Druk nr 1674

Warszawa, 22 czerwca 2017 r.

SEJM
RZECZYPOSPOLITEJ POLSKIEJ
VIII kadencja
Prezes Rady Ministrów
RM-111-94-17

Pan
Marek Kuchciński
Marszałek Sejmu
Rzeczypospolitej Polskiej

Szanowny Panie Marszałku.

Na podstawie art. 89 ust. 2 Konstytucji Rzeczypospolitej Polskiej, uprzejmie zawiadamiam Pana Marszałka, że Rada Ministrów zamierza przedstawić do ratyfikacji Prezydentowi Rzeczypospolitej Polskiej

- Umowę między Rządem Rzeczypospolitej Polskiej a Rządem Republiki Chorwacji o wzajemnej ochronie informacji niejawnych, podpisaną w Warszawie dnia 6 października 2016 r.,

której ratyfikacja - zdaniem Rady Ministrów - nie wymaga uprzedniej zgody wyrażonej w ustawie.

W załączeniu przekazuję tekst wymienionego dokumentu wraz z uzasadnieniem.

W razie niezgłoszenia, w terminie 30 dni - zgodnie z art. 15 ust. 4 ustawy o umowach międzynarodowych - negatywnej opinii co do zasadności wyboru trybu ratyfikacji dokumentu, zostanie on przedstawiony Prezydentowi Rzeczypospolitej Polskiej do ratyfikacji.

Z wyrazami szacunku

(-) Beata Szydło

PROJEKT

W imieniu Rzeczypospolitej Polskiej
PREZYDENT RZECZYPOSPOLITEJ POLSKIEJ
podaje do powszechnej wiadomości:

Dnia 6 października 2016 r. w Warszawie została podpisana Umowa między Rządem Rzeczypospolitej Polskiej a Rządem Republiki Chorwacji o wzajemnej ochronie informacji niejawnych.

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

PREZYDENT RZECZYPOSPOLITEJ POLSKIEJ

Andrzej Duda

PREZES RADY MINISTRÓW

Beata Szydło

UZASADNIENIE

I. Wyjaśnienie potrzeby i celu związania Rzeczypospolitej Polskiej Umową

Obowiązująca Umowa między Rządem Rzeczypospolitej Polskiej a Rządem Republiki Chorwacji w sprawie wzajemnej ochrony informacji niejawnych została podpisana w Zagrzebiu w dniu 17 września 2003 r. (Dz. U. z 2007 r. poz. 992). Rozwijająca się współpraca polityczna i gospodarcza, a przede wszystkim zmiany jakie zaszły w tym czasie w prawie wewnętrznym obu państw, sprawiają, iż postanowienia obowiązującej Umowy okazują się dziś niewystarczające i nieprzystające do aktualnych potrzeb współpracy w zakresie wzajemnej ochrony informacji niejawnych.

Mając na uwadze czas, jaki upłynął od chwili podpisania ww. Umowy, a w szczególności fakt wejścia w Rzeczypospolitej Polskiej w życie ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2016 r. poz. 1167 i 1948 oraz z 2017 r. poz. 935) oraz zmiany obowiązujących klauzul tajności w Republice Chorwacji, Strony uzgodniły, iż opracowany zostanie nowy projekt Umowy, który w sposób kompleksowy i wyczerpujący ureguluje kwestie dotyczące wymiany i wzajemnej ochrony informacji niejawnych.

II. Wskazanie różnic między dotychczasowym i projektowanym stanem prawnym

Podpisana w Warszawie dnia 6 października 2016 r. Umowa w znacznym stopniu modyfikuje postanowienia obecnie obowiązującej Umowy, dostosowując ją nie tylko do przepisów odnoszących się do ochrony informacji niejawnych obowiązujących obecnie w prawie krajowym obu Stron, ale również do aktualnych standardów współpracy bilateralnej.

Art. 1 Umowy określa cel i zakres jej stosowania. Kompleksowy charakter Umowy powoduje, iż będzie miała ona zastosowanie do wszelkich działań, kontraktów lub umów dotyczących informacji niejawnych zawieranych między Stronami, osobami fizycznymi, osobami prawnymi lub innymi jednostkami organizacyjnymi pozostającymi pod ich jurysdykcją.

W art. 2 zdefiniowano kluczowe dla Umowy pojęcia, w tym przede wszystkim termin „informacje niejawne", w celu ujednolicenia pojęć na użytek niniejszej Umowy.

Kolejne definicje precyzują m.in. takie terminy jak: „kontrakt niejawny", „strona wytwarzająca" czy „strona otrzymująca".

W art. 3 zestawiono odpowiadające sobie klauzule tajności w celu usystematyzowania ich nazewnictwa. W rezultacie zmian, jakie zaszły w chorwackim prawie wewnętrznym od czasu wejścia w życie obowiązującej Umowy, aktualizacji poddano chorwackie klauzule tajności. Ponadto w tabeli ekwiwalencji umieszczono oprócz polskich i chorwackich klauzul tajności ich odpowiedniki w języku angielskim. Odmienna niż w obowiązującej Umowie, tj. zaktualizowana, a przez to zgodna ze stanem prawnym Strony polskiej oraz Strony chorwackiej, systematyka klauzul tajności została już wprowadzona do Umowy między Rządem Rzeczypospolitej Polskiej a Rządem Republiki Chorwacji o współpracy w zwalczaniu przestępczości, podpisanej w Dubrowniku w dniu 9 lipca 2010 r. (Dz. U. z 2015 r. poz. 400). Wobec odmiennego uregulowania kwestii równoważności klauzul tajności w obu ww. umowach, istnieje pilna potrzeba jej uporządkowania, czego odzwierciedleniem jest treść art. 3 przedmiotowej Umowy.

W art. 4 wskazano krajowe władze bezpieczeństwa, które są odpowiedzialne za realizację postanowień niniejszej Umowy. Organami tymi są Szef Agencji Bezpieczeństwa Wewnętrznego w Rzeczypospolitej Polskiej oraz Biuro Rady Bezpieczeństwa Narodowego w Republice Chorwacji.

Art. 5 podpisanej Umowy określa zasady ochrony informacji niejawnych, które mają gwarantować właściwą ochronę przekazywanym informacjom niejawnym. Ustalono między innymi, iż Strony zobowiążą się do stosowania zasady ograniczonego dostępu przy udostępnianiu informacji niejawnych, zgodnie z którą informacje niejawne będą udostępniane jedynie osobom, których zadania wymagają zapoznania się z nimi. Strony zobowiązały się ponadto uznawać wzajemnie poświadczenia bezpieczeństwa oraz świadectwa bezpieczeństwa przemysłowego.

Kolejne trzy artykuły Umowy dotyczą kwestii, które nie zostały uwzględnione w dotychczasowej Umowie. W art. 6–8 uregulowano kolejno: przekazywanie, powielanie, tłumaczenie oraz niszczenie informacji niejawnych, co pozwoli na ujednolicenie postępowania z informacjami niejawnymi w stosunkach bilateralnych.

Art. 9 reguluje możliwość zawierania kontraktów niejawnych, a więc takich, których realizacja wiąże się z dostępem do informacji niejawnych, bądź

z wytworzeniem takich informacji. Zgodnie z postanowieniami ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych, do posiadania świadectwa bezpieczeństwa przemysłowego zostali zobligowani jedynie przedsiębiorcy ubiegający się o kontrakty związane z dostępem do informacji niejawnych o klauzuli „poufne" lub wyższej.

W art. 10 określono zasady i warunki wzajemnych wizyt związanych z dostępem do informacji niejawnych. W stosunku do obowiązującej Umowy znacznie uszczegółowiono zakres danych, które powinien zawierać wniosek o wyrażenie zgody na wizytę. Ponadto, zgodnie z międzynarodową praktyką ustalono, iż wizyty związane z dostępem do informacji niejawnych o klauzuli „zastrzeżone" będą uzgadniane bezpośrednio między zainteresowanymi podmiotami, bez pośrednictwa krajowych władz bezpieczeństwa. Wprowadzono również regulację stanowiącą, iż Strony zapewnią, zgodnie ze swoim prawem wewnętrznym, ochronę danych osobowych osób przybywających z wizytą.

W art. 11 zostały określone zasady postępowania w przypadkach naruszenia regulacji dotyczących wzajemnej ochrony informacji niejawnych. W artykule tym jest przewidziana między innymi możliwość współpracy krajowych władz bezpieczeństwa obu Stron przy czynnościach wyjaśniających.

