SEJM
RZECZYPOSPOLITEJ POLSKIEJ
IX kadencja
Prezes Rady Ministrów
RM-06111-279-22

Druk nr 2947
Warszawa, 16 stycznia 2023 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 Federacyjnej Republiki Brazylii o wymianie i wzajemnej ochronie informacji niejawnych, podpisaną w Nowym Jorku dnia 20 września 2022 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/

Projekt

W imieniu Rzeczypospolitej Polskiej

PREZYDENT RZECZYPOSPOLITEJ POLSKIEJ

podaje do powszechnej wiadomości:

Dnia 20 września 2022 roku w Nowym Jorku została podpisana Umowa między Rządem Rzeczypospolitej Polskiej a Rządem Federacyjnej Republiki Brazylii 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 wydany został 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 międzynarodową

Rozwijająca się współpraca polityczna i ekonomiczna z innymi państwami wiąże się z koniecznością tworzenia podstaw prawnych stosunków dwustronnych, również w sferze ochrony informacji niejawnych.

Podpisana w dniu 20 września 2022 r. w Nowym Jorku Umowa między Rządem Rzeczypospolitej Polskiej a Rządem Federacyjnej Republiki Brazylii o wymianie i wzajemnej ochronie informacji niejawnych reguluje prawne aspekty współpracy polskich i brazylijskich podmiotów upoważnionych, zgodnie ze swoim prawem krajowym, do przetwarzania informacji niejawnych. Po wejściu w życie, niniejsza Umowa stanowić będzie podstawę do nawiązania ściślejszej współpracy sektorów przemysłu obronnego obu krajów, a także w zakresie bezpieczeństwa wewnętrznego – szczególnie w zwalczaniu przestępczości i przeciwdziałaniu terroryzmowi. Wejście w obieg prawny przedmiotowej Umowy wpłynie korzystnie na ożywienie stosunków gospodarczych, ponieważ umożliwi polskim i brazylijskim przedsiębiorcom zawieranie kontraktów związanych z dostępem do informacji niejawnych.

II. Wskazanie różnic między dotychczasowym i projektowanym stanem prawnym

Umowa między Rządem Rzeczypospolitej Polskiej a Rządem Federacyjnym Republiki Brazylii o wymianie i wzajemnej ochronie informacji niejawnych będzie pierwszą tego typu umową zawartą z tym partnerem zagranicznym.

W artykule 1 określono przedmiot niniejszej Umowy i wskazano zakres jej stosowania. Kompleksowy charakter tej Umowy powoduje, że po wejściu w życie będzie ona miała zastosowanie do wszelkich działań lub umów dotyczących informacji niejawnych zawieranych pomiędzy Stronami.

W celu ujednolicenia terminów na użytek niniejszej Umowy, w artykule 2 zdefiniowano kluczowe pojęcia, w tym „informacji niejawnych", „kontraktu niejawnego", „Krajowej Władzy Bezpieczeństwa", „kontrahenta" i „zlecającego".

W artykule 3 zestawiono odpowiadające sobie klauzule tajności oraz uregulowano obowiązek Strony otrzymującej do zagwarantowania otrzymanym informacjom niejawnym co najmniej równorzędnego poziomu ochrony. Ponadto ze względu na brak po stronie brazylijskiej

odpowiednika klauzuli „Zastrzeżone”, w ustępie 4 tego artykułu uregulowano zasady postępowania z tak oznaczonymi polskimi informacjami niejawnymi.

W artykule 4 zostały wskazane Krajowe Władze Bezpieczeństwa właściwe do realizacji postanowień niniejszej Umowy, którymi są: w Rzeczypospolitej Polskiej – Szef Agencji Bezpieczeństwa Wewnętrznego, w Federacyjnej Republice Brazylii – Biuro Bezpieczeństwa Instytucjonalnego Prezydenta Federacyjnej Republiki Brazylii. Ponadto w tym artykule zawarto postanowienia regulujące obowiązek informacyjny dotyczący zmian tych organów lub ich kompetencji.

W artykule 5 określono zasady ochrony informacji niejawnych, zgodnie z którymi są one udostępniane wyłącznie tym osobom, które zgodnie z prawem krajowym Strony otrzymującej zostały uprawnione do dostępu do nich i których zadania służbowe wymagają zapoznania się z takimi informacjami.

W artykule 6 określono zasadę wzajemnego uznawania przez Strony poświadczenia bezpieczeństwa oraz świadectwa bezpieczeństwa przemysłowego. Ponadto w artykule tym wskazano, że, na wniosek, Krajowe Władze Bezpieczeństwa będą współpracować podczas procedur sprawdzających dotyczących wymienionych dokumentów.

Artykuł 7 niniejszej Umowy reguluje możliwość zawierania kontraktów niejawnych, a więc takich, których realizacja wiąże się z dostępem bądź wytworzeniem informacji niejawnych. Zgodnie z ustępem 4 omawianego artykułu, zlecający przekazuje kontrahentowi instrukcję bezpieczeństwa przemysłowego, w szczególności wykaz rodzajów informacji niejawnych odnoszących się do danego kontraktu niejawnego, jak również zasady nadawania klauzul tajności informacjom niejawnym wytworzonym podczas jego realizacji. Ustęp 6 tego artykułu określa, że realizacja kontraktu niejawnego w części związanej z dostępem do informacji niejawnych będzie możliwa wyłącznie po spełnieniu przez kontrahenta warunków niezbędnych do ochrony informacji niejawnych, zgodnie z instrukcją bezpieczeństwa przemysłowego.

Zgodnie z postanowieniami artykułu 8 niniejszej Umowy informacje niejawne są przekazywane między Stronami w drodze dyplomatycznej lub w inny sposób zapewniający ochronę przed nieuprawnionym ujawnieniem, uzgodniony między Krajowymi Władzami Bezpieczeństwa Stron. Zgodnie z ust. 2 przedmiotowego artykułu organy uprawnione do wymiany informacji niejawnych na postawie innych umów międzynarodowych, zawartych między Stronami, mogą wymieniać informacje niejawne bezpośrednio.

W artykułach 9 i 10 uregulowano kolejno powielanie, tłumaczenie oraz niszczenie informacji niejawnych, co pozwoli na ujednolicenie postępowania z informacjami niejawnymi w stosunkach bilateralnych.

W artykule 11 niniejszej Umowy określono zasady i warunki przeprowadzania wizyt związanych z dostępem do informacji niejawnych, w tym także obowiązek ochrony danych osobowych przekazywanych na potrzeby ich realizacji.

W artykule 12 wskazany został tryb postępowania w przypadku naruszenia lub podejrzenia naruszenia regulacji dotyczących wzajemnej ochrony informacji niejawnych. Ustęp 4 w tym artykule przewiduje możliwość współpracy właściwych organów Stron przy czynnościach wyjaśniających, na wniosek jednego z nich.

Artykuł 13 przedmiotowej Umowy określa, że w zakresie stosowania jej postanowień Strony używają języka angielskiego lub swoich języków urzędowych, dołączając wówczas tłumaczenie na język urzędowy drugiej Strony lub na język angielski.

W artykule 14 niniejszej Umowy ustalono, że każda ze Stron pokrywa koszty własne związane z jej realizacją.

