definitions mean:

1) **classified information** – any information, irrespective of the form, carrier and manner of recording thereof, as well as objects or any parts thereof, also in the process of being generated, which require protection against unauthorized disclosure in accordance with the internal law of the Party and this Agreement;
2) **competent authorities** – the authorities referred to in Article 3 of this Agreement;
3) **authorized bodies** – individuals, legal entities or other organizational units, competent to handle classified information in accordance with the internal law of their Party;
4) **classified contract** – a contract, performance of which involves access to classified information or originating of such information;
5) **contractor** – an individual, a legal entity or other organizational unit under the law of one of the Parties, which has legal capacity to conclude classified contracts;
6) **principal** – an individual, a legal entity or other organizational unit under the law of one of the Parties, which has legal capacity to let classified contracts;
7) **third party** – any state, including individuals, legal entities or other organizational units under its jurisdiction, or an international organization, not being a Party to this Agreement.

ARTICLE 2
SECURITY CLASSIFICATION LEVELS

1. Classified information is granted a security classification level in accordance to its content, pursuant to the internal law of the originating Party. The authorized receiving body shall guarantee at least an equivalent level of protection of the received classified information, pursuant to the provisions of Paragraph 3.
2. The security classification level may be changed or removed only by the authorized body which has granted it. The authorized receiving body shall be notified in writing of every change or removal of the security classification level of previously received classified information.
3. The Parties agree that the following security classification levels are equivalent:

THE REPUBLIC OF POLAND	MONTENEGRO	EQUIVALENT IN ENGLISH
ŚCIŚLE TAJNE	STROGO TAJNO	TOP SECRET
TAJNE	TAJNO	SECRET
POUFNE	POVJERLJIVO	CONFIDENTIAL
ZASTRZEŻONE	INTERNO	RESTRICTED

ARTICLE 3
COMPETENT AUTHORITIES

1. For the purpose of this Agreement, the competent authorities shall be:
   1) for the Republic of Poland: the Head of the Internal Security Agency;
   2) for Montenegro: Directorate for protection of classified information (National Security Authority).

2. The Parties shall inform each other via diplomatic channels about changes of the competent authorities referred to in Paragraph 1 or amendments to their competences.

ARTICLE 4
PRINCIPLES OF CLASSIFIED INFORMATION PROTECTION

1. The Parties shall adopt every measure provided in this Agreement and their internal laws in order to protect classified information exchanged or originated as a result of cooperation between the Parties or authorized bodies, including this originated in connection with performance of classified contracts.
2. The authorized receiving body shall use classified information exclusively for the purposes defined at its transmission.
3. Access to classified information shall be granted only to those individuals who have a need-to-know and who have been authorized to access such information in accordance with the internal law of the receiving Party.
4. The authorized receiving body shall not release classified information referred to in Paragraph 1 to any third party without a prior written consent of the authorized originating body.

ARTICLE 5
SECURITY CLEARANCES

In the scope of this Agreement, the Parties shall recognize Personnel Security Clearances and Facility Security Clearances issued in accordance with the internal law of the other Party.

ARTICLE 6
CLASSIFIED CONTRACTS

1. Before concluding a classified contract connected with access to information classified as POUFNE / POVJERLJIVO / CONFIDENTIAL or above, the principal shall apply to its competent authority to request that the competent authority of the other Party confirm in writing that the contractor is a holder of a valid Facility Security Clearance relevant to the security classification level of the classified information the contractor is to have access to.
2. Written confirmation referred to in Paragraph 1 shall be considered as a guarantee that necessary actions have been conducted in order to declare that the contractor meets the criteria in the scope of the protection of classified information defined in the internal law of the Party in the territory of which it is located.
3. Classified information shall not be released to the contractor until the receipt of the written confirmation referred to in Paragraph 1.
4. The principal shall transmit to the contractor a facility security instruction necessary to perform a classified contract, which is an integral part of every classified contract. The facility security instruction contains provisions on the security requirements, in particular:
   1) the list of types of classified information related to a given classified contract, including their security classification levels;
   2) the rules for granting security classification levels to information originated during the performance of a given classified contract.
5. The principal shall submit a copy of the facility security instruction to the competent authority of its Party, which shall forward it to the competent authority of the contractor's Party.

