



SEJM  
RZECZYPOSPOLITEJ POLSKIEJ  
VIII kadencja  
Prezes Rady Ministrów  
RM-111-106-19

**Druk nr 3832**  
Warszawa, 9 października 2019 r.

Pani  
Elżbieta Witek  
Marszałek Sejmu  
Rzeczypospolitej Polskiej

*Szanowna Pani Marszałek*

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

**- Umowę między Rządem Rzeczypospolitej  
Polskiej a Rządem Republiki Azerbejdżanu  
o wymianie i wzajemnej ochronie informacji  
niejawnych podpisaną w Baku dnia 31 maja  
2019 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 poważaniem*

(-) Mateusz Morawiecki

*/podpisano kwalifikowanym podpisem elektronicznym/*

W imieniu Rzeczypospolitej Polskiej

PREZYDENT RZECZYPOSPOLITEJ POLSKIEJ

podaje do powszechnej wiadomości:

Dnia 31 maja 2019 r. w Baku została podpisana Umowa między Rządem Rzeczypospolitej Polskiej a Rządem Republiki Azerbejdżanu o wymianie i wzajemnej ochronie informacji niejawnych w następującym brzmieniu:

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 został wydany akt niniejszy, opatrzony pieczęcią Rzeczypospolitej Polskiej.

Dano w Warszawie dnia

PREZYDENT RZECZYPOSPOLITEJ  
POLSKIEJ

Andrzej Duda

PREZES RADY MINISTRÓW

Mateusz Morawiecki

## UZASADNIENIE

### **I. Wyjaśnienie potrzeby i celu związania Rzeczypospolitej Polskiej Umową**

Rozwijająca się współpraca polityczna i gospodarcza z innymi państwami pociąga za sobą konieczność stworzenia podstaw prawnych regulujących zasady ochrony informacji niejawnych wymienianych w relacjach bilateralnych.

Podpisana w dniu 31 maja 2019 r. *Umowa między Rządem Rzeczypospolitej Polskiej a Rządem Republiki Azerbejdżanu o wymianie i wzajemnej ochronie informacji niejawnych* reguluje aspekty prawne współpracy właściwych polskich podmiotów z ich azerbejdżańskimi odpowiednikami upoważnionymi, zgodnie ze swoim prawem krajowym, do przetwarzania informacji niejawnych. Po wejściu w życie Umowa będzie stanowić podstawę do nawiązania ściślejszej współpracy w zakresie obronności i bezpieczeństwa wewnętrznego – szczególnie w zwalczaniu najgroźniejszych form przestępczości oraz przeciwdziałania terroryzmowi. Uregulowanie przedmiotowych kwestii będzie, po wejściu tej Umowy w obieg prawny, również istotne dla rozwoju współpracy gospodarczej, gdyż stworzy polskim i azerbejdżańskim przedsiębiorcom podstawy prawne do zawierania kontraktów, których realizacja wiąże się z dostępem do informacji niejawnych lub wytwarzaniem takich informacji. Umowa ta otworzy zatem nowe perspektywy dla polskiego przemysłu zbrojeniowego, umożliwiając przedsiębiorcom z tego sektora uczestnictwo w przetargach związanych z dostępem do informacji niejawnych organizowanych w Azerbejdżanie.

### **II. Wskazanie różnic między dotychczasowym a projektowanym stanem prawnym**

Umowa między Rządem Rzeczypospolitej Polskiej a Rządem Republiki Azerbejdżanu o wymianie i wzajemnej ochronie informacji niejawnych jest pierwszą umową tego rodzaju zawartą z ww. partnerem zagranicznym.

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.

Art. 1 Umowy definiuje przedmiot i zakres jej stosowania. Kompleksowy charakter Umowy powoduje, iż po wejściu w życie będzie miała ona zastosowanie do

wszelkich działań, kontraktów lub umów dotyczących informacji niejawnych zawieranych między Stronami, osobami fizycznymi, osobami prawnymi lub innymi podmiotami (np. jednostkami organizacyjnymi) pozostającymi pod ich jurysdykcją, niezależnie od ich osobowości prawnej.

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 toku przeprowadzonych negocjacji wyrażenie „inne jednostki organizacyjne” zostało zastąpione przez „inny podmiot i jednostkę, niezależnie od jej formy prawnej”.

W art. 3 zestawiono odpowiadające sobie klauzule tajności celem usystematyzowania ich nazewnictwa oraz uszczegółowiono obowiązek klasyfikowania informacji niejawnych zgodnie z prawem krajowym Stron. Strona polska może przekazywać także informacje niejawne o klauzuli „Zastrzeżone”, które na podstawie przyjętych przez Stronę azerbejdzańską zobowiązań będą chronione w Republice Azerbejdżanu w stopniu odpowiadającym klauzuli „Poufne”. Ponadto Strony uzgodniły, że nie będą wymieniały informacji niejawnych o klauzuli „Ścisłe tajne”, natomiast gdyby wymiana taka była niezbędna, będzie ona regulowana odrębnymi przepisami, uzgodnionymi między Stronami.

W art. 4 wskazano właściwe organy bezpieczeństwa, które są odpowiedzialne za realizację postanowień niniejszej Umowy.