W art. 12 uregulowano szereg spraw związanych z wykonywaniem Umowy, w tym kwestię języków jakimi będą posługiwały się Strony, czy ponoszonych przez nie kosztów. W celu zapewnienia skutecznej współpracy przy realizacji postanowień Umowy wprowadzono tryb konsultacji krajowych władz bezpieczeństwa obu Stron oraz możliwość zawierania przez nie szczegółowych uzgodnień technicznych.

Ponadto, w Umowie przewidziano tryb rozstrzygania sporów (art. 13), uregulowano stosunek Umowy do wcześniejszych porozumień regulujących kwestię wzajemnej ochrony informacji niejawnych oraz określono procedurę wejścia w życie Umowy, czas jej obowiązywania oraz tryb wypowiedzenia (art. 14), które to regulacje stanowią niezbędny element każdej umowy międzynarodowej o takim charakterze.

III. Wskazanie przewidywanych skutków społecznych, gospodarczych, finansowych, politycznych i prawnych, związanych z wejściem w życie Umowy, wraz z określeniem źródeł finansowania

Wejście w życie niniejszej Umowy nie spowoduje znaczących skutków społecznych. Skutkiem o charakterze prawnym będzie określenie jednolitych zasad

ochrony informacji niejawnych, wymienianych w ramach szeroko rozumianej współpracy między Rzecząpospolitą Polską a Republiką Chorwacji.

Umowa o wzajemnej ochronie informacji niejawnych, poza kompleksowym uregulowaniem kwestii związanych z wymianą, warunkami i środkami ochrony informacji niejawnych, będzie stanowić również podstawę prawną do zawierania pisemnych szczegółowych uzgodnień technicznych lub organizacyjnych.

Skutkiem politycznym będzie dalsze zacieśnienie współpracy i pogłębienie dotychczasowych relacji między Rzecząpospolitą Polską a Republiką Chorwacji. Zawarcie Umowy o wzajemnej ochronie informacji niejawnych może przynieść również wymierne korzyści wynikające ze współpracy gospodarczej, ponieważ jej postanowienia umożliwiają zawieranie kontraktów niejawnych, istotnych m.in. dla przemysłu zbrojeniowego.

Wejście w życie Umowy nie spowoduje skutków finansowych dla podmiotów sektora finansów publicznych w postaci zmniejszenia ich dochodów lub zwiększenia ich wydatków ani dodatkowych skutków dla budżetu państwa.

IV. **Tryb związania**

Wejście w życie niniejszej Umowy nie będzie wiązało się z koniecznością wprowadzenia zmian w polskim prawie krajowym, ponieważ jej postanowienia nie odbiegają od obowiązującego w Rzeczypospolitej Polskiej porządku prawnego, a w szczególności rozwiązań przyjętych w ustawie z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych. Umowa dotyczy wprawdzie ochrony przekazywanych za granicę i otrzymywanych z zagranicy informacji niejawnych, ale nie wprowadza żadnych dodatkowych zasad ochrony lub wymiany tych informacji – innych, aniżeli określone w ustawie z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych. Nie zostały zatem spełnione przesłanki, wymienione w art. 89 ust. 1 Konstytucji Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz. U. poz. 483, z późn. zm.), a więc ratyfikacja przedmiotowej Umowy nie wymaga uprzedniej zgody wyrażonej w ustawie.

Niniejsza Umowa dotyczy takich podmiotów prawa krajowego, jak osoby fizyczne, osoby prawne oraz jednostki organizacyjne w rozumieniu ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych. W odniesieniu do zakresu, w jakim przedmiotowa Umowa dotyczy osób fizycznych, osób prawnych i jednostek

organizacyjnych, należy wskazać na przewidzianą w Umowie możliwość zawierania kontraktów niejawnych związanych z dostępem do informacji niejawnych, w tym występowania w roli kontrahenta oraz podwykonawcy. Ponadto w odniesieniu do osób fizycznych, Umowa przewiduje także możliwość przeprowadzania na terytorium państwa drugiej Strony wizyt, związanych z dostępem do informacji niejawnych. Artykuł 10 Umowy dotyczy spraw uregulowanych w prawie krajowym, objętych przepisami ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2016 r. poz. 922).

W Rzeczypospolitej Polskiej związanie przedmiotową Umową powinno nastąpić przez jej ratyfikację w trybie art. 89 ust. 2 Konstytucji Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r., zgodnie z postanowieniami art. 12 ust. 2 ustawy z dnia 14 kwietnia 2000 r. o umowach międzynarodowych (Dz. U. poz. 443, z późn. zm.).

Wybór trybu tzw. małej ratyfikacji jest poparty potrzebą uznania przedmiotowej Umowy za źródło prawa powszechnie obowiązującego w Rzeczypospolitej Polskiej, gdyż jej postanowienia będą miały zastosowanie do szerokiego kręgu podmiotów (organy administracji państwowej, przedsiębiorcy). W związku z faktem, iż zgodnie z art. 87 Konstytucji Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. źródłem prawa powszechnie obowiązującego w Rzeczypospolitej Polskiej są wyłącznie ratyfikowane Umowy międzynarodowe, a nie zaistniały przesłanki ratyfikacji Umowy za uprzednią zgodą wyrażoną w ustawie, związanie Rzeczypospolitej Polskiej przedmiotową Umową powinno nastąpić w drodze ratyfikacji bez uprzedniej zgody wyrażonej w ustawie.

Zawarcie Umowy jest zgodne z innymi działaniami podejmowanymi przez Rzeczpospolitą Polską na arenie międzynarodowej i nie jest sprzeczne z Umową między Stronami Traktatu Północnoatlantyckiego o ochronie informacji, sporządzoną w Brukseli dnia 6 marca 1997 r. (Dz. U. z 2000 r. poz. 740) ani prawem Unii Europejskiej.

Przedmiotowa Umowa zawiera postanowienia kwalifikujące się do bezpośredniego stosowania, które po dokonaniu ratyfikacji Umowy oraz jej ogłoszeniu w Dzienniku Urzędowym Rzeczypospolitej Polskiej staną się częścią krajowego porządku prawnego.

Z uwagi na powyższe przesłanki uzasadniające proponowany tryb związania Rzeczypospolitej Polskiej przedmiotową Umową, zostanie ona ratyfikowana.

UMOWA

między Rządem Rzeczypospolitej Polskiej a Rządem Republiki Chorwacji o wzajemnej ochronie informacji niejawnych

Rząd Rzeczypospolitej Polskiej i Rząd Republiki Chorwacji,
zwane dalej „Stronami",

mając świadomość, iż bliska współpraca może pociągać za sobą konieczność wymiany informacji niejawnych,

kierując się zamiarem przyjęcia uregulowań prawnych w zakresie wzajemnej ochrony informacji niejawnych wymienianych między Stronami lub wytwarzanych w wyniku współpracy,

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

uzgodniły, co następuje:

ARTYKUŁ 1
CEL I ZAKRES

1. Celem niniejszej Umowy jest zapewnienie ochrony informacjom niejawnym wytwarzanym w wyniku współpracy lub wymienianym między Stronami oraz osobami fizycznymi, osobami prawnymi lub innymi jednostkami organizacyjnymi pozostającymi pod ich jurysdykcją.
2. Niniejsza Umowa ma zastosowanie do wszelkich kontraktów lub umów międzynarodowych dotyczących informacji niejawnych, realizowanych bądź zawieranych między Stronami oraz osobami fizycznymi, osobami prawnymi lub innymi jednostkami organizacyjnymi pozostającymi pod ich jurysdykcją, oraz do wszelkich działań realizowanych między nimi.

ARTYKUŁ 2
DEFINICJE

W rozumieniu niniejszej Umowy:

1) **informacje niejawne** oznaczają wszelkie informacje niezależnie od formy, nośnika i sposobu ich utrwalenia oraz przedmioty lub dowolne ich części, będące także w trakcie ich opracowywania, które zostały oznaczone klauzulą tajności zgodnie z prawem krajowym Strony wytwarzającej;
2) **Strona wytwarzająca** oznacza Stronę, jak również osoby fizyczne, osoby prawne lub inne jednostki organizacyjne uprawnione do wytwarzania i przekazywania informacji niejawnych zgodnie z prawem krajowym swojej Strony;
3) **Strona otrzymująca** oznacza Stronę, jak również osoby fizyczne, osoby prawne lub inne jednostki organizacyjne uprawnione do otrzymywania informacji niejawnych zgodnie z prawem krajowym swojej Strony;
4) **krajowa władza bezpieczeństwa** oznacza organ państwowy, o którym mowa w artykule 4, odpowiedzialny za realizację oraz nadzór nad niniejszą Umową;

5) **kontrahent** oznacza osobę fizyczną, osobę prawną albo inną jednostkę organizacyjną, uprawnioną do zawierania kontraktów niejawnych;

6) **kontrakt niejawny** oznacza umowę pomiędzy kontrahentami, która zawiera informacje niejawne lub której realizacja związana jest z dostępem do informacji niejawnych;

7) **naruszenie regulacji dotyczących ochrony informacji niejawnych** oznacza działanie lub zaniechanie sprzeczne z niniejszą Umową lub prawem krajowym Stron, w zakresie dotyczącym ochrony informacji niejawnych;

8) **Strona trzecia** oznacza organizację międzynarodową lub państwo, w tym również osoby fizyczne, osoby prawne lub inne jednostki organizacyjne, podlegające jego jurysdykcji, niebędące Stroną niniejszej Umowy.

