DZIENNIK USTAW
RZECZYPOSPOLITEJ POLSKIEJ

Warszawa, dnia 27 czerwca 2017 r.

Poz. 1254

UMOWA

między Rządem Rzeczypospolitej Polskiej a Radą Ministrów Bośni i Hercegowiny o ochronie informacji niejawnych,

podpisana w Sarajewie dnia 7 czerwca 2016 r.

W imieniu Rzeczypospolitej Polskiej

PREZYDENT RZECZYPOSPOLITEJ POLSKIEJ

podaje do powszechnej wiadomości:

Dnia 7 czerwca 2016 r. w Sarajewie została podpisana Umowa między Rządem Rzeczypospolitej Polskiej a Radą Ministrów Bośni i Hercegowiny o ochronie informacji niejawnych, w następującym brzmieniu:

UMOWA
między Rządem Rzeczypospolitej Polskiej a Radą Ministrów Bośni i Hercegowiny o ochronie informacji niejawnych

Rząd Rzeczypospolitej Polskiej i Rada Ministrów Bośni i Hercegowiny,

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 norm prawa międzynarodowego i prawa krajowego 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, będące także w trakcie ich wytwarzania, które wymagają ochrony przed nieuprawnionym ujawnieniem lub wykorzystaniem zgodnie z prawem krajowym jednej Strony;
2) „**właściwe organy**" – organy, o których mowa w artykule 3 niniejszej Umowy;
3) „**Strona wytwarzająca**" – Stronę, osobę fizyczną, osobę prawną lub inną jednostkę organizacyjną, uprawnioną do wytwarzania informacji niejawnych zgodnie z prawem krajowym swojej Strony;
4) „**Strona otrzymująca**" – Stronę, osobę fizyczną, osobę prawną lub inną jednostkę organizacyjną, uprawnioną do otrzymywania informacji niejawnych zgodnie z prawem krajowym swojej Strony;
5) „**kontrakt niejawny**" – umowę, której realizacja wiąże się z dostępem do informacji niejawnych, bądź z wytworzeniem takich informacji;
6) „**kontrahent**" – osobę fizyczną, osobę prawną lub inną jednostkę organizacyjną, uprawnioną do zawierania kontraktów niejawnych zgodnie z prawem krajowym jednej ze Stron;
7) „**zlecający**" – kontrahenta uprawnionego do zlecania kontraktów niejawnych zgodnie z prawem krajowym jednej ze Stron;
8) „**poświadczenie bezpieczeństwa**" – dokument wydany zgodnie z prawem krajowym Strony przez właściwy organ lub inny uprawniony podmiot, który potwierdza, że osoba fizyczna została poddana postępowaniu sprawdzającemu i jest uprawniona do dostępu do informacji niejawnych;
9) „**świadectwo bezpieczeństwa przemysłowego**" – dokument wydany zgodnie z prawem krajowym Strony przez właściwy organ lub inny

uprawniony podmiot, który potwierdza, że kontrahent posiada zdolność do ochrony informacji niejawnych; w przypadku kontrahentów będących osobami fizycznymi funkcję świadectwa bezpieczeństwa przemysłowego pełni poświadczenie bezpieczeństwa;

10) „**Strona trzecia**" – państwo oraz osoby fizyczne, osoby prawne lub inne jednostki organizacyjne podlegające jego jurysdykcji lub organizację międzynarodową, niebędące Stroną niniejszej Umowy.

ARTYKUŁ 2
KLAUZULE TAJNOŚCI

1. Informacjom niejawnym przyznaje się odpowiednią do ich treści klauzulę tajności zgodnie z prawem krajowym Strony wytwarzającej. Strona otrzymująca gwarantuje co najmniej równorzędny poziom ochrony otrzymanych informacji niejawnych, zgodnie z postanowieniami ustępu 3.
2. Klauzula tajności może być zmieniona lub zniesiona wyłącznie przez Stronę wytwarzającą. Strona otrzymująca jest pisemnie powiadamiana o każdym przypadku zmiany lub zniesienia klauzuli tajności otrzymanych uprzednio informacji niejawnych.
3. Strony uzgadniają, że niżej wymienione klauzule tajności są równorzędne:

RZECZPOSPOLITA POLSKA	BOŚNIA I HERCEGOWINA	ODPOWIEDNIK W JĘZYKU ANGIELSKIM
ŚCIŚLE TAJNE	VRLO TAJNO	TOP SECRET
TAJNE	TAJNO	SECRET
POUFNE	POVJERLJIVO	CONFIDENTIAL
ZASTRZEŻONE	INTERNO	RESTRICTED

ARTYKUŁ 3
WŁAŚCIWE ORGANY

1. W rozumieniu niniejszej Umowy właściwymi organami, odpowiedzialnymi za stosowanie niniejszej Umowy, są:
   1) w Rzeczypospolitej Polskiej: Szef Agencji Bezpieczeństwa Wewnętrznego;
   2) w Bośni i Hercegowinie: Ministerstwo Bezpieczeństwa Bośni i Hercegowiny, Departament Ochrony Informacji Niejawnych – Krajowa Władza Bezpieczeństwa.
2. Strony powiadamiają się drogą dyplomatyczną o zmianach właściwych organów lub zmianach ich właściwości.

ARTYKUŁ 4
ZASADY OCHRONY INFORMACJI NIEJAWNYCH

1. Strony podejmą wszelkie działania przewidziane w niniejszej Umowie i ich prawie krajowym w celu ochrony informacji niejawnych przekazywanych lub wytwarzanych w ramach współpracy między Stronami, w tym w związku z realizacją kontraktów niejawnych.
2. Strona otrzymująca wykorzystuje informacje niejawne wyłącznie w celach, dla których zostały one przekazane.
3. Strona otrzymująca nie udostępnia informacji, o których mowa w ustępie 1, Stronie trzeciej bez uprzedniej pisemnej zgody Strony wytwarzającej.
4. Informacje niejawne mogą być udostępniane tylko tym osobom, których zadania wymagają zapoznania się z nimi i które posiadają poświadczenie bezpieczeństwa lub zostały w inny sposób upoważnione do dostępu do tych informacji zgodnie z prawem krajowym Strony otrzymującej.

ARTYKUŁ 5
POŚWIADCZENIA BEZPIECZEŃSTWA I ŚWIADECTWA BEZPIECZEŃSTWA PRZEMYSŁOWEGO

1. W zakresie niniejszej Umowy, właściwe organy uznają wzajemnie poświadczenia bezpieczeństwa i świadectwa bezpieczeństwa przemysłowego wydane zgodnie z prawem krajowym drugiej Strony.
2. Na wniosek właściwego organu jednej ze Stron i zgodnie ze swoim prawem krajowym, właściwe organy współpracują podczas przeprowadzania postępowań sprawdzających wobec własnych obywateli zamieszkałych na terytorium państwa drugiej Strony w celu wydania decyzji dotyczącej poświadczenia bezpieczeństwa.

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 w celu wystąpienia do właściwego organu drugiej Strony z prośbą o wydanie zaświadczenia, że kontrahent posiada ważne świadectwo bezpieczeństwa przemysłowego, odpowiednie do klauzuli informacji niejawnych, do których będzie miał dostęp.
2. Wydanie zaświadczenia, 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 krajowym Strony, na terytorium państwa której kontrahent ma swoją siedzibę.
3. Informacje niejawne nie są udostępniane kontrahentowi do czasu uzyskania zaświadczenia, 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. W instrukcji bezpieczeństwa przemysłowego zamieszcza się 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 niejawnym wytworzonym podczas realizacji danego kontraktu niejawnego.
5. Zlecający przekazuje kopię instrukcji bezpieczeństwa przemysłowego właściwemu organowi swojej Strony, który przekazuje ją właściwemu organowi Strony kontrahenta.
6. Realizacja kontraktu niejawnego w części związanej z dostępem do informacji niejawnych jest możliwa po spełnieniu przez kontrahenta niezbędnych warunków zapewniających ochronę informacji niejawnych, zgodnie z instrukcją bezpieczeństwa przemysłowego.
7. Każdy podwykonawca podlega tym samym obowiązkom ochrony informacji niejawnych, jakie ustalono dla kontrahenta.

ARTYKUŁ 7
PRZEKAZYWANIE INFORMACJI NIEJAWNYCH

1. Informacje niejawne są przekazywane drogą dyplomatyczną.
2. Właściwe organy mogą ustalić inne sposoby przekazywania informacji niejawnych zapewniające ich ochronę przed nieuprawnionym ujawnieniem.
3. Strona otrzymująca potwierdza pisemnie odbiór informacji niejawnych.

ARTYKUŁ 8
POWIELANIE LUB TŁUMACZENIE INFORMACJI NIEJAWNYCH

1. Powielanie lub tłumaczenie informacji niejawnych odbywa się w sposób zgodny z prawem krajowym Stron. Powielone lub przetłumaczone informacje niejawne podlegają takiej samej ochronie jak ich oryginały. Liczbę kopii lub tłumaczeń należy ograniczyć do liczby wymaganej dla celów służbowych.
2. Informacje niejawne o klauzuli ŚCIŚLE TAJNE / VRLO TAJNO / TOP SECRET są powielane lub tłumaczone tylko po uprzednim uzyskaniu pisemnego zezwolenia wydanego przez Stronę wytwarzającą.

ARTYKUŁ 9
NISZCZENIE INFORMACJI NIEJAWNYCH

1. Informacje niejawne, z zastrzeżeniem ustępu 2, są niszczone zgodnie z prawem krajowym Strony otrzymującej, w sposób uniemożliwiający ich częściowe lub całkowite odtworzenie.
2. Informacje niejawne o klauzuli ŚCIŚLE TAJNE / VRLO TAJNO / TOP SECRET nie są niszczone; są one zwracane Stronie wytwarzającej.

