Warszawa, dnia 12 listopada 2025 r.

Poz. 1538

UMOWA

między Rządem Rzeczypospolitej Polskiej a Rządem Stanów Zjednoczonych Ameryki w sprawie środków bezpieczeństwa służących ochronie informacji niejawnych,

podpisana w Warszawie dnia 16 kwietnia 2025 r.

W imieniu Rzeczypospolitej Polskiej

PREZYDENT RZECZYPOSPOLITEJ POLSKIEJ

podaje do powszechnej wiadomości:

Dnia 16 kwietnia 2025 roku w Warszawie została podpisana Umowa między Rządem Rzeczypospolitej Polskiej a Rządem Stanów Zjednoczonych Ameryki w sprawie środków bezpieczeństwa służących ochronie informacji niejawnych, w następującym brzmieniu:

UMOWA MIĘDZY RZĄDEM RZECZYPOSPOLITEJ POLSKIEJ A RZĄDEM STANÓW ZJEDNOCZONYCH AMERYKI W SPRAWIE ŚRODKÓW BEZPIECZEŃSTWA SŁUŻĄCYCH OCHRONIE INFORMACJI NIEJAWNYCH

PREAMBUŁA

Rząd Rzeczypospolitej Polskiej („Rzeczpospolita Polska") oraz Rząd Stanów Zjednoczonych Ameryki („Stany Zjednoczone") (każdy z nich zwany dalej „Stroną" oraz łącznie „Stronami"),

Mając na uwadze współdziałanie Stron, w szczególności w zakresie spraw zagranicznych, obrony, bezpieczeństwa, ochrony porządku publicznego, nauki, przemysłu i technologii, oraz

Kierując się wspólnym interesem Stron w zakresie ochrony informacji niejawnych wymienianych w poufności między Stronami,

Uzgodniły, co następuje:

ARTYKUŁ 1
DEFINICJE

W rozumieniu niniejszej Umowy:

1) informacje niejawne: informacje przekazywane przez jedną ze Stron drugiej Stronie, oznaczone przez Stronę udostępniającą klauzulą tajności z uwagi na względy bezpieczeństwa narodowego i wymagające ochrony przed nieuprawnionym ujawnieniem. Informacje te mogą mieć formę przekazu ustnego, wizualnego, elektronicznego lub dokumentu, lub też formę materiału, w tym sprzętu lub technologii;
2) kontrakt niejawny: umowa, której realizacja wiąże się lub będzie wiązała się z dostępem do lub wytwarzaniem informacji niejawnych przez kontrahenta;
3) kontrahent: osoba fizyczna lub inny podmiot będący jedną ze stron kontraktu niejawnego i posiadający zdolność do zawierania umów;
4) świadectwo bezpieczeństwa przemysłowego: zapewnienie udzielone przez wskazaną w artykule 4 krajową władzę bezpieczeństwa jednej ze Stron wobec kontrahenta znajdującego się pod jej jurysdykcją, stwierdzające, że kontrahent został odpowiednio sprawdzony i, jeśli ma to zastosowanie, posiada również odpowiednie środki bezpieczeństwa fizycznego do ochrony informacji niejawnych do określonej klauzuli tajności. Zapewnienie takie oznacza, że kontrahent, wobec którego je udzielono, chroni informacje niejawne o klauzuli POUFNE / CONFIDENTIAL lub wyższej zgodnie z postanowieniami niniejszej Umowy, a nadzór nad ich stosowaniem sprawuje właściwa krajowa władza bezpieczeństwa;
5) poświadczenie bezpieczeństwa: zapewnienie udzielone przez wskazaną w artykule 4 krajową władzę bezpieczeństwa jednej ze Stron, że osoba będąca jej obywatelem lub zatrudniona przez kontrahenta podlegającego jej jurysdykcji lub osoba, która jest obywatelem jednej ze Stron i ma zostać zatrudniona przez drugą Stronę lub jednego z kontrahentów drugiej Strony, jest uprawniona do dostępu do informacji niejawnych do określonej klauzuli tajności;

6) zasada ograniczonego dostępu: zasada, zgodnie z którą uprawniony dysponent informacji niejawnych stwierdza, że zadania lub obowiązki służbowe potencjalnego odbiorcy wymagają dostępu do, zapoznania się z lub posiadania informacji niejawnych.

ARTYKUŁ 2
OGRANICZENIA W ZAKRESIE OBOWIĄZYWANIA UMOWY

Celem niniejszej Umowy jest zapewnienie ochrony informacjom niejawnym wytwarzanym lub wymienianym przez Strony, chyba że wskazano inaczej w niniejszym artykule. Niniejszej Umowy nie stosuje się do informacji niejawnych określonych w postanowieniach innych umów lub porozumień między Stronami lub organami, zawartych w celu ochrony konkretnego przedmiotu lub kategorii informacji niejawnych wymienianych między Stronami lub organami, z wyjątkiem przypadków, w których takie umowy lub porozumienia wyraźnie wskazują, że postanowienia niniejszej Umowy mają zastosowanie. Niniejszej Umowy nie stosuje się do wymiany informacji chronionych, o których mowa w obowiązującej w Stanach Zjednoczonych ustawie o energii atomowej (dalej zwaną „ustawą AEA") z 1954 roku, z późniejszymi zmianami, oraz do informacji uprzednio sklasyfikowanych jako chronione, które zostały wyodrębnione ze zbioru informacji chronionych zgodnie z ustawą AEA, ale pozostają związane ze sferą obronności Stanów Zjednoczonych.

ARTYKUŁ 3
ZOBOWIĄZANIE DO OCHRONY INFORMACJI NIEJAWNYCH

1. Każda ze Stron chroni informacje niejawne drugiej Strony zgodnie z postanowieniami określonymi w niniejszej Umowie.

2. Strona otrzymująca zapewnia informacjom niejawnym co najmniej taką samą ochronę, jaka obowiązuje w stosunku do informacji niejawnych Strony udostępniającej.
3. Każda ze Stron niezwłocznie powiadamia drugą Stronę o wszelkich zmianach w swoim prawie krajowym mających wpływ na ochronę informacji niejawnych wymienianych na podstawie niniejszej Umowy. Zmiany w prawie krajowym nie wpływają na zobowiązania wynikające z niniejszej Umowy. W przypadku ich wystąpienia, Strony konsultują się w celu rozważenia wprowadzenia ewentualnych zmian do niniejszej Umowy lub zastosowania innych odpowiednich środków do utrzymania ochrony informacji niejawnych wymienianych na podstawie niniejszej Umowy.