ARTYKUŁ 3
KLAUZULE TAJNOŚCI

Strony uzgadniają, że niżej wymienione klauzule tajności są równorzędne:

W RZECZYPOSPOLITEJ POLSKIEJ	W REPUBLICE CHORWACJI	ODPOWIEDNIK W JĘZYKU ANGIELSKIM
ŚCIŚLE TAJNE	VRLO TAJNO	TOP SECRET
TAJNE	TAJNO	SECRET
POUFNE	POVJERLJIVO	CONFIDENTIAL
ZASTRZEŻONE	OGRANIČENO	RESTRICTED

ARTYKUŁ 4
KRAJOWE WŁADZE BEZPIECZEŃSTWA

1. Krajowymi władzami bezpieczeństwa Stron są:

w Rzeczypospolitej Polskiej: Szef Agencji Bezpieczeństwa Wewnętrznego;

w Republice Chorwacji: Biuro Rady Bezpieczeństwa Narodowego.

2. Strony informują się drogą dyplomatyczną o zmianach krajowych władz bezpieczeństwa lub zmianach ich właściwości.

ARTYKUŁ 5
ZASADY OCHRONY INFORMACJI NIEJAWNYCH

1. Zgodnie ze swoim prawem krajowym, Strony podejmują wszelkie działania w celu ochrony informacji niejawnych przekazywanych lub wytwarzanych na podstawie niniejszej Umowy, w tym także wytworzonych w związku z realizacją kontraktów niejawnych.
2. 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 artykułu 3.
3. Klauzula tajności może być zmieniona lub zniesiona wyłącznie przez Stronę wytwarzającą. Strona wytwarzająca pisemnie informuje Stronę otrzymującą o każdym przypadku zmiany klauzuli tajności przekazanych informacji niejawnych.
4. Informacje niejawne są udostępniane tylko osobom, których zadania wymagają zapoznania się z nimi i które zgodnie z prawem krajowym zostały upoważnione do dostępu do informacji niejawnych oznaczonych równorzędną klauzulą tajności.
5. W zakresie niniejszej Umowy, każda ze Stron uznaje poświadczenia bezpieczeństwa i świadectwa bezpieczeństwa przemysłowego wydane przez drugą Stronę.
6. W zakresie niniejszej Umowy, krajowe władze bezpieczeństwa niezwłocznie informują się o każdej zmianie w odniesieniu do wydanych poświadczeń bezpieczeństwa oraz świadectw bezpieczeństwa przemysłowego, w szczególności o przypadkach ich cofnięcia.

7. Na wniosek i zgodnie ze swoim prawem krajowym Strony współpracują podczas przeprowadzania postępowań sprawdzających związanych z wykonywaniem niniejszej Umowy.
8. Strona otrzymująca jest zobowiązana do:
   1) udostępniania informacji niejawnych Stronie trzeciej wyłącznie za uprzednią pisemną zgodą Strony wytwarzającej;
   2) oznaczania otrzymywanych informacji niejawnych zgodnie z tabelą równorzędności klauzul tajności, określoną w artykule 3;
   3) wykorzystywania informacji niejawnych wyłącznie w celach, dla których zostały one przekazane.

ARTYKUŁ 6
PRZEKAZYWANIE INFORMACJI NIEJAWNYCH

1. Informacje niejawne są przekazywane drogą dyplomatyczną.
2. Informacje niejawne o klauzuli ZASTRZEŻONE / OGRANIČENO / RESTRICTED mogą być przekazywane również za pośrednictwem uprawnionych do tego przewoźników, zgodnie z prawem krajowym Strony wytwarzającej.
3. W pilnych przypadkach, o ile nie można skorzystać z innej formy przekazania, jeżeli spełnione są wymogi bezpieczeństwa określone prawem krajowym Strony wytwarzającej, dopuszczalny jest przewóz osobisty informacji niejawnych o klauzuli ZASTRZEŻONE / OGRANIČENO / RESTRICTED oraz POUFNE / POVJERLJIVO / CONFIDENTIAL przez osoby do tego upoważnione.
4. Krajowe władze bezpieczeństwa mogą ustalić inne sposoby przekazywania informacji niejawnych zapewniające ochronę przed ich nieuprawnionym ujawnieniem.
5. Strona otrzymująca potwierdza pisemnie odbiór informacji niejawnych.

6. Organy uprawnione do wymiany informacji niejawnych na podstawie innych umów międzynarodowych, zawartych między Stronami, mogą wymieniać informacje niejawne bezpośrednio.

ARTYKUŁ 7
POWIELANIE I TŁUMACZENIE INFORMACJI NIEJAWNYCH

1. Powielanie lub tłumaczenie informacji niejawnych odbywa się w sposób zgodny z prawem krajowym każdej ze Stron. Wszystkie kopie i tłumaczenia informacji niejawnych oznacza się oryginalną klauzulą tajności. Powielone lub przetłumaczone informacje podlegają takiej samej ochronie jak 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 w wyjątkowych przypadkach, po uprzednim uzyskaniu pisemnego zezwolenia wydanego przez Stronę wytwarzającą.
3. Przetłumaczone informacje niejawne oznacza się oryginalną klauzulą tajności oraz adnotacją w języku tłumaczenia, wskazującą, iż tłumaczenie zawiera informacje niejawne Strony wytwarzającej.

ARTYKUŁ 8
NISZCZENIE INFORMACJI NIEJAWNYCH

1. Informacje niejawne 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.
3. Strona wytwarzająca może, poprzez umieszczenie dodatkowych oznaczeń lub przesłanie pisemnego powiadomienia, zakazać zniszczenia informacji

niejawnych. W przypadku zakazu zniszczenia informacji niejawnych są one zwracane Stronie wytwarzającej.

4. W wyjątkowych okolicznościach, jeśli nie jest możliwe zapewnienie ochrony lub zwrócenie informacji niejawnych przekazanych lub wytworzonych na podstawie niniejszej Umowy, informacje niejawne zostaną niezwłocznie zniszczone. Strona otrzymująca poinformuje bez zbędnej zwłoki krajową władzę bezpieczeństwa Strony wytwarzającej o ich zniszczeniu.

ARTYKUŁ 9
KONTRAKTY NIEJAWNE

1. Kontrakty niejawne w części związanej z dostępem do informacji niejawnych są zawierane i realizowane zgodnie z prawem krajowym każdej ze Stron.
2. Przed zawarciem kontraktu niejawnego, związanego z dostępem do informacji niejawnych o klauzuli POUFNE / POVJERLJIVO / CONFIDENTIAL lub wyższej, potencjalny kontrahent składa wniosek do krajowej władzy bezpieczeństwa swojej Strony, o wystąpienie do krajowej władzy bezpieczeństwa drugiej Strony, z prośbą o wydanie zaświadczenia, że kontrahent drugiej Strony posiada ważne świadectwo bezpieczeństwa przemysłowego odpowiednie do klauzuli informacji niejawnych, do których będzie miał dostęp.
3. Wydanie zaświadczenia, o którym mowa w ustępie 2 niniejszego artykułu, jest równoznaczne z gwarancją, że zostały przeprowadzone czynności niezbędne do stwierdzenia, że kontrahent otrzymujący informacje niejawne spełnia warunki w zakresie ochrony informacji niejawnych określone w prawie krajowym Strony, na terytorium której posiada siedzibę.
4. Informacje niejawne nie są udostępniane kontrahentowi do czasu uzyskania zaświadczenia, o którym mowa w ustępie 2 niniejszego artykułu.
5. Kontrahent będący odbiorcą informacji niejawnych otrzymuje od kontrahenta drugiej Strony instrukcję bezpieczeństwa przemysłowego niezbędną do

realizacji kontraktu niejawnego. Instrukcja bezpieczeństwa przemysłowego stanowi integralną część każdego kontraktu niejawnego i 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.