ARTYKUŁ 10
WIZYTY

1. Obywatelom jednej Strony przybywającym z wizytą na terytorium drugiej Strony, z zastrzeżeniem ustępu 4, 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, o której mowa w ustępie 1, a w pilnych przypadkach w krótszym czasie.

3. Wniosek, o którym mowa w ustępie 2, zawiera:
   1) cel, termin i program wizyty, w tym najwyższą klauzulę tajności informacji niejawnych, z dostępem do których związana jest wizyta;
   2) imię i nazwisko, datę i miejsce urodzenia, obywatelstwo, numer paszportu lub innego dokumentu tożsamości osoby przybywającej z wizytą;
   3) stanowisko służbowe osoby przybywającej z wizytą wraz z nazwą instytucji lub jednostki, którą reprezentuje;
   4) potwierdzenie poziomu oraz daty ważności poświadczenia bezpieczeństwa posiadanego przez osobę przybywającą z wizytą;
   5) nazwę i adres odwiedzanej jednostki;
   6) imię i nazwisko oraz stanowisko służbowe osoby przyjmującej;
   7) datę, podpis oraz oficjalną pieczęć właściwego organu Strony wysyłającej.

4. Właściwe organy mogą wyrazić zgodę na ustalenie wykazów osób upoważnionych do składania wielokrotnych wizyt związanych z realizacją konkretnego projektu, programu lub kontraktu niejawnego. Wykazy te zawierają dane określone w ustępie 3 i są ważne przez okres dwunastu miesięcy od dnia ich zatwierdzenia. Po zatwierdzeniu takich wykazów przez właściwe organy Stron terminy wizyt uzgadniane są bezpośrednio między jednostką wysyłającą a jednostką przyjmującą wizytę, zgodnie z ustalonymi warunkami. Właściwe organy Stron informują się wzajemnie o wszelkich zmianach dotyczących danych określonych w powyższych wykazach.

5. Do ochrony danych osobowych, o których mowa w ustępie 3, przekazywanych w związku z postanowieniami ustępów 1 i 4, stosuje się, z uwzględnieniem prawa krajowego Stron, następujące postanowienia:

   1) wykorzystanie danych osobowych przez Stronę przyjmującą wizytę jest dopuszczalne wyłącznie w celu określonym przez Stronę przekazującą dane osobowe oraz na warunkach określonych przez tę Stronę;

   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 prawem krajowym Strony przekazującej dane osobowe, Strona ta 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 merytoryczną poprawność przekazywanych danych 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 przekazująca dane osobowe oraz Strona przyjmująca wizytę są zobowiązane do rejestrowania przekazywania, otrzymywania i usuwania danych osobowych;

   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.

ARTYKUŁ 11
NARUSZENIE REGULACJI DOTYCZĄCYCH WZAJEMNEJ OCHRONY INFORMACJI NIEJAWNYCH

1. Naruszeniem regulacji dotyczących wzajemnej ochrony informacji niejawnych jest działanie lub zaniechanie sprzeczne z niniejszą Umową lub prawem krajowym Stron dotyczącym ochrony informacji niejawnych.
2. Informację o każdym przypadku naruszenia lub podejrzeniu naruszenia regulacji dotyczących wzajemnej ochrony informacji niejawnych przekazanych przez Stronę wytwarzającą lub informacji niejawnych wytworzonych w wyniku wspólnego działania Stron przekazuje się niezwłocznie właściwemu organowi Strony, na terytorium państwa której miało miejsce naruszenie lub zaistniało podejrzenie takiego naruszenia.
3. Każdy przypadek naruszenia lub podejrzenia naruszenia regulacji dotyczących wzajemnej ochrony informacji niejawnych wyjaśnia się zgodnie z prawem krajowym Strony, na terytorium państwa której zdarzenie miało miejsce.
4. W przypadku naruszenia regulacji dotyczących wzajemnej ochrony informacji niejawnych, o którym mowa w ustępie 1, właściwy organ Strony, na terytorium państwa której naruszenie miało miejsce, pisemnie powiadamia właściwy organ drugiej Strony o tym zdarzeniu, okolicznościach naruszenia, jego skutkach oraz wyniku czynności, o których mowa w ustępie 3.
5. Jeżeli naruszenie regulacji dotyczących informacji niejawnych miało miejsce na terytorium Strony trzeciej, właściwy organ Strony, która przekazała informacje niejawne, podejmie we współpracy ze Stroną trzecią działania, o których mowa w ustępach 2, 3 i 4.
6. Właściwe organy 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. W przypadku stosowania języków urzędowych Strony zobowiązują się przekazywać także tłumaczenie na język urzędowy drugiej Strony lub na język angielski.

ARTYKUŁ 13
KOSZTY

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

ARTYKUŁ 14
KONSULTACJE

1. Właściwe organy informują się wzajemnie o wszelkich zmianach w swoim prawie krajowym dotyczącym ochrony informacji niejawnych, w zakresie niezbędnym do wykonywania 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 Strona zezwoli przedstawicielom właściwego organu drugiej Strony na składanie wizyt na terytorium swojego państwa w celu konsultacji w zakresie stosowania 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 właściwym

organom w prawie krajowym każdej ze 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 rozstrzygane są w drodze bezpośrednich konsultacji między właściwymi organami.
2. Jeśli nie jest możliwe rozwiązanie sporu w sposób, o którym mowa w ustępie 1, jest on rozstrzygany drogą dyplomatyczną.

ARTYKUŁ 16
POSTANOWIENIA KOŃCOWE

1. Niniejsza Umowa podlega przyjęciu zgodnie z prawem krajowym 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 notyfikacji przez każdą ze Stron. W takim przypadku Umowa utraci moc po upływie sześciu miesięcy od dnia otrzymania noty powiadamiającej o wypowiedzeniu.
4. W przypadku wypowiedzenia, informacje niejawne przekazane lub wytworzone na podstawie niniejszej Umowy będą nadal chronione zgodnie z jej postanowieniami.

Sporządzono w Sarajewie dnia 7/06/2016 roku w dwóch jednobrzmiących egzemplarzach, każdy w językach polskim, językach urzędowych Bośni i Hercegowiny (bośniackim, chorwackim, serbskim) i angielskim, przy czym wszystkie teksty mają jednakową moc. W przypadku rozbieżności przy ich interpretacji, za rozstrzygający uważa się tekst w języku angielskim.

Z UPOWAŻNIENIA RZĄDU RZECZYPOSPOLITEJ POLSKIEJ	Z UPOWAŻNIENIA RADY MINISTRÓW BOŚNI I HERCEGOWINY

SPORAZUM

između Vlade Republike Poljske
i Vijeća ministara Bosne i Hercegovine
o zaštiti tajnih podataka

Vlada Republike Poljske

i Vijeće ministara Bosne i Hercegovine,

u daljnjem tekstu „Stranke“

Imajući u vidu potrebu za osiguranjem djelotvorne zaštite tajnih podataka koji su razmijenjeni između Stranaka ili su nastali u području njihove suradnje,

u nakani da usvoje jedinstvene propise za obje Stranke u području zaštite tajnih podataka,

poštujući osiguravajuća pravila međunarodnog prava i nacionalnog zakonodavstva Stranaka,

sporazumjele su se o slijedećem:

ČLANAK 1.
DEFINICIJE

Radi primjene ovog Sporazuma navedeni pojmovi imaju slijedeće značenje:

1) **Tajni podatak** – bilo koja informacija, bez obzira na oblik, sredstva za njihovo zapisivanje i način na koji su zapisani, kao i svi predmeti ili njihovi dijelovi čija je izrada u tijeku i koji zahtijevaju zaštitu od neovlaštenog otkrivanja ili zlouporaba, sukladno s državnim zakonodavstvom Stranaka;
2) **Nadležna tijela** – jesu tijela navedena u članku 3. ovog Sporazuma;
3) **Stranka pošiljatelj** – Stranka, fizičke osobe, pravne osobe ili druge organizacijske jedinice, nadležne da stvaraju tajne podatke, sukladno s državnim zakonodavstvom svake Stranke;
4) **Stranka primatelj** – Stranka, fizičke osobe, pravne osobe ili druge organizacijske jedinice, nadležne da primaju tajne podatke sukladno s državnim zakonodavstvom Stranaka;
5) **Ugovor sa tajnim podatcima** – predstavlja ugovor čije izvršenje podrazumijeva ostvarivanje uvida u tajne podatke ili stvaranje takvih podataka;
6) **Ugovarač – izvršitelj posla** – jeste fizička osoba, pravna osoba ili druga organizacijska jedinica u kontekstu državnog zakonodavstva jedne od Stranaka koji posjeduju poslovnu sposobnost da izvršavaju ugovore sa tajnim podatcima;
7) **Naručilac posla** – Ugovarač koji prema državnom zakonodavstvu jedne Stranke posjeduje poslovnu sposobnost da zaključuje ugovore sa tajnim podatcima;
8) **Sigurnosna dozvola** – dokument koji izdaje nadležno tijelo ili druga ovlaštena osoba sukladno s državnim zakonodavstvom Stranke kojom se potvrđuje da je pojedinac prošao sigurnosne provjere i da je ovlašten za pristup tajnom podatku;

9) **Sigurnosna dozvola za pravne osobe** – dokument koji izdaje nadležno tijelo ili druga ovlaštena osoba sukladno s državnim zakonodavstvom Stranke kojom se potvrđuje da ugovarač – izvršitelj posla ima sposobnost da zaštiti tajni podatak; u slučaju kada samostalni djelatnici djeluju kao ugovarači – izvršitelji posla sigurnosna dozvola će biti jednaka sigurnosnoj dozvoli za pravne osobe;

10) **Treća stranka** – država, kao i fizička osoba, pravna osoba ili druge organizacijske jedinice u okviru pravnog sistema te države ili međunarodna organizacija koja nije Stranka u ovom Sporazumu.