6. The performance of a classified contract in the part connected with access to classified information shall be possible on condition that the contractor meets the criteria necessary for the protection of classified information, pursuant to the facility security instruction.
7. Every subcontractor shall comply with the same conditions for the protection of classified information as those laid down for the contractor.

ARTICLE 7
TRANSMISSION OF CLASSIFIED INFORMATION

1. Classified information shall be transmitted via diplomatic channels.
2. Information classified as ZASTRZEŻONE / INTERNO / RESTRICTED or POUFNE / POVJERLJIVO / CONFIDENTIAL may be also transmitted by authorized couriers, in accordance with the internal law of the transmitting Party.
3. In urgent cases, if it is not possible to use other form of transmission but the security requirements defined in the internal law of the transmitting Party are complied with, a personal hand carriage of information classified as ZASTRZEŻONE / INTERNO / RESTRICTED or POUFNE / POVJERLJIVO / CONFIDENTIAL is acceptable.
4. The competent authorities may agree on other forms of transmission of classified information which ensure its protection against unauthorized disclosure.
5. The authorized receiving body shall confirm in writing the receipt of classified information.

ARTICLE 8
REPRODUCTION OR TRANSLATION OF CLASSIFIED INFORMATION

1. Reproduction or translation of classified information shall be conducted pursuant to the internal law of each of the Parties. Reproduced or translated classified information shall be placed under the same protection as the original information. The number of copies and translations shall be limited to that required for official purposes.
2. Information classified as ŚCIŚLE TAJNE / STROGO TAJNO / TOP SECRET shall be reproduced or translated only after obtaining a prior written consent issued by the authorized originating body.

ARTICLE 9
DESTRUCTION OF CLASSIFIED INFORMATION

1. Subject to Paragraph 2, classified information shall be destroyed in accordance with the internal law of the receiving Party in such a manner as to eliminate its partial or total reconstruction.
2. Information classified as ŚCIŚLE TAJNE / STROGO TAJNO / TOP SECRET shall not be destroyed, it shall be returned to the authorized originating body.

ARTICLE 10
VISITS

1. Subject to Paragraphs 5 and 6, individuals arriving on a visit in the territory of the other Party shall be allowed access to classified information only after receiving a prior written consent issued by the competent authority of the other Party.

2. The competent authority of the visiting Party shall apply with a request for a visit to the competent authority of the hosting Party at least 30 days prior to a planned date of the visit.

3. The request referred to in Paragraph 2 should include:

1) purpose, date and program of the visit;

2) name and surname of the visitor, their date and place of birth, nationality and passport or other identification document's number;

3) position of the visitor together with the name of the entity which he or she represents;

4) level and the validity date of Personnel Security Clearance held by the visitor;

5) name and address of the entity to be visited;

6) name, surname and position of the person to be visited;

7) date, signature and official seal of the competent authority.

4. In order to protect personal data referred to in Paragraph 3, transmitted in connection with the provisions of Paragraphs 1, 5 and 6, the following provisions – subject to the internal law of each of the Parties – shall apply:

1) personal data received by the hosting Party shall be used exclusively for the purpose and on condition defined by the Party transmitting it;

2) personal data shall be stored by the hosting Party no longer than it is necessary for achieving the purpose of its processing;

3) in case of personal data transmitted against the internal law of the Party, the Party transmitting it shall notify the hosting Party, which shall be obliged to remove the data in such a manner as to eliminate its partial or total reconstruction;

4) the Party transmitting personal data shall take responsibility for its correctness and, in a case the data appears to be untrue or incomplete, shall notify the hosting Party, which shall be obliged to correct or remove the data;

5) the hosting Party and the Party transmitting personal data shall be obliged to register its transmission, receipt and removal;

6) the Party transmitting personal data and the hosting Party shall be obliged to protect processed personal data efficiently against its disclosure to unauthorized persons, unauthorized modifications of the data, its loss, damage or destruction.

5. The competent authorities of the Parties may agree to establish lists of persons authorized to make recurring visits connected with implementation of a specific project, program or classified contract. The lists shall contain the data specified in Paragraph 3 and are valid for a period of 12 months. Once such lists have been approved by the competent authorities, the dates of the visits shall be arranged directly between the visiting and hosting entities.