Art. 5 Umowy określa zasady ochrony informacji niejawnych, które mają gwarantować właściwą ochronę przekazywanym informacjom niejawnym. Na ich podstawie, po wejściu w życie Umowy, 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.

W art. 6 Strony uznały wzajemnie poświadczenia bezpieczeństwa oraz świadectwa bezpieczeństwa przemysłowego.

Art. 7 reguluje możliwość zawierania kontraktów niejawnych, których realizacja wiąże się z dostępem do informacji niejawnych bądź z wytworzeniem takich informacji.

W art. 8, art. 9 i art. 10 uregulowano kolejno: przekazywanie, powielanie, tłumaczenie oraz niszczenie informacji niejawnych, co pozwoli na ujednoczenie postępowania z informacjami niejawnymi w stosunkach bilateralnych. Natomiast informacje niejawne o klauzuli „Ścisłe tajne” nie będą powielane ani tłumaczone.

W art. 11 określono warunki i tryb przeprowadzania wzajemnych wizyt związanych z dostępem do informacji niejawnych jak również zasady ochrony danych osobowych osób przybywających z wizytą.

W art. 12 zostały określone zasady postępowania w przypadkach naruszenia regulacji dotyczących wzajemnej ochrony informacji niejawnych. W artykule tym jest przewidziana m.in. możliwość współpracy właściwych organów obu Stron przy czynnościach wyjaśniających.

W art. 13 uregulowano kwestię języków, jakimi Strony będą się posługiwały w zakresie stosowania postanowień niniejszej Umowy.

W sposób jednoznaczny uregulowano w art. 14 kwestię ponoszenia przez Strony kosztów związanych z realizacją niniejszej Umowy.

W art. 15 wprowadzono tryb konsultacji właściwych organów państw obu Stron w celu współpracy przy realizacji postanowień Umowy.

Ponadto Umowa przewiduje tryb rozstrzygania sporów (art. 16) przy czym na wniosek Strony azerbejdżańskiej, ustęp 1 został uzupełniony o sformułowanie „interpretacji i” natomiast ustęp 2 o sformułowanie „między Stronami”.

W art. 17 określono tryb wprowadzania zmian do Umowy, natomiast w art. 18 procedurę wejścia w życie Umowy, czas jej obowiązywania oraz tryb wypowiedzenia, 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 Rzeczpospolitą Polską a Republiką Azerbejdżanu. Umowa

stanowić będzie podstawę do nawiązania ściślejszej współpracy w zakresie bezpieczeństwa wewnętrznego oraz w zwalczaniu najgroźniejszych form przestępczości.

Po wejściu w życie 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 zacieśnienie współpracy i pogłębienie dotychczasowych relacji między Rzeczpospolitą Polską i Republiką Azerbejdżanu. 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 (Dz. U. z 2019 r. poz. 742). Umowa ta dotyczy wprowadzie 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 o ochronie informacji niejawnych. Nie zostały zatem spełnione przesłanki wymienione w art. 89 ust. 1 Konstytucji Rzeczypospolitej Polskiej (Dz. U. poz. 483, z 2001 r. poz. 319, z 2006 r. poz. 1471 oraz z 2009 r. poz. 946), a więc ratyfikacja przedmiotowej Umowy nie wymaga uprzedniej zgody wyrażonej w ustawie.

Umowa ta dotyczy takich podmiotów prawa wewnętrznego Rzeczypospolitej Polskiej, jak osoby fizyczne, osoby prawne oraz inne podmioty (np. jednostki organizacyjne) w rozumieniu ustawy o ochronie informacji niejawnych. W odniesieniu

do zakresu, podmiotowego niniejszej Umowy należy wskazać, na przewidzianą jej postanowieniami, możliwość zawierania kontraktów niejawnych związanych z dostępem do informacji niejawnych, w tym występowania określonych podmiotów w roli zlecającego, kontrahenta oraz podwykonawcy. Ponadto w art. 11 Umowa przewiduje w odniesieniu do osób fizycznych także możliwość przeprowadzania wizyt na terytorium państwa drugiej Strony związanych z dostępem do informacji niejawnych. W tym zakresie Umowa dotyczy spraw uregulowanych w prawie wewnętrznym Rzeczypospolitej Polskiej, objętych zarówno przepisami ustawy o ochronie informacji niejawnych, jak też ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2018 r. poz. 1000 i 1669).

Ze względu na opisany powyżej zakres regulacji, w Rzeczypospolitej Polskiej związanie przedmiotową Umową powinno nastąpić przez jej ratyfikację w trybie artykułu 89 ust. 2 Konstytucji Rzeczypospolitej Polskiej oraz zgodnie z postanowieniami art. 12 ust. 2 ustawy z dnia 14 kwietnia 2000 r. o umowach międzynarodowych (Dz. U. poz. 443, z 2002 r. poz. 1824, z 2010 r. poz. 1395, z 2011 r. poz. 676 oraz z 2019 r. poz. 109). Zgodnie bowiem z art. 87 Konstytucji źródłem powszechnie obowiązującego prawa w Rzeczypospolitej Polskiej są wyłącznie ratyfikowane umowy międzynarodowe, a nie zaistniały przesłanki ratyfikacji Umowy za uprzednią zgodą wyrażoną w ustawie.