ČLANAK 2.
OZNAKE STUPNJA TAJNOSTI

1. Tajnim podatcima se dodjeljuju oznake stupnja tajnosti sukladno s njihovim sadržajem i državnim zakonodavstvom Stranke pošiljatelja. Stranka primatelj garantira da će tajnim podatcima koje zaprimi osigurati najmanje ekvivalentan stupanj zaštite prema odredbama stavke 3.
2. Oznaka stupnja tajnosti može biti izmijenjena ili uklonjena samo od Stranke pošiljatelja. Stranka primatelj će biti pismeno informirana o svakoj promjeni ili uklanjanju oznake stupnja tajnosti sa podatkom koji je prethodno zaprimio.
3. Stranke su suglasne da su sljedeće oznake stupnja tajnosti ekvivalentne:

REPUBLIKA POLJSKA	BOSNA I HERCEGOVINA	EKVIVALENT NA ENGLESKOM JEZIKU:
ŚCIŚLE TAJNE	VRLO TAJNO	TOP SECRET
TAJNE	TAJNO	SECRET
POUFNE	POVJERLJIVO	CONFIDENTIAL
ZASTRZEŻONE	INTERNO	RESTRICTED

ČLANAK 3.
NADLEŽNA TIJELA

1. U cilju ovog Sporazuma, nadležna tijela odgovorna za provođenje su:
   1) za Republiku Poljsku: Ravnatelj Agencije za unutarnju sigurnost;
   2) za Bosnu i Hercegovinu: Ministarstvo sigurnosti Bosne i Hercegovine, Sektor za zaštitu tajnih podataka – Državno sigurnosno tijelo.
2. Stranke međusobno informiraju diplomatskim putem o svim izmjenama u vezi sa nadležnim tijelom ili o izmjenama njihovih nadležnosti.

ČLANAK 4.
PRINCIPI ZAŠTITE TAJNIH PODATAKA

1. Stranke donose potrebite mjere radi zaštite tajnih podataka prema uvjetima ovog Sporazuma i koje su predmet njihovog državnog zakonodavstva u cilju zaštite tajnih podataka koji su preneseni ili su nastali kao rezultat suradnje između Stranaka, uključujući podatke koji su nastali u vezi sa izvršenjem ugovora sa tajnim podatcima.
2. Stranka primatelj će koristiti tajne podatke isključivo u svrhe u koje su dostavljeni.
3. Stranka primatelj neće ustupiti trećoj stranki podatke koji se navode u stavci 1., bez prethodnog pisanog odobrenja Stranke pošiljatelja.
4. Pristup tajnim podatcima bit će odobren samo onim osobama koja postupaju sukladno s principom „potrebno znati“ i imaju sigurnosnu dozvolu ili koja su ovlaštena da izvrše uvid u takve podatke, sukladno sa državnim zakonodavstvom Stranke primatelja.

ČLANAK 5.
SIGURNOSNE DOZVOLE

1. U okviru ovog Sporazuma, nadležna tijela će uzajamno priznati sigurnosne dozvole i sigurnosne dozvole za pravne osobe koje su izdate sukladno sa državnim zakonodavstvom druge Stranke.
2. Nadležna tijela, na zahtjev nadležnog tijela jedne od Stranaka, postupajući skladno s njihovim državnim zakonodavstvom, uzajamno surađuju u postupcima provjera njihovih građana koji borave na državnom području druge Stranke, u svrhu donošenja odluke o sigurnosnoj dozvoli.

ČLANAK 6.
UGOVORI SA TAJNIM PODATCIMA

1. Prije zaključivanja ugovora sa tajnim podatcima koji se odnosi na ostvarivanje uvida u podatke sa oznakom stupnja tajnosti POUFNE / POVJERLJIVO / CONFIDENTIAL ili više, naručitelj posla podnosi zahtjev svom nadležnom tijelu da od nadležnog tijela druge Stranke traži izdavanje certifikata da ugovaratelj – izvršitelj posla posjeduje važeću sigurnosnu dozvolu za pravne osobe koje odgovaraju stupnju tajnosti podataka u koje ugovaratelj – izvršitelj treba ostvariti uvid.
2. Izdavanje certifikata iz stavke 1. bit će jednako garanciji da su provedene potrebite radnje na osnovu kojih se smatra da ugovaratelj – izvršitelj posla zadovoljava kriterije s područja zaštite tajnih podataka koji su utvrđeni državnim zakonodavstvom Stranke na čijem području države se nalazi.
3. Tajni podatci neće biti dostupni ugovaratelju – izvršitelju posla dok ne dobije certifikat koji se navodi u stavci 1.
4. Naručitelj posla dostavlja ugovaratelju – izvršitelju posla sigurnosno uputstvo za pravne osobe koje je potrebito za izvršenje ugovora sa tajnim podatcima i čini sastavni dio svakog ugovora s tajnim podatcima.

Sigurnosno uputstvo za pravne osobe sadrži odredbe o sigurnosnim zahtjevima i to:

1) spis vrsta tajnih podataka koje se odnose na ugovor sa tajnim podatcima, pri čemu se uzimaju u obzir njihovi stupnji tajnosti;
2) pravila za dodjeljivanje oznake stupnja tajnosti podatcima koji su nastali tijekom izvršenja datog ugovora sa tajnim podatcima.

5. Naručitelj posla dostavlja primjerak sigurnosnog uputstva za pravnu osobu svom nadležnom tijelu koji će ga proslijediti nadležnom tijelu ugovaratelja – izvršiotelja posla.
6. Izvršenje ugovora sa tajnim podatcima u dijelu koji se odnosi na ostvarivanje uvida u tajne podatke bit će moguće pod uvjetom da ugovaratelj - izvršitelj posla ispuni kriterije za zaštitu tajnih podataka, sukladno s sigurnosnim uputstvom za pravnu osobu.
7. Svaki podugovaratelj – izvršitelj posla dužan je da ispuni iste uvjete za zaštitu tajnih podataka kao i ugovaratelj – izvršitelj posla.

ČLANAK 7.
DOSTAVLJANJE TAJNIH PODATAKA

1. Tajni podatci dostavljaju se diplomatskim putem.
2. Nadležna tijela mogu se dogovoriti i oko drugih načina dostavljanja tajnih podataka koji osiguravaju zaštitu od neovlaštenog otkrivanja.
3. Stranka primatelj pisanim putem potvrđuje prijem tajnih podataka.

ČLANAK 8.
UMNOŽAVANJE ILI PREVOĐENJE TAJNIH PODATAKA

1. Množenje ili prevođenje tajnih podataka vrši se na osnovu državnog zakonodavstva svake Stranke. Množeni ili prevedeni podatci bit će

zaštićeni na isti način kao originalni. Broj množenih primjeraka ili prevoda treba svesti na broj koji se zahtijeva u službene svrhe.

2. Podatci sa oznakom ŚCIŚLE TAJNE / VRLO TAJNO / TOP SECRET množe se ili prevode samo uz prethodno pribavljeno odobrenje Stranke pošiljatelja.

ČLANAK 9.
UNIŠTENJE TAJNIH PODATAKA

1. Prema stavci 2., tajni podatci uništavaju se sukladno sa državnim zakonodavstvom Stranke primatelja tako da se onemogući njihova djelimična ili potpuna rekonstrukcija.
2. Podatci sa oznakom stupnja tajnosti ŚCIŚLE TAJNE / VRLO TAJNO / TOP SECRET ne uništavaju se, već se vraćaju Stranki pošiljatelju.

ČLANAK 10.
POSJETE

1. Prema stavci 4. osobama koje dolaze u posjetu na područje države druge Stranke bit će odobren uvid u tajne podatke po prijemu pismenog odobrenja nadležnog tijela druge Stranke.
2. Nadležno tijelo stranke posjetitelja podnosi zahtjev za posjetu nadležnom tijelu stranke domaćina najmanje 30 dana prije planirane posjete iz stavke 1., a u vanrednim slučajevima i u kraćem roku.
3. Zahtjev za posjetu iz stavke 2. treba da sadrži:
   1) svrhu, datum i program posjete, uključujući najviši nivo oznake stupnja tajnosti podataka kojima se pristupa;
   2) ime i prezime, datum i mjesto rođenja, državljanstvo i broj putne isprave ili drugog identifikacionog dokumenta posjetitelja;
   3) funkciju posjetitelja i naziv tijela koji oni predstavljaju;

4) stupanj tajnosti i datum važenja sigurnosne dozvole koju posjeduje posjetitelj;
5) naziv i adresa tijela koji se posjećuje;
6) ime, prezime i funkcija osobe koje će biti posjećeno;
7) datum, potpis i službeni pečat nadležnog tijela stranke koja se posjećuje.