ARTYKUŁ 4
KRAJOWE WŁADZE BEZPIECZEŃSTWA

1. Krajowymi władzami bezpieczeństwa w rozumieniu niniejszej Umowy są:
   a. w Rzeczypospolitej Polskiej: Szef Agencji Bezpieczeństwa Wewnętrznego;
   b. w Stanach Zjednoczonych: Zastępca Dyrektora Zarządu do spraw Międzynarodowych, Agencja do spraw Bezpieczeństwa Technologii Zbrojeniowych, Biuro Podsekretarza Obrony do spraw Polityki Departamentu Obrony Stanów Zjednoczonych Ameryki.
2. Strony informują się w drodze dyplomatycznej o wszelkich zmianach organów, o których mowa w ustępie 1 niniejszego artykułu.
3. Strony mogą zawierać uzupełniające porozumienia wykonawcze do niniejszej Umowy w przypadku konieczności zastosowania dodatkowych technicznych środków bezpieczeństwa do ochrony informacji niejawnych.

ARTYKUŁ 5
OZNACZANIE INFORMACJI NIEJAWNYCH

1. Informacjom niejawnym nadaje się klauzulę tajności i jeśli to możliwe oznacza je, jedną z następujących krajowych klauzul tajności oraz nazwą Strony udostępniającej. W celu zapewnienia odpowiedniego postępowania z informacjami niejawnymi, Strony uzgadniają, że niżej wymienione klauzule tajności są równorzędne:

RZECZPOSPOLITA POLSKA	**STANY ZJEDNOCZONE AMERYKI**
ŚCIŚLE TAJNE	TOP SECRET
TAJNE	SECRET
POUFNE	CONFIDENTIAL
ZASTRZEŻONE	BRAK ODPOWIEDNIKA

2. W ramach realizacji niniejszej Umowy, informacje niejawne oznaczone klauzulą ZASTRZEŻONE przekazywane przez Rzeczpospolitą Polską są przetwarzane przez Stany Zjednoczone zgodnie z załącznikiem do niniejszej Umowy.

ARTYKUŁ 6
ODPOWIEDZIALNOŚĆ ZA INFORMACJE NIEJAWNE

Strona otrzymująca jest odpowiedzialna za ochronę wszelkich informacji niejawnych Strony udostępniającej, co najmniej na takim poziomie, jaki zapewnia im Strona udostępniająca, kiedy są pod jej kontrolą. W trakcie przewozu, Strona

udostępniająca jest odpowiedzialna za wszystkie przekazywane informacje niejawne do chwili ich odbioru potwierdzonego przez Stronę otrzymującą.

ARTYKUŁ 7
OCHRONA INFORMACJI NIEJAWNYCH

1. W zakresie niniejszej Umowy, Strony mogą uznać świadectwa bezpieczeństwa przemysłowego i poświadczenia bezpieczeństwa wydane zgodnie z prawem krajowym drugiej Strony.
2. Informacji niejawnych nie udostępnia się jedynie na podstawie posiadanego stopnia, pełnionej funkcji, stanowiska lub poświadczenia bezpieczeństwa. Dostęp do informacji niejawnych przyznaje się wyłącznie osobom, wobec których stosuje się zasadę ograniczonego dostępu, którym wydano poświadczenie bezpieczeństwa oraz które zostały upoważnione do dostępu zgodnie z zasadami określonymi przez Stronę otrzymującą.
3. O ile niniejsza Umowa nie stanowi inaczej, Strona otrzymująca nie udostępni informacji niejawnych jakiejkolwiek stronie trzeciej, w tym jej rządowi, osobie, organizacji czy innemu podmiotowi bez uprzedniej pisemnej zgody Strony udostępniającej.
4. Strona otrzymująca nie wykorzysta informacji niejawnych, ani nie zezwoli na ich wykorzystanie w innym celu, niż ten, w jakim zostały one przekazane bez uprzedniej pisemnej zgody Strony udostępniającej.
5. Strona otrzymująca uznaje prawa osobiste związane z informacjami niejawnymi Strony udostępniającej, w tym te, które odnoszą się do patentów, praw autorskich, tajemnic przedsiębiorstwa. Udostępnianie, wykorzystanie lub przekazanie takich informacji niejawnych w sposób niezgodny z prawami osobistymi wymaga uprzedniego pisemnego upoważnienia ich właściciela.

6. Strona otrzymująca zapewnia, że każdy podmiot, w którym w ramach niniejszej Umowy przetwarzane są informacje niejawne, prowadzi wykaz osób upoważnionych do dostępu do takich informacji.
7. Każda ze Stron opracuje procedury mające na celu zapewnienie rozliczalności informacji niejawnych oraz kontrolę nad ich dostępem oraz obiegiem.
8. Każda ze Stron zobowiązuje się przestrzegać wszelkich ograniczeń dotyczących wykorzystania, przekazania lub dostępu do informacji niejawnych w przypadku ich określenia przez Stronę udostępniającą w momencie przekazania. Gdy jedna ze Stron nie jest w stanie spełnić wskazanych wymogów w tym względzie, niezwłocznie powiadamia o tym drugą Stronę i podejmuje wszelkie przewidziane prawem środki mające na celu zapobieżenie lub ograniczenie wykorzystania, przekazania lub dostępu do takich informacji niejawnych.

ARTYKUŁ 8
POŚWIADCZENIA BEZPIECZEŃSTWA

1. Strony zapewniają, że wszystkie osoby, które w ramach wykonywania swoich zadań służbowych lub pełnionej funkcji wymagają dostępu do informacji niejawnych zgodnie z niniejszą Umową, otrzymają odpowiednie poświadczenie bezpieczeństwa przed uzyskaniem do nich dostępu.
2. Strona wydająca poświadczenie bezpieczeństwa stwierdza, zgodnie ze swoim prawem krajowym, że osoba daje rękojmię zachowania tajemnicy.
3. Zanim uprawniony przedstawiciel jednej ze Stron udostępni informacje niejawne uprawnionemu przedstawicielowi drugiej Strony, Strona otrzymująca udzieli Stronie przekazującej zapewnienia, że dany przedstawiciel posiada niezbędne poświadczenie bezpieczeństwa, wymaga dostępu do informacji niejawnych zgodnie z zasadą ograniczonego dostępu

oraz że informacje niejawne będą chronione przez Stronę otrzymującą zgodnie z niniejszą Umową.