6. Kontrahent przekazuje kopię instrukcji bezpieczeństwa przemysłowego krajowej władzy bezpieczeństwa swojej Strony.
7. Każdy podwykonawca podlega tym samym obowiązkom ochrony informacji niejawnych, jakie nałożono na kontrahenta.

ARTYKUŁ 10
WIZYTY

1. Osobom przybywającym z wizytą na terytorium drugiej Strony zezwala się na dostęp do informacji niejawnych, tylko po uprzednim uzyskaniu pisemnego zezwolenia wydanego przez krajową władzę bezpieczeństwa drugiej Strony.
2. Krajowa władza bezpieczeństwa Strony wysyłającej zwraca się do krajowej władzy bezpieczeństwa Strony przyjmującej z wnioskiem o wyrażenie zgody na wizytę co najmniej trzydzieści dni przed planowanym terminem wizyty, o której mowa w ustępie 1 niniejszego artykułu, a w pilnych przypadkach w krótszym czasie.
3. Wniosek, o którym mowa w ustępie 2 niniejszego artykułu, zawiera:
   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) inne informacje, jeżeli zostało tak ustalone przez krajowe władze bezpieczeństwa;

jak również datę, podpis oraz oficjalną pieczęć krajowej władzy bezpieczeństwa Strony wysyłającej.

4. Krajowe władze bezpieczeństwa 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 niniejszego artykułu i są ważne przez okres dwunastu miesięcy. Po zatwierdzeniu takich wykazów przez krajowe władze bezpieczeństwa, terminy wizyt uzgadniane są bezpośrednio między podmiotem wysyłającym a podmiotem przyjmującym wizytę, zgodnie z ustalonymi warunkami.
5. Wizyty związane z dostępem do informacji niejawnych o klauzuli ZASTRZEŻONE / OGRANIČENO / RESTRICTED są uzgadniane bezpośrednio między podmiotem wysyłającym a podmiotem przyjmującym wizytę.
6. Strony odpowiadają, zgodnie ze swoim prawem krajowym, za ochronę danych osobowych osób przybywających z wizytą związaną z dostępem do informacji niejawnych.

ARTYKUŁ 11
NARUSZENIE REGULACJI DOTYCZĄCYCH OCHRONY INFORMACJI NIEJAWNYCH

1. Informację o każdym przypadku naruszenia lub o podejrzeniu naruszenia regulacji dotyczących ochrony informacji niejawnych przekazanych przez Stronę wytwarzającą lub informacji niejawnych wytworzonych w wyniku

wspólnego działania Stron, przekazuje się niezwłocznie krajowej władzy bezpieczeństwa Strony, na terytorium której miało miejsce lub zaistniało podejrzenie takiego naruszenia.

2. Każdy przypadek naruszenia lub podejrzenia naruszenia regulacji dotyczących ochrony informacji niejawnych wyjaśnia się zgodnie z prawem krajowym Strony, na terytorium której zdarzenie miało miejsce.
3. W przypadku naruszenia regulacji dotyczących ochrony informacji niejawnych, krajowa władza bezpieczeństwa Strony, na terytorium której naruszenie miało miejsce, pisemnie informuje krajową władzę bezpieczeństwa drugiej Strony o fakcie, o okolicznościach naruszenia oraz o wyniku czynności, o których mowa w ustępie 2 niniejszego artykułu.
4. Krajowe władze bezpieczeństwa współpracują przy czynnościach, o których mowa w ustępie 2 niniejszego artykułu, na wniosek jednej z nich.
5. Jeżeli naruszenie regulacji dotyczących informacji niejawnych miało miejsce na terytorium Strony trzeciej, krajowa władza bezpieczeństwa Strony wytwarzającej podejmie we współpracy ze Stroną trzecią działania zmierzające do wyjaśnienia okoliczności naruszenia.

ARTYKUŁ 12
WYKONYWANIE UMOWY

1. Krajowe władze bezpieczeństwa informują się wzajemnie o wszelkich zmianach w swoim prawie krajowym dotyczącym ochrony informacji niejawnych, w zakresie niezbędnym do wykonywania postanowień niniejszej Umowy.
2. W celu zapewnienia ścisłej współpracy przy realizacji postanowień niniejszej Umowy krajowe władze bezpieczeństwa konsultują się, na wniosek jednego z tych organów.
3. W celu zapewnienia skutecznej współpracy wynikającej z postanowień niniejszej Umowy, krajowe władze bezpieczeństwa mogą, w razie potrzeby,

zawierać pisemne szczegółowe uzgodnienia techniczne lub organizacyjne w zakresie kompetencji przyznanych im prawem krajowym własnej Strony.

4. W zakresie stosowania postanowień niniejszej Umowy, Strony używają języka angielskiego lub swoich języków urzędowych. W przypadku stosowania języków urzędowych, Strony zobowiązują się przekazać także tłumaczenie na język urzędowy drugiej Strony lub na język angielski.
5. Każda ze Stron pokrywa koszty własne, poniesione w związku z realizacją i nadzorem nad wykonywaniem postanowień niniejszej Umowy.

ARTYKUŁ 13
ROZSTRZYGANIE SPORÓW

1. Wszelkie sporne kwestie dotyczące interpretacji lub stosowania niniejszej Umowy rozstrzygane są w drodze bezpośrednich konsultacji między krajowymi władzami bezpieczeństwa i nie są przekazywane do rozstrzygnięcia jakimkolwiek międzynarodowym trybunałom ani Stronie trzeciej.
2. Jeśli nie jest możliwe rozwiązanie sporu w sposób, o którym mowa w ustępie 1 niniejszego artykułu, jest on rozstrzygany drogą dyplomatyczną.

ARTYKUŁ 14
POSTANOWIENIA KOŃCOWE

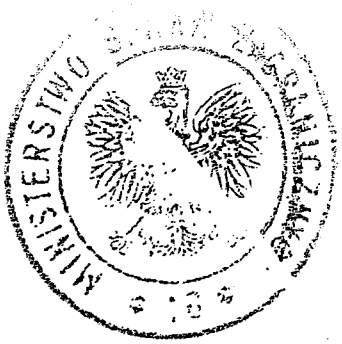
1. Niniejsza Umowa wejdzie w życie trzydziestego dnia od daty otrzymania późniejszej z not, w której Strony informują się wzajemnie drogą dyplomatyczną o zakończeniu wewnętrznych procedur niezbędnych dla jej wejścia w życie.
2. Niniejsza Umowa może zostać zmieniona na podstawie wspólnej pisemnej zgody obu Stron. Takie zmiany wejdą w życie zgodnie z postanowieniami ustępu 1 niniejszego artykułu.

3. Niniejsza Umowa zawarta jest na czas nieokreślony. Może być ona wypowiedziana w drodze 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 niniejszej Umowy, wszystkie informacje niejawne przekazane na jej podstawie będą nadal chronione zgodnie z jej postanowieniami, a na wniosek jednej ze Stron zostaną zwrócone Stronie wytwarzającej.
5. Z dniem wejścia w życie niniejszej Umowy, traci moc Umowa między Rządem Rzeczypospolitej Polskiej a Rządem Republiki Chorwacji w sprawie wzajemnej ochrony informacji niejawnych, podpisana w Zagrzebiu w dniu 17 września 2003 r. Informacje niejawne wymienione na jej podstawie są chronione zgodnie z postanowieniami niniejszej Umowy.

Sporządzono w Warszawie dnia 6 października 2016 roku w dwóch jednobrzmiących egzemplarzach, każdy w językach polskim, chorwackim 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

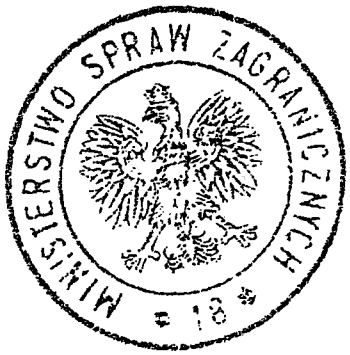
Z UPOWAŻNIENIA RZĄDU REPUBLIKI CHORWACJI



Stwierdzam zgodność
fotokopii z oryginałem/~~odpisem~~

Warszawa, dnia 14.10.2016

Dyrektor Departamentu
Prawno-Traktatowego
Andrzej Misztal



UGOVOR

između Vlade Republike Poljske

i Vlade Republike Hrvatske

o uzajamnoj zaštiti klasificiranih podataka

Vlada Republike Poljske i Vlada Republike Hrvatske,
u daljnjem tekstu „stranke“,

shvaćajući da dobra suradnja može zahtijevati razmjenu
klasificiranih podataka između stranaka,

želeći uspostaviti skup pravila koja uređuju uzajamnu zaštitu klasificiranih podataka koji se razmjenjuju ili nastaju tijekom suradnje između stranaka,

uz uvjet poštivanja obvezujućih pravila međunarodnog prava
i nacionalnog prava stranaka,

sporazumjele su se kako slijedi:

ČLANAK 1.

