SEJM
RZECZYPOSPOLITEJ POLSKIEJ
IX kadencja
Prezes Rady Ministrów
RM-06111-278-22

Druk nr 2946
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 Radą Federalną Konfederacji Szwajcarskiej o wzajemnej ochronie informacji niejawnych, podpisaną w Thun dnia 7 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 7 września 2022 roku w Thun została podpisana Umowa między Rządem Rzeczypospolitej Polskiej a Radą Federalną Konfederacji Szwajcarskiej o 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 7 września 2022 r. w Thun Umowa między Rządem Rzeczypospolitej Polskiej a Radą Federalną Konfederacji Szwajcarskiej o wzajemnej ochronie informacji niejawnych reguluje prawne aspekty współpracy polskich i szwajcarskich podmiotów upoważnionych do przetwarzania informacji niejawnych, zgodnie ze swoim prawem krajowym. Po wejściu w życie niniejsza Umowa stanowić będzie podstawę do nawiązania ściślejszej współpracy w zakresie obronności, bezpieczeństwa wewnętrznego, jak również wpłynie na ożywienie stosunków gospodarczych, ponieważ umożliwi polskim i szwajcarskim przedsiębiorcom zawieranie kontraktów związanych z dostępem do informacji niejawnych lub ich wytwarzaniem.

II. Wskazanie różnic między dotychczasowym i projektowanym stanem prawnym

Umowa między Rządem Rzeczypospolitej Polskiej a Radą Federalną Konfederacji Szwajcarskiej o wzajemnej ochronie informacji niejawnych będzie pierwszą tego typu umową zawartą z tym państwem.

W artykule 1 zawarto definicje kluczowych dla postanowień niniejszej Umowy pojęć, w tym „informacji niejawnych", „właściwych organów" i „uprawnionych podmiotów" oraz „zasady ograniczonego dostępu".

W artykule 2 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 szwajcarskiej odpowiednika klauzuli „Ściśle tajne", w ustępie 5 tego artykułu uregulowano zasady postępowania z tak oznaczonymi polskimi informacjami niejawnymi.

W artykule 3 wskazane zostały organy właściwe do realizacji postanowień niniejszej Umowy, którymi są: w Rzeczypospolitej Polskiej – Szef Agencji Bezpieczeństwa Wewnętrznego, w Konfederacji Szwajcarskiej – Zarząd Bezpieczeństwa Informacyjnego

i Ochrony Obiektowej. W ustępie 2 tego artykułu Strony uzgodniły, że właściwe organy mogą zawierać pisemne szczegółowe porozumienia techniczne lub organizacyjne.

W artykule 4 określono zasady ochrony informacji niejawnych, zgodnie z którymi są one udostępniane wyłącznie tym osobom, które zgodnie z prawem krajowym zostały uprawnione do dostępu do nich – z zachowaniem zasady ograniczonego dostępu. Ponadto na Strony został nałożony obowiązek zapewnienia informacjom niejawnym poziomu ochrony odpowiadającego poziomowi stosowanemu względem własnych informacji niejawnych o równorzędnej klauzuli tajności. Ponadto w ustępie 6 tego artykułu Strony uzgodniły, że w przypadku braku innych dwustronnych lub wielostronnych umów dotyczących wymiany informacji niejawnych w ramach współpracy organów policyjnych lub granicznych czy służb wywiadowczych, współpraca ta będzie odbywała się zgodnie z postanowieniami niniejszej Umowy.

W artykule 5 zawarto regulacje niezbędne do zawierania kontraktów niejawnych, a więc takich, których realizacja wiąże się z dostępem do informacji niejawnych bądź ich wytworzeniem. Zgodnie z ustępem 3 omawianego artykułu, zlecający przekazuje kontrahentowi wymogi bezpieczeństwa, 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 podjęciu przez kontrahenta wszelkich czynności zapewniających ochronę informacjom niejawnym, zgodnie z wymogami bezpieczeństwa określonymi w ustępie 3.