Wybór trybu tzw. małej ratyfikacji jest poparty zatem potrzebą uznania przedmiotowej Umowy za źródło powszechnie obowiązującego prawa w Rzeczypospolitej Polskiej, gdyż jej postanowienia będą miały zastosowanie do szerokiego kręgu podmiotów (organy administracji państwowej, przedsiębiorcy). 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.

## **UMOWA**

**między Rządem Rzeczypospolitej Polskiej**

**a**

**Rządem Republiki Azerbejdżanu**

**o wymianie i wzajemnej ochronie informacji niejawnych**

**Rząd Rzeczypospolitej Polskiej i Rząd Republiki Azerbejdżanu,  
zwane dalej „Stronami”,**

**mając na uwadze zagwarantowanie wzajemnej ochrony wszystkich informacji,  
które zostały zakwalifikowane jako informacje niejawne, zgodnie z prawem**

**Państwa jednej ze Stron**

**i przekazane drugiej Stronie lub powstały w wyniku współpracy,**

**kierując się w tym celu zamiarem przyjęcia regulacji**

**w zakresie wzajemnej ochrony informacji niejawnych, które znajdą zastosowanie**

**w odniesieniu do wszelkiej wspólnej działalności, związanej z wymianą**

**informacji niejawnych,**

**z zastrzeżeniem poszanowania norm prawa międzynarodowego i prawa Państw**

**Stron, kierując się zasadami równości, wzajemności i obustronnych korzyści,**

**uzgodniły, co następuje:**

## ARTYKUŁ 1 PRZEDMIOT UMOWY

1. Przedmiotem niniejszej Umowy jest zapewnienie ochrony informacjom niejawnym wytwarzanym w wyniku współpracy lub wymienianym między Stronami oraz osobami fizycznymi, osobami prawnymi lub innymi podmiotami i jednostkami organizacyjnymi, niezależnie od ich formy prawnej, 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 podmiotami i jednostkami organizacyjnymi, niezależnie od ich formy prawnej pozostającymi pod ich jurysdykcją, oraz do wszelkich działań realizowanych między nimi.

## ARTYKUŁ 2 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 opracowywania, które wymagają ochrony przed nieuprawnionym ujawnieniem, zgodnie z prawem Państwa jednej ze Stron niniejszej Umowy;
- 2) **właściwe organy** – organy, o których mowa w artykule 4 niniejszej Umowy;
- 3) **Strona wytwarzająca** – Stronę, osobę fizyczną, osobę prawną lub inny podmiot i jednostkę organizacyjną, niezależnie od jej formy prawnej uprawnioną do wytwarzania i przekazywania informacji niejawnych zgodnie z prawem Państwa swojej Strony;

- 4) **Strona otrzymująca** – Stronę, osobę fizyczną, osobę prawną lub inny podmiot i jednostkę organizacyjną, niezależnie od jej formy prawnej uprawnioną do otrzymywania informacji niejawnych zgodnie z prawem Państwa swojej Strony;
- 5) **kontrakt niejawny** – umowę, która zawiera informacje niejawne lub której realizacja wiąże się z dostępem do takich informacji, bądź ich wytworzeniem;
- 6) **kontrahent** – osobę fizyczną, osobę prawną albo inny podmiot i jednostkę organizacyjną, niezależnie od jej formy prawnej podlegającą prawu Państwa jednej ze Stron, uprawnioną do zawierania kontraktów niejawnych;
- 7) **zlecający** – osobę fizyczną, osobę prawną albo inny podmiot i jednostkę organizacyjną, niezależnie od jej formy prawnej podlegającą prawu Państwa jednej ze Stron, uprawnioną do zlecania kontraktów niejawnych;
- 8) **poświadczenie bezpieczeństwa** – dokument wydany zgodnie z prawem Państwa jednej Strony przez jej właściwy organ lub inny uprawniony podmiot, który potwierdza, że osoba fizyczna została poddana postępowaniu sprawdzającemu i jest uprawniona do dostępu do informacji niejawnych;
- 9) **świadczenie bezpieczeństwa przemysłowego** – dokument wydany zgodnie z prawem Państwa jednej Strony przez jej 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, osobę fizyczną, osobę prawną lub inny podmiot i jednostkę organizacyjną, niezależnie od jej formy prawnej, znajdującą się pod jego jurysdykcją lub organizację międzynarodową niebędące Stroną niniejszej Umowy.

**ARTYKUŁ 3**  
**KLAUZULE TAJNOŚCI**

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

<b>RZECZPOSPOLITA POLSKA</b>	<b>REPUBLIKA AZERBEJDŻANU</b>	<b>ODPOWIEDNIK W JĘZYKU ANGIELSKIM</b>
TAJNE	TAM MƏXFİ	SECRET
POUFNE	MƏXFİ	CONFIDENTIAL
ZASTRZEŻONE	(brak odpowiednika)	RESTRICTED

4. Informacje otrzymane z Rzeczypospolitej Polskiej o klauzuli ZASTRZEŻONE są chronione jako MƏXFİ w Republice Azerbejdżanu.
5. W przypadku potrzeby wymiany informacji o klauzuli ŚCIŚLE TAJNE/ XÜSUSİ ƏHƏMİYYƏTLİ /TOP SECRET, odrębne przepisy zostaną uzgodnione pomiędzy Stronami.