ARTYKUŁ 9
UDOSTĘPNIANIE INFORMACJI NIEJAWNYCH KONTRAHENTOM

Przekazanie przez Stronę otrzymującą informacji niejawnych kontrahentowi lub potencjalnemu kontrahentowi, którego zadania wiążą się z dostępem do takich informacji, wymaga uprzedniej pisemnej zgody Strony udostępniającej. Przed udostępnieniem jakichkolwiek informacji niejawnych kontrahentowi lub potencjalnemu kontrahentowi, Strona otrzymująca:

a. zapewni, że kontrahent lub potencjalny kontrahent oraz – o ile ma to zastosowanie – użytkowane przez niego obiekty, posiadają zdolność do ochrony takich informacji, zgodnie z postanowieniami niniejszej Umowy;
b. zapewni, że kontrahent lub potencjalny kontrahent oraz użytkowane przez niego obiekty – o ile ma to zastosowanie – posiadają odpowiednie poświadczenia bezpieczeństwa lub świadectwa bezpieczeństwa przemysłowego;
c. zapewni, że kontrahent lub potencjalny kontrahent stosuje procedury gwarantujące, że wszystkie osoby mające dostęp do takich informacji są informowane o odpowiedzialności za ich ochronę zgodnie z właściwym prawem krajowym;
d. przeprowadzi okresowe inspekcje obiektów w celu zapewnienia, że takie informacje są chronione zgodnie z niniejszą Umową; oraz
e. zapewni, że kontrahent lub potencjalny kontrahent stosuje procedury gwarantujące, że dostęp do takich informacji jest przyznawany zgodnie z zasadą ograniczonego dostępu.

ARTYKUŁ 10
KONTRAKTY NIEJAWNE

1. W przypadku gdy jedna ze Stron zleci lub upoważni kontrahenta ze swojego Państwa do zlecenia kontraktu niejawnego o klauzuli POUFNE / CONFIDENTIAL lub wyższej kontrahentowi z Państwa drugiej Strony, Strona, która zleci lub upoważni kontrahenta do zlecenia takiego kontraktu występuje do krajowej władzy bezpieczeństwa drugiej Strony z wnioskiem o zapewnienie, że potencjalny kontrahent posiada świadectwo bezpieczeństwa przemysłowego wydane zgodnie z jej prawem krajowym. Krajowa władza bezpieczeństwa Strony, do której skierowano wniosek, prowadzi nadzór i podejmuje odpowiednie działania w celu zapewnienia, że kontrahent spełnia wymagania bezpieczeństwa zgodnie ze swoim prawem krajowym.
2. Strona lub jej upoważniony przedstawiciel negocjujący kontrakt niejawny, który ma być realizowany w Państwie drugiej Strony, zamieszcza w treści tego kontraktu, zapytania ofertowego lub umowy podwykonawczej odpowiednią instrukcję bezpieczeństwa przemysłowego oraz inne istotne postanowienia, w tym te dotyczące kosztów zapewnienia ochrony oraz obligujące wszystkich kontrahentów do uwzględniania w dokumentacji podwykonawczej analogicznych instrukcji bezpieczeństwa.

ARTYKUŁ 11
ODPOWIEDZIALNOŚĆ ZA BEZPIECZEŃSTWO OBIEKTÓW

Każda Strona odpowiada za bezpieczeństwo wszystkich obiektów rządowych i prywatnych, w których przechowuje informacje niejawne drugiej Strony oraz zapewnia, że każdy taki obiekt posiada wykwalifikowane i odpowiednio sprawdzone osoby, które wyznaczono i upoważniono do kontroli oraz ochrony takich informacji niejawnych.

ARTYKUŁ 12
PRZECHOWYWANIE INFORMACJI NIEJAWNYCH

Informacje niejawne wymieniane między Stronami są przechowywane w taki sposób, aby dostęp do nich miały wyłącznie osoby będące do tego upoważnione, zgodnie z artykułem 7 ustęp 2.

ARTYKUŁ 13
PRZEKAZYWANIE

1. Informacje niejawne są przekazywane między Stronami drogą rządową lub w inny sposób uprzednio uzgodniony pisemnie przez właściwe krajowe władze bezpieczeństwa Stron.
2. Minimalne wymagania dotyczące bezpieczeństwa informacji niejawnych podczas przekazywania przedstawiają się następująco:

   a. Dokumenty lub inne nośniki:

1) dokumenty lub inne nośniki zawierające informacje niejawne są przekazywane w podwójnych zapieczętowanych kopertach. Na kopercie wewnętrznej umieszcza się jedynie klauzulę tajności, którą oznaczono dokumenty lub inne nośniki oraz służbowy adres właściwego odbiorcy.

   Na kopercie zewnętrznej umieszcza się służbowy adres właściwego odbiorcy, służbowy adres nadawcy oraz numer, za którym przekazywany jest dany dokument w przypadku, kiedy ma to zastosowanie;

2) na kopercie zewnętrznej nie umieszcza się informacji o klauzuli tajności załączonych dokumentów lub innych nośników. Podwójna zapieczętowana koperta jest przekazywana zgodnie z obowiązującymi Strony procedurami;

3) w przypadku przesyłek przekazywanych między Stronami, zawierających dokumenty lub inne nośniki z informacjami niejawnymi, przygotowuje się ich potwierdzenia odbioru, które docelowy odbiorca podpisuje i przekazuje nadawcy.

b. Materiały:

1) materiały, w tym sprzęt, objęte klauzulą tajności przewozi się w zaplombowanych, zakrytych pojazdach oraz szczelnie pakuje i zabezpiecza w celu uniemożliwienia identyfikacji ich kształtu, rozmiaru lub zawartości i utrzymuje pod stałą kontrolą w celu uniemożliwienia dostępu osobom nieupoważnionym;

2) materiały, w tym sprzęt, objęte klauzulą tajności, które muszą być tymczasowo przechowywane w oczekiwaniu na wysłanie, umieszcza się w miejscach objętych ochroną. Miejsca te są chronione za pomocą urządzeń antywłamaniowych lub pracowników ochrony posiadających wymagane poświadczenia bezpieczeństwa i prowadzących stały nadzór. Dostęp do takich miejsc posiada wyłącznie upoważniony personel;

3) w przypadku, kiedy podczas transportu zmieniają się osoby odpowiedzialne za materiały, w tym sprzęt, objęte klauzulą tajności, należy każdorazowo wystawić potwierdzenie, które jest podpisywane przez docelowego odbiorcę i przekazywane nadawcy.

c. Przekazywanie drogą elektroniczną:

1) informacje niejawne o klauzuli POUFNE / CONFIDENTIAL lub wyższej przeznaczone do wysłania drogą elektroniczną, przesyła się za pośrednictwem bezpiecznych środków zatwierdzonych do użytku przez krajową władzę bezpieczeństwa każdej ze Stron.

ARTYKUŁ 14
WIZYTY W OBIEKTACH STRON

1. Wizyty przedstawicieli jednej Strony w obiektach należących do drugiej Strony, w których wymagany jest dostęp do informacji niejawnych, lub do których warunkiem wstępu jest posiadanie poświadczenia bezpieczeństwa, odbywają się wyłącznie w celach służbowych. Zgodę na taką wizytę udziela się wyłącznie przedstawicielom, którzy posiadają ważne poświadczenie bezpieczeństwa.