4. Nadležno tijelo može dogovoriti da se izrade popisi osoba ovlaštenih da realiziraju periodične posjete u vezi s provođenjem određenog projekta, programa ili ugovora sa tajnim podatcima. Takvi popisi sadrže podatke koji su predviđeni u stavci 3., a rok njihovog važenja je dvanaest (12) mjeseci nakon odobrenja. Kada nadležno tijelo Stranaka odobre takve popise, datume posjeta će dogovoriti direktno tijelo koji šalje posjetitelje i tijelo koje ih prima, sukladno s dogovorenim uvjetima. Nadležno tijelo Stranaka će se uzajamno informirati o svakoj izmjeni koja se tiče podataka u ranije navedenim popisima.
5. Radi zaštite osobnih podataka iz stavke 3. koji se dostavljaju u vezi sa odredbama stavaka 1. i 4., sukladno s državnim zakonodavstvom Stranaka, primjenjuju se sljedeće odredbe:
   1) osobni podatci koje primi stranka kojoj se podatci dostavljaju bit će korišteni isključivo u svrhu i pod uvjetima koje je definirala stranka koja dostavlja osobne podatke;
   2) stranka kojoj se podatci dostavljaju čuvat će osobne podatke onoliko koliko je potrebito da se postigne svrha njihove obrade;
   3) u slučaju da osobni podatci budu dostavljeni suprotno državnom zakonodavstvu Stranke, stranka koja dostavlja podatke informira o tome stranku kojoj se podatci dostavljaju koja će biti obvezna da te podatke ukloni na način da onemogući njihovu djelimičnu ili potpunu rekonstrukciju;

4) stranka koja dostavlja osobne podatke preuzima odgovornost za točnost osobnih podataka koje dostavlja i, u slučaju da su oni neistiniti ili nepotpuni, informira o tome stranku kojoj se podatci dostavljaju koja će biti obvezna da ispravi ili ukloni te podatke;
5) stranka kojoj se podtci dostavljaju i stranka koja dostavlja osobne podatke su obvezni da vode evidenciju o dostavi, prijemu i uklanjanju losobnih podataka;
6) stranka koja dostavlja osobne podatke i stranka kojoj se podatci dostavljaju su obvezne da osobne podatke koji su predmet obrade djelotvorno zaštite od otkrivanja neovlaštenim osobama, nedozvoljenih izmjena, gubitka, oštećenje ili uništenja.

ČLANAK 11.
POVREDA SIGURNOSTI

1. Povreda sigurnosti tajnih podataka predstavlja čin ili propust suprotno odredbama ovog Sporazuma ili državnom zakonodavstvu Stranaka koje se odnosi na zaštitu tajnih podataka.
2. O povredi sigurnosti tajnih podataka Stranke pošiljatelja ili tajnih podataka nastalih kao rezultat suradnje Stranaka, odnosno o postojanju sumnje da je povreda nastupila, odmah se informira nadležno tijelo Stranke na čijem području države je došlo do povrede ili postoji sumnja da je povreda nastupila.
3. Svaka povreda sigurnosti, ili postojanje sumnje o njenom nastupanju, bit će istražena sukladno s državnim zakonodavstvom Stranke na čijem području države je došlo do povrede.
4. U slučaju povrede sigurnosti iz stavke 1. nadležno tijelo Stranke na čijem području države je došlo do povrede pisanim putem će informirati nadležno tijelo druge Stranke o toj činjenici, okolnostima, učincima i rezultatima radnji iz stavke 3.

5. U slučaju pojave povrede sigurnosti na području treće Stranke, nadležno tijelo Stranke koja je poslala tajne podatke poduzima – u suradnji sa trećom Strankom - radnje iz stavke 2, 3 i 4.
6. Nadležno tijelo, na zahtjev jednog od njih, će surađivati u provođenju radnji koje su predviđene u stavci 3.

ČLANAK 12.
JEZICI

U primjeni odredbi ovog Sporazuma Stranke će koristiti engleski jezik ili svoje službene jezike dostavljajući tada i prevod na službeni jezik druge Stranke, odnosno prevod na engleski jezik.

ČLANAK 13.
TROŠKOVI

Svaka Stranka će snositi troškove koji nastanu u primjeni odredbi ovog Sporazuma.

ČLANAK 14.
KONSULTACIJE

1. Nadležna tijela međusobno se informiraju o svim izmjenama i dopunama njihovog državnog zakonodavstva u vezi sa zaštitom tajnih podataka koje utiču na sprovođenje ovog Sporazuma.
2. Nadležna tijela Stranaka će se konsultovati, na zahtjev jednog od njih, u cilju ostvarivanja neposredne suradnje u provođenju odredbi ovog Sporazuma.

3. Svaka Stranka će omogućiti predstavnicima nadležnog tijela druge Stranke da dođu u posjetu na području te države, kako bi razmotrile procedure za zaštitu tajnih podataka koje je dostavila druga Stranka.
4. Radi ostvarivanja efikasne suradnje, koja je predmet ovog Sporazuma, nadležna tijela Stranaka mogu, ako je to potrebito, u okviru svojih ovlaštenja utvrđenih državnim zakonodavstvom, zaključiti detaljnije tehničke ili organizacijske aranžmane.

ČLANAK 15.
RJEŠAVANJE SPOROVA

1. Svi sporovi u vezi sa primjenom ovog Sporazuma će se rješavati neposrednim pregovorima između nadležnih tijela.
2. Ukoliko rješenje spora ne može biti postignuto na način naveden u stavci 1. isti će biti riješen diplomatskim putem.

ČLANAK 16.
ZAVRŠNE ODREDBE

1. Ovaj Sporazum stupa na snagu sukladno s državnim zakonodavstvom svake Stranke što će biti potvrđeno međusobnom razmjenom nota. Sporazum stupa na snagu prvog dana drugog mjeseca nakon prijema posljednje note.
2. Ovaj Sporazum može biti izmijenjen na osnovu pismene suglasnosti obje Stranke. Takve izmjene stupaju na snagu sukladno s odredbama stavke 1.
3. Ovaj Sporazum se zaključuje na neodređeno vrijeme. Svaka Stranka može otkazati ovaj Sporazum dostavljanjem pismenog informiranja o otkazu drugoj Stranci. U tom slučaju važenje ovog Sporazuma ističe nakon šest mjeseci od prijema informacije o otkazu.

4. U slučaju otkaza, svi tajni podatci koji su razmijenjeni ili nastali na osnovu ovog Sporazuma bit će zaštićeni prema odrebama istog.

Zaključeno u Sarajevu dana 7/06/2016 u dva originalna primjerka, svaki na poljskom, službenim jezicima Bosne i Hercegovine (bosanskom, hrvatskom, srpskom) i engleskom jeziku, pri čemu su svi tekstovi podjednako vjerodostojni. U slučaju neslaganja u tumačenju, bit će mjerodavan tekst Sporazuma na engleskom jeziku.

ZA VLADU REPUBLIKE POLJSKE	ZA VIJEĆE MINISTARA BOSNE I HERCEGOVINE

SPORAZUM

između Vlade Republike Poljske
i Vijeća ministara Bosne i Hercegovine
o zaštiti tajnih podataka

Vlada Republike Poljske

i Vijeće ministara Bosne i Hercegovine,

u daljem tekstu „Strane“

Uzimajući u obzir potrebu za osiguranjem djelotvorne zaštite tajnih podataka koji su razmijenjeni između Strana ili su nastali u okviru njihove saradnje,

u namjeri da usvoje jedinstvene propise za obje Strane u oblasti zaštite tajnih podataka,

poštujući obezbjeđujuća pravila međunarodnog prava i nacionalnog zakonodavstva Strana,

sporazumjele su se sljedeće:

ČLAN 1.

DEFINICIJE

Radi primjene ovog Sporazuma navedeni pojmovi imaju slijedeće značenje:

1) **Tajni podatak** – bilo koja informacija, bez obzira na oblik, sredstva za njihovo zapisivanje i način na koji su zapisani, kao i svi predmeti ili njihovi dijelovi čija je izrada u toku i koji zahtijevaju zaštitu od neovlaštenog otkrivanja ili zloupotreba, u skladu sa državnim zakonodavstvom Strana;
2) **Nadležni organi** – jesu organi navedeni u članu 3. ovog Sporazuma;
3) **Strana pošiljalac** – Strana, fizička lica, pravna lica ili druge organizacione jedinice, nadležne da stvaraju tajne podatke, u skladu sa državnim zakonodavstvom svake Strane;
4) **Strana primalac** – Strana, fizička lica, pravna lica ili druge organizacione jedinice, nadležne da primaju tajne podatke u skladu sa državnim zakonodavstvom Strana;
5) **Ugovor sa tajnim podacima** – jeste ugovor čije izvršenje podrazumijeva ostvarivanje uvida u tajne podatke ili stvaranje takvih podataka;
6) **Ugovarač – izvršilac posla** – jeste fizičko lice, pravno lice ili druga organizaciona jedinica u okviru državnog zakonodavstva jedne od Strana koji posjeduju poslovnu sposobnost da izvršavaju ugovore sa tajnim podacima;
7) **Naručilac posla** – Ugovarač koji prema državnom zakonodavstvu jedne Strane posjeduje poslovnu sposobnost da zaključuje ugovore sa tajnim podacima;
8) **Sigurnosna dozvola** – dokument koji izdaje nadležni organ ili drugo ovlašteno lice u skladu sa državnim zakonodavstvom Strane kojim se potvrđuje da je pojedinac prošao sigurnosne provjere i da je ovlašten za pristup tajnom podatku;
9) **Sigurnosna dozvola za pravna lica** – dokument koji izdaje nadležni organ ili drugo ovlašteno lice u skladu sa državnim zakonodavstvom

Strane kojim se potvrđuje da ugovarač – izvršilac posla ima sposobnost da zaštiti tajni podatak; u slučaju kada samostalni djelatnici djeluju kao ugovarači – izvršioci posla sigurnosna dozvola će biti jednaka sigurnosnoj dozvoli za pravna lica;

10) **Treća strana** – država, kao i fizičko lice, pravno lice ili druge organizacione jedinice u okviru pravnog sistema te države ili međunarodna organizacija koja nije Strana u ovom Sporazumu.