**ARTYKUŁ 4**  
**WŁAŚCIWE ORGANY**

1. W rozumieniu niniejszej Umowy właściwymi organami są:
  - 1) dla Rządu Rzeczypospolitej Polskiej: Szef Agencji Bezpieczeństwa Wewnętrznego;
  - 2) dla Rządu Republiki Azerbejdżanu: Służba Bezpieczeństwa Narodowego.
2. Strony informują się drogą dyplomatyczną o zmianach właściwych organów, o których mowa w ustępie 1, lub zmianach ich właściwości.

**ARTYKUŁ 5**  
**ZASADY OCHRONY INFORMACJI NIEJAWNYCH**

1. Strony podejmują wszelkie działania określone w niniejszej Umowie, zgodnie z prawem swoich Państw w celu ochrony informacji niejawnych przekazywanych lub wytwarzanych w wyniku wspólnej działalności Stron, w tym także wytworzonych w związku z realizacją kontraktów niejawnych.
2. Strona otrzymująca wykorzystuje informacje niejawne wyłącznie w celach, dla których zostały one przekazane.
3. Informacje niejawne mogą być udostępniane tylko tym osobom, których zadania wymagają zapoznania się z nimi i które zgodnie z prawem Państwa Strony otrzymującej zostały upoważnione do dostępu do nich.
4. Strona otrzymująca nie udostępnia informacji, o których mowa w ustępie 1, Stronie trzeciej, bez uprzedniej pisemnej zgody Strony wytwarzającej.

**ARTYKUŁ 6**  
**POŚWIADCZENIA BEZPIECZEŃSTWA ORAZ ŚWIADECTWA**  
**BEZPIECZEŃSTWA PRZEMYSŁOWEGO**

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

**ARTYKUŁ 7**  
**KONTRAKTY NIEJAWNE**

1. Przed zawarciem kontraktu niejawnego, związanego z dostępem do informacji niejawnych o klauzuli POUFNE/MƏXFİ/CONFIDENTIAL lub wyższej, zlecający składa wniosek do właściwego organu swojej Strony o wystąpienie do właściwego organu drugiej Strony z prośbą o wydanie pisemnego 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 Państwa Strony, na terytorium którego posiada 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. Instrukcja bezpieczeństwa przemysłowego zawiera postanowienia dotyczące wymogów bezpieczeństwa, w szczególności:

- 1) wykaz rodzajów informacji niejawnych odnoszących się do danego kontraktu niejawnego, z uwzględnieniem ich klauzul tajności;
- 2) zasady przyznawania klauzul tajności informacjom wytworzonym podczas realizacji danego kontraktu niejawnego.
5. Zlecający przekazuje kopię instrukcji bezpieczeństwa przemysłowego właściwemu organowi swojej Strony, który kieruje ją do właściwego organu Strony kontrahenta.
6. Realizacja kontraktu niejawnego w części związanej z dostępem do informacji niejawnych, jest możliwa po spełnieniu przez kontrahenta warunków niezbędnych do ochrony informacji niejawnych, zgodnie z instrukcją bezpieczeństwa przemysłowego.
7. Każdy podwykonawca podlega tym samym obowiązkom ochrony informacji niejawnych, jakie nałożono na kontrahenta.

## **ARTYKUŁ 8**

### **PRZEKAZYWANIE INFORMACJI NIEJAWNYCH**

1. Informacje niejawne są przekazywane drogą dyplomatyczną.
2. Informacje niejawne o klauzuli ZASTRZEŻONE/RESTRICTED oraz POUFNE/MƏXFİ/CONFIDENTIAL mogą być przekazywane również za pośrednictwem uprawnionych do tego przewoźników, zgodnie z prawem Państwa Strony wytwarzającej.
3. W pilnych przypadkach, o ile nie można skorzystać z innej formy przekazania informacji niejawnych, jeżeli spełnione są wymogi bezpieczeństwa określone prawem Państwa Strony wytwarzającej, dopuszcza się przewóz osobisty informacji niejawnych o klauzuli ZASTRZEŻONE/RESTRICTED oraz POUFNE/MƏXFİ/CONFIDENTIAL przez osoby do tego upoważnione.
4. Właściwe organy Stron mogą ustalić inne sposoby przekazywania informacji niejawnych zapewniające ich ochronę przed 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 9**

### **POWIELANIE LUB TŁUMACZENIE INFORMACJI NIEJAWNYCH**

1. Powielanie lub tłumaczenie informacji niejawnych odbywa się w sposób zgodny z prawem Państwa Strony otrzymującej oraz następującymi zasadami:
- 1) osoby wykonujące tłumaczenia lub kopie informacji niejawnych posiadają poświadczenia bezpieczeństwa, odpowiednie do klauzuli tajności przetłumaczonych lub powielonych informacji niejawnych;
  - 2) powielone lub przetłumaczone informacje podlegają takiej samej ochronie jak oryginały;
  - 3) liczbę kopii lub tłumaczeń należy ograniczyć do liczby wymaganej dla celów służbowych;
  - 4) przetłumaczone informacje należy opatrzyć adnotacją w języku tłumaczenia, wskazującą, iż zawierają one informacje niejawne otrzymane od Strony wytwarzającej.