2. Zgodę na złożenie wizyty w takich obiektach wydaje wyłącznie Strona, na terytorium której znajduje się ten obiekt. Strona przyjmująca lub jej wyznaczeni przedstawiciele odpowiadają za przekazanie odwiedzanej jednostce informacji o proponowanej wizycie, jej zakresie oraz najwyższej klauzuli tajności informacji niejawnych, do jakich może mieć dostęp osoba przybywająca z wizytą.
3. Wnioski o wizyty przedstawicieli Stron są przekazywane przez Ambasadę Stanów Zjednoczonych w Warszawie w przypadku osób przybywających z wizytą ze Stanów Zjednoczonych oraz Ambasadę Rzeczypospolitej Polskiej w Waszyngtonie D.C. w przypadku osób przybywających z wizytą z Rzeczypospolitej Polskiej.

ARTYKUŁ 15
INSPEKCJE BEZPIECZEŃSTWA

Realizacja określonych w niniejszej Umowie wymogów bezpieczeństwa może być weryfikowana poprzez obustronne wizyty przedstawicieli krajowych władz bezpieczeństwa Stron, którzy po wcześniejszych konsultacjach otrzymają zgodę na złożenie wizyty drugiej Stronie w celu omówienia procedur oraz wglądu w ich realizację przez drugą Stronę, co pozwoli na uzyskanie porównywalnych systemów bezpieczeństwa. Strona przyjmująca pomaga przedstawicielom krajowej władzy bezpieczeństwa drugiej Strony w ustaleniu, czy informacje niejawne przekazywane przez drugą Stronę są właściwie chronione.

ARTYKUŁ 16
STANDARDY BEZPIECZEŃSTWA

Na wniosek, każda ze Stron przekaże drugiej Stronie informacje na temat swoich standardów bezpieczeństwa, sposobów postępowania oraz procedur związanych z ochroną informacji niejawnych.

ARTYKUŁ 17
POWIELANIE I TŁUMACZENIE INFORMACJI NIEJAWNYCH

W przypadku powielania lub tłumaczenia informacji niejawnych, wszystkie znajdujące się na nich oryginalne klauzule tajności są również powielane bądź umieszczane na każdej ich kopii. Kopie i tłumaczenia informacji niejawnych podlegają takiej samej ochronie, jak oryginalne informacje. Liczba kopii lub tłumaczeń jest ograniczona do niezbędnego minimum wymaganego do celów służbowych.

ARTYKUŁ 18
NISZCZENIE INFORMACJI NIEJAWNYCH

Informacje niejawne oraz materiały je zawierające są niszczone za pomocą środków, które uniemożliwiają ich odczytanie oraz wykluczają odtworzenie.

ARTYKUŁ 19
OBNIŻENIE LUB ZNIESIENIE KLAUZUL TAJNOŚCI

1. Strony zgadzają się, że z chwilą, gdy informacje niejawne nie wymagają określonego stopnia ochrony, należy obniżyć ich klauzulę lub znieść ją w przypadku ustania dalszej potrzeby ich ochrony przed nieuprawnionym ujawnieniem.
2. Strona udostępniająca ma pełną swobodę w zakresie obniżania lub znoszenia klauzul tajności swoich informacji niejawnych. Strona otrzymująca nie obniży, ani nie zniesie klauzuli tajności nadanej informacjom niejawnym przez Stronę udostępniającą bez jej uprzedniej pisemnej zgody, niezależnie od widniejących w tym względzie adnotacji na dokumencie.

ARTYKUŁ 20
UTRATA LUB NARAŻENIE NA SZWANK

Strona otrzymująca informuje niezwłocznie Stronę udostępniającą o utracie lub narażeniu na szwank, a także o domniemaniu utraty lub narażenia na szwank informacji niejawnych Strony przekazującej. W przypadku zaistnienia bądź domniemania utraty lub narażenia informacji niejawnych na szwank, Strona otrzymująca niezwłocznie wszczyna postępowanie wyjaśniające w celu ustalenia okoliczności zdarzenia. Wyniki postępowania wraz z informacją na temat środków podjętych w celu uniknięcia podobnego zdarzenia w przyszłości są przekazywane Stronie udostępniającej.

ARTYKUŁ 21
SPORY

Kwestie sporne między Stronami wynikające z niniejszej Umowy lub z nią związane będą rozstrzygane wyłącznie w drodze konsultacji między Stronami i nie będą przedkładane do rozstrzygnięcia sądom krajowym, międzynarodowym trybunałom czy innym osobom lub podmiotom.

ARTYKUŁ 22
KOSZTY

Każda ze Stron pokrywa koszty własne ponoszone w związku z realizacją niniejszej Umowy. Wszystkie zobowiązania Stron wynikające z niniejszej Umowy są uzależnione od dostępności środków finansowych.

ARTYKUŁ 23
POSTANOWIENIA KOŃCOWE

1. Umowa niniejsza wejdzie w życie zgodnie z prawem krajowym każdej ze Stron z datą późniejszej z pisemnych not przekazanych w drodze dyplomatycznej, w których Strony wzajemnie się informują, że każda z nich zakończyła procedury wewnętrzne niezbędne do wejścia w życie niniejszej Umowy.
2. Umowa niniejsza może zostać zmieniona na podstawie pisemnej zgody obu Stron.
3. Każda ze Stron może wypowiedzieć niniejszą Umowę w drodze pisemnej notyfikacji drogą dyplomatyczną zachowując dziewięćdziesięciodniowy termin jej wypowiedzenia.
4. Bez względu na wypowiedzenie niniejszej Umowy, wszystkie informacje niejawne wymienione lub przekazane na jej podstawie będą nadal chronione zgodnie z jej postanowieniami.
5. Z chwilą wejścia w życie niniejszej Umowy, traci moc Umowa między Rządem Rzeczypospolitej Polskiej a Rządem Stanów Zjednoczonych Ameryki w sprawie środków bezpieczeństwa służących ochronie informacji niejawnych w sferze wojskowej (Umowa o Bezpieczeństwie Informacji), podpisana w Warszawie dnia 8 marca 2007 roku.
6. Jakiekolwiek odniesienie do Umowy o Bezpieczeństwie Informacji w innych umowach lub porozumieniach zawartych między Stronami uznaje się za odniesienie do niniejszej Umowy.

Na dowód czego niżej podpisani, należycie do tego upoważnieni przez swoje Rządy, podpisali niniejszą Umowę.

SPORZĄDZONO w dwóch egzemplarzach w WARSZAWIE dnia 16 KWIETNIA 2025, w językach polskim i angielskim, przy czym obydwa teksty są jednakowo autentyczne.