ČLAN 2.
OZNAKE STEPENA TAJNOSTI

1. Tajnim podacima se dodjeljuju oznake stepena tajnosti u skladu sa njihovim sadržajem i državnim zakonodavstvom Strane pošiljaoca. Strana primalac garantuje da će tajnim podacima koje primi osigurati najmanje ekvivalentan stepen zaštite prema odredbama stava 3.
2. Oznaka stepena tajnosti može biti izmijenjena ili uklonjena samo od Strane pošiljaoca. Strana primalac će biti pismeno obaviještena o svakoj promjeni ili uklanjanju oznake stepena tajnosti sa podatka koji je prethodno primio.
3. Strane su saglasne da su sljedeće oznake stepena tajnosti ekvivalentne:

REPUBLIKA POLJSKA	BOSNA I HERCEGOVINA	EKVIVALENT NA ENGLESKOM JEZIKU:
ŚCIŚLE TAJNE	VRLO TAJNO	TOP SECRET
TAJNE	TAJNO	SECRET
POUFNE	POVJERLJIVO	CONFIDENTIAL
ZASTRZEŻONE	INTERNO	RESTRICTED

ČLAN 3.
NADLEŽNI ORGANI

1. U svrhu ovog Sporazuma, nadležni organi odgovorni za provođenje su:
   1) za Republiku Poljsku: Direktor Agencije za unutrašnju sigurnost;
   2) za Bosnu i Hercegovinu: Ministarstvo sigurnosti Bosne i Hercegovine, Sektor za zaštitu tajnih podataka – Državni sigurnosni organ.
2. Strane se uzajamno obavještavaju diplomatskim putem o svim izmjenama u vezi sa nadležnim organima ili o izmjenama njihovih nadležnosti.

ČLAN 4.
PRINCIPI ZAŠTITE TAJNIH PODATAKA

1. Strane donose potrebne mjere radi zaštite tajnih podataka prema uslovima ovog Sporazuma i koje su predmet njihovog državnog zakonodavstva u svrhu zaštite tajnih podataka koji su preneseni ili su nastali kao rezultat saradnje između Strana, uključujući podatke koji su nastali u vezi sa izvršenjem ugovora sa tajnim podacima.
2. Strana primalac će koristiti tajne podatke isključivo u svrhe u koje su dostavljeni.
3. Strana primalac neće ustupiti trećoj strani podatke koji se navode u stavu 1., bez prethodnog pisanog odobrenja Strane pošiljaoca.
4. Pristup tajnim podacima bit će odobren samo onim licima koja postupaju u skladu s principom „potrebno znati“ i imaju sigurnosnu dozvolu ili koja su ovlaštena da izvrše uvid u takve podatke, u skladu sa državnim zakonodavstvom Strane primaoca.

ČLAN 5.
SIGURNOSNE DOZVOLE

1. U okviru ovog Sporazuma, nadležni organi će međusobno priznati sigurnosne dozvole i sigurnosne dozvole za pravna lica koje su izdate u skladu sa državnim zakonodavstvom druge Strane.
2. Nadležni organi, na zahtjev nadležnog organa jedne od Strana, postupajući u skladu sa njihovim državnim zakonodavstvom, međusobno sarađuju u postupcima provjera njihovih građana koji borave na državnoj teritoriji druge Strane, u svrhu donošenja odluke o sigurnosnoj dozvoli.

ČLAN 6.
UGOVORI SA TAJNIM PODACIMA

1. Prije zaključivanja ugovora sa tajnim podacima koji se odnosi na ostvarivanje uvida u podatke sa oznakom stepena tajnosti POUFNE / POVJERLJIVO / CONFIDENTIAL ili više, naručilac posla podnosi zahtjev svom nadležnom organu da od nadležnog organa druge Strane traži izdavanje certifikata da ugovarač – izvršilac posla posjeduje važeću sigurnosnu dozvolu za pravna lica koja odgovara stepenu tajnosti podataka u koje ugovarač – izvršilac treba ostvariti uvid.
2. Izdavanje certifikata iz stava 1. bit će jednako garanciji da su provedene potrebne radnje na osnovu kojih se smatra da ugovarač – izvršilac posla zadovoljava kriterije iz oblasti zaštite tajnih podataka koji su utvrđeni državnim zakonodavstvom Strane na čijem području države se nalazi.
3. Tajni podaci neće biti dostupni ugovaraču – izvršiocu posla dok ne dobije certifikat koji se navodi u stavu 1.
4. Naručilac posla dostavlja ugovaraču – izvršiocu posla sigurnosno uputstvo za pravno lice koje je potrebno za izvršenje ugovora sa tajnim podacima i čini sastavni dio svakog ugovora s tajnim podacima. Sigurnosno uputstvo za pravno lice sadrži odredbe o sigurnosnim zahtjevima i to:

1) popis vrsta tajnih podataka koje se odnose na ugovor sa tajnim podacima, pri čemu se uzimaju u obzir njihovi stepeni tajnosti;
2) pravila za dodjeljivanje oznake stepena tajnosti podacima koji su nastali tokom izvršenja datog ugovora sa tajnim podacima.

5. Naručilac posla dostavlja primjerak sigurnosnog uputstva za pravno lice svom nadležnom organu koji će ga proslijediti nadležnom organu ugovarača – izvršioca posla.
6. Izvršenje ugovora sa tajnim podacima u dijelu koji se odnosi na ostvarivanje uvida u tajne podatke bit će moguće pod uslovom da ugovarač – izvršilac posla ispuni kriterije za zaštitu tajnih podataka, u skladu sa sigurnosnim uputstvom za pravno lice.
7. Svaki podugovarač – izvršilac posla dužan je da ispuni iste uslove za zaštitu tajnih podataka kao i ugovarač – izvršilac posla.

ČLAN 7.
DOSTAVLJANJE TAJNIH PODATAKA

1. Tajni podaci dostavljaju se diplomatskim putem.
2. Nadležni organi mogu se dogovoriti i oko drugih načina dostavljanja tajnih podataka koji osiguravaju zaštitu od neovlaštenog otkrivanja.
3. Strana primalac pisanim putem potvrđuje prijem tajnih podataka.

ČLAN 8.
UMNOŽAVANJE ILI PREVOĐENJE TAJNIH PODATAKA

1. Umnožavanje ili prevođenje tajnih podataka vrši se na osnovu državnog zakonodavstva svake Strane. Umnoženi ili prevedeni podaci bit će zaštićeni na isti način kao originalni. Broj umnoženih primjeraka ili prevoda treba svesti na broj koji se zahtijeva u službene svrhe.

2. Podaci sa oznakom ŠCIŠLE TAJNE / VRLO TAJNO / TOP SECRET umnožavaju se ili prevode samo uz prethodno pribavljeno odobrenje Strane pošiljaoca.

ČLAN 9.
UNIŠTENJE TAJNIH PODATAKA

1. Prema stavu 2., tajni podaci uništavaju se u skladu sa državnim zakonodavstvom Strane primaoca tako da se onemogući njihova djelimična ili potpuna rekonstrukcija.
2. Podaci sa oznakom stepena tajnosti ŠCIŠLE TAJNE / VRLO TAJNO / TOP SECRET ne uništavaju se, već se vraćaju Strani pošiljaocu.

ČLAN 10.
POSJETE

1. Prema stavu 4. licima koja dolaze u posjetu na teriotoriju države druge Strane bit će odobren uvid u tajne podatke po prijemu pismenog odobrenja nadležnog organa druge Strane.
2. Nadležni organ strane posjetioca podnosi zahtjev za posjetu nadležnom organu strane domaćina najmanje 30 dana prije planirane posjete iz stava 1., a u vanrednim slučajevima i u kraćem roku.
3. Zahtjev za posjetu iz stava 2. treba da sadrži:
   1) svrhu, datum i program posjete, uključujući najviši nivo oznake stepena tajnosti podataka kojima se pristupa;
   2) ime i prezime, datum i mjesto rođenja, državljanstvo i broj putne isprave ili drugog identifikacionog dokumenta posjetioca;
   3) funkciju posjetioca i naziv organa koji oni predstavljaju;
   4) stepen tajnosti i datum važenja sigurnosne dozvole koju posjeduje posjetilac;

5) naziv i adresa organa koji se posjećuje;
6) ime, prezime i funkcija lica koje će biti posjećeno;
7) datum, potpis i službeni pečat nadležnog organa strane koja se posjećuje.