Artykuł 15 reguluje kwestie wzajemnych konsultacji przy realizacji postanowień przedmiotowej Umowy, obowiązku wzajemnego informowania o zmianach prawa krajowego w zakresie dotyczącym ochrony informacji niejawnych. Ponadto w ustępie 3 tego artykułu określono, że przedstawiciele Krajowej Władzy Bezpieczeństwa składają wzajemnie wizyty w celu omówienia procedur służących ochronie przekazywanych informacji niejawnych.

W artykule 16 niniejszej Umowy przewidziano także tryb rozwiązywania sporów dotyczących stosowania lub interpretacji jej postanowień.

Ponadto w przedmiotowej Umowie określono procedurę wejścia w życie, jak również czas jej obowiązywania oraz tryb wypowiedzenia (artykuł 17).

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

Wejście w życie Umowy nie spowoduje powstania skutków społecznych. Skutkiem o charakterze prawnym będzie określenie jednolitych zasad ochrony informacji niejawnych, wymienianych w ramach szeroko rozumianej współpracy między Rzecząpospolitą Polską

a Federacyjną Republiką Brazylii. Niniejsza Umowa stanowić będzie podstawę do nawiązania ściślejszej współpracy w zakresie bezpieczeństwa wewnętrznego.

Z uwagi na fakt, że podstawowym celem niniejszej Umowy jest stworzenie podstaw prawnych do wymiany informacji niejawnych, jej zawarcie spowoduje pozytywne skutki gospodarcze, a w związku z możliwością zawierania kontraktów niejawnych, wzrośnie pewność dwustronnego obrotu gospodarczego między zainteresowanymi podmiotami obu Stron.

Skutkiem politycznym będzie znaczące zacieśnienie współpracy i pogłębienie dotychczasowych relacji między obydwoma krajami.

Wejście niniejszej Umowy w życie nie spowoduje skutków finansowych dla podmiotów sektora finansów publicznych w postaci zmniejszenia ich dochodów lub zwiększenia ich wydatków ani dodatkowych skutków finansowych dla budżetu państwa, innych niż przewidziane w ramach właściwej części 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 oraz z 2022 r. poz. 655 i 1933). Umowa dotyczy wprawdzie ochrony przekazywanych za granicę i otrzymywanych z zagranicy informacji niejawnych, ale nie wprowadza żadnych dodatkowych zasad ochrony lub wymiany tych informacji – innych niż określone w ustawie z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych. Nie zostały zatem spełnione przesłanki wymienione w artykule 89 ustęp 1 Konstytucji Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz. U. poz. 483, z późn. zm.), a więc ratyfikacja przedmiotowej Umowy nie wymaga uprzedniej zgody wyrażonej w ustawie.

Niniejsza Umowa dotyczy takich podmiotów prawa wewnętrznego Rzeczypospolitej Polskiej, jak: osoby fizyczne, osoby prawne oraz inne podmioty w rozumieniu ustawy z dnia 5 sierpnia 2010 r. 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 lub podwykonawcy. Ponadto w artykule 9 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 krajowym Rzeczypospolitej Polskiej, objętych zarówno przepisami ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych, jak również ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2019 r. poz. 1781).

W Rzeczypospolitej Polskiej związanie przedmiotową Umową powinno nastąpić przez jej ratyfikację w trybie artykułu 89 ustęp 2 Konstytucji Rzeczypospolitej Polskiej, zgodnie z postanowieniami artykułu 12 ustęp 2 ustawy z dnia 14 kwietnia 2000 r. o umowach międzynarodowych (Dz. U. z 2020 r. poz. 127).

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

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

W związku z faktem, że realizacja Umowy wiąże się z udostępnianiem za granicę danych osobowych, istnieje potrzeba zagwarantowania odpowiedniej ochrony przekazywanych danych osobowych, zgodnie z przepisami ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych oraz określonej w artykule 47 Konstytucji Rzeczypospolitej Polskiej zasadzie ochrony prawa do prywatności. Z uwagi na powyższe zaproponowany tryb związania spełnia w najwyższym stopniu funkcję gwarancyjną zapewnienia należytej ochrony przekazywanych danych osobowych i jest spełniona tym samym przesłanka szczególnych okoliczności uzasadniających wymóg tzw. małej ratyfikacji, zgodnie z brzmieniem artykułu 12 ustęp 2 ustawy z dnia 14 kwietnia 2000 r. o umowach międzynarodowych.

UMOWA

między Rządem Rzeczypospolitej Polskiej

a Rządem Federacyjnej Republiki Brazylii

o wymianie i wzajemnej ochronie informacji niejawnych

Rząd Rzeczypospolitej Polskiej
i Rząd Federacyjnej Republiki Brazylii,
zwane dalej „Stronami"
lub z osobna „Stroną",

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

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

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

uzgodniły, co następuje:

ARTYKUŁ 1
PRZEDMIOT UMOWY

1. Przedmiotem niniejszej Umowy jest zapewnienie ochrony informacjom niejawnym wytwarzanym w wyniku współpracy lub wymienianym między Stronami.
2. Niniejsza Umowa ma zastosowanie do wszelkich kontraktów lub umów dotyczących informacji niejawnych, realizowanych bądź zawieranych między Stronami oraz do wszelkich działań prowadzonych między nimi.

ARTYKUŁ 2
DEFINICJE

W rozumieniu niniejszej Umowy następujące terminy 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 krajowym każdej ze Stron i niniejszą Umową;
2) **Krajowa Władza Bezpieczeństwa** – organ krajowy, o którym mowa w artykule 4, właściwy w zakresie bezpieczeństwa informacji niejawnych wymienianych zgodnie z niniejszą Umową;
3) **Strona wytwarzająca** – Stronę, osoby fizyczne, osoby prawne lub inne jednostki organizacyjne uprawnione do wytwarzania i przekazywania informacji niejawnych zgodnie z prawem krajowym swojej Strony;
4) **Strona otrzymująca** – Stronę, osoby fizyczne, osoby prawne lub inne jednostki organizacyjne uprawnione do otrzymywania informacji niejawnych zgodnie z prawem krajowym swojej Strony;
5) **kontrakt niejawny** – umowę, której realizacja jest związana z dostępem do informacji niejawnych, bądź z wytworzeniem takich informacji;

6) **kontrahent** – osobę fizyczną, osobę prawną albo inną jednostkę organizacyjną podlegającą prawu krajowemu jednej ze Stron, uprawnioną do realizacji kontraktów niejawnych zgodnie z postanowieniami niniejszej Umowy;

7) **zlecający** – osobę fizyczną, osobę prawną albo inną jednostkę organizacyjną podlegającą prawu krajowemu jednej ze Stron, uprawnioną do zlecania kontraktów niejawnych zgodnie z postanowieniami niniejszej Umowy;

8) **poświadczenie bezpieczeństwa** – dokument wydany zgodnie z prawem krajowym Strony przez Krajową Władzę Bezpieczeństwa lub inny uprawniony podmiot potwierdzający, że osoba fizyczna została poddana postępowaniu sprawdzającemu i jest uprawniona do dostępu do informacji niejawnych;

9) **świadectwo bezpieczeństwa przemysłowego** – dokument wydany zgodnie z prawem krajowym Strony przez Krajową Władzę Bezpieczeństwa lub inny uprawniony podmiot potwierdzający, że kontrahent posiada zdolność do ochrony informacji niejawnych; w przypadku kontrahentów będących osobami fizycznymi funkcję świadectwa bezpieczeństwa przemysłowego pełni poświadczenie bezpieczeństwa;

10) **strona trzecia** – organizację międzynarodową lub państwo, osoby fizyczne, osoby prawne lub inne jednostki organizacyjne podlegające jego jurysdykcji, niebędące Stroną niniejszej Umowy;

11) **zasada ograniczonego dostępu** – zasadę, zgodnie z którą dostęp do informacji niejawnych może być przyznany osobie wyłącznie w związku z realizacją przez nią obowiązków służbowych lub określonych zadań;

12) **naruszenie regulacji dotyczących ochrony informacji niejawnych** – działanie lub zaniechanie sprzeczne z niniejszą Umową lub prawem krajowym Stron w zakresie dotyczącym ochrony informacji niejawnych.