Z UPOWAŻNIENIA
RZĄDU RZECZYPOSPOLITEJ
POLSKI

Z UPOWAŻNIENIA
RZĄDU STANÓW
ZJEDNOCZONYCH AMERYKI

ZAŁĄCZNIK

PROCEDURY DOTYCZĄCE OCHRONY POLSKICH INFORMACJI NIEJAWNYCH OZNACZONYCH KLAUZULĄ ZASTRZEŻONE W STANACH ZJEDNOCZONYCH

Polskie informacje niejawne oznaczone klauzulą ZASTRZEŻONE otrzymane przez Stany Zjednoczone są chronione zgodnie z następującymi procedurami:

1. Informacje o klauzuli ZASTRZEŻONE przechowuje się w sposób, który chroni przed nieuprawnionym dostępem, w zamkniętych szafach lub wydzielonych strefach, które uniemożliwiają dostęp osobom nieuprawnionym.
2. Dostęp do informacji o klauzuli ZASTRZEŻONE ograniczony jest do osób, które są obywatelami Stanów Zjednoczonych, zostały przeszkolone w zakresie ochrony tych informacji i których zadania służbowe wymagają zapoznania się z nimi, zgodnie z zasadą ograniczonego dostępu. Poświadczenie bezpieczeństwa nie jest wymagane w przypadku dostępu do informacji niejawnych o klauzuli ZASTRZEŻONE.
3. Nie udostępnia się informacji o klauzuli ZASTRZEŻONE osobom lub podmiotom do tego nieuprawnionym bez uprzedniej pisemnej zgody Strony udostępniającej za wyjątkiem przypadków określonych amerykańskim prawem, w tym ustawy o dostępie do informacji publicznej. Rzeczpospolita Polska nie udostępnia informacji o klauzuli ZASTRZEŻONE publicznie i może przekazać informacje o klauzuli ZASTRZEŻONE Stanom Zjednoczonym pod warunkiem, że nie zostaną one udostępnione publicznie. W przypadku gdy do agencji lub jednostki administracji rządowej Stanów Zjednoczonych wpłynie wniosek o udostępnienie informacji na podstawie ustawy o dostępie do informacji publicznej dotyczący informacji o klauzuli ZASTRZEŻONE, Stany Zjednoczone wykorzystają wszelkie dostępne środki prawne, aby zapobiec publicznemu udostępnieniu informacji o klauzuli ZASTRZEŻONE.

4. Informacje o klauzuli ZASTRZEŻONE, o ile ma to zastosowanie, są przechowywane, przetwarzane lub przesyłane drogą elektroniczną za pomocą akredytowanych systemów organu rządowego lub kontrahenta. W szczególności, przed wykorzystaniem jakiegokolwiek systemu do przechowywania, przetwarzania lub przesyłania informacji o klauzuli ZASTRZEŻONE, musi on zostać zatwierdzony pod względem bezpieczeństwa, czyli uzyskać akredytację bezpieczeństwa teleinformatycznego. Akredytacja bezpieczeństwa teleinformatycznego to formalne dopuszczenie systemu do użytkowania przez właściwy organ akredytujący, potwierdzające, że system spełnia odpowiednie wymogi bezpieczeństwa, a korzystanie z niego nie stanowi niedopuszczalnego ryzyka. Procedury bezpiecznej eksploatacji to techniczne procedury wdrażania polityki i wymogów bezpieczeństwa, charakterystyczne dla konkretnej jednostki, w celu ochrony systemów teleinformatycznych, w których przetwarzane są informacje niejawne. W przypadku wydzielonych systemów teleinformatycznych, takich jak komputery stacjonarne i przenośne, używanych w obiektach rządowych Stanów Zjednoczonych, procedury bezpiecznej eksploatacji i dokumenty rejestracyjne systemu spełniają rolę wymaganej akredytacji bezpieczeństwa teleinformatycznego. W przypadku kontrahentów wytyczne dotyczące wykorzystania systemów teleinformatycznych zamieszcza się w stosownej instrukcji bezpieczeństwa przemysłowego kontraktu.

5. Przekazywanie informacji o klauzuli ZASTRZEŻONE odbywa się w drodze dyplomatycznej, za pośrednictwem kurierów wojskowych, listem poleconym lub osobiście. Informacje o klauzuli ZASTRZEŻONE przesyłane listem poleconym na terenie Stanów Zjednoczonych i poza nimi umieszczane są w podwójnych, zapieczętowanych kopertach, przy czym koperta wewnętrzna oznaczona jest polską klauzulą ZASTRZEŻONE. Na kopercie zewnętrznej nie umieszcza się oznaczeń wskazujących, że przesyłka zawiera informacje o klauzuli ZASTRZEŻONE. Przekazywanie informacji poza Stany Zjednoczone realizuje się w sposób umożliwiający

śledzenie przesyłki z wykorzystaniem komercyjnych usług kurierskich lub w inny sposób uzgodniony pisemnie przez Strony. Krajowe władze bezpieczeństwa Stron mogą również uzgodnić inne sposoby przekazywania informacji o klauzuli ZASTRZEŻONE, zapewniające ochronę przed ich nieuprawnionym ujawnieniem.

6. Dokument przewodni oraz pierwsza strona dokumentów Strony amerykańskiej, które zawierają informacje o klauzuli ZASTRZEŻONE, oznacza się klauzulą ZASTRZEŻONE. Fragmenty dokumentów zawierające informacje o klauzuli ZASTRZEŻONE oznacza się w ten sam sposób.
7. Informacje o klauzuli ZASTRZEŻONE mogą być przesyłane lub udostępniane elektronicznie poprzez ogólnie dostępne sieci, jak Internet przy zastosowaniu rządowych lub komercyjnych urządzeń szyfrujących zaakceptowanych przez krajowe władze bezpieczeństwa obu Stron. Taka transmisja może mieć postać rozmów telefonicznych, wideokonferencji lub faksu.
8. Nie wymaga się świadectwa bezpieczeństwa przemysłowego od kontrahenta przy dostępie do informacji o klauzuli ZASTRZEŻONE.

AGREEMENT BETWEEN THE GOVERNMENT OF THE REPUBLIC OF POLAND AND THE GOVERNMENT OF THE UNITED STATES OF AMERICA CONCERNING SECURITY MEASURES FOR THE PROTECTION OF CLASSIFIED INFORMATION

PREAMBLE

The Government of the Republic of Poland ("the Republic of Poland") and the Government of the United States of America (the "United States") (each a "Party," and collectively the "Parties"),

Considering that the Parties cooperate in matters including, but not limited to, foreign affairs, defense, security, law enforcement, science, industry, and technology, and

Having a mutual interest in the protection of Classified Information exchanged in confidence between the Parties,

Have agreed as follows:

ARTICLE 1 – DEFINITIONS

For the purpose of this Agreement:

1. Classified Information: Information provided by one Party to the other Party that is designated as classified by the releasing Party for national security purposes and therefore requires protection against unauthorized disclosure. The information may be in oral, visual, electronic, or documentary form, or in the form of material, including equipment or technology.