## **ARTYKUŁ 10**

### **NISZCZENIE INFORMACJI NIEJAWNYCH**

1. Informacje niejawne są niszczone zgodnie z prawem Państwa Strony otrzymującej w sposób uniemożliwiający ich częściowe lub całkowite odtworzenie.
2. Protokoły dotyczące zniszczenia dokumentów zawierających informacje niejawne wraz z tłumaczeniem na język angielski są przekazywane właściwemu organowi Strony wytwarzającej na jej wniosek.

- 2) Strona przyjmująca wizytę nie przechowuje danych osobowych dłużej, aniżeli jest to niezbędne dla osiągnięcia celu ich przetwarzania;
  - 3) w przypadku przekazania danych, których nie wolno było przekazać zgodnie z prawem Państwa Strony przekazującej dane osobowe, Strona ta zawiadamia o tym Stronę przyjmującą wizytę; Strona przyjmująca wizytę jest zobowiązana do usunięcia tych danych w sposób uniemożliwiający ich częściowe lub całkowite odtworzenie;
  - 4) Strona przekazująca dane osobowe odpowiada za ich poprawność, a w przypadku przekazania danych nieprawdziwych lub niekompletnych, zawiadamia o tym Stronę przyjmującą wizytę; Strona przyjmująca wizytę jest zobowiązana do sprostowania lub usunięcia tych danych;
  - 5) Strona przekazująca dane osobowe oraz Strona przyjmująca wizytę są zobowiązane do rejestrowania ich przekazywania, otrzymywania i usuwania;
  - 6) Strona przekazująca dane osobowe oraz Strona przyjmująca wizytę są zobowiązane do skutecznego zabezpieczenia przetwarzanych danych przed ich udostępnieniem osobom nieupoważnionym, nieuprawnionym dokonywaniem zmian tych danych, ich utratą, uszkodzeniem lub zniszczeniem.
5. Właściwe organy Stron 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. Po zatwierdzeniu takich wykazów przez właściwe organy Stron, terminy wizyt uzgadniane są bezpośrednio między podmiotem wysyłającym a podmiotem przyjmującym wizytę, zgodnie z ustalonymi warunkami.

## ARTYKUŁ 11

### WIZYTY

1. Osobom przybywającym z wizytą na terytorium Państwa drugiej Strony zezwala się na dostęp do informacji niejawnych tylko po uprzednim uzyskaniu pisemnego zezwolenia wydanego przez właściwy organ drugiej Strony.
2. Właściwy organ Strony wysyłającej zwraca się do właściwego organu Strony przyjmującej z wnioskiem o wyrażenie zgody na wizytę co najmniej trzydzieści dni przed planowanym terminem wizyty, o której mowa w ustępie 1, a w pilnych przypadkach w krótszym czasie.
3. We wniosku, o którym mowa w ustępie 2, zamieszcza się informacje o:
  - 1) celu, terminie i programie wizyty;
  - 2) imieniu i nazwisku, dacie i miejscu urodzenia, obywatelstwie i numerze paszportu lub innego dokumentu tożsamości osoby przybywającej z wizytą;
  - 3) stanowisku służbowym osoby przybywającej z wizytą wraz z nazwą podmiotu, który reprezentuje;
  - 4) poziomie i dacie ważności poświadczenia bezpieczeństwa posiadanego przez osobę przybywającą z wizytą;
  - 5) nazwie i adresie odwiedzanego podmiotu;
  - 6) imieniu i nazwisku oraz stanowisku służbowym osoby przyjmującej;wniosek zawiera ponadto datę, podpis oraz oficjalną pieczęć właściwego organu Strony wysyłającej.
4. Do ochrony danych osobowych, o których mowa w ustępie 3, przekazywanych w związku z postanowieniami ustępu 1 i 5 stosuje się, z uwzględnieniem prawa Państw Stron, następujące postanowienia:
  - 1) wykorzystanie danych osobowych przez Stronę przyjmującą wizytę jest dopuszczalne wyłącznie w celu oraz na warunkach określonych przez Stronę przekazującą dane osobowe;