ARTYKUŁ 3

KLAUZULE TAJNOŚCI

1. Informacjom niejawnym przyznaje się odpowiednią do ich treści klauzulę tajności zgodnie z prawem krajowym Strony wytwarzającej. Strona otrzymująca gwarantuje co najmniej równorzędny poziom ochrony otrzymanych informacji niejawnych, zgodnie z postanowieniami ustępów 3 i 4.
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 otrzymanych uprzednio informacji niejawnych.
3. Strony uzgadniają, że niżej wymienione klauzule tajności są równorzędne:

RZECZPOSPOLITA POLSKA	**FEDERACYJNA REPUBLIKA BRAZYLII**	**ODPOWIEDNIK W JĘZYKU ANGIELSKIM**
ŚCIŚLE TAJNE	ULTRASSECRETO	TOP SECRET
TAJNE	SECRETO	SECRET
POUFNE	RESERVADO	CONFIDENTIAL
ZASTRZEŻONE	NO EQUIVALENT	RESTRICTED

4. Informacje o klauzuli „ZASTRZEŻONE" otrzymane z Rzeczypospolitej Polskiej są przetwarzane w Federacyjnej Republice Brazylii tak, jak informacje o klauzuli „POUFNE/RESERVADO/CONFIDENTIAL".

ARTYKUŁ 4

KRAJOWE WŁADZE BEZPIECZEŃSTWA

1. Krajowymi Władzami Bezpieczeństwa, właściwymi w zakresie realizacji i nadzoru nad stosowaniem niniejszej Umowy, są:
    1) w Rzeczypospolitej Polskiej: Szef Agencji Bezpieczeństwa Wewnętrznego;
    2) w Federacyjnej Republice Brazylii: Biuro Bezpieczeństwa Instytucjonalnego Prezydenta Federacyjnej Republiki Brazylii (Gabinete de Segurança Institucional da Presidência da República Federativa do Brasil).
2. Strony informują się w drodze dyplomatycznej o zmianach Krajowych Władz Bezpieczeństwa, o których mowa w ustępie 1, lub o zmianach ich właściwości.
3. Strony przekażą pisemnie dane kontaktowe swoich Krajowych Władz Bezpieczeństwa.

ARTYKUŁ 5

ZASADY OCHRONY INFORMACJI NIEJAWNYCH

1. Strony podejmują wszelkie określone w niniejszej Umowie oraz zgodne ze swoim prawem krajowym działania 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 krajowym 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

1. W zakresie niniejszej Umowy, Strony uznają poświadczenia bezpieczeństwa i świadectwa bezpieczeństwa przemysłowego wydane zgodnie z prawem krajowym drugiej Strony.
2. Na wniosek, Krajowe Władze Bezpieczeństwa współpracują podczas procedur sprawdzających dotyczących poświadczenia bezpieczeństwa i świadectwa bezpieczeństwa przemysłowego.
3. Krajowe Władze Bezpieczeństwa informują się wzajemnie o zmianach w wydanych poświadczeniach bezpieczeństwa i świadectwach bezpieczeństwa przemysłowego.

ARTYKUŁ 7
KONTRAKTY NIEJAWNE

1. Przed zawarciem kontraktu niejawnego związanego z dostępem do informacji niejawnych o klauzuli POUFNE /RESERVADO/ CONFIDENTIAL lub wyższej zlecający składa wniosek do Krajowej Władzy Bezpieczeństwa swojej Strony o wystąpienie do Krajowej Władzy Bezpieczeństwa drugiej Strony z prośbą o wydanie zaświadczenia, że kontrahent posiada ważne świadectwo bezpieczeństwa przemysłowego odpowiednie do klauzuli informacji niejawnych, do których będzie miał dostęp.
2. Wydanie zaświadczenia, o którym mowa w ustępie 1, jest równoznaczne z gwarancją, że zostały przeprowadzone czynności niezbędne do stwierdzenia, że kontrahent spełnia warunki w zakresie ochrony informacji niejawnych określone w prawie krajowym Strony, na terytorium Państwa której 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;
    3) procedury dotyczące przetwarzania informacji niejawnych przekazanych kontrahentowi lub wytworzonych w związku z realizacją kontraktu niejawnego.
5. Zlecający przekazuje kopię instrukcji bezpieczeństwa przemysłowego Krajowej Władzy Bezpieczeństwa swojej Strony, która przesyła ją Krajowej Władzy Bezpieczeństwa 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 w drodze dyplomatycznej lub w inny sposób zapewniający ochronę przed nieuprawnionym ujawnieniem, uzgodniony pomiędzy Krajowymi Władzami Bezpieczeństwa Stron. Strona otrzymująca potwierdza pisemnie odbiór informacji niejawnych.

2. 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 krajowym Strony otrzymującej. Powielone lub przetłumaczone informacje podlegają takiej samej ochronie jak oryginały. Liczbę kopii lub tłumaczeń należy ograniczyć do liczby wymaganej dla celów służbowych.
2. Informacje niejawne o klauzuli ŚCIŚLE TAJNE / ULTRASSECRETO/ TOP SECRET są powielane lub tłumaczone tylko po uprzednim uzyskaniu pisemnego zezwolenia wydanego przez Stronę wytwarzającą.

ARTYKUŁ 10
NISZCZENIE INFORMACJI NIEJAWNYCH

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

ARTYKUŁ 11
WIZYTY

1. Osobom przybywającym z wizytą na terytorium Państwa drugiej Strony i do obiektów drugiej Strony zezwala się na dostęp do informacji niejawnych

tylko po uprzednim uzyskaniu pisemnego zezwolenia wydanego przez Krajową Władzę Bezpieczeństwa strony przyjmującej.

2. Krajowa Władza Bezpieczeństwa strony wysyłającej zwraca się do Krajowej Władzy Bezpieczeństwa strony przyjmującej z wnioskiem o wyrażenie zgody na wizytę co najmniej trzydzieści dni przed planowanym terminem wizyty, o której mowa w ustępie 1.

3. Wniosek, o którym mowa w ustępie 2, zawiera następujące informacje, które są wykorzystywane wyłącznie w celu realizacji wizyty:

   1) cel, termin i program wizyty;

   2) imię i nazwisko, datę i miejsce urodzenia, narodowość, posiadane obywatelstwa i numer paszportu lub innego dokumentu tożsamości osoby przybywającej z wizytą;

   3) stanowisko służbowe osoby przybywającej z wizytą wraz z nazwą podmiotu, który reprezentuje;

   4) poziom i datę ważności poświadczenia bezpieczeństwa posiadanego przez osobę przybywającą z wizytą;

   5) nazwę i adres odwiedzanego podmiotu;

   6) imię i nazwisko oraz stanowisko służbowe osoby przyjmującej;

   7) jak również datę, podpis oraz oficjalną pieczęć Krajowej Władzy Bezpieczeństwa strony wysyłającej.