PREDMET I PODRUČJE PRIMJENE

1. Predmet ovog Ugovora je osiguravanje zaštite klasificiranih podataka koji nastaju ili se razmjenjuju između stranaka, fizičkih osoba, pravnih osoba ili drugih oblika organizacija pod njihovom nadležnošću.
2. Ovaj Ugovor primjenjuje se na bilo koje ugovore ili međunarodne ugovore koji uključuju klasificirane podatke, a koji se provode ili sklapaju između stranaka, fizičkih osoba, pravnih osoba ili drugih oblika organizacija pod njihovom nadležnošću, kao i na bilo koje aktivnosti koje se između njih provode.

ČLANAK 2.

DEFINICIJE

Za potrebe ovog Ugovora:

1) „**klasificirani podaci**" označava bilo koje podatke, neovisno o obliku, sredstvu prijenosa i načinu bilježenja, kao i predmete ili bilo koje njihove dijelove, također i u postupku stvaranja, koji su klasificirani u skladu s nacionalnim pravom stranke pošiljateljice;
2) „**stranka pošiljateljica**" označava stranku, kao i fizičke osobe, pravne osobe ili druge oblike organizacija, nadležne za stvaranje i prijenos klasificiranih podataka u skladu s nacionalnim pravom te stranke;
3) „**stranka primateljica**" označava stranku, kao i fizičke osobe, pravne osobe ili druge oblike organizacija, nadležne za primanje klasificiranih podataka u skladu s nacionalnim pravom te stranke;
4) „**nacionalno sigurnosno tijelo**" označava nacionalno tijelo iz članka 4. odgovorno za provedbu i nadzor ovog Ugovora;
5) „**ugovaratelj**" označava fizičku osobu, pravnu osobu ili drugi oblik organizacije, koja ima pravnu sposobnost sklapati klasificirane ugovore;
6) „**klasificirani ugovor**" označava ugovor između ugovaratelja koji sadrži klasificirane podatke ili čija provedba zahtijeva pristup klasificiranim podacima;

7) „**povreda sigurnosti**“ označava činjenje ili nečinjenje koje je suprotno ovom Ugovoru ili nacionalnom pravu stranaka koje se odnosi na zaštitu klasificiranih podataka;

8) „**treća strana**“ označava bilo koju državu, uključujući fizičke osobe, pravne osobe ili druge oblike organizacija pod njezinom nadležnošću, ili međunarodnu organizaciju, koje nisu stranke ovog Ugovora.

ČLANAK 3.
STUPNJEVI TAJNOSTI

Stranke su suglasne da su sljedeći stupnjevi tajnosti istoznačni:

ZA REPUBLIKU POLJSKU	ZA REPUBLIKU HRVATSKU	ISTOZNAČNICA NA ENGLESKOM
ŚCIŚLE TAJNE	VRLO TAJNO	TOP SECRET
TAJNE	TAJNO	SECRET
POUFNE	POVJERLJIVO	CONFIDENTIAL
ZASTRZEŻONE	OGRANIČENO	RESTRICTED

ČLANAK 4.
NACIONALNA SIGURNOSNA TIJELA

1. Nacionalna sigurnosna tijela stranaka su:

   Za Republiku Poljsku

   - čelnik Agencije za unutarnju sigurnost;

   Za Republiku Hrvatsku

   - Ured Vijeća za nacionalnu sigurnost.

2. Stranke obavješćuju jedna drugu, diplomatskim putem, o promjenama nacionalnih sigurnosnih tijela ili izmjenama i dopunama njihovih nadležnosti.

ČLANAK 5.

PRAVILA ZAŠTITE KLASIFICIRANIH PODATAKA

1. Stranke, u skladu sa svojim nacionalnim pravom, poduzimaju sve odgovarajuće mjere za zaštitu klasificiranih podataka koji se razmjenjuju ili nastaju u skladu s ovim Ugovorom, uključujući one koji nastaju u vezi s provedbom klasificiranih ugovora.
2. Klasificiranim podacima dodjeljuje se stupanj tajnosti u skladu s njihovim sadržajem, u skladu s nacionalnim pravom stranke pošiljateljice. Stranka primateljica jamči najmanje isti stupanj zaštite primljenih klasificiranih podataka, u skladu s odredbama članka 3.
3. Samo stranka pošiljateljica može promijeniti ili ukloniti stupanj tajnosti. Stranka pošiljateljica pisano obavješćuje stranku primateljicu o svakoj promjeni stupnja tajnosti ustupljenih klasificiranih podataka.
4. Pristup klasificiranim podacima imaju samo osobe kojima je u skladu s nacionalnim pravom odobren pristup klasificiranim podacima istoznačnog stupnja tajnosti i kojima je to nužno za obavljanje poslova iz djelokruga.
5. U okviru područja primjene ovog Ugovora, svaka stranka priznaje uvjerenja o sigurnosnoj provjeri osobe i uvjerenja o sigurnosnoj provjeri pravne osobe koje je izdala druga stranka.
6. U okviru područja primjene ovog Ugovora, nacionalna sigurnosna tijela bez odgode obavješćuju jedno drugo o svakoj promjeni u pogledu uvjerenja o sigurnosnoj provjeri osobe i uvjerenja o sigurnosnoj provjeri pravne osobe, posebice o njihovom povlačenju.
7. Stranke, na zahtjev i u skladu s nacionalnim pravom, pomažu jedna drugoj u provedbi sigurnosnih provjera nužnih za primjenu ovog Ugovora.
8. Stranka primateljica:
    1) dostavlja klasificirane podatke trećoj strani samo na temelju prethodnog pisanog pristanka stranke pošiljateljice;
    2) označava primljene klasificirane podatke u skladu s istoznačnim stupnjem tajnosti utvrđenim u članku 3.;
    3) koristi klasificirane podatke samo za svrhu za koju su dostavljeni.

ČLANAK 6.

PRIJENOS KLASIFICIRANIH PODATAKA

1. Klasificirani podaci prenose se diplomatskim putem.
2. Podaci stupnja tajnosti ZASTRZEŽONE / OGRANIČENO / RESTRICTED mogu se prenositi i putem ovlaštenih sredstava prijenosa u skladu s nacionalnim pravom stranke pošiljateljice.
3. U žurnim slučajevima, ako nije moguće koristiti druge oblike prijenosa, ako su ispunjeni sigurnosni zahtjevi određeni nacionalnim pravom stranke pošiljateljice, dopušten je osobni prijenos podataka stupnja tajnosti ZASTRZEŽONE / OGRANIČENO / RESTRICTED i POUFNE / POVJERLJIVO / CONFIDENTIAL od strane ovlaštenih osoba.
4. Nacionalna sigurnosna tijela mogu dogovoriti druge oblike prijenosa klasificiranih podataka koji osiguravaju njihovu zaštitu od neovlaštenog otkrivanja.
5. Stranka primateljica pisano potvrđuje primitak klasificiranih podataka.
6. Tijela nadležna za razmjenu klasificiranih podataka na temelju drugih međunarodnih ugovora sklopljenih između stranaka mogu izravno razmjenjivati klasificirane podatke.

ČLANAK 7.

UMNOŽAVANJE I PREVOĐENJE KLASIFICIRANIH PODATAKA

1. Umnožavanje ili prevođenje klasificiranih podataka obavlja se u skladu s nacionalnim pravom svake od stranaka. Svi umnoženi primjerci i prijevodi klasificiranih podataka označavaju se izvornom oznakom stupnja tajnosti. Takvi umnoženi ili prevedeni podaci stavljaju se pod istu zaštitu kao izvorni podaci. Broj umnoženih primjeraka i prijevoda ograničen je na broj potreban za službene svrhe.
2. Podaci stupnja tajnosti ŠCIŠLE TAJNE / VRLO TAJNO / TOP SECRET prevode se ili umnožavaju samo u iznimnim slučajevima na temelju prethodnog pisanog pristanka stranke pošiljateljice.
3. Prevedeni klasificirani podaci označavaju se izvornom oznakom stupnja tajnosti i nose odgovarajuću napomenu, na jeziku na koji su prevedeni, da prijevod sadrži klasificirane podatke stranke pošiljateljice.