## ARTYKUŁ 12

### NARUSZENIE REGULACJI DOTYCZĄCYCH OCHRONY INFORMACJI NIEJAWNYCH

1. Naruszeniem regulacji dotyczących ochrony informacji niejawnych jest działanie lub zaniechanie sprzeczne z niniejszą Umową lub prawem Państw Stron, w zakresie dotyczącym ochrony informacji niejawnych, w tym również nieuprawnione ujawnienie informacji niejawnych.
2. 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 właściwemu organowi Strony, na terytorium której miało miejsce lub zaistniało podejrzenie takiego naruszenia.
3. Każdy przypadek naruszenia lub podejrzenia naruszenia regulacji dotyczących ochrony informacji niejawnych wyjaśnia się zgodnie z prawem Państwa Strony, na terytorium której zdarzenie miało miejsce.
4. W przypadku naruszenia regulacji dotyczących ochrony informacji niejawnych, o którym mowa w ustępie 1, właściwy organ Strony, na terytorium której naruszenie miało miejsce, pisemnie informuje właściwy organ drugiej Strony o fakcie, okolicznościach naruszenia i wyniku czynności, o których mowa w ustępie 3.
5. Jeżeli naruszenie regulacji dotyczących ochrony informacji niejawnych miało miejsce na terytorium Strony trzeciej, Strona, która przekazała informacje niejawne podejmie we współpracy ze Stroną trzecią działania, o których mowa w ustępach 2, 3 i 4.
6. Właściwe organy Stron współpracują przy czynnościach, o których mowa w ustępie 3, na wniosek jednego z nich.

### **ARTYKUŁ 13**

#### **JĘZYKI**

W zakresie stosowania postanowień niniejszej Umowy Strony używają języka angielskiego lub swoich języków urzędowych. W przypadku stosowania języków urzędowych, Strony dołączają tłumaczenie na język urzędowy drugiej Strony lub na język angielski.

### **ARTYKUŁ 14**

#### **KOSZTY**

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

### **ARTYKUŁ 15**

#### **KONSULTACJE**

1. Właściwe organy Stron informują się wzajemnie o wszelkich zmianach w prawie swoich Państw dotyczącym ochrony informacji niejawnych, w zakresie niezbędnym do wykonywania postanowień niniejszej Umowy.
2. W celu zapewnienia ścisłej współpracy przy realizacji postanowień niniejszej Umowy właściwe organy Stron konsultują się, na wniosek jednego z tych organów.
3. Każda ze Stron zezwala przedstawicielom właściwego organu drugiej Strony na składanie wizyt na terytorium swojego Państwa, w celu omawiania procedur służących ochronie informacji niejawnych, które zostały jej przekazane przez drugą Stronę.
4. W celu zapewnienia skutecznej współpracy wynikającej z postanowień niniejszej Umowy, właściwe organy mogą, w razie potrzeby, zawierać pisemne szczegółowe uzgodnienia techniczne i organizacyjne w zakresie kompetencji przyznanych im prawem Państw swoich Stron.

**ARTYKUŁ 16**  
**ROZSTRZYGANIE SPORÓW**

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

**ARTYKUŁ 17**  
**ZMIANY**

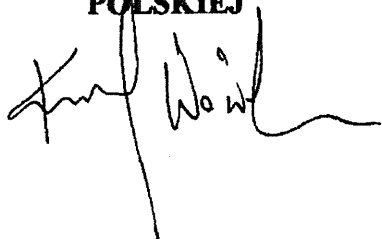
Na podstawie wspólnej zgody Stron zmiany do Umowy są nanoszone w formie odrębnego protokołu będącego jej integralną częścią i wejdą w życie zgodnie z procedurą określoną w artykule 18 niniejszej Umowy.

**ARTYKUŁ 18**  
**POSTANOWIENIA KOŃCOWE**

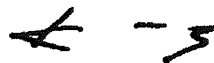
1. Niniejsza Umowa wejdzie w życie w pierwszym dniu drugiego miesiąca, który nastąpi po dacie otrzymania noty późniejszej przekazanej przez Strony drogą dyplomatyczną, potwierdzającej zakończenie przez nie niezbędnych procedur wewnętrznych.
2. Niniejsza Umowa zawarta jest na czas nieokreślony. W dowolnym czasie może być ona wypowiedziana przez każdą ze Stron w drodze notyfikacji. W takim przypadku utraci moc po upływie sześciu miesięcy od daty otrzymania noty informującej o wypowiedzeniu.
3. W przypadku wypowiedzenia niniejszej Umowy, informacje niejawne przekazane lub wytworzone na jej podstawie będą nadal chronione zgodnie z jej postanowieniami.

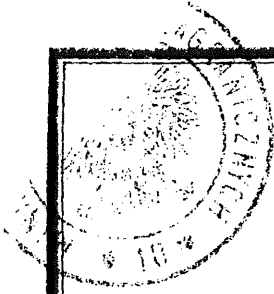
Sporządzono w Baku dnia 31 maja 2019 roku  
w dwóch jednobrzmiących egzemplarzach, każdy w językach polskim, azerskim  
i angielskim, przy czym wszystkie teksty posiadają jednakową moc.  
W przypadku rozbieżności przy ich interpretacji, za rozstrzygający uważa się  
tekst w języku angielskim.