Zgodnie z postanowieniami artykułu 6 niniejszej Umowy informacje niejawne są przekazywane między Stronami w drodze dyplomatycznej. Ustęp 3 tego artykułu przewiduje możliwość przesyłania informacji niejawnych akredytowanymi systemami lub sieciami teleinformatycznymi. Zgodnie z postanowieniami ustępu 4 tego artykułu odbiór informacji niejawnych jest potwierdzany pisemnie przez odbiorcę.

W artykule 7 określono, że na powielane lub przetłumaczone informacje niejawne nanoszona jest adnotacja wskazująca, iż kopie lub tłumaczenia zawierają informacje niejawne pochodzące od Strony wytwarzającej i wymagają takiej samej ochrony jak ich oryginały. Ponadto ustęp 2 tego artykułu reguluje kwestie kopiowania i tłumaczenia informacji niejawnych oznaczonych klauzulą „Tajne”, które mogą zostać wykonane wyłącznie po uzyskaniu pisemnej zgody Strony wytwarzającej.

Zgodnie z postanowieniami artykułu 8 informacje niejawne o klauzuli „Tajne” nie są niszczone, ale są zwracane Stronie wytwarzającej. W przypadku informacji niejawnych, oznaczonych niższą niż wymieniona klauzulą tajności, niszczenie odbywa się zgodnie z prawem krajowym Strony otrzymującej.

W artykule 9 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 10 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.

W artykule 11 niniejszej Umowy ustalono, że każda Strona pokrywa koszty własne związane z jej realizacją.

Artykuł 12 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 po uzyskaniu zgody, przedstawiciele jednej ze Stron składają wizyty na terytorium drugiej Strony w celu omówienia procedur służących ochronie przekazywanych informacji niejawnych.

Artykuł 13 reguluje wzajemne uznawanie przez Strony poświadczeń bezpieczeństwa i świadectw bezpieczeństwa przemysłowego, wydanych zgodnie z ich prawem krajowym. Ponadto Strony zobowiązały się do niezwłocznego informowania o wszelkich zmianach dotyczących uznanych lub wydanych poświadczeń bezpieczeństwa oraz świadectw bezpieczeństwa przemysłowego.

W artykule 14 niniejszej Umowy przewidziano także tryb rozwiązywania sporów dotyczących interpretacji jej postanowień.

Ponadto w Umowie określono procedurę wejścia w życie, jak również czas jej obowiązywania oraz tryb wypowiedzenia (artykuł 15).

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 Konfederacją Szwajcarską. 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.

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 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 zasady 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

Radą Federalną Konfederacji Szwajcarskiej

o wzajemnej ochronie informacji niejawnych

Rząd Rzeczypospolitej Polskiej i Rada Federalna Konfederacji Szwajcarskiej

zwane dalej „Stronami",

mając na uwadze zagwarantowanie wzajemnej ochrony wszystkich informacji niejawnych,

które zgodnie z prawem krajowym każdej ze Stron zostały jako takie zaklasyfikowane i przekazane drugiej Stronie,

kierując się potrzebą stworzenia regulacji w zakresie wzajemnej ochrony informacji niejawnych, które będą obowiązywać w odniesieniu do wszelkiej wspólnej działalności, związanej z ich wymianą

uzgodniły, co następuje:

ARTYKUŁ 1
DEFINICJE

Dla celów niniejszej Umowy:

1) „informacje niejawne" - oznaczają wszelkie informacje niezależnie od formy i sposobu ich utrwalenia, jak również przedmioty lub dowolne ich części, które wymagają ochrony przed nieuprawnionym ujawnieniem i zostały jako takie oznaczone;
2) „właściwe organy" - oznaczają organy, o których mowa w artykule 3 ustęp 1 niniejszej Umowy, właściwe w zakresie ochrony informacji niejawnych;
3) „uprawnione podmioty" - oznaczają osoby fizyczne, osoby prawne lub jednostki organizacyjne nieposiadające osobowości prawnej, które zgodnie z prawem krajowym swojej Strony są właściwe do wytwarzania, otrzymywania, przechowywania, ochrony i wykorzystywania informacji niejawnych;
4) „Strona wytwarzająca" - oznacza właściwe organy i uprawnione podmioty, które wytwarzają, przekazują lub przesyłają informacje niejawne;
5) „Strona otrzymująca" – oznacza właściwe organy i uprawnione podmioty, którym informacje niejawne są przekazywane lub przesyłane;
6) „kontrakt niejawny" – oznacza umowę, której realizacja związana jest z dostępem do informacji niejawnych lub wytworzeniem takich informacji;
7) „kontrahent" – oznacza osobę fizyczną, osobę prawną lub jednostkę organizacyjną, która posiada zdolność do zawierania kontraktów niejawnych;
8) „zlecający" – oznacza osobę fizyczną, osobę prawną lub jednostkę organizacyjną, która posiada zdolność do zlecania kontraktów niejawnych;
9) „zasada ograniczonego dostępu" – oznacza konieczność dostępu do informacji niejawnych w celu realizacji zadań służbowych;
10) „poświadczenie bezpieczeństwa" – oznacza dokument potwierdzający, że wobec osoby przeprowadzone zostało postępowanie sprawdzające oraz, że jest uprawniona do dostępu do informacji niejawnych oznaczonych

klauzulą POUFNE /VERTRAULICH/ CONFIDENTIEL/ CONDITENZIALE/ CONFIDENTIAL lub wyższą, wydany zgodnie z jej prawem krajowym;

11) „świadectwo bezpieczeństwa przemysłowego" – oznacza dokument potwierdzający, że kontrahent posiada zdolność do ochrony informacji niejawnych oznaczonych klauzulą POUFNE /VERTRAULICH/ CONFIDENTIEL/ CONDITENZIALE/ CONFIDETIAL lub wyższą, wydany zgodnie z jego prawem krajowym;

12) „strona trzecia" – oznacza państwo, w tym wszelkie podmioty publiczne lub prywatne znajdujące się pod jego jurysdykcją albo organizację międzynarodową, niebędące stroną niniejszej Umowy.

ARTYKUŁ 2
KLAUZULE TAJNOŚCI

1. Informacjom niejawnym nadaje się odpowiednią do ich treści klauzulę tajności, zgodnie z prawem krajowym strony wytwarzającej. Otrzymanym informacjom niejawnym zapewnia się równorzędny poziom ochrony, zgodnie z postanowieniami ustępu 4.
2. Obowiązek, o którym mowa w ustępie 1, odnosi się również do informacji niejawnych, które powstaną w wyniku wspólnej działalności Stron, uprawnionych podmiotów, właściwych organów jak również w związku z realizacją kontraktów niejawnych.
3. Klauzula tajności może być zmieniona lub zniesiona wyłącznie przez Stronę wytwarzającą, która ją nadała. Strona otrzymująca jest niezwłocznie informowana o każdej zmianie lub zniesieniu klauzuli tajności informacji niejawnych.
4. Strony uzgadniają, że następujące klauzule tajności są równorzędne:

W RZECZYPOSPOLITEJ POLSKIEJ	W KONFEDERACJI SZWAJCARSKIEJ	ODPOWIEDNIK W JĘZYKU ANGIELSKIM
TAJNE	GEHEIM/SECRET/SEGRETO	SECRET
POUFNE	VERTRAULICH/CONFIDENTIEL/ CONFIDENZIALE	CONFIDENTIAL
ZASTRZEŻONE	INTERN/INTERNE/AD USO INTERNO	RESTRICTED

5. W przypadku przekazywania lub przesyłania i ochrony informacji niejawnych oznaczonych przez Stronę polską jako „ŚCIŚLE TAJNE", każdorazowo między właściwymi organami zawierane będą specjalne porozumienia.