4. Nadležni organi mogu dogovoriti da se izrade spiskovi lica ovlaštenih da realizuju periodične posjete u vezi s provođenjem određenog projekta, programa ili ugovora sa tajnim podacima. Takvi spiskovi sadrže podatke koji su predviđeni u stavu 3., a rok njihovog važenja je dvanaest (12) mjeseci nakon odobrenja. Kada nadležni organi Strana odobre takve spiskove, datume posjeta će dogovoriti direktno organ koji šalje posjetioce i organ koji ih prima, u skladu sa dogovorenim uslovima. Nadležni organi Strana će se međusobno obavještavati o svakoj izmjeni koja se tiče podataka u ranije navedenim spiskovima.
5. Radi zaštite ličnih podataka iz stava 3. koji se dostavljaju u vezi sa odredbama stavova 1. i 4., u skladu sa državnim zakonodavstvom Strana, primjenjuju se sljedeće odredbe:
   1) lični podaci koje primi strana kojoj se podaci dostavljaju bit će korišteni isključivo u svrhu i pod uslovima koje je definisala strana koja dostavlja lične podatke;
   2) strana kojoj se podaci dostavljaju čuvat će lične podatke onoliko koliko je potrebno da se postigne svrha njihove obrade;
   3) u slučaju da lični podaci budu dostavljeni suprotno državnom zakonodavstvu Strane, strana koja dostavlja podatke obvještava o tome stranu kojoj se podaci dostavljaju koja će biti obavezna da te podatke ukloni na način da onemogući njihovu djelimičnu ili potpunu rekonstrukciju;
   4) strana koja dostavlja lične podatke preuzima odgovornost za tačnost ličnih podataka koje dostavlja i, u slučaju da su oni neistiniti ili nepotpuni, obavještava o tome stranu kojoj se podaci dostavljaju koja će biti obavezna da ispravi ili ukloni te podatke;

5) strana kojoj se podaci dostavljaju i strana koja dostavlja lične podatke su obavezne da vode evidenciju o dostavi, prijemu i uklanjanju ličnih podataka;
6) strana koja dostavlja lične podatke i strana kojoj se podaci dostavljaju su obavezne da lične podatke koji su predmet obrade djelotvorno zaštite od otkrivanja neovlaštenim licima, nedozvoljenih izmjena, gubitka, oštećenje ili uništenja.

ČLAN 11.
POVREDA SIGURNOSTI

1. Povreda sigurnosti tajnih podataka predstavlja činjenje ili nečinjenje suprotno odredbama ovog Sporazuma ili državnom zakonodavstvu Strana koje se odnosi na zaštitu tajnih podataka.
2. O povredi sigurnosti tajnih podataka Strane pošiljaoca ili tajnih podataka nastalih kao rezultat saradnje Strana, odnosno o postojanju sumnje da je povreda nastupila, odmah se obavještava nadležni organ Strane na čijoj teritoriji države je došlo do povrede ili postoji sumnja da je povreda nastupila.
3. Svaka povreda sigurnosti, ili postojanje sumnje o njenom nastupanju, bit će istražena u skladu sa državnim zakonodavstvom Strane na čijoj teritoriji države je došlo do povrede.
4. U slučaju povrede sigurnosti iz stava 1. nadležni organ Strane na čijoj teritoriji države je došlo do povrede pisanim putem će obavijestiti nadležni organ druge Strane o toj činjenici, okolnostima, učincima i rezultatima radnji iz stava 3.
5. U slučaju pojave povrede sigurnosti na području treće Strane, nadležni organ Strane koja je poslala tajne podatke preduzima – u saradnji sa trećom Stranom - radnje iz stava 2, 3 i 4.

6. Nadležni organi, na zahtjev jednog od njih, će sarađivati u provođenju radnji koje su predviđene u stavu 3.

ČLAN 12.
JEZICI

U primjeni odredbi ovog Sporazuma Strane će koristiti engleski jezik ili svoje službene jezike dostavljajući tada i prevod na službeni jezik druge Strane, odnosno prevod na engleski jezik.

ČLAN 13.
TROŠKOVI

Svaka Strana će snositi troškove koji nastanu u primjeni odredbi ovog Sporazuma.

ČLAN 14.
KONSULTACIJE

1. Nadležni organi uzajamno se obavještavaju o svim izmjenama i dopunama njihovog državnog zakonodavstva u vezi sa zaštitom tajnih podataka koje utiču na provođenje ovog Sporazuma.
2. Nadležni organi Strana će se konsultovati, na zahtjev jednog od njih, u cilju ostvarivanja neposredne saradnje u provođenju odredbi ovog Sporazuma.
3. Svaka Strana će omogućiti predstavnicima nadležnog organa druge Strane da dođu u posjetu na teritoriju te države, kako bi razmotrile procedure za zaštitu tajnih podataka koje je dostavila druga Strana.

4. Radi ostvarivanja efikasne saradnje, koja je predmet ovog Sporazuma, nadležni organi Strana mogu, ako je to potrebno, u okviru svojih ovlaštenja utvrđenih državnim zakonodavstvom, zaključiti detaljnije tehničke ili organizacione aranžmane.

ČLAN 15.
RJEŠAVANJE SPOROVA

1. Svi sporovi u vezi sa primjenom ovog Sporazuma će se rješavati neposrednim pregovorima između nadležnih organa.
2. Ukoliko rješenje spora ne može biti postignuto na način naveden u stavu 1. isti će biti riješen diplomatskim putem.

ČLAN 16.
ZAVRŠNE ODREDBE

1. Ovaj Sporazum stupa na snagu u skladu sa državnim zakonodavstvom svake Strane što će biti potvrđeno uzajamnom razmjenom nota. Sporazum stupa na snagu prvog dana drugog mjeseca nakon prijema posljednje note.
2. Ovaj Sporazum može biti izmijenjen na osnovu pismene saglasnosti obje Strane. Takve izmjene stupaju na snagu u skladu sa odredbama stava 1.
3. Ovaj Sporazum se zaključuje na neodređeno vrijeme. Svaka Strana može otkazati ovaj Sporazum dostavljanjem pismenog obavještenja o otkazu drugoj Strani. U tom slučaju važenje ovog Sporazuma ističe nakon šest mjeseci od prijema obavještenja o otkazu.
4. U slučaju otkaza, svi tajni podaci koji su razmijenjeni ili nastali na osnovu ovog Sporazuma bit će zaštićeni prema odrebama istog.

Zakljućeno u Sarajevu dana 7/06/2016 u dva originalna primjerka, svaki na poljskom, službenim jezicima Bosne i Hercegovine (bosanskom, hrvatskom, srpskom) i engleskom jeziku, pri čemu su svi tekstovi podjednako vjerodostojni. U slučaju neslaganja u tumačenju, bit će mjerodavan tekst Sporazuma na engleskom jeziku.

ZA VLADU REPUBLIKE POLJSKE	ZA VIJEĆE MINISTARA BOSNE I HERCEGOVINE

СПОРАЗУМ

између Владе Републике Пољске и Савјета министара Босне и Херцеговине о заштити тајних података

Влада Републике Пољске и
Савјет министара Босне и Херцеговине,
у даљем тексту „Стране“

Узимајући у обзир потребу за обезбјеђењем дјелотворне заштите тајних података који су размијењени између Страна или су настали у оквиру њихове сарадње,

у намјери да усвоје јединствене прописе за обје Стране у области заштите тајних података,

поштујући обезбјеђујућа правила међународног права и националног законодавства Страна,

споразумјеле су се сљедеће:

ЧЛАН 1.
ДЕФИНИЦИЈЕ

Ради примјене овог Споразума наведени појмови имају сљедеће значење:

1) **Тајни податак** – било која информација, без обзира на облик, средства за њихово записивање и начин на који су записани, као и сви предмети или њихови дијелови чија је израда у току и који захтијевају заштиту од неовлаштеног откривања или злоупотреба, у складу са државним законодавством Страна;
2) **Надлежни органи** – јесу органи наведени у члану 3. овог Споразума;
3) **Страна пошиљалац** – Страна, физичка лица, правна лица или друге организационе јединице, надлежне да стварају тајне податке, у складу са државним законодавством сваке Стране;
4) **Страна прималац** – Страна, физичка лица, правна лица или друге организационе јединице, надлежне да примају тајне податке у складу са државним законодавством Страна;
5) **Уговор са тајним подацима** – јесте уговор чије извршење подразумијева остваривање увида у тајне податке или стварање таквих података;
6) **Уговарач – извршилац посла** – јесте физичко лице, правно лице или друга организациона јединица у оквиру државног законодавства једне од Страна који посједују пословну способност да извршавају уговоре са тајним подацима;
7) **Наручилац посла** – Уговарач који према државном законодавству једне Стране посједује пословну способност да закључује уговоре са тајним подацима;
8) **Безбједносна дозвола** – документ који издаје надлежни орган или друго овлаштено лице у складу са државним законодавством Стране којим се потврђује да је појединац прошао безбједносне провјере и да је овлаштен за приступ тајном податку;

9) **Безбједносна дозвола за правна лица** – документ који издаје надлежни орган или друго овлаштено лице у складу са државним законодавством Стране којим се потврђује да уговарач – извршилац посла има способност да заштити тајни податак; у случају када самостални дјелатници дјелују као уговарачи – извршиоци посла безбједносна дозвола ће бити једнака безбједносној дозволи за правна лица;

10) **Трећа страна** – држава, као и физичко лице, правно лице или друге организационе јединице у оквиру правног система те државе или међународна организација која није Страна у овом Споразуму.

ЧЛАН 2.
ОЗНАКЕ СТЕПЕНА ТАЈНОСТИ

1. Тајним подацима се додјељују ознаке степена тајности у складу са њиховим садржајем и државним законодавством Стране пошиљаоца. Страна прималац гарантује да ће тајним подацима које прими обезбједити најмање еквивалентан степен заштите према одредбама става 3.
2. Ознака степена тајности може бити измијењена или уклоњена само од Стране пошиљаоца. Страна прималац ће бити писмено обавијештена о свакој промјени или уклањању ознаке степена тајности са податка који је претходно примио.
3. Стране су сагласне да су сљедеће ознаке степена тајности еквивалентне:

РЕПУБЛИКА ПОЉСКА	БОСНА И ХЕРЦЕГОВИНА	ЕКВИВАЛЕНТ НА ЕНГЛЕСКОМ ЈЕЗИКУ:
ŚCIŚLE TAJNE	ВРЛО ТАЈНО	TOP SECRET
TAJNE	ТАЈНО	SECRET

POUFNE	ПОВЈЕРЉИВО	CONFIDENTIAL
ZASTRZEŻONE	ИНТЕРНО	RESTRICTED

ЧЛАН 3.