**Z UPOWAŻNIENIA  
RZĄDU RZECZYPOSPOLITEJ  
POLSKIEJ**



**Z UPOWAŻNIENIA  
RZĄDU REPUBLIKI  
AZERBEJDŻANU**





## **AGREEMENT**

**between the Government of the Republic of Poland  
and  
the Government of the Republic of Azerbaijan  
on the exchange and mutual protection of Classified Information**

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

Having due regard for necessity of guaranteeing mutual protection of all information that has been classified in accordance with the legislation of the State of one of the Parties and transmitted to the other Party or has been originated during the course of cooperation,

Being guided by the intention to adopt regulations in the scope of the mutual protection of Classified Information, applicable to any joint activity relating to exchange of Classified Information,

Emphasizing the respect for universally recognized principles and norms of the international law and the legislation of the States of the Parties, guided by the principles of equality, reciprocity and mutual benefits,

Have agreed as follows:

**ARTICLE 1**  
**OBJECTIVE OF THE AGREEMENT**

1. The objective of this Agreement is to ensure the protection of Classified Information that is generated as a result of cooperation or exchanged between the Parties, individuals, legal entities or other establishments and organizations not depending on their organizational-legal form 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 establishments and organizations not depending on their-organizational-legal form under their jurisdiction as well as to any activities conducted between them.

**ARTICLE 2**  
**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 in accordance with the legislation of the State of the one of the Parties of this Agreement;
- 2) **Competent Authorities** – the authorities referred to in Article 4 of this Agreement;
- 3) **Originating Party** – the Party, as well as individual, legal entity or other establishment and organization not depending on its organizational-legal form competent to originate and transmit Classified Information in accordance with the legislation of the State of the Party;
- 4) **Recipient Party** – the Party, as well as individual, legal entity or other establishment and organization not depending on its organizational-legal form

competent to receive Classified Information in accordance with the legislation of the State of the Party;

5) **Classified Contract** – a contract which contains Classified Information or performance of which involves access to or originating of such information;

6) **Contractor** – an individual, a legal entity or other establishment and organization not depending on its organizational-legal form under the legislation of the State of one of the Parties, which has legal capacity to perform Classified Contracts;

7) **Principal** – an individual, a legal entity or other establishment and organization not depending on its organizational-legal form under the legislation of the State of one of the Parties, which has legal capacity to let Classified Contracts;

8) **Personnel Security Clearance** – a document issued in accordance with the legislation of the State of the 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 legislation of the State of the 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 individual, legal entity or other establishment and organization not depending on its organizational-legal form under its jurisdiction or an international organization not being the Party to this Agreement.

**ARTICLE 3**  
**SECURITY CLASSIFICATION LEVELS**

1. Classified Information is granted a security classification level in accordance to its content, pursuant to the legislation of the State 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 immediately notified in writing of every change or removal of security classification level of previously received Classified Information.
3. The Parties agree that the following security classification levels are equivalent:

<b>THE REPUBLIC OF POLAND</b>	<b>THE REPUBLIC OF AZERBAIJAN</b>	<b>EQUIVALENT IN ENGLISH</b>
<b>TAJNE</b>	<b>TAM MƏXFİ</b>	<b>SECRET</b>
<b>POUFNE</b>	<b>MƏXFİ</b>	<b>CONFIDENTIAL</b>
<b>ZASTRZEŻONE</b>	<b>(NO EQUIVALENT)</b>	<b>RESTRICTED</b>

4. Information received from the Republic of Poland classified as ZASTRZEŻONE shall be protected as MƏXFİ in the Republic of Azerbaijan.
5. In the event that information classified as ŚCIŚLE TAJNE/ XÜSUSİ ƏHƏMİYYƏTLİ / TOP SECRET needs to be exchanged, separate provisions shall be agreed between the Parties.

**ARTICLE 4**  
**COMPETENT AUTHORITIES**

1. For the purpose of this Agreement, the Competent Authorities shall be:

- 1) for the Government of the Republic of Poland: the Head of the Internal Security Agency;
- 2) for the Government of the Republic of Azerbaijan: State Security Service.

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

**ARTICLE 5**  
**PRINCIPLES OF CLASSIFIED INFORMATION PROTECTION**

1. The Parties shall adopt every measure provided in this Agreement and subject to the legislation of their States 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 purposes for which it has been exchanged.

3. Access to Classified Information shall be granted only to those individuals who have a need-to-know and who have been authorized to access such information in accordance with the legislation of the State of the Recipient Party.

4. 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.

**ARTICLE 6**  
**SECURITY CLEARANCES**

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

**ARTICLE 7**  
**CLASSIFIED CONTRACTS**

1. Before concluding a Classified Contract connected with the access to information classified as POUFNE/ MØXFÍ/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 legislation of the State of the Party in the territory of which it is located.
3. Classified Information shall not be released to the Contractor until the receipt of the 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. That 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 8**

#### **TRANSMISSION OF CLASSIFIED INFORMATION**

1. Classified Information shall be transmitted via diplomatic channels.
2. Information classified as ZASTRZEŻONE/RESTRICTED and POUFNE/ MƏXFİ /CONFIDENTAL may be transmitted also through authorized couriers in accordance with the legislation of the State 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 legislation of the State of the Originating Party are met, the personal carriage of information classified as ZASTRZEŻONE/RESTRICTED and POUFNE/ MƏXFİ /CONFIDENTAL by authorized individuals is admissible.
4. The Competent Authorities of the Parties may agree on other forms of transmitting Classified Information which ensure its protection against unauthorized disclosure.
5. The Recipient 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 9**  
**REPRODUCTION OR TRANSLATION OF CLASSIFIED**  
**INFORMATION**

1. Reproduction or translation of Classified Information shall be conducted in accordance with the legislation of the State of the Recipient Party and the following principles:

- 1) individuals who translate or make copies of Classified Information shall hold Personnel Security Clearances relevant to the security classification level of the translated or reproduced Classified Information;
- 2) reproduced or translated information shall be placed under the same protection as the original information;
- 3) the number of copies or translations shall be reduced to that required for official purposes;
- 4) translated information shall all bear an appropriate note in the language into which it is translated that the translation contains Classified Information of the Originating Party.