6. Visits involving access to information classified as ZASTRZEŻONE / INTERNO / RESTRICTED are arranged directly between the visiting and hosting entities.

ARTICLE 11
BREACH OF SECURITY

1. Breach of security is an action or an omission which is contrary to this Agreement or the internal law of the Parties concerning classified information protection.

2. Information on every breach of security or a suspicion thereof concerning classified information of the authorized originating body or classified information originated as a result of cooperation of the authorized bodies of the Parties shall be immediately reported to the competent authority of the Party in the territory of which the breach or suspicion thereof has occurred.

3. Every breach of security or a suspicion thereof shall be investigated pursuant to the internal law of the Party in the territory of which it has occurred.

4. In case of a breach of security referred to in Paragraph 1, the competent authority of the Party in the territory of which the breach has occurred shall inform the competent authority of the other Party in writing about the fact, circumstances of the breach and the outcome of the actions referred to in Paragraph 3.

5. The competent authorities shall cooperate in the actions referred to in Paragraph 3, upon the request of one of them.

ARTICLE 12
LANGUAGES

In the scope of the implementation of the provisions of this Agreement, the Parties shall use English or their official languages, in case of which the translation into the official language of the other Party or English shall be attached.

ARTICLE 13
EXPENSES

Each Party shall cover its expenses resulting from the implementation of the provisions of this Agreement.

ARTICLE 14
CONSULTATIONS

1. The competent authorities shall notify each other of any amendments to their internal law on the protection of classified information concerning implementation of this Agreement.

2. The competent authorities shall consult each other, upon the request of one of them, in order to ensure close cooperation in the implementation of the provisions of this Agreement.
3. Each Party shall allow the representatives of the competent authority of the other Party to pay visits to its own territory to discuss the procedures for the protection of classified information received from the other Party.
4. In order to ensure effective cooperation, which is the objective of this Agreement, and in the scope of authority acknowledged by the internal law of their Parties, the competent authorities may, if necessary, conclude written detailed technical or organizational arrangements.

ARTICLE 15
SETTLEMENT OF DISPUTES

1. Any disputes concerning the implementation of this Agreement shall be settled by direct negotiations between the competent authorities.
2. If settlement of a dispute cannot be reached in the manner referred to in Paragraph 1, such a dispute shall be settled through diplomatic channels.

ARTICLE 16
FINAL PROVISIONS

1. This Agreement shall enter into force in accordance with the internal law of each of the Parties, which shall be confirmed by exchange of the notes. The Agreement shall enter into force on the first day of the second month following the receipt of the latter note.
2. This Agreement may be amended on the basis of mutual written consent of both Parties. Such amendments shall enter into force in accordance with the provisions of Paragraph 1.

3. **This Agreement is concluded for an unlimited period of time. It may be terminated by either Party by giving written notice to the other Party. In such a case, this Agreement shall expire after six months following the receipt of the termination notice.**

4. **In case of termination, classified information exchanged or originated on the basis of this Agreement shall be protected in accordance with the provisions hereof.**

Done at ....WARSAW..... **on** .18TH NOVEMBER 2014. **in two original copies, each in the Polish, Montenegrin and English languages, all texts being equally authentic. In case of divergences of interpretation, the English text shall prevail.**

FOR THE GOVERNMENT OF THE REPUBLIC OF POLAND

FOR THE GOVERNMENT OF MONTENEGRO

Po zaznajomieniu się z powyższą umową, w imieniu Rzeczypospolitej Polskiej oświadczam, że:

– została ona uznana za słuszną zarówno w całości, jak i każde z postanowień w niej zawartych,

– jest przyjęta, ratyfikowana i potwierdzona,

– będzie niezmiennie zachowywana.

Na dowód czego wydany został akt niniejszy, opatrzony pieczęcią Rzeczypospolitej Polskiej.

Dano w Warszawie dnia 28 grudnia 2015 r.

Prezydent Rzeczypospolitej Polskiej: *A. Duda*

L.S.

Prezes Rady Ministrów: *B. Szydło*