ČLANAK 8.

UNIŠTAVANJE KLASIFICIRANIH PODATAKA

1. Klasificirani podaci uništavaju se na način koji onemogućava njihovo djelomično ili potpuno obnavljanje, u skladu s nacionalnim pravom stranke primateljice.
2. Podaci stupnja tajnosti ŠCIŠLE TAJNE / VRLO TAJNO / TOP SECRET ne uništavaju se. Oni se vraćaju stranci pošiljateljici.
3. Stranka pošiljateljica može, dodatnim označavanjem ili slanjem naknadne pisane obavijesti, zabraniti uništavanje klasificiranih podataka. Ako je uništavanje klasificiranih podataka zabranjeno, oni se vraćaju stranci pošiljateljici.
4. U izvanrednim okolnostima, u kojima je nemoguće zaštititi ili vratiti klasificirane podatke koji su razmijenjeni ili nastali u skladu s ovim Ugovorom, klasificirani podaci se odmah uništavaju. Stranka primateljica obavješćuje nacionalno sigurnosno tijelo stranke pošiljateljice o tom uništavanju što je prije moguće.

ČLANAK 9.

KLASIFICIRANI UGOVORI

1. Klasificirani ugovori, u dijelu vezanom uz pristup klasificiranim podacima, sklapaju se i provode u skladu s nacionalnim pravom svake stranke.
2. Prije sklapanja klasificiranog ugovora vezanog uz pristup podacima stupnja tajnosti POUFNE / POVJERLJIVO / CONFIDENTIAL ili višeg, potencijalni ugovaratelj obraća se svom nacionalnom sigurnosnom tijelu sa zahtjevom da nacionalno sigurnosno tijelo druge stranke izda potvrdu da potencijalni ugovaratelj druge stranke posjeduje valjano uvjerenje o sigurnosnoj provjeri pravne osobe odgovarajuće za stupanj tajnosti klasificiranih podataka kojima bi ugovaratelj trebao imati pristup.
3. Izdavanje potvrde iz stavka 2. ovog članka jednako je jamstvu da su provedene potrebne radnje kako bi se ustvrdilo da ugovaratelj koji prima klasificirane podatke ispunjava mjerila iz djelokruga njihove zaštite određena u nacionalnom pravu stranke na čijem se državnom području ugovaratelj nalazi.
4. Klasificirani podaci ne ustupaju se ugovaratelju do primitka potvrde iz stavka 2. ovog članka.

5. Ugovaratelj koji prima klasificirane podatke pribavlja od ugovaratelja druge stranke sigurnosnu uputu potrebnu za provedbu klasificiranog ugovora. Sigurnosna uputa sastavni je dio svakog klasificiranog ugovora i sadrži odredbe o sigurnosnim zahtjevima, a posebno:
   1) popis vrsta klasificiranih podataka vezanih uz određeni klasificirani ugovor, uključujući njihove stupnjeve tajnosti;
   2) pravila za dodjeljivanje stupnjeva tajnosti podacima koji nastaju tijekom provedbe određenog klasificiranog ugovora.
6. Ugovaratelj dostavlja primjerak sigurnosne upute svom nacionalnom sigurnosnom tijelu.
7. Svaki podugovaratelj pridržava se istih uvjeta za zaštitu klasificiranih podataka kakvi su utvrđeni za ugovaratelja.

ČLANAK 10.

POSJETI

1. Osobama koje dolaze u posjet na državno područje druge stranke pristup klasificiranim podacima odobrava se tek nakon primitka prethodnog pisanog pristanka koji je izdalo nacionalno sigurnosno tijelo druge stranke.
2. Nacionalno sigurnosno tijelo stranke posjetitelja obraća se sa zahtjevom za posjet nacionalnom sigurnosnom tijelu stranke domaćina najmanje 30 dana prije planiranog posjeta iz stavka 1. ovog članka, a u žurnim slučajevima u kraćem vremenu.
3. Zahtjev iz stavka 2. ovog članka sadrži:
   1) svrhu, datum i program posjeta;
   2) ime i prezime posjetitelja, njegov datum i mjesto rođenja, državljanstvo i broj putovnice ili druge identifikacijske isprave;
   3) radno mjesto posjetitelja, uz naziv tijela koje predstavlja;
   4) stupanj i datum valjanosti uvjerenja o sigurnosnoj provjeri osobe koje posjetitelj posjeduje;
   5) naziv i adresu tijela koje se posjećuje;
   6) ime, prezime i radno mjesto osobe koju se posjećuje;
   7) druge podatke, ako su tako dogovorila nacionalna sigurnosna tijela;

kao i datum, potpis te službeni pečat nacionalnog sigurnosnog tijela stranke posjetitelja.

4. Nacionalna sigurnosna tijela mogu dogovoriti utvrđivanje popisa osoba kojima su odobreni ponovljeni posjeti u vezi s provedbom određenog projekta, programa ili klasificiranog ugovora. Ti popisi sadrže podatke naznačene u stavku 3. ovog članka i vrijede u razdoblju od 12 mjeseci. Nakon što te popise odobre nacionalna sigurnosna tijela, datumi posjeta dogovaraju se neposredno između ovlaštenih tijela posjetitelja i domaćina, u skladu s dogovorenim uvjetima.
5. Posjeti koji uključuju pristup podacima stupnja tajnosti ZASTRZEŽONE / OGRANIČENO / RESTRICTED dogovaraju se neposredno između ovlaštenih tijela posjetitelja i domaćina.
6. Stranke, u skladu sa svojim nacionalnim pravom, osiguravaju zaštitu osobnih podataka osoba koje dolaze u posjet koji uključuje pristup klasificiranim podacima.

ČLANAK 11.
POVREDA SIGURNOSTI

1. Podaci o svakoj povredi sigurnosti ili sumnji u povredu sigurnosti koja se odnosi na klasificirane podatke stranke pošiljateljice ili klasificirane podatke koji su nastali kao rezultat suradnje stranaka odmah se prijavljuju nacionalnom sigurnosnom tijelu stranke na čijem je državnom području do nje došlo.
2. U slučaju bilo koje povrede sigurnosti ili sumnje u povredu sigurnosti, pokreće se odgovarajući postupak u skladu s nacionalnim pravom stranke na čijem je državnom području do nje došlo.
3. U slučaju povrede sigurnosti, nacionalno sigurnosno tijelo stranke na čijem je državnom području do nje došlo, pisano obavješćuje nacionalno sigurnosno tijelo druge stranke o činjenici, okolnostima povrede i ishodu radnji iz stavka 2. ovog članka.
4. Nacionalna sigurnosna tijela surađuju u radnjama iz stavka 2. ovog članka, na zahtjev jednog od njih.
5. Kada do povrede sigurnosti dođe na državnom području treće strane, nacionalno sigurnosno tijelo stranke pošiljateljice, u suradnji s trećom stranom, poduzima radnje kako bi se utvrdile okolnosti povrede.

ČLANAK 12.
PROVEDBA

1. Nacionalna sigurnosna tijela obavješćuju jedno drugo o bilo kojim izmjenama i dopunama njihovog nacionalnog prava o zaštiti klasificiranih podataka koje se odnose na provedbu ovog Ugovora.
2. Nacionalna sigurnosna tijela, na zahtjev jednog od njih, međusobno se savjetuju kako bi osigurala blisku suradnju u provedbi odredaba ovog Ugovora.
3. Kako bi se osigurala učinkovita suradnja koja proizlazi iz odredaba ovog Ugovora, i u okviru ovlasti priznatih nacionalnim pravom svojih stranaka, nacionalna sigurnosna tijela mogu, ako je to potrebno, sklapati pisane detaljne tehničke ili organizacijske dogovore.
4. U okviru provedbe odredaba ovog Ugovora, stranke koriste engleski ili svoje službene jezike, u kojem se slučaju prilaže prijevod na službeni jezik druge stranke ili engleski jezik.
5. Svaka stranka snosi svoje vlastite troškove koji su nastali u provedbi ovog Ugovora i njegovom nadzoru.

ČLANAK 13.
RJEŠAVANJE SPOROVA

1. Svaki spor u vezi s tumačenjem ili primjenom ovog Ugovora rješavat će se izravno između nacionalnih sigurnosnih tijela i neće se podnositi na rješavanje bilo kojem međunarodnom sudu ili trećoj strani.
2. Ako se rješenje spora ne može postići na način iz stavka 1. ovog članka, taj će se spor riješiti diplomatskim putem.