**ARTICLE 10**  
**DESTRUCTION OF CLASSIFIED INFORMATION**

1. Classified Information shall be destroyed in accordance with the legislation of the State of the Recipient Party in such a manner as to eliminate its partial or total reconstruction.

2. Records of destruction of documents containing Classified Information along with the English translations of the records shall be provided for the Competent Authority of the Recipient Party upon its request.

## **ARTICLE 11**

### **VISITS**

1. Persons arriving on a visit in the territory of the State 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;
  - 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;
- as well as the date, signature and official seal of the Competent Authority of the visiting Party.

4. In order to protect personal data referred to in Paragraph 3, transmitted in connection with the provisions of Paragraphs 1 and 5 the following provisions shall apply, subject to the legislation of the States 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 legislation of the State 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 Party transmitting personal data and the hosting Party shall be obliged to register its transmission, receipt and removal;
- 6) the Party transmitting personal data and the hosting Party shall be obliged to protect processed personal data efficiently against its disclosure to unauthorized persons, unauthorized modifications of the data, its loss, damage or destruction.

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

## **ARTICLE 12**

### **BREACH OF SECURITY**

1. Breach of security is an action or an omission which is contrary to this Agreement or the legislation of the States of the Parties concerning Classified Information protection, including unauthorized disclosure of Classified Information.

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 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 legislation of the State of the Party in the territory of which it has occurred.

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

5. Should a breach of security occur in the territory of a Third Party, 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 of the Parties shall cooperate in the actions referred to in Paragraph 3, upon the request of one of them.

### **ARTICLE 13 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 14 EXPENSES**

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

**ARTICLE 15**  
**CONSULTATIONS**

1. The Competent Authorities of the Parties shall notify each other of any amendments to the legislation of their States 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 its State territory to discuss the procedures for the protection of Classified Information transmitted by the other Party.

4. In order to ensure effective cooperation resulting from the provisions of this Agreement, and in the scope of authority acknowledged by the legislation of the States of the Parties, the Competent Authorities may, if necessary, conclude written detailed technical or organizational arrangements.

**ARTICLE 16**  
**SETTLEMENT OF DISPUTES**

1. Any disputes concerning the interpretation and implementation of this Agreement shall be settled by direct consultations between the Competent Authorities of the Parties.

2. If settlement of a dispute cannot be reached in the manner referred to in Paragraph 1, such a dispute shall be settled between the Parties through diplomatic channels.

**ARTICLE 17**  
**AMENDMENTS**

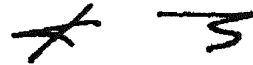
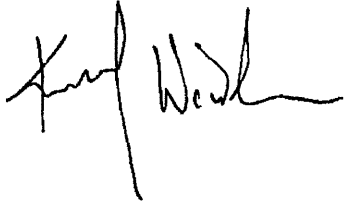
By mutual consent of the Parties amendments may be made to this Agreement in the form of separate Protocols being an integral part of thereof and entering into force in accordance with the procedure set forth in Article 18 of this Agreement.

**ARTICLE 18**  
**FINAL PROVISIONS**

1. This Agreement shall enter into force on the first day of the second month following the date of receipt by the Parties of the last written notification through diplomatic channels confirming the completion of their respective internal procedures required for the entry into force of this Agreement.
2. 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 at any time. In such case, this Agreement shall expire after six months following the date of receipt of the termination notice through diplomatic channels.
3. In case of termination of this Agreement, Classified Information exchanged or originated on its basis shall be protected in accordance with the provisions thereof.

Done at Baku on 31<sup>st</sup> of May 2019 in two original copies, each in the Polish, Azerbaijani and English languages, all texts being equally authentic. In case of divergences of interpretation, the English text shall prevail.

**FOR** **FOR**  
**THE GOVERNMENT OF** **THE GOVERNMENT OF**  
**THE REPUBLIC OF POLAND** **THE REPUBLIC OF AZERBAIJAN**





Warszawa, 20 lipca 2019 r.

Minister  
Spraw Zagranicznych

DPUE.920.1379.2014/bc/10

dot.: P-9647/2019/14/JS z 11.07.2019 r.

**Pan Piotr Pogonowski**  
**Szef Agencji Bezpieczeństwa Wewnętrznego**

**Opinia**


**o zgodności z prawem Unii Europejskiej umowy między Rządem Rzeczypospolitej Polskiej a Rządem Republiki Azerbejdżanu o wymianie i wzajemnej ochronie informacji niejawnych, wyrażona przez ministra właściwego do spraw członkostwa Rzeczypospolitej Polskiej w Unii Europejskiej**

*Szanowny Panie Ministrze,*

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  
**Piotr Wierzyk**  
Podsekretarz Stanu