4. Krajowe Władze Bezpieczeństwa 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 Krajowe Władze Bezpieczeństwa Stron, terminy wizyt są uzgadniane bezpośrednio między stroną wysyłającą a stroną przyjmującą, zgodnie z ustalonymi warunkami.

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

1) wykorzystanie danych osobowych przez stronę przyjmującą jest dopuszczalne wyłącznie w celu oraz na warunkach określonych przez stronę przekazującą te dane osobowe;

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

3) w przypadku przekazania danych, których nie wolno było przekazać zgodnie z prawem krajowym strony przekazującej dane osobowe, strona ta zawiadamia o tym stronę przyjmującą; strona przyjmująca 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; strona przyjmująca jest zobowiązana do sprostowania lub usunięcia tych danych;

5) strona przekazująca dane osobowe oraz strona przyjmująca są zobowiązane do rejestrowania przekazywania, otrzymywania i usuwania danych osobowych;

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

ARTYKUŁ 12
NARUSZENIE REGULACJI DOTYCZĄCYCH OCHRONY INFORMACJI NIEJAWNYCH

1. Informację o każdym przypadku naruszenia lub o podejrzeniu naruszenia regulacji dotyczących ochrony informacji niejawnych przekazanych przez

Stronę wytwarzającą lub informacji niejawnych wytworzonych w wyniku wspólnego działania Stron przekazuje się niezwłocznie Krajowej Władzy Bezpieczeństwa Strony, na terytorium Państwa której miało miejsce lub zaistniało podejrzenie takiego naruszenia.

2. Każdy przypadek naruszenia lub podejrzenia naruszenia regulacji dotyczących ochrony informacji niejawnych wyjaśnia się zgodnie z prawem krajowym Strony, na terytorium Państwa której zdarzenie miało miejsce.
3. W przypadku naruszenia regulacji dotyczących ochrony informacji niejawnych, Krajowa Władza Bezpieczeństwa Strony, na terytorium Państwa której naruszenie miało miejsce, pisemnie informuje Krajową Władzę Bezpieczeństwa drugiej Strony o fakcie, okolicznościach naruszenia oraz wyniku czynności, o których mowa w ustępie 2.
4. Krajowe Władze Bezpieczeństwa Stron współpracują przy czynnościach, o których mowa w ustępie 2, na wniosek jednej z nich.
5. Jeśli naruszenie regulacji dotyczących ochrony informacji niejawnych miało miejsce na terytorium państwa strony trzeciej, Krajowa Władza Bezpieczeństwa Strony, która przekazała informacje niejawne, podejmuje we współpracy ze stroną trzecią działania, o których mowa w ustępach 1,2 i 3.

ARTYKUŁ 13
JĘZYKI

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

ARTYKUŁ 14
KOSZTY

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

ARTYKUŁ 15
KONSULTACJE

1. Krajowe Władze Bezpieczeństwa Stron informują się wzajemnie o wszelkich zmianach w swoim prawie krajowym dotyczącym ochrony informacji niejawnych, w zakresie niezbędnym do wykonywania postanowień niniejszej Umowy.
2. W celu zapewnienia ścisłej współpracy przy realizacji postanowień niniejszej Umowy Krajowe Władze Bezpieczeństwa Stron konsultują się, na wniosek jednej z nich.
3. Przedstawiciele Krajowych Władz Bezpieczeństwa składają sobie wzajemnie wizyty w celu omówienia procedur służących ochronie informacji niejawnych.
4. W celu zapewnienia skutecznej współpracy, będącej przedmiotem niniejszej Umowy, i w zakresie kompetencji przyznanych Krajowym Władzom Bezpieczeństwa prawem krajowym każdej ze Stron, Krajowe Władze Bezpieczeństwa mogą, w razie potrzeby, zawierać pisemne szczegółowe uzgodnienia techniczne lub organizacyjne.

ARTYKUŁ 16
ROZSTRZYGANIE SPORÓW

1. Wszelkie sporne kwestie dotyczące stosowania lub interpretacji niniejszej Umowy rozstrzygane są w drodze bezpośrednich konsultacji między Krajowymi Władzami Bezpieczeństwa Stron.

2. Jeśli nie jest możliwe rozwiązanie sporu w sposób, o którym mowa w ustępie 1, jest on rozstrzygany w drodze dyplomatycznej.

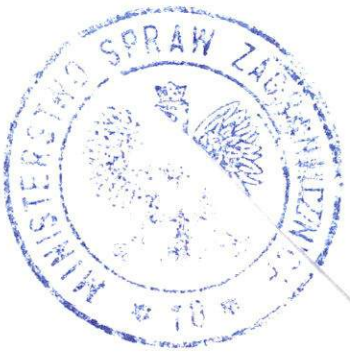
ARTYKUŁ 17
POSTANOWIENIA KOŃCOWE

1. Umowa niniejsza podlega przyjęciu zgodnie z prawem krajowym każdej ze Stron, co zostanie stwierdzone w drodze wymiany not. Umowa wejdzie w życie w pierwszym dniu drugiego miesiąca, który nastąpi po dniu otrzymania noty późniejszej.
2. Umowa niniejsza może zostać zmieniona na podstawie pisemnej zgody obu Stron. Takie zmiany wejdą w życie zgodnie z postanowieniami ustępu 1.
3. Umowa niniejsza zawarta jest na czas nieokreślony. Może być ona wypowiedziana w drodze notyfikacji przez każdą ze Stron. W takim przypadku utraci moc po upływie sześciu miesięcy od dnia otrzymania noty informującej o wypowiedzeniu.
4. W przypadku wypowiedzenia niniejszej Umowy informacje niejawne przekazane lub wytworzone na jej podstawie będą nadal chronione zgodnie z jej postanowieniami.

Podpisano w Nowym Jorku dnia 20 września 2022 roku w dwóch jednobrzmiących egzemplarzach, każdy w językach polskim, portugalskim i angielskim, przy czym wszystkie teksty są jednakowo autentyczne. W przypadku rozbieżności przy ich interpretacji tekst w języku angielskim będzie uważany za rozstrzygający.

Z upoważnienia Rządu Rzeczypospolitej Polskiej

Z upoważnienia Rządu Federacyjnej Republiki Brazylii



Stwierdzam zgodność
fotokopii z oryginałem/~~odpisem~~

Warszawa, dnia 25/10/2022 r.

Sławomir Majszyk

Sławomir Majszyk
Zastępca Dyrektora
DEPARTAMENT PRAWNO-TRAKTATOWY

AGREEMENT

between the Government of the Republic of Poland and the Government of the Federative Republic of Brazil on the Exchange and Mutual Protection of Classified Information

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

or individually referred as a "Party"

Having due regard for the necessity of guaranteeing the effective protection of Classified Information exchanged between the Parties or originated during the course of cooperation,

Being guided by the intention to adopt uniform regulations for both Parties in the scope of the protection of Classified Information,

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

Have agreed as follows:

ARTICLE 1
SCOPE 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.