ČLANAK 14.
ZAVRŠNE ODREDBE

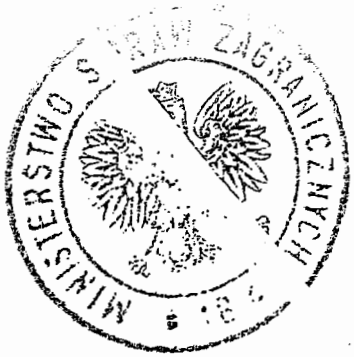
1. Ovaj Ugovor stupa na snagu tridesetog dana koji slijedi nakon datuma primitka posljednje pisane obavijesti kojom stranke obavješćuju jedna drugu, diplomatskim putem, da su ispunjeni njihovi unutarnji pravni uvjeti potrebni za njegovo stupanje na snagu.

2. Ovaj Ugovor može se izmijeniti i dopuniti uzajamnim pisanim pristankom stranaka. Izmjene i dopune stupaju na snagu u skladu s odredbom stavka 1. ovog članka.
3. Ovaj Ugovor sklapa se na neodređeno vrijeme. Svaka stranka može otkazati ovaj Ugovor pisanom obaviješću drugoj stranci diplomatskim putem. U tom slučaju, ovaj Ugovor prestaje šest mjeseci od datuma na koji je druga stranka primila obavijest o otkazu.
4. U slučaju prestanka ovog Ugovora, svi klasificirani podaci razmijenjeni u skladu s ovim Ugovorom nastavljaju se štititi u skladu s ovdje utvrđenim odredbama te se, na zahtjev, vraćaju stranci pošiljateljici.
5. Datumom stupanja na snagu ovog Ugovora, prestaje Sporazum između Vlade Republike Poljske i Vlade Republike Hrvatske o uzajamnoj zaštiti tajnih podataka, potpisan u Zagrebu dana 17. rujna 2003. Klasificirani podaci razmijenjeni na temelju gore spomenutog Sporazuma štite se u skladu s odredbama ovog Ugovora.

Sastavljeno u Varšavi dana 6. listopada 2016. u dva izvornika, svaki na poljskom, hrvatskom i engleskom jeziku, pri čemu su svi tekstovi jednako vjerodostojni. U slučaju razlika u tumačenju, mjerodavan je engleski tekst.

ZA VLADU
REPUBLIKE POLJSKE

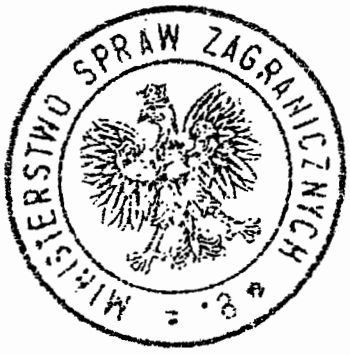
ZA VLADU
REPUBLIKE HRVATSKE



Oświadczam zgodność
fotokopii z oryginałem/~~odpisem~~

Warszawa, dnia 14.10.2016

Dyrektor Departamentu
Prawno-Traktatowego
Andrzej Misztal



AGREEMENT

between the Government of the Republic of Poland and the Government of the Republic of Croatia on Mutual Protection of Classified Information

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

Realizing that good co-operation may require exchange of
Classified Information between the Parties,

Desiring to establish a set of rules regulating the mutual protection of
Classified Information exchanged or generated in the course of
the cooperation between the Parties,

Subject to respect binding rules of the international law
and the national law of the Parties,

Have agreed as follows:

ARTICLE 1
OBJECTIVE AND SCOPE

1. The objective of this Agreement is to ensure the protection of Classified Information that is generated or exchanged between the Parties, individuals, legal entities or other forms of organizations under their jurisdiction.
2. This Agreement shall be applicable to any contracts or international agreements involving Classified Information performed or concluded between the Parties, individuals, legal entities or other forms of organizations under their jurisdiction as well as to any activities conducted between them.

ARTICLE 2
DEFINITIONS

For the purposes of this Agreement:

1) "**Classified Information**" means any information, irrespective of the form, carrier and manner of recording, as well as objects or any parts thereof, also in the process of being generated, which has been classified in accordance with the national law of the Originating Party;
2) "**Originating Party**" means the Party, as well as individuals, legal entities or other forms of organizations, competent to generate and transmit Classified Information in accordance with the national law of that Party;
3) "**Receiving Party**" means 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 that Party;
4) "**National Security Authority**" means the national authority referred to in Article 4 responsible for the implementation and supervision of this Agreement;
5) "**Contractor**" means an individual, a legal entity or other form of organization possessing the legal capacity to conclude Classified Contracts;

6) "**Classified Contract**" means an agreement between Contractors which contains or the execution of which requires access to Classified Information;

7) "**Security Breach**" means an action or an omission which is contrary to this Agreement or the national law of the Parties concerning Classified Information protection;

8) "**Third Party**" means any state, including individuals, legal entities or other forms of organizations under its jurisdiction or an international organization not being a Party to this Agreement.

ARTICLE 3
SECURITY CLASSIFICATION LEVELS

The Parties agree that the following security classification levels are equivalent:

FOR THE REPUBLIC OF POLAND	FOR THE REPUBLIC OF CROATIA	EQUIVALENT IN ENGLISH
ŚCIŚLE TAJNE	VRLO TAJNO	TOP SECRET
TAJNE	TAJNO	SECRET
POUFNE	POVJERLJIVO	CONFIDENTIAL
ZASTRZEŻONE	OGRANIČENO	RESTRICTED

ARTICLE 4
NATIONAL SECURITY AUTHORITIES

1. The National Security Authorities of the Parties are:

   For the Republic of Poland

   - the Head of the Internal Security Agency;

   For the Republic of Croatia

- Office of the National Security Council.

2. The Parties shall inform each other through diplomatic channels of changes of the National Security Authorities or amendments to their competences.

ARTICLE 5
RULES OF CLASSIFIED INFORMATION PROTECTION

1. In accordance with their national law, the Parties shall take all appropriate measures for the protection of Classified Information which is exchanged or generated under this Agreement, including this generated in connection with the performance of Classified Contracts.
2. Classified Information is granted a security classification level in accordance with its content, pursuant to the national law of the Originating Party. The Receiving Party shall guarantee at least an equivalent level of protection of the received Classified Information pursuant to the provisions of Article 3.
3. The security classification level may be changed or removed only by the Originating Party. The Originating Party shall inform the Receiving Party in writing about any change of the security classification level of the released Classified Information.
4. Classified Information shall only be made accessible to persons who are authorized in accordance with the national law to have access to Classified Information of the equivalent security classification level and who have a need-to-know.
5. Within the scope of this Agreement, each Party shall recognize the personnel and facility security clearances issued by the other Party.
6. Within the scope of this Agreement, the National Security Authorities shall inform each other without delay about any alteration with regard to personnel and facility security clearances, in particular about their revocation.

7. The Parties shall assist each other upon request and in accordance with the national law in carrying out vetting procedures necessary for the application of this Agreement.

8. The Receiving Party shall:

   1) submit Classified Information to a Third Party only upon prior written consent of the Originating Party;

   2) mark the received Classified Information in accordance with the security classification level equivalence set forth in Article 3;

   3) use Classified Information only for the purposes that it has been provided for.

ARTICLE 6
TRANSMISSION OF CLASSIFIED INFORMATION

1. Classified Information shall be transmitted via diplomatic channels.
2. Information classified as ZASTRZEŻONE / OGRANIČENO / RESTRICTED may be transmitted also through authorized carriers in accordance with the national law of the Originating Party.
3. In urgent cases, unless it is possible to use other forms of transmission, if the security requirements defined by the national law of the Originating Party are met, the personal carriage of information classified as ZASTRZEŻONE / OGRANIČENO / RESTRICTED and POUFNE / POVJERLJIVO / CONFIDENTIAL by authorized individuals is admissible.
4. The National Security Authorities may agree on other forms of transmitting Classified Information which ensure its protection against unauthorized disclosure.
5. The Receiving Party shall confirm in writing the receipt of Classified Information.

6. The authorities competent to exchange Classified Information on the basis of other international agreements concluded between the Parties may exchange Classified Information directly.

ARTICLE 7
REPRODUCTION AND TRANSLATION OF CLASSIFIED INFORMATION

1. Reproduction or translation of Classified Information shall be conducted pursuant to the national law of each of the Parties. All copies and translations of Classified Information shall be marked with the original security classification marking. Such reproduced or translated information shall be placed under the same protection as the original information. The number of copies and translations shall be restricted to that required for official purposes.
2. Information classified as ŚCIŚLE TAJNE / VRLO TAJNO / TOP SECRET shall be translated or reproduced only in exceptional cases upon prior written consent of the Originating Party.
3. The translated Classified Information shall be marked with the original security classification marking and shall bear an appropriate note in the language into which it is translated that the translation contains Classified Information of the Originating Party.