2. Classified Contract: A contract that requires, or will require, access to, or production of, Classified Information by a Contractor in the performance of the contract.

3. Contractor: An individual or an entity, possessing the legal capacity to conclude contracts, who is a party to a Classified Contract.

4. Facility Security Clearance: An assurance provided by the National Security Authority of a Party, as designated in Article 4, for a Contractor under the Party's jurisdiction that indicates the Contractor is cleared to a specified level and, if applicable, also has suitable security safeguards in place at a specified level to safeguard Classified Information. Such an assurance shall signify that Classified Information at the POUFNE / CONFIDENTIAL level or above shall be protected by the Contractor for which the Facility Security Clearance is provided in accordance with the provisions of this Agreement and that compliance shall be monitored and enforced by the relevant National Security Authority.

5. Personnel Security Clearance: An assurance provided by the National Security Authority of a Party, as designated in Article 4, that an individual who is a citizen of that Party, or who is employed by a Contractor under the jurisdiction of that Party, or an individual who is a citizen of one Party but is to be employed by the other Party or by one of the other Party's Contractors, is authorized to access Classified Information up to a specified level.

6. Need to Know: A positive determination made by an authorized holder of Classified Information that a prospective recipient has a requirement for access to, knowledge of, or possession of specific Classified Information in order to perform official tasks or services.

ARTICLE 2 – LIMITATIONS ON SCOPE OF THE AGREEMENT

The objective of this Agreement is to ensure the protection of Classified Information that is generated by or exchanged between the Parties except as otherwise stated in this Article. This Agreement shall not apply to Classified Information within the scope of the terms of another agreement or arrangement between the Parties or agencies thereof providing for the protection of a particular item or category of Classified Information exchanged between the Parties or agencies thereof, except to the extent that such other agreement or arrangement expressly makes this Agreement's terms applicable. This Agreement shall not apply to the exchange of Restricted Data, as defined in the U.S. Atomic Energy Act of 1954, as amended (the "AEA"), or to Formerly Restricted Data, which is data removed from the Restricted Data category in accordance with the AEA but still considered to be defense information by the United States.

ARTICLE 3 – COMMITMENT TO THE PROTECTION OF CLASSIFIED INFORMATION

1. Each Party shall protect Classified Information of the other Party according to the terms set forth herein.

2. Classified Information shall be protected by the recipient Party in a manner that is at least equivalent to the protection afforded to Classified Information by the releasing Party.

3. Each Party shall promptly notify the other of any changes to its national laws and regulations that would affect the protection of Classified Information under this Agreement. The obligations in this Agreement shall not be affected by such changes in national laws and regulations. In such cases, the Parties shall consult regarding possible amendments to this Agreement or other measures that may be appropriate to maintain protection of Classified Information exchanged under this Agreement.

ARTICLE 4 – NATIONAL SECURITY AUTHORITIES

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

a. for the Republic of Poland: Head of Internal Security Agency

b. for the United States: Assistant Director, International Engagement Directorate, Defense Technology Security Administration, Office of the Under Secretary of Defense for Policy, U.S. Department of Defense.

2. The Parties shall inform each other via diplomatic channels of any subsequent changes to the National Security Authorities referred to in paragraph 1 of this Article.

3. The Parties may conclude supplemental implementing arrangements to this Agreement where additional technical security measures may be required to protect Classified Information.

ARTICLE 5 – DESIGNATION OF CLASSIFIED INFORMATION

1. Classified Information shall be designated, and marked where possible, by the releasing Party as classified at one of the following national security classification levels with the name of the releasing Party. For purposes of ensuring equivalent treatment, the Parties agree that the following security classification levels are equivalent:

THE REPUBLIC OF POLAND	UNITED STATES OF AMERICA
ŚCIŚLE TAJNE	TOP SECRET
TAJNE	SECRET
POUFNE	CONFIDENTIAL
ZASTRZEŻONE	NO EQUIVALENT

2. During the implementation of this Agreement, if the Republic of Poland provides Classified Information designated as ZASTRZEŻONE, the United States shall handle it in accordance with the Appendix to this Agreement.

ARTICLE 6 – RESPONSIBILITY FOR CLASSIFIED INFORMATION

The recipient Party shall be responsible for the protection of all Classified Information of the releasing Party in a manner that is at least equivalent to the protection afforded to Classified Information by the releasing Party while the Classified Information is under its control. While in transit, the releasing Party shall be responsible for all Classified Information until custody of the Classified Information is formally transferred to the recipient Party.

ARTICLE 7 – PROTECTION OF CLASSIFIED INFORMATION

1. Within the scope of this Agreement, the Parties may recognize Personnel Security Clearances and Facility Security Clearances issued in accordance with the national laws and regulations of the other Party.

2. No individual shall be entitled to have access to Classified Information solely by virtue of rank, position, appointment, or Personnel Security Clearance. Access to Classified Information shall be granted only to individuals who have a Need

to Know, for whom a Personnel Security Clearance has been provided, and who have been authorized for access to such information in accordance with the prescribed standards of the recipient Party.

3. Except as otherwise provided in this Agreement, the recipient Party shall not release Classified Information of the releasing Party to any third party, including any third party government, individual, organization, or other entity, without the prior written consent of the releasing Party.

4. The recipient Party shall not use or permit the use of Classified Information of the releasing Party for any other purpose than that for which it was provided without the prior written consent of the releasing Party.

5. The recipient Party shall respect any private rights that are associated with Classified Information of the releasing Party, including those rights with respect to patents, copyrights, or trade secrets, and shall not release, use, exchange, or disclose such Classified Information in a manner inconsistent with those rights without the prior written authorization of the owner of those rights.

6. The recipient Party shall ensure that each entity that handles Classified Information covered by this Agreement maintains a list of individuals who are authorized to have access to such information.

7. Each Party shall develop accountability and control procedures to manage the dissemination of, and access to, Classified Information.

8. Each Party shall comply with any and all limitations on use, disclosure, release, and access to Classified Information as may be specified by the releasing Party when it discloses such Classified Information. If a Party is unable to comply with the specified limitations, that Party shall immediately consult with the other Party and shall undertake all lawful measures to prevent or minimize any such use, disclosure, release, or access.