2. This Agreement shall be applicable to any contracts or agreements involving Classified Information that will be conducted or concluded between the Parties - 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 national law of either Party and this Agreement;

2) **National Security Authority** – the national authority referred to in Article 4 responsible for the security of Classified Information exchanged under this Agreement;

3) **Originating Party** – the Party, as well as individuals, legal entities or other forms of organization, competent to originate and transmit Classified Information in accordance with the national law of its Party;

4) **Recipient Party** – the Party, as well as individuals, legal entities or other forms of organization, competent to receive Classified Information in accordance with the national law of its Party;

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

6) **Contractor** – an individual, a legal entity or other form of organization under the national law of each of the Parties, which has legal capacity to perform Classified Contracts in accordance with the provisions of this Agreement;

7) **Principal** – an individual, a legal entity or other form of organization under the national law of each of the Parties, which has legal capacity to let Classified Contracts in accordance with the provisions of this Agreement;

8) **Personnel Security Clearance** – a document issued in accordance with the national law of a Party by the National Security Authority or other authorized entity confirming that an individual has undergone security vetting and is eligible to have access to Classified Information;

9) **Facility Security Clearance** – a document issued in accordance with the national law of a Party by the National Security 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, individuals, legal entities or other forms of organization under its jurisdiction or an international organization not being a Party to this Agreement.

11) **Need-to-know** – a principle by which access to Classified Information may be granted to an individual only in connection with his or her official duties and/or for the performance of the specific task;

12) **Breach of security** – an action or an omission which is contrary to this Agreement or the national law of the Parties concerning Classified Information protection.

ARTICLE 3

SECURITY CLASSIFICATION LEVELS

1. A security classification level is granted to Classified Information in accordance to its content, pursuant to the national law of the Originating Party. The Recipient Party shall guarantee at least an equivalent level of protection of the received Classified Information pursuant to the provisions of Paragraphs 3 and 4.
2. The security classification level may be changed or removed only by the Originating Party. The Recipient Party shall be notified in writing of every change or removal of the security classification level of previously received Classified Information.
3. The Parties agree that the following security classification levels are equivalent:

THE REPUBLIC OF POLAND	THE FEDERATIVE REPUBLIC OF BRAZIL	EQUIVALENT IN ENGLISH
ŚCIŚLE TAJNE	ULTRASSECRETO	TOP SECRET
TAJNE	SECRETO	SECRET
POUFNE	RESERVADO	CONFIDENTIAL
ZASTRZEŻONE	NO EQUIVALENT	RESTRICTED

4. Information from the Republic of Poland classified as „ZASTRZEŻONE" shall be handled as „POUFNE/RESERVADO/CONFIDENTIAL" in the Federative Republic of Brazil.

ARTICLE 4

NATIONAL SECURITY AUTHORITIES

1. The National Security Authorities, responsible for the implementation and supervision of this Agreement, shall be:
    1) for the Republic of Poland: the Head of the Internal Security Agency;
    2) for the Federative Republic of Brazil: the Institutional Security Cabinet of the Presidency of the Federative Republic of Brazil (Gabinete de Segurança Institucional da Presidência da República Federativa do Brasil).
2. The Parties shall inform each other via diplomatic channels about changes of the National Security Authorities, referred to in Paragraph 1 or amendments to their competences.
3. Each Party shall provide to the other the contact data of their respective National Security Authority, in writing.

ARTICLE 5

PRINCIPLES OF CLASSIFIED INFORMATION PROTECTION

1. The Parties shall adopt every measure provided in this Agreement and subject to their national laws in order to protect Classified Information transmitted or originated as a result of cooperation between the Parties, including information originated in connection with performance of Classified Contracts.
2. The Recipient Party shall use Classified Information exclusively for the purposes for which it has been exchanged.
3. 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 national law 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

1. In the scope of this Agreement, the Parties shall recognize Personnel Security Clearances and Facility Security Clearances issued in accordance with the national law of the other Party.
2. Upon request, the National Security Authorities shall assist each other with Personnel Security Clearance and Facility Security Clearance procedures.
3. The National Security Authorities shall inform each other about any modification regarding to their Personnel Security Clearances or Facility Security Clearances.

ARTICLE 7
CLASSIFIED CONTRACTS

1. Before concluding a Classified Contract connected with access to information classified as POUFNE /RESERVADO/ CONFIDENTIAL or above, the Principal shall apply to its National Security Authority to request that the National Security Authority of the other Party issue a certificate that the Contractor is a holder of a valid Facility Security Clearance relevant to the security classification level of the Classified Information the Contractor is to have access to.
2. Issuing the certificate referred to in Paragraph 1 shall be tantamount to a guarantee that necessary actions have been conducted in order to declare that the Contractor meets the criteria in the scope of the protection of Classified Information defined in the national law of the Party in the territory of the State of which it is located.
3. Classified Information shall not be released to the Contractor until the receipt of the certificate referred to in Paragraph 1.
4. The Principal shall transmit to the Contractor a facility security instruction necessary to perform a Classified Contract, which is an integral part of every

Classified Contract. The facility security instruction contains provisions on the security requirements, in particular:

1) the list of types of Classified Information related to a given Classified Contract, including their security classification levels;
2) the rules for granting security classification levels to information originated during the performance of a given Classified Contract;
3) all procedures for handling Classified Information provided to the Contractor or generated during the performance of a Classified Contract.

5. The Principal shall put forward a copy of the facility security instruction to the National Security Authority of its Party, which shall transmit it to the National Security 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 or other channels which ensure its protection against unauthorized disclosure, agreed upon between the National Security Authorities of the Parties. The Recipient Party shall confirm in writing the receipt of Classified Information.
2. 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 pursuant to the national law of the Recipient Party. Reproduced or translated information shall be placed under the same protection as the original information. The number of copies or translations shall be reduced to that required for official purposes.
2. Information classified as ŚCIŚLE TAJNE / ULTRASSECRETO/ TOP SECRET shall be reproduced or translated only after obtaining a prior written consent issued by the Originating Party.

ARTICLE 10

DESTRUCTION OF CLASSIFIED INFORMATION

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

ARTICLE 11

VISITS

1. Persons arriving on a visit to the territory of the State of the other Party and facilities of the other Party shall be allowed access to Classified Information only after receiving a prior written consent issued by the National Security Authority of the hosting Party.

2. The National Security Authority of the visiting Party shall apply with a request for a visit to the National Security Authority of the hosting Party at least 30 days prior to the planned visit referred to in Paragraph 1.

3. The request referred to in Paragraph 2 shall include the following data that will be only used for the purpose of the visiting:

   1) purpose, date and program of the visit;

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

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

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

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

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

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

4. The National Security 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 National Security Authorities of the Parties, the dates of the visits shall be arranged directly between visiting and hosting Parties, in accordance with the conditions agreed upon.

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

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

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

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

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

5) the 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.

ARTICLE 12
BREACH OF SECURITY

1. 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 National Security Authority of the Party in the territory of the State of which the breach or suspicion of the breach has occurred.
2. Every breach of security or a suspicion of a breach of security shall be investigated pursuant to the national law of the Party in the territory of the State of which it has occurred.
3. In case of a breach of security the National Security Authority of the Party in the territory of the State of which the breach has occurred shall inform the National Security Authority of the other Party in writing about the fact, circumstances of the breach and the outcome of the actions referred to in Paragraph 2.

4. The National Security Authorities of the Parties shall cooperate in the actions referred to in Paragraph 2, upon the request of one of them.
5. If a breach of security has occurred in the territory of the State of the Third Party, the National Security Authority of the Party who transmitted Classified Information shall take all the measures referred to in Paragraphs 1, 2 and 3 in cooperation with the Third Party.

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 provided.