ARTICLE 8
DESTRUCTION OF CLASSIFIED INFORMATION

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

3. The Originating Party may, by additional marking or sending subsequent written notice, prohibit the destruction of Classified Information. If destruction of Classified Information is prohibited, it shall be returned to the Originating Party.
4. In exceptional circumstances in which it is impossible to protect or return Classified Information exchanged or generated under this Agreement, the Classified Information shall be destroyed immediately. The Receiving Party shall inform the National Security Authority of the Originating Party about this destruction as soon as possible.

ARTICLE 9
CLASSIFIED CONTRACTS

1. Classified Contracts in the part connected with access to Classified Information shall be concluded and implemented in accordance with the national law of each Party.
2. Before concluding a Classified Contract connected with access to information classified as POUFNE / POVJERLJIVO / CONFIDENTIAL or above, a potential Contractor shall apply to its National Security Authority to request that the National Security Authority of the other Party issue a certificate that the potential Contractor of the other Party 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.
3. Issuing the certificate referred to in paragraph 2 of this Article shall be tantamount to a guarantee that necessary actions have been conducted in order to declare that the Contractor receiving Classified Information meets the criteria in the scope of its protection defined in the national law of the Party in the territory of which the Contractor is located.
4. Classified Information shall not be released to the Contractor until the receipt of the certificate referred to in paragraph 2 of this Article.

5. The Contractor receiving Classified Information shall obtain from the Contractor of the other Party a security instruction necessary to perform a Classified Contract. The security instruction shall be an integral part of every Classified Contract and shall contain 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 generated during the performance of a given Classified Contract.
6. The Contractor shall put forward a copy of the security instruction to its National Security Authority.
7. Every subcontractor shall comply with the same conditions for the protection of Classified Information as those laid down for the Contractor.

ARTICLE 10
VISITS

1. Persons arriving on a visit in the territory of the other Party shall be allowed access to Classified Information only after receiving prior written consent issued by the National Security Authority of the other Party.
2. The National Security Authority of the visiting Party shall apply with a request for a visit to the National Security Authority of the hosting Party at least 30 days prior to the planned visit referred to in paragraph 1 of this Article, and in urgent cases in shorter time.
3. The request referred to in paragraph 2 of this Article shall include:
   1) purpose, date and program of the visit;
   2) name and surname of the visitor, their date and place of birth, citizenship 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) other data, if agreed upon by the National Security Authorities;

as well as the date, signature and official seal of the National Security Authority of the visiting Party.

4. The National Security 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 of this Article and shall be valid for a period of 12 months. Once such lists have been approved by the National Security Authorities, the dates of the visits shall be arranged directly between authorized visiting and hosting entities, in accordance with the conditions agreed upon.
5. Visits involving access to information classified as ZASTRZEŻONE / OGRANIČENO / RESTRICTED are arranged directly between authorized visiting and hosting entities.
6. The Parties shall ensure, pursuant to their national law, the protection of the personal data of the persons arriving on a visit involving access to Classified Information.

ARTICLE 11
SECURITY BREACH

1. Information on every Security Breach or a suspicion of a Security Breach 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 National Security Authority of the Party in the territory of which it has occurred.

2. In case of any Security Breach or a suspicion of a Security Breach, appropriate proceedings shall be initiated pursuant to the national law of the Party in the territory of which it has occurred.
3. In case of a Security Breach, the National Security Authority of the Party in the territory of which it has occurred shall inform the National Security Authority of the other Party in writing about the fact, circumstances of the breach and the outcome of the actions referred to in paragraph 2 of this Article.
4. The National Security Authorities shall cooperate in the actions referred to in paragraph 2 of this Article, upon the request of one of them.
5. When the Security Breach has occurred in the territory of a Third Party, the National Security Authority of the Originating Party shall take, in cooperation with the Third Party, the actions in order to determine the circumstances of the breach.

ARTICLE 12
IMPLEMENTATION

1. The National Security 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 National Security 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. In order to ensure effective cooperation resulting from the provisions of this Agreement, and in the scope of authority acknowledged by the national law of their Parties, the National Security Authorities may, if necessary, conclude written detailed technical or organizational arrangements.
4. 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.

5. Each Party shall bear its own expenses incurred in the implementation of this Agreement and its supervision.

ARTICLE 13
SETTLEMENT OF DISPUTES

1. Any dispute regarding the interpretation or application of this Agreement shall be settled directly between the National Security Authorities and shall not be referred to any international tribunal or Third Party for settlement.
2. If settlement of a dispute cannot be reached in the manner referred to in paragraph 1 of this Article, such a dispute shall be settled through diplomatic channels.

ARTICLE 14
FINAL PROVISIONS

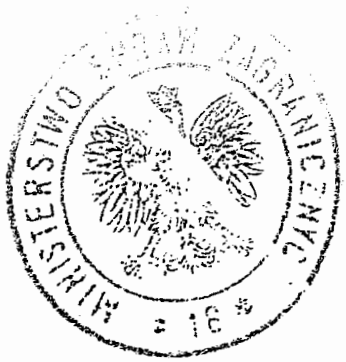
1. This Agreement shall enter into force on the thirtieth day following the date of receipt of the last written notification by which the Parties have informed each other, through diplomatic channels, that their internal legal requirements necessary for its entry into force have been fulfilled.
2. This Agreement may be amended by mutual written consent of the Parties. Amendments shall enter into force in accordance with the provision of paragraph 1 of this Article.
3. This Agreement is concluded for an indefinite period of time. Either Party may denounce this Agreement by giving the other Party notice in writing through diplomatic channels. In that case, this Agreement shall terminate six months from the date on which the other Party has received the denunciation notice.
4. In case of termination of this Agreement, all Classified Information exchanged pursuant to this Agreement shall continue to be protected in accordance with the provisions set forth herein and, upon request, returned to the Originating Party.

5. Upon the date of entry into force of this Agreement, the Agreement between the Government of the Republic of Poland and the Government of the Republic of Croatia on the Mutual Protection of Classified Information, signed in Zagreb on 17 September 2003, shall terminate. Classified Information exchanged on the basis of the above Agreement shall be protected in accordance with the provisions of this Agreement.

Done at Warsaw on 6 October 2016 in two originals, each in the Polish, Croatian and English languages, all texts being equally authentic. In case of any divergence of interpretation, the English text shall prevail.

FOR THE GOVERNMENT OF THE REPUBLIC OF POLAND

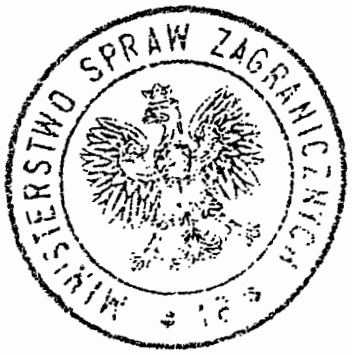
FOR THE GOVERNMENT OF THE REPUBLIC OF CROATIA



Stwierdzam zgodność
fotokopii z oryginałem/~~odpisem~~

Warszawa, dnia 14.10.2016

Dyrektor Departamentu
Prawno-Traktatowego
Andrzej Misztal



Warszawa, 9 grudnia 2016 r.

[redacted]

Minister
Spraw Zagranicznych

DPUE.920.1022.2014 / 7/MN

dot.: P-16441/2016/5665/2014/MN z 30.11.2016 r.

Pan
Piotr Pogonowski
Szef
Agencji Bezpieczeństwa Wewnętrznego

Opinia
o zgodności z prawem Unii Europejskiej *Umowy między Rządem Rzeczypospolitej Polskiej a Rządem Republiki Chorwacji o wzajemnej ochronie informacji niejawnych*, wyrażona przez ministra właściwego do spraw członkostwa Rzeczypospolitej Polskiej w Unii Europejskiej

Szanowny Panie Profesorze,

w związku z przedłożonym projektem wniosku o ratyfikację umowy międzynarodowej pozwalam sobie wyrazić poniższą opinię.

Umowa nie jest sprzeczna z prawem Unii Europejskiej.

Z poważaniem

z up. Ministra Spraw Zagranicznych
Podsekretarz Stanu
Joanna Wronecka

Do wiadomości:
Pani Jolanta Rusiniak
Sekretarz Rady Ministrów