НАДЛЕЖНИ ОРГАНИ

1. У сврху овог Споразума, надлежни органи одговорни за провођење су:
   1) за Републику Пољску: Директор Агенције за унутрашњу безбједност;
   2) за Босну и Херцеговину: Министарство безбједности Босне и Херцеговине, Сектор за заштиту тајних података – Државни сигурносни орган.
2. Стране се узајамно обавјештавају дипломатским путем о свим измјенама у вези са надлежним органима или о измјенама њихових надлежности.

ЧЛАН 4.

ПРИНЦИПИ ЗАШТИТЕ ТАЈНИХ ПОДАТАКА

1. Стране доносе потребне мјере ради заштите тајних података према условима овог Споразума и које су предмет њиховог државног законодавства у сврху заштите тајних података који су пренесени или су настали као резултат сарадње између Страна, укључујући податке који су настали у вези са извршењем уговора са тајним подацима.
2. Страна прималац ће користити тајне податке искључиво у сврхе у које су достављени.
3. Страна прималац неће уступити трећој страни податке који се наводе у ставу 1., без претходног писаног одобрења Стране пошиљаоца.

4. Приступ тајним подацима биће одобрен само оним лицима која поступају у складу с принципом „потребно знати“ и имају безбједносну дозволу или која су овлаштена да изврше увид у такве податке, у складу са државним законодавством Стране примаоца.

ЧЛАН 5.
БЕЗБЈЕДНОСНЕ ДОЗВОЛЕ

1. У оквиру овог Споразума, надлежни органи ће међусобно признати безбједносне дозволе и безбједносне дозволе за правна лица које су издате у складу са државним законодавством друге Стране.
2. Надлежни органи, на захтјев надлежног органа једне од Страна, поступајући у складу са њиховим државним законодавством, међусобно сарађују у поступцима провјера њихових грађана који бораве на државној територији друге Стране, у сврху доношења одлуке о безбједносној дозволи.

ЧЛАН 6.
УГОВОРИ СА ТАЈНИМ ПОДАЦИМА

1. Прије закључивања уговора са тајним подацима који се односи на остваривање увида у податке са ознаком степена тајности POUFNE / ПОВЈЕРЉИВО / CONFIDENTIAL или више, наручилац посла подноси захтјев свом надлежном органу да од надлежног органа друге Стране тражи издавање цертификата да уговарач – извршилац посла посједује важећу безбједносну дозволу за правна лица која одговара степену тајности података у које уговарач – извршилац треба остварити увид.
2. Издавање цертификата из става 1. биће једнако гаранцији да су проведене потребне радње на основу којих се сматра да уговарач – извршилац посла задовољава критерије из области заштите тајних

података који су утврђени државним законодавством Стране на чијем подручју државе се налази.

3. Тајни подаци неће бити доступни уговарачу – извршиоцу посла док не добије цертификат који се наводи у ставу 1.
4. Наручилац посла доставља уговарачу – извршиоцу посла безбједносно упутство за правно лице које је потребно за извршење уговора са тајним подацима и чини саставни дио сваког уговора с тајним подацима. Безбједносно упутство за правно лице садржи одредбе о безбједносним захтјевима и то:
   1) попис врста тајних података које се односе на уговор са тајним подацима, при чему се узимају у обзир њихови степени тајности;
   2) правила за додјељивање ознаке степена тајности подацима који су настали током извршења датог уговора са тајним подацима.
5. Наручилац посла доставља примјерак безбједносног упутства за правно лице свом надлежном органу који ће га прослиједити надлежном органу уговарача – извршиоца посла.
6. Извршење уговора са тајним подацима у дијелу који се односи на остваривање увида у тајне податке биће могуће под условом да уговарач – извршилац посла испуни критерије за заштиту тајних података, у складу са безбједносним упутством за правно лице.
7. Сваки подуговарач – извршилац посла дужан је да испуни исте услове за заштиту тајних података као и уговарач – извршилац посла.

ЧЛАН 7.
ДОСТАВЉАЊЕ ТАЈНИХ ПОДАТАКА

1. Тајни подаци достављају се дипломатским путем.
2. Надлежни органи могу се договорити и око других начина достављања тајних података који обезбјеђују заштиту од неовлаштеног откривања.
3. Страна прималац писаним путем потврђује пријем тајних података.

ЧЛАН 8.
УМНОЖАВАЊЕ ИЛИ ПРЕВОЂЕЊЕ ТАЈНИХ ПОДАТАКА

1. Умножавање или превођење тајних података врши се на основу државног законодавства сваке Стране. Умножени или преведени подаци биће заштићени на исти начин као оригинални. Број умножених примјерака или превода треба свести на број који се захтијева у службене сврхе.
2. Подаци са ознаком ŚCIŚLE TAJNE / ВРЛО ТАЈНО / TOP SECRET умножавају се или преводе само уз претходно прибављено одобрење Стране пошиљаоца.

ЧЛАН 9.
УНИШТЕЊЕ ТАЈНИХ ПОДАТАКА

1. Према ставу 2., тајни подаци уништавају се у складу са државним законодавством Стране примаоца тако да се онемогући њихова дјелимична или потпуна реконструкција.
2. Подаци са ознаком степена тајности ŚCIŚLE TAJNE / ВРЛО ТАЈНО / TOP SECRET не уништавају се, већ се враћају Страни пошиљаоцу.

ЧЛАН 10.
ПОСЈЕТЕ

1. Према ставу 4. лицима која долазе у посјету на териоторију државе друге Стране биће одобрен увид у тајне податке по пријему писменог одобрења надлежног органа друге Стране.
2. Надлежни орган стране посјетиоца подноси захтјев за посјету надлежном органу стране домаћина најмање 30 дана прије планиране посјете из става 1., а у ванредним случајевима и у краћем року.
3. Захтјев за посјету из става 2. треба да садржи:

1) сврху, датум и програм посјете, укључујући највиши ниво ознаке степена тајности података којима се приступа;
2) име и презиме, датум и мјесто рођења, држављанство и број путне исправе или другог идентификационог документа посјетиоца;
3) функцију посјетиоца и назив органа који они представљају;
4) степен тајности и датум важења безбједносне дозволе коју посједује посјетилац;
5) назив и адреса органа који се посјећује;
6) име, презиме и функција лица које ће бити посјећено;
7) датум, потпис и службени печат надлежног органа стране која се посјећује.

4. Надлежни органи могу договорити да се израде спискови лица овлаштених да реализују периодичне посјете у вези с провођењем одређеног пројекта, програма или уговора са тајним подацима. Такви спискови садрже податке који су предвиђени у ставу 3., а рок њиховог важења је дванаест (12) мјесеци након одобрења. Када надлежни органи Страна одобре такве спискове, датуме посјета ће договорити директно орган који шаље посјетиоце и орган који их прима, у складу са договореним условима. Надлежни органи Страна ће се међусобно обавјештавати о свакој измјени која се тиче података у раније наведеним списковима.
5. Ради заштите личних података из става 3. који се достављају у вези са одредбама ставова 1. и 4., у складу са државним законодавством Страна, примјењују се сљедеће одредбе:
   1) лични подаци које прими страна којој се подаци достављају биће кориштени искључиво у сврху и под условима које је дефинисала страна која доставља личне податке;
   2) страна којој се подаци достављају чуваће личне податке онолико колико је потребно да се постигне сврха њихове обраде;
   3) у случају да лични подаци буду достављени супротно државном законодавству Стране, страна која доставља податке обвјештава

о томе страну којој се подаци достављају која ће бити обавезна да те податке уклони на начин да онемогући њихову дјелимичну или потпуну реконструкцију;

4) страна која доставља личне податке преузима одговорност за тачност личних података које доставља и, у случају да су они неистинити или непотпуни, обавјештава о томе страну којој се подаци достављају која ће бити обавезна да исправи или уклони те податке;

5) страна којој се подаци достављају и страна која доставља личне податке су обавезне да воде евиденцију о достави, пријему и уклањању личних података;

6) страна која доставља личне податке и страна којој се подаци достављају су обавезне да личне податке који су предмет обраде дјелотворно заштите од откривања неовлаштеним лицима, недозвољених измјена, губитка, оштећење или уништења.

ЧЛАН 11.
ПОВРЕДА БЕЗБЈЕДНОСТИ

1. Повреда безбједности тајних података представља чињење или нечињење супротно одредбама овог Споразума или државном законодавству Страна које се односи на заштиту тајних података.
2. О повреди безбједности тајних података Стране пошиљаоца или тајних података насталих као резултат сарадње Страна, односно о постојању сумње да је повреда наступила, одмах се обавјештава надлежни орган Стране на чијој територији државе је дошло до повреде или постоји сумња да је повреда наступила.
3. Свака повреда безбједности, или постојање сумње о њеном наступању, биће истражена у складу са државним законодавством Стране на чијој територији државе је дошло до повреде.

4. У случају повреде безбједности из става 1. надлежни орган Стране на чијој територији државе је дошло до повреде писаним путем ће обавијестити надлежни орган друге Стране о тој чињеници, околностима, учинцима и резултатима радњи из става 3.
5. У случају појаве повреде безбједности на подручју треће Стране, надлежни орган Стране која је послала тајне податке предузима – у сарадњи са трећом Страном – радње из става 2, 3 и 4.
6. Надлежни органи, на захтјев једног од њих, сарађиваће у провођењу радњи које су предвиђене у ставу 3.

ЧЛАН 12.
ЈЕЗИЦИ

У примјени одредби овог Споразума Стране ће користити енглески језик или своје службене језике достављајући тада и превод на службени језик друге Стране, односно превод на енглески језик.