ARTICLE 14
COSTS

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

ARTICLE 15
CONSULTATIONS

1. The National Security Authorities of the Parties shall notify each other of any amendments to their national law on the protection of Classified Information concerning implementation of this Agreement.
2. The National Security Authorities 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. Representatives of the National Security Authorities may visit each other in order to discuss the procedures for the protection of Classified Information.

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

ARTICLE 16
SETTLEMENT OF DISPUTES

1. Any disputes concerning the implementation or interpretation of this Agreement shall be settled by direct consultations between the National Security 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 through diplomatic channels.

ARTICLE 17
FINAL PROVISIONS

1. This Agreement shall enter into force in accordance with the national law of each of the Parties, which shall be confirmed by exchange of notes. The Agreement shall enter into force on the first day of the second month following the receipt of the latter note.
2. This Agreement may be amended on the basis of written consent of both Parties. Such amendments shall enter into force in accordance with the provisions of Paragraph 1.
3. This Agreement is concluded for an unlimited period of time. It may be terminated by either Party by giving written notice to the other Party. In such case, this Agreement shall expire after six months following the receipt of the termination notice.
4. In case of termination of this Agreement, Classified Information exchanged or originated on the basis of this Agreement shall be protected in accordance with the provisions thereof.

Done at New York on 20th September 2022, in two original copies, each in the Polish, Portuguese and English languages, all texts being equally authentic. In case of divergence of interpretation, the English text shall prevail.

For the Government

of the Republic of Poland

For the Government

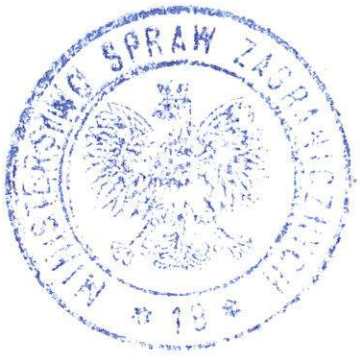
of the Federative Republic of Brazil

Stwierdzam zgodność
fotokopii z oryginałem/~~odpisem~~

Warszawa, dnia 25/10/2022 r.

Sławomir Majszyk

Sławomir Majszyk
Zastępca Dyrektora
DEPARTAMENT PRAWNO-TRAKTATOWY



ACORDO ENTRE O GOVERNO DA REPÚBLICA DA POLÔNIA E O GOVERNO DA REPÚBLICA FEDERATIVA DO BRASIL SOBRE TROCA E PROTEÇÃO MÚTUA DE INFORMAÇÕES CLASSIFICADAS

O Governo da República da Polônia,

e

o Governo da República Federativa do Brasil

doravante denominados "Partes",

ou individualmente referidos como "Parte"

Tendo a devida consideração à necessidade de garantir a proteção efetiva das Informações Classificadas trocadas entre as Partes originadas no decurso da cooperação,

Orientados pela intenção de adotar normas uniformes para ambas as Partes no âmbito da proteção de Informações Classificadas,

Em respeito às regras vinculativas do direito internacional e da legislação nacional das Partes,

Concordam com o seguinte:

ARTIGO 1
ESCOPO DO ACORDO

1. O objetivo deste Acordo é assegurar a proteção das Informações Classificadas que são geradas em decorrência da cooperação ou trocadas entre as Partes.

2. Este Acordo será aplicável a quaisquer contratos ou acordos envolvendo Informação Classificada que serão conduzidos ou celebrados entre as Partes, bem como a quaisquer atividades conduzidas entre elas.

ARTIGO 2
DEFINIÇÕES

Para os fins deste Acordo, as seguintes definições representam:

1) Informações Classificadas - qualquer informação, independentemente da sua forma, suporte e modo de registro, bem como objetos ou quaisquer partes deles, também em processo de geração, que requeiram proteção contra divulgação não autorizada de acordo com a legislação nacional de cada Parte e com este Acordo;

2) Autoridade Nacional de Segurança - a autoridade nacional referida no Artigo 4, responsável pela segurança da Informação Classificada nos termos deste Acordo;

3) Parte Originadora - a Parte, bem como indivíduos, entidades legais ou outras formas de organização, competentes para originar e transmitir Informações Classificadas de acordo com a legislação nacional de sua Parte;

4) Parte Receptora - a Parte, bem como indivíduos, entidades legais ou outras formas de organização, competentes para receber Informações Classificadas de acordo com a legislação nacional de sua Parte;

5) Contrato Classificado - um contrato cuja execução envolve o acesso a Informações Classificadas ou que tenha origem neste tipo de informação;

6) Contratado - uma pessoa física, jurídica ou outra forma de organização nos termos da legislação nacional de cada uma das Partes, que tem capacidade legal para executar Contratos Classificados de acordo com as disposições deste Acordo;

7) Contratante - uma pessoa física, jurídica ou outra forma de organização nos termos da legislação nacional de cada uma das Partes que tem capacidade legal para celebrar Contratos Classificados em conformidade com as disposições deste Acordo;

8) Credencial de Segurança de Pessoas- documento emitido de acordo com a legislação nacional de cada Parte por sua respectiva Autoridade de Segurança Nacional ou outra entidade autorizada, confirmando que um indivíduo passou por verificação de segurança e é elegível para ter acesso a Informações Classificadas;

9) Credencial de Segurança de Instalações - documento emitido de acordo com a legislação nacional de cada Parte por sua Autoridade Nacional de Segurança ou outra entidade autorizada, confirmando que um Contratado tem capacidade para proteger as Informações Classificadas; no caso de proprietários individuais atuando como contratados, uma Credencial de Segurança de Pessoas será equivalente a uma Credencial de Segurança das Instalações;

10) Terceira Parte - qualquer Estado, indivíduo, entidade legal ou outras formas de organização sob sua jurisdição ou uma organização internacional que não seja Parte deste Acordo.

11) Necessidade de conhecer - princípio pelo qual o acesso à Informação Classificada pode ser concedido a pessoa física apenas em relação às suas funções oficiais e/ou para o desempenho de determinada tarefa específica;

12) Quebra de Segurança - ação ou omissão contrária a este Acordo ou à legislação nacional das Partes com relação à proteção de Informações Classificadas.

ARTIGO 3

NÍVEIS DE CLASSIFICAÇÃO DE SEGURANÇA

1. Um Nível de Classificação de Segurança é atribuído às Informações Classificadas de acordo com seu conteúdo, nos termos da legislação nacional da Parte de Origem. A Parte Receptora deverá garantir, no mínimo, o mesmo nível equivalente de proteção das Informações Classificadas recebidas de acordo os Parágrafos 3 e 4.

2. O Nível de Classificação de Segurança pode ser alterado ou removido apenas pela Parte Originadora. A Parte Receptora deverá ser notificada por escrito de cada alteração ou remoção do Nível de Classificação de Segurança das Informações Classificadas que tenham sido previamente recebidas.

3. As Partes concordam que os seguintes Níveis de Classificação de Segurança são equivalentes:

REPÚBLICA DA POLÔNIA	**REPÚBLICA FEDERATIVA DO BRASIL**	**EQUIVALENTE EM INGLÊS**
ŚCIŚLE TAJNE	ULTRASSECRETO	TOP SECRET
TAJNE	SECRETO	SECRET
POUFNE	RESERVADO	CONFIDENTIAL
ZASTRZEŻONE	SEM EQUIVALÊNCIA	RESTRICTED

4. Informações da República da Polônia classificadas como "ZASTRZEŻONE" serão tratadas como "POUFNE/RESERVADO/ CONFIDENTIAL" pela República Federativa do Brasil.