ARTICLE 8 – PERSONNEL SECURITY CLEARANCES

1. The Parties shall ensure that all individuals who in the conduct of their official duties require access or whose duties or functions may afford access to Classified Information pursuant to this Agreement receive an appropriate Personnel Security Clearance before they are granted access to such information.

2. The Party providing the Personnel Security Clearance shall determine, in accordance with the national laws and regulations of that Party, an individual's suitability for access to Classified Information.

3. Before an authorized representative of one Party releases Classified Information to an authorized representative of the other Party, the recipient Party shall provide to the releasing Party an assurance that the authorized representative has the necessary Personnel Security Clearance level and a Need to Know and that the Classified Information will be protected by the recipient Party in accordance with this Agreement.

ARTICLE 9 – RELEASE OF CLASSIFIED INFORMATION TO CONTRACTORS

Classified Information received by a recipient Party may be provided by the recipient Party to a Contractor or prospective Contractor whose duties require access to such information with the prior written consent of the releasing Party. Prior to releasing any Classified Information to a Contractor or prospective Contractor, the recipient Party shall:

a. Confirm that such Contractor or prospective Contractor and, when applicable, the Contractor's facility have the capability to safeguard the information in accordance with the terms of this Agreement;

b. Confirm that such Contractor or prospective Contractor and the Contractor's facility have been granted appropriate Personnel Security Clearances and Facility Security Clearances, as applicable;

c. Confirm that the Contractor or prospective Contractor has procedures in place to ensure that all individuals having access to the information are informed of their responsibilities to protect the information in accordance with applicable laws and regulations;

d. Carry out periodic security inspections of cleared facilities to ensure that the information is protected as required by this Agreement; and

e. Confirm that the Contractor or prospective Contractor has procedures in place to ensure that access to the information is limited to those individuals who have a Need to Know.

ARTICLE 10 – CLASSIFIED CONTRACTS

1. When a Party proposes to place, or authorizes a Contractor in its country to place, a Classified Contract that is classified at the POUFNE / CONFIDENTIAL level or above, with a Contractor in the country of the other Party, the Party that is to place or authorize the Contractor to place such Classified Contract shall request an assurance from the National Security Authority of the other Party that the proposed Contractor has been issued a Facility Security Clearance in accordance with the national laws and regulations of the other Party. The National Security Authority of the requested Party shall monitor and take all appropriate steps to ensure the security conduct by the Contractor will be in accordance with applicable laws and regulations.

2. A Party, or its authorized representative, negotiating a Classified Contract to be performed in the country of the other Party shall incorporate in the Classified Contract, request for proposal, or subcontract document appropriate security clauses and other relevant provisions, including costs for security. This includes provisions

requiring any Contractors to include appropriate security clauses in their subcontract documents.

ARTICLE 11 – RESPONSIBILITY FOR FACILITIES

Each Party shall be responsible for the security of all government and private facilities and establishments where it stores Classified Information of the other Party and shall ensure that such facilities or establishments have qualified and appropriately cleared individuals appointed with the responsibility and authority for the control and protection of such information.

ARTICLE 12 – STORAGE OF CLASSIFIED INFORMATION

Classified Information exchanged between the Parties shall be stored in a manner that ensures access only by those individuals who have been authorized access consistent with Article 7.2.

ARTICLE 13 – TRANSMISSION

1. Classified Information shall be transmitted between the Parties through government-to-government channels or other channels mutually approved in advance in writing by the respective National Security Authorities of the Parties.

2. The minimum requirements for the security of Classified Information during transmission shall be as follows:

a. Documents or other media:

(1) Documents or other media containing Classified Information shall be transmitted in double, sealed envelopes. The inner envelope shall indicate only the classification of the documents or other media and the organizational address of the intended recipient. The outer envelope shall indicate the organizational address

of the intended recipient, the organizational address of the sender, and the document control number, if applicable.

(2) No indication of the classification of the enclosed documents or other media shall be made on the outer envelope. The double sealed envelope shall be transmitted according to the prescribed procedures of the Parties.

(3) Receipts shall be prepared by the recipient for packages containing documents or other media containing Classified Information that are transmitted between the Parties, and such receipts shall be signed by the final recipient and returned to the sender.

b. Material:

(1) Material, including equipment, that contains Classified Information shall be transported in sealed, covered vehicles, or shall otherwise be securely packaged or protected in order to prevent identification of its shape, size, or contents, and kept under continuous control to prevent access by unauthorized persons.

(2) Material, including equipment that contains Classified Information that must be stored temporarily awaiting shipment shall be placed in protected storage areas. Such areas shall be protected by intrusion detection equipment or guards with requisite Personnel Security Clearance who shall maintain continuous surveillance of those areas. Only authorized personnel with the requisite Personnel Security Clearance shall have access to the protected storage areas.

(3) Receipts shall be obtained whenever material that contains Classified Information, including equipment, changes hands during transit, and a receipt for such material shall be signed by the final recipient and returned to the sender.

c. Electronic transmissions:

(1) Classified Information that is classified at the POUFNE / CONFIDENTIAL level or above that is to be transferred electronically shall be transmitted using secure means that have been approved by each Party's National Security Authority.

ARTICLE 14 – VISITS TO FACILITIES AND ESTABLISHMENTS OF THE PARTIES

1. Visits by representatives of one Party to facilities and establishments of the other Party that require access to Classified Information, or visits for which a Personnel Security Clearance is required to permit access, shall be limited to those necessary for official purposes. Authorization shall only be granted to representatives who possess a valid Personnel Security Clearance.

2. Authorization to visit such facilities and establishments shall be granted only by the Party in whose territory the facility or establishment to be visited is located. The visited Party, or its designated officials, shall be responsible for advising the facility or establishment of the proposed visit, and the scope and highest level of Classified Information that may be furnished to the visitor.

3. Requests for visits by representatives of the Parties shall be submitted by the Embassy of the United States in Warsaw in the case of U.S. visitors, and by the Embassy of the Republic of Poland in Washington, D.C., in the case of Polish visitors.

ARTICLE 15 – SECURITY VISITS

Implementation of security requirements set out in this Agreement may be verified through reciprocal visits by representatives of the National Security Authorities of the Parties, who after prior consultation, shall be permitted to visit the other Party to discuss and observe the implementing procedures of the other Party in the interest of achieving reasonable comparability of security systems. The host Party shall assist

the representatives of the visiting National Security Authority in determining whether Classified Information received from the other Party is being adequately protected.

ARTICLE 16 – SECURITY STANDARDS

On request, each Party shall provide the other Party with information about its security standards, practices, and procedures for safeguarding of Classified Information.

ARTICLE 17 – REPRODUCTION AND TRANSLATION OF CLASSIFIED INFORMATION

When Classified Information is reproduced or translated, all of the original security markings thereon shall also be reproduced or marked on each reproduction of such information. Such reproductions or translations shall be subject to the same protections as the original information. The number of reproductions or translations shall be limited to the minimum number required for official purposes.