ЧЛАН 13.
ТРОШКОВИ

Свака Страна ће сносити трошкове који настану у примјени одредби овог Споразума.

ЧЛАН 14.
КОНСУЛТАЦИЈЕ

1. Надлежни органи узајамно се обавјештавају о свим измјенама и допунама њиховог државног законодавства у вези са заштитом тајних података које утичу на провођење овог Споразума.

2. Надлежни органи Страна ће се консултовати, на захтјев једног од њих, у циљу остваривања непосредне сарадње у провођењу одредби овог Споразума.
3. Свака Страна ће омогућити представницима надлежног органа друге Стране да дођу у посјету на територију те државе, како би размотриле процедуре за заштиту тајних података које је доставила друга Страна.
4. Ради остваривања ефикасне сарадње, која је предмет овог Споразума, надлежни органи Страна могу, ако је то потребно, у оквиру својих овлаштења утврђених државним законодавством, закључити детаљније техничке или организационе аранжмане.

ЧЛАН 15.
РЈЕШАВАЊЕ СПОРОВА

1. Сви спорови у вези са примјеном овог Споразума ће се рјешавати непосредним преговорима између надлежних органа.
2. Уколико рјешење спора не може бити постигнуто на начин наведен у ставу 1. исти ће бити ријешен дипломатским путем.

ЧЛАН 16.
ЗАВРШНЕ ОДРЕДБЕ

1. Овај Споразум ступа на снагу у складу са државним законодавством сваке Стране што ће бити потврђено узајамном размјеном нота. Споразум ступа на снагу првог дана другог мјесеца након пријема посљедње ноте.
2. Овај Споразум може бити измијењен на основу писмене сагласности обје Стране. Такве измјене ступају на снагу у складу са одредбама става 1.

3. Овај Споразум се закључује на неодређено вријеме. Свака Страна може отказати овај Споразум достављањем писменог обавјештења о отказу другој Страни. У том случају важење овог Споразума истиче након шест мјесеци од пријема обавјештења о отказу.
4. У случају отказа, сви тајни подаци који су размијењени или настали на основу овог Споразума биће заштићени према одребама истог.

Закључено у Сарајеву дана 7/06/2016 у два оригинална примјерка, сваки на пољском, службеним језицима Босне и Херцеговине (босанском, хрватском, српском) и енглеском језику, при чему су сви текстови подједнако вјеродостојни. У случају неслагања у тумачењу, биће мјеродаван текст Споразума на енглеском језику.

ЗА ВЛАДУ	ЗА САВЈЕТ МИНИСТАРА
РЕПУБЛИКЕ ПОЉСКЕ	БОСНЕ И ХЕРЦЕГОВИНЕ

AGREEMENT

between the Government of the Republic of Poland and the Council of Ministers of Bosnia and Herzegovina on the Protection of Classified Information

The Government of the Republic of Poland and

The Council of Ministers of Bosnia and Herzegovina,

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 national 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 its form, carrier and manner of recording, as well as objects or any parts thereof, also in the process of being generated, which require protection against unauthorized disclosure or misuse in accordance with the national law of either Party;
2) **Competent Authorities** – the authorities referred to in Article 3 of this Agreement;
3) **Originating Party** – the Party, as well as individuals, legal entities or other forms of organizations, competent to originate Classified Information in accordance with the national law of its Party;
4) **Recipient Party** – the Party, as well as individuals, legal entities or other forms of organizations, competent to receive Classified Information in accordance with the national law of its Party;
5) **Classified Contract** – a contract, performance of which involves access to Classified Information or originating of such information;
6) **Contractor** – an individual, a legal entity or other form of organization under the national law of one of the Parties, which has legal capacity to perform Classified Contracts;
7) **Principal** – a Contractor, which under the national law of one of the Parties has legal capacity to let Classified Contracts;
8) **Personnel Security Clearance** – a document issued in accordance with the national law of a Party by the Competent Authority or other authorized entity confirming that an individual has undergone security vetting and is eligible to have access to Classified Information;
9) **Facility Security Clearance** – a document issued in accordance with the national law of a Party by the Competent Authority or other authorized entity confirming that a Contractor has capability to protect Classified

Information; in case of sole proprietors acting as Contractors, a Personnel Security Clearance shall be an equivalent of a Facility Security Clearance;

10) **Third Party** – any state, as well as individuals, legal entities or other forms of organizations 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 national law of the Originating Party. The Recipient Party 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 Originating Party. The Recipient Party 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	BOSNIA AND HERZEGOVINA	EQUIVALENT IN ENGLISH
ŚCIŚLE TAJNE	VRLO 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 responsible for the implementation of this Agreement shall be:
   1) for the Republic of Poland: the Head of the Internal Security Agency;
   2) for Bosnia and Herzegovina: the Ministry of Security of Bosnia and Herzegovina, Sector for Protection of Classified Information – the National Security Authority.
2. The Parties shall inform each other via diplomatic channels about changes of the Competent Authorities or amendments to their competences.

ARTICLE 4
PRINCIPLES OF CLASSIFIED INFORMATION PROTECTION

1. The Parties shall adopt every measure provided in this Agreement and subject to their national laws in order to protect Classified Information transmitted or originated as a result of cooperation between the Parties, including this originated in connection with performance of Classified Contracts.
2. The Recipient Party shall use Classified Information exclusively for the purposes for which it has been exchanged.
3. The Recipient Party shall not release the information referred to in Paragraph 1 to any Third Party without a prior written consent of the Originating Party.
4. Access to Classified Information shall be granted only to those individuals who have a need-to-know and have a Personnel Security Clearance or have been otherwise authorized to access such information in accordance with the national law of the Recipient Party.

ARTICLE 5
SECURITY CLEARANCES

1. In the scope of this Agreement, the Competent Authorities shall recognize Personnel Security Clearances and Facility Security Clearances issued in accordance with the national law of the other Party.
2. On request of the Competent Authority of one of the Parties, the Competent Authorities, acting in accordance with their national law, shall assist each other in the vetting procedures of their citizens residing in the territory of the state of the other Party, for the purpose of issuing the decision on the Personnel Security Clearance.

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 issue a certificate 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. Issuing the certificate referred to in Paragraph 1 shall be tantamount to 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 national law of the Party in the territory of the state of which it is located.
3. Classified Information shall not be released to the Contractor until the receipt of the certificate 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 put forward a copy of the facility security instruction to the Competent Authority of its Party, which shall transmit 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. The Competent Authorities may agree on other forms of transmitting Classified Information which ensure its protection against unauthorized disclosure.
3. The Recipient Party 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 national law of each of the Parties. Reproduced or translated information shall be placed under the same protection as the original information. The number of copies or translations shall be reduced to that required for official purposes.
2. Information classified as ŚCIŚLE TAJNE / VRLO TAJNO / TOP SECRET shall be reproduced or translated only after obtaining a prior written consent issued by the Originating Party.

ARTICLE 9
DESTRUCTION OF CLASSIFIED INFORMATION

1. Subject to Paragraph 2, Classified Information shall be destroyed in accordance with the national law of the Recipient Party in such a manner as to eliminate its partial or total reconstruction.
2. Information classified as ŚCIŚLE TAJNE / VRLO TAJNO / TOP SECRET shall not be destroyed, it shall be returned to the Originating Party.

ARTICLE 10
VISITS

1. Subject to Paragraph 4, persons 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 the planned visit referred to in Paragraph 1, and in urgent cases in shorter time.
3. The request referred to in Paragraph 2 shall include:
   1) purpose, date and program of the visit, including the highest level of Classified Information to be accessed;
   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 they represent;
   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 of the visiting party.
4. The Competent Authorities 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 following their approval. Once such lists have been approved by the Competent Authorities of the Parties, the dates of the visits shall be arranged directly between authorized sending and hosting entities, in accordance with the conditions agreed upon. The Competent Authorities of the Parties shall notify each other of any changes regarding the data specified in the above-mentioned lists.
5. In order to protect personal data referred to in Paragraph 3, transmitted in connection with the provisions of Paragraphs 1 and 4, the following provisions shall apply, pursuant to the national law of the Parties:

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 national 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.

ARTICLE 11
BREACH OF SECURITY

1. Breach of security is an act or an omission which is contrary to this Agreement or the national law of the Parties concerning Classified Information protection.
2. Information on every breach of security or a suspicion of a breach of security concerning Classified Information of the Originating Party or Classified Information originated as a result of cooperation of the Parties shall be immediately reported to the Competent Authority of the Party in the territory of the state of which the breach or suspicion of the breach has occurred.

3. Every breach of security or a suspicion of a breach of security shall be investigated pursuant to the national law of the Party in the territory of the state 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 the state of which the breach has occurred shall inform the Competent Authority of the other Party in writing about the fact, circumstances of the breach, its effects and the outcome of the actions referred to in Paragraph 3.
5. Should a breach of security occur in the territory of a Third Party, the Competent Authority of the Party that has transmitted Classified Information shall take – in cooperation with the Third Party – the actions referred to in Paragraphs 2, 3 and 4.
6. 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 national law on the protection of Classified Information concerning implementation of this Agreement.
2. The Competent Authorities of the Parties 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 the territory of its state to discuss the procedures for the protection of Classified Information transmitted by 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 national 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 national 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 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 thereof.

Done at Sarajevo on 7/06/2016 in two original copies, each in the Polish, the official languages of Bosnia and Herzegovina (Bosnian, Croatian, Serbian) 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 COUNCIL OF MINISTERS OF BOSNIA AND HERZEGOVINA

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 21 listopada 2016 r.

Prezydent Rzeczypospolitej Polskiej: *A. Duda*

L.S.

Prezes Rady Ministrów: *B. Szydło*