ARTIGO 4

AUTORIDADE NACIONAL DE SEGURANÇA

1. As Autoridades Nacionais de Segurança, responsáveis pela implementação e supervisão deste Acordo, são:

1. pela República da Polônia: o Chefe da Agência de Segurança Interna;

2. pela República Federativa do Brasil: o Gabinete de Segurança Institucional da Presidência da República Federativa do Brasil.

2. As Partes deverão informar-se mutuamente, por via diplomática, sobre as alterações das Autoridades de Segurança Nacionais referidas no parágrafo 1 ou sobre as alterações relativas às suas competências.

3. Cada Parte disponibilizará à outra os dados de contato de sua respectiva Autoridade Nacional de Segurança, por escrito.

ARTIGO 5
PRINCÍPIOS DE PROTEÇÃO DE INFORMAÇÕES CLASSIFICADAS

1. As Partes adotarão todas as medidas previstas neste Acordo e sujeitas às suas legislações nacionais a fim de proteger as Informações Classificadas transmitidas ou originadas como resultado da cooperação entre as Partes, incluindo as informações originadas em decorrência de execução de Contratos Classificados.

2. A Parte Receptora deverá utilizar as Informações Classificadas exclusivamente para os fins para os quais foram trocadas.

3. O acesso às Informações Classificadas será concedido apenas às pessoas que tenham necessidade de conhecê-las e que tenham sido autorizadas a acessar essas informações de acordo com a legislação nacional da Parte Receptora.

4. A Parte Receptora não poderá divulgar as informações referidas no Parágrafo 1 a uma Terceira Parte sem consentimento prévio por escrito da Parte Originadora.

ARTIGO 6
CREDENCIAMENTO DE SEGURANÇA

1. No âmbito do presente Acordo, as Partes reconhecerão as Credenciais de Segurança de Pessoal e as Credenciais de Segurança das Instalações emitidas de acordo com a legislação nacional da outra Parte.

2. Mediante solicitação, as Autoridades Nacionais de Segurança devem auxiliar-se quanto aos procedimentos relacionados ao Credenciamento de Segurança de Pessoal e de Instalações.

3. As Autoridades Nacionais de Segurança devem informar-se sobre qualquer modificação relativa às suas Credenciais de Segurança de Pessoal ou Credenciais de Segurança das Instalações.

ARTIGO 7
CONTRATOS CLASSIFICADOS

1. Antes de concluir um Contrato Classificado relacionado com o acesso a informações classificadas como POUFNE / RESERVADO / CONFIDENCIAL ou superior, a Contratante deverá solicitar à sua Autoridade Nacional de Segurança que seja demandado à Autoridade Nacional de Segurança da outra Parte a emissão de um certificado que comprove que a Contratada é titular de autorização de segurança de instalação válida relevante para o nível de classificação de segurança das informações classificadas que o contrato requer.

2. A emissão do certificado referido no parágrafo 1 será equivalente à garantia de que as ações necessárias foram realizadas com o objetivo de declarar que a Contratada cumpre os critérios no âmbito da proteção de Informações Classificadas definidos na legislação nacional da Parte em território do Estado em que está localizada.

3. As Informações Classificadas não serão divulgadas ao Contratado até o recebimento do certificado referido no Parágrafo 1.

4. O Contratante deve transmitir ao Contratado uma instrução de segurança de instalação necessária para executar um Contrato Classificado, que é parte integrante de todo Contrato Classificado. A instrução de segurança de instalação contém disposições sobre os requisitos de segurança, em especial:

1) a lista de tipos de Informações Classificadas relacionadas a um determinado Contrato Classificado, incluindo seus níveis de classificação de segurança;

2) as regras para atribuição de níveis de classificação de segurança às informações originadas durante a execução de um determinado Contrato Classificado;

3) todos os procedimentos para lidar com as Informações Classificadas fornecidas à Contratada ou geradas durante a execução de um Contrato Classificado.

5. O Contratante apresentará uma cópia da instrução de segurança das instalações à Autoridade Nacional de Segurança de sua Parte, a qual deverá transmiti-la à Autoridade Nacional de Segurança da Parte do Contratado.

6. A execução de um Contrato Classificado pela parte relacionada com o acesso às Informações Classificadas será possível desde que o Contratado cumpra os critérios necessários para a proteção das Informações Classificadas, nos termos da instrução de segurança das instalações.

7. Todos os subcontratados devem cumprir as mesmas condições para a proteção das Informações Classificadas estabelecidas para o Contratado.

ARTIGO 8
TRANSMISSÃO DA INFORMAÇÃO CLASSIFICADA

1. As Informações Classificadas serão transmitidas por via diplomática ou outros canais que assegurem sua proteção contra divulgação não autorizada, acordados entre as Autoridades Nacionais de Segurança das Partes. A Parte Receptora deverá confirmar por escrito o recebimento das Informações Classificadas.

2. As autoridades competentes para trocar Informações Classificadas com base em outros acordos internacionais realizados entre as Partes podem trocar informações classificadas diretamente.

ARTIGO 9

REPRODUÇÃO OU TRADUÇÃO DA INFORMAÇÃO CLASSIFICADA

1. A reprodução ou tradução das Informações Classificadas será realizada de acordo com a legislação nacional de cada uma das Partes. As informações reproduzidas ou traduzidas devem ser colocadas sob a mesma proteção que as informações originais. O número de cópias ou traduções deverá ser reduzido ao exigido para fins oficiais.

2. As informações classificadas como ŚCIŚLE TAJNE/ ULTRASSECRETO / TOP SECRET devem ser reproduzidas ou traduzidas somente após a obtenção de consentimento prévio por escrito emitido pela Parte Originadora.

ARTIGO 10

DESTRUIÇÃO DE INFORMAÇÃO CLASSIFICADA

1. As Informações Classificadas deverão ser destruídas de acordo com a legislação nacional da Parte Receptora, de forma a impossibilitar sua reconstrução parcial ou total.

2. As Informações Classificadas como ŚCIŚLE TAJNE/ ULTRASSECRETO / TOP SECRET não podem ser destruídas, devem ser devolvidas à Parte Originadora.

ARTIGO 11

VISITAS

1. As pessoas que chegam para visitar as instalações da outra Parte naquele território só terão acesso às Informações Classificadas após receber o consentimento prévio por escrito da Autoridade Nacional de Segurança da Parte anfitriã.

2. A Autoridade Nacional de Segurança da Parte visitante deve solicitar a visita à Autoridade Nacional de Segurança da Parte anfitriã com pelo menos 30 dias antes da visita planejada referida no parágrafo 1.

3. O pedido a que se refere o parágrafo 2 deve conter os seguintes dados que apenas serão utilizados para efeito da visita:

1) motivo, data e programação da visita;

2) nome e sobrenome do visitante, data e local de nascimento, nacionalidade, todas as cidadanias e passaporte ou outro número de documento de identificação;

3) cargo do visitante juntamente com o nome da entidade que representa;

4) nível de classificação de segurança e validade da Credencial de Segurança do visitante;

5) nome e endereço da unidade a ser visitada;

6) nome, sobrenome e cargo da pessoa que será visitada;

7) bem como a data, assinatura e selo oficial da Autoridade Nacional de Segurança do visitante.