ARTICLE 18 – DESTRUCTION OF CLASSIFIED INFORMATION

Classified Information and material containing Classified Information shall be destroyed through means that render the Classified Information or material containing Classified Information no longer recognizable so as to preclude reconstruction of the Classified Information.

ARTICLE 19 – DOWNGRADING AND DECLASSIFICATION

1. The Parties agree that Classified Information should be downgraded in classification as soon as the information ceases to require that higher degree

of protection or should be declassified as soon as the information no longer requires protection against unauthorized disclosure.

2. The releasing Party has complete discretion concerning downgrading or declassification of its Classified Information. The recipient Party shall not downgrade the security classification or declassify Classified Information received from the releasing Party, notwithstanding any apparent declassification instructions on the document, without the prior written consent of the releasing Party.

ARTICLE 20 – LOSS OR COMPROMISE

The recipient Party shall inform the releasing Party immediately upon discovery of all losses or compromises, as well as possible losses or compromises, of Classified Information of the releasing Party. In the event of an actual or possible loss or compromise of such information, the recipient Party shall initiate an investigation immediately to determine the circumstances of the actual or possible loss or compromise. The results of the investigation and information regarding measures taken to prevent recurrence shall be provided to the releasing Party.

ARTICLE 21 – DISPUTES

Disagreements between the Parties arising under or relating to this Agreement shall be settled solely through consultations between the Parties and shall not be referred to a national court, an international tribunal, or any other person or entity for settlement.

ARTICLE 22 – COSTS

Each Party shall be responsible for bearing its own costs incurred in implementing this Agreement. All obligations of the Parties under this Agreement shall be subject to the availability of funds.

ARTICLE 23 – FINAL PROVISIONS

1. This Agreement shall enter into force in accordance with the national laws and regulations of each Party and upon the date of the later of the written notifications, through diplomatic channels, whereby the Parties inform each other that all their internal procedures necessary to bring this Agreement into force have been fulfilled.

2. This Agreement may be amended by mutual written agreement of the Parties.

3. Either Party may terminate this Agreement by notifying the other Party in writing through diplomatic channels ninety days in advance of its intention to terminate the Agreement.

4. Notwithstanding the termination of this Agreement, all Classified Information exchanged or otherwise provided pursuant to this Agreement shall continue to be protected in accordance with the provisions set forth herein.

5. The Agreement between the Government of the Republic of Poland and the Government of the United States of America Concerning Security Measures for the Protection of Classified Information in the Military Sphere (the "Security of Information Agreement"), done at Warsaw, March 8, 2007, shall terminate on the date that this Agreement enters into force.

6. Any reference in any other existing agreement or arrangement between the Parties to the Security of Information Agreement shall be considered to be a reference to this Agreement.

IN WITNESS WHEREOF, the undersigned, being duly authorized thereto by their respective Governments, have signed this Agreement.

Done in duplicate at WARSAW this 16 day of APRIL 2025, in the Polish and English languages, both texts being equally authentic.

FOR THE GOVERNMENT OF THE REPUBLIC OF POLAND:

FOR THE GOVERNMENT OF THE UNITED STATES OF AMERICA:

APPENDIX
PROCEDURES FOR PROTECTING THE REPUBLIC OF POLAND ZASTRZEŻONE CLASSIFIED INFORMATION PROVIDED TO THE UNITED STATES

Upon receipt, the Republic of Poland Classified Information provided to the United States and designated as ZASTRZEŻONE shall be protected by the United States in accordance with the following procedures:

1. Information designated as ZASTRZEŻONE shall be stored in a manner that deters unauthorized access, in locked containers, or in closed areas that prevent access by unauthorized personnel.

2. Access to such ZASTRZEŻONE information shall be restricted to individuals who are U.S. citizens and have been briefed on protection of such information and who have a Need to Know. A Personnel Security Clearance is not required for access to information classified ZASTRZEŻONE.

3. ZASTRZEŻONE information shall not be disclosed to unauthorized persons or entities without prior written approval from the releasing Party except as required by U.S. law, including the Freedom of Information Act. The Republic of Poland witholds ZASTRZEŻONE information from public disclosure and may provide ZASTRZEŻONE information to the United States on the condition that such information not be released to the public. In the event a U.S. Government department or agency receives a request for information under the Freedom of Information Act that includes ZASTRZEŻONE information, the United States shall use all available legal remedies to withold the release of ZASTRZEŻONE information to the public.

4. ZASTRZEŻONE information shall, as applicable, be stored, processed, or transmitted electronically using government- or Contractor-accredited systems. In particular, before any system is used to store, process, or transmit ZASTRZEŻONE information, it must receive security approval, known as Accreditation. An Accreditation is a formal statement by the appropriate accrediting authority

confirming that the use of a system meets the appropriate security requirements and does not present an unacceptable risk. Security Standard Operating Procedures are technical procedures to implement security policies and requirements unique to a specific facility to protect automated information systems processing Classified Information. For stand-alone automated information systems such as desktop and laptop computers utilized in U.S. Government establishments, the system registration document together with the Security Standard Operating Procedures shall fulfill the role of the required Accreditation. For Contractors, guidance on the use of communications and information systems shall be incorporated into the appropriate security clauses in the Contract.

5. Transmission of ZASTRZEŻONE information shall be by diplomatic pouch, military courier, registered (first class) mail or personal carriage. ZASTRZEŻONE information shall be transmitted by registered (first class) mail within and outside of the United States in double sealed envelopes, with the inner envelope marked the Republic of Poland ZASTRZEŻONE. The markings on the outer envelope shall not reveal that it contains ZASTRZEŻONE information. Transmission outside the United States shall be by traceable means such as commercial courier or other means agreed upon by the Parties in writing. The National Security Authorities of the Parties may also agree on other forms of transmitting ZASTRZEŻONE information which ensure its protection against unauthorized disclosure.

6. U.S. documents that contain ZASTRZEŻONE information shall bear on the cover and the first page the marking ZASTRZEŻONE. The portion of the documents containing ZASTRZEŻONE information also shall be identified with the same marking.

7. ZASTRZEŻONE information may be transmitted or accessed electronically via a public network like the Internet using government or commercial encryption devices mutually accepted by the National Security Authorities of the Parties. Such transmission includes telephone conversations, video conferencing, or facsimile.

8. A Facility Security Clearance is not required for a Contractor to access ZASTRZEŻONE information.

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 1 sierpnia 2025 roku.

Prezydent Rzeczypospolitej Polskiej: *A. Duda*

L.S.

Prezes Rady Ministrów: *D. Tusk*