4. As Autoridades Nacionais de Segurança das Partes podem acordar em estabelecer listas de pessoas autorizadas a fazer visitas recorrentes relacionadas com a implementação de algum projeto, programa ou Contrato Classificado específico. As listas devem conter os dados especificados no parágrafo 3 e são válidas por um período de 12 meses. Uma vez que tais listas tenham sido aprovadas pelas Autoridades Nacionais de Segurança das Partes, as datas das visitas serão combinadas diretamente entre as Partes visitante e anfitriã, de acordo com as condições acordadas.

5. A fim de proteger os dados pessoais referidos no Parágrafo 3, transmitidos em conexão com as disposições dos Parágrafos 1 e 4, as seguintes disposições devem ser aplicadas, de acordo com a legislação nacional das Partes:

1) os dados pessoais recebidos pela Parte anfitriã devem ser utilizados exclusivamente para o fim e nas condições definidas pela Parte que o transmite;

2) os dados pessoais devem ser armazenados pela Parte anfitriã apenas pelo período necessário para atingir os objetivos de seu processamento;

3) no caso de dados pessoais transmitidos contra a legislação nacional da Parte, a Parte que os transmite deve notificar a Parte anfitriã, que é obrigada a remover os dados de forma a eliminar sua reconstrução parcial ou total;

4) a Parte que transmite os dados pessoais deve assumir a responsabilidade pela sua correção e, caso os dados pareçam inválidos ou incompletos, deve notificar a Parte que os recebe, o qual é obrigada a corrigir ou remover os dados;

5) a Parte que transmite os dados pessoais e a Parte que os recebe são obrigadas a registrar sua transmissão, recebimento e retirada;

6) a Parte que transmite os dados pessoais e a Parte que os recebe são obrigadas a proteger os dados pessoais processados de forma eficiente contra sua divulgação a pessoas não autorizadas, modificações não autorizadas dos dados, sua perda, dano ou destruição.

ARTIGO 12
QUEBRA DE SEGURANÇA

1. As informações sobre cada violação de segurança ou suspeita de violação de segurança em relação às Informações Classificadas da Parte de Origem ou às Informações Classificadas originadas como resultado da cooperação das Partes devem ser imediatamente comunicadas à Autoridade Nacional de Segurança da Parte no território do Estado em que ocorreu a violação ou suspeita de violação.

2. Toda quebra de segurança ou suspeita de quebra de segurança deve ser investigada de acordo com a legislação nacional da Parte no território do Estado em que ocorreu.

3. Em caso de quebra de segurança, a Autoridade Nacional de Segurança da Parte no território do Estado em que a violação ocorreu deve informar à Autoridade Nacional de Segurança da outra Parte, por escrito, sobre o fato, as circunstâncias da violação e o resultado das ações a que se refere o parágrafo 2.

4. As Autoridades Nacionais de Segurança das Partes cooperarão nas ações a que se refere o § 2º, a pedido de uma delas.

5. Se uma quebra de segurança tiver ocorrido no território de uma Terceira Parte, a Autoridade Nacional de Segurança da Parte que transmitiu as Informações Classificadas deverá tomar todas as medidas referidas nos Parágrafos 1, 2 e 3 em cooperação com a Terceira Parte.

ARTIGO 13
IDIOMAS

No âmbito da implementação das disposições do presente Acordo, as Partes deverão utilizar o inglês ou suas línguas oficiais, situação na qual deverá ser fornecida a tradução para a língua oficial da outra Parte ou para o inglês.

ARTIGO 14
CUSTOS

Cada Parte deverá cobrir seus próprios custos decorrentes da implementação das disposições deste Acordo.

ARTIGO 15
CONSULTAS

1. As Autoridades Nacionais de Segurança das Partes deverão notificar-se sobre quaisquer emendas às suas legislações nacionais afetas à proteção de Informações Classificadas relativas à implementação deste Acordo.

2. As Autoridades Nacionais de Segurança das Partes poderão consultar-se mutualmente, mediante pedido de um deles, a fim de assegurar cooperação estreita na implementação das disposições do presente Acordo.

3. Os representantes das Autoridades Nacionais de Segurança podem visitar-se para deliberar acerca dos procedimentos de proteção das Informações Classificadas.

4. A fim de assegurar uma eficaz cooperação, que é o objetivo deste Acordo, e no âmbito da autoridade reconhecida pela legislação nacional de suas Partes, as Autoridades Nacionais de Segurança podem, se necessário, definir por escrito outros detalhes técnicos ou organizacionais.

ARTIGO 16
RESOLUÇÃO DE CONTROVÉRSIAS

1. Quaisquer controvérsias relativas à implementação ou interpretação deste Acordo serão resolvidas por consultas diretas entre as Autoridades Nacionais de Segurança das Partes.

2. Se não for possível chegar à solução de controvérsia da maneira prevista no parágrafo 1, a controvérsia será resolvida por via diplomática.

ARTIGO 17
DISPOSIÇÕES FINAIS

1. O presente Acordo entrará em vigor de acordo com a legislação nacional de cada uma das Partes, o que será confirmado por troca de notas. O Acordo entrará em vigor no primeiro dia do segundo mês seguinte ao recebimento da última notificação.

2. Este Acordo pode ser alterado com base no consentimento por escrito de ambas as Partes. Essas Emendas entrarão em vigor conforme de acordo com as disposições do parágrafo 1.

3. O presente Acordo tem validade por período ilimitado. Pode ser denunciado por qualquer das Partes mediante notificação por escrito à outra Parte. Nesse caso, o presente Acordo deverá expirar seis meses após o recebimento da notificação de denúncia.

4. Em caso de denúncia deste Acordo, as Informações Classificadas trocadas ou originadas com base neste Acordo serão protegidas de acordo com suas disposições.

Feito em Nova York em 20 setembro 2022, em dois exemplares originais, em polonês, português e inglês, sendo todos os textos igualmente autênticos. Em caso de divergência de interpretação, o texto em inglês prevalecerá.

PELO GOVERNO DA REPÚBLICA DA POLÔNIA

PELO GOVERNO DA REPÚBLICA FEDERATIVA DO BRASIL

Stwierdzam zgodność
fotokopii z oryginałem/~~odpisem~~

Warszawa, dnia 25/10/2022 r.

Sławomir Majszyk
Zastępca Dyrektora
DEPARTAMENT PRAWNO-TRAKTATOWY

Minister do Spraw
Unii Europejskiej

DPUE.920.1876.2021.EBK(8)
Warszawa, 29 listopada 2022 r.
Dot.:P-12436/2022/D-93467/2019/KD z 0.11.2022 r.

Pan Krzysztof Wacławek
Szef Agencji Bezpieczeństwa Wewnętrznego

Opinia
o zgodności z prawem Unii Europejskiej *umowy między Rządem Rzeczypospolitej Polskiej a Rządem Federacyjnej Republiki Brazylii o wymianie i wzajemnej ochronie informacji niejawnych, podpisanej w Nowym Jorku dnia 20 września 2022 r.,* 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 wyrazami szacunku

z upoważnienia Ministra do Spraw Unii Europejskiej

Karolina Rudzińska
Podsekretarz Stanu w Kancelarii Prezesa Rady Ministrów
/podpisano kwalifikowanym podpisem elektronicznym/

Telefon: +48 22 694 7540
adres email: SMUE@kprm.gov.pl
www.gov.pl/web/premier

Kancelaria Prezesa Rady Ministrów
Al. Ujazdowskie 1/3
00-583 Warszawa