ARTYKUŁ 3
WŁAŚCIWE ORGANY

1. Dla celów niniejszej Umowy właściwymi organami są:
   1) w Rzeczypospolitej Polskiej:
      Szef Agencji Bezpieczeństwa Wewnętrznego:
   2) w Konfederacji Szwajcarskiej:
      Zarząd Bezpieczeństwa Informacyjnego i Ochrony Obiektowej.
2. W celu zapewnienia skutecznej współpracy, będącej przedmiotem niniejszej Umowy i w zakresie kompetencji przyznanych im prawem krajowym, właściwe organy mogą, w razie potrzeby, zawierać pisemne szczegółowe porozumienia techniczne lub organizacyjne.

ARTYKUŁ 4
OCHRONA INFORMACJI NIEJAWNYCH

1. Strony, zgodnie z niniejszą Umową i swoim prawem krajowym, podejmą wszelkie niezbędne środki służące ochronie wymienianych informacji niejawnych.
2. Strony zapewnią informacjom niejawnym, o których mowa w ustępie 1, przynajmniej taką samą ochronę jaka obowiązuje w stosunku do własnych informacji niejawnych oznaczonych równoważną klauzulą tajności, zgodnie z artykułem 2 ustęp 4.
3. Informacje niejawne, o których mowa w ustępie 1, będą wykorzystywane wyłącznie w celach, dla których zostały przekazane lub przesłane.
4. Strona otrzymująca nie udostępnia informacji niejawnych, o których mowa w ustępie 1, stronie trzeciej bez uprzedniej pisemnej zgody Strony wytwarzającej, która nadała klauzulę tajności.
5. Informacje niejawne mogą być udostępniane tylko tym osobom, które wypełniają zasadę ograniczonego dostępu i które zostały uprawnione do dostępu do nich zgodnie z prawem krajowym Strony otrzymującej.
6. O ile inne umowy dwustronne lub wielostronne nie stanowią inaczej, wymiana informacji niejawnych pomiędzy służbami wywiadowczymi, organami policyjnymi lub granicznymi będzie odbywała się zgodnie z postanowieniami niniejszej Umowy.

ARTYKUŁ 5
KONTRAKTY NIEJAWNE

1. W przypadku zamiaru zawarcia kontraktu niejawnego zawierającego informacje oznaczone klauzulą POUFNE /VERTRAULICH/ CONFIDENTIEL/ CONDITENZIALE/ CONFIDENTIAL lub wyższą,

zlecający otrzymuje uprzednio od właściwego organu potencjalnego kontrahenta pisemne zapewnienie, że posiada on ważne świadectwo bezpieczeństwa przemysłowego.

2. Do czasu otrzymania zapewnienia, o którym mowa w ustępie 1, informacje niejawne nie będą udostępniane kontrahentowi.

3. Zlecający przekazuje kontrahentowi wymogi bezpieczeństwa niezbędne do realizacji kontraktu niejawnego, które zawierają w szczególności wykaz rodzajów informacji niejawnych i zasady nadawania klauzul tajności informacjom wytworzonym w trakcie realizacji kontraktu niejawnego.

4. Kopia dokumentu, o którym mowa w ustępie 3, jest przekazywana właściwym organom obu Stron.

5. Właściwy organ kontrahenta zapewnia, że informacje niejawne przekazywane lub przesyłane kontrahentowi lub wytwarzane w związku z realizacją kontraktu niejawnego są chronione zgodnie z wymogami bezpieczeństwa, o których mowa w ustępie 3 i jego prawem krajowym.

6. Realizacja kontraktu niejawnego w części związanej z dostępem do informacji niejawnych będzie możliwa wyłącznie po podjęciu przez kontrahenta wszelkich czynności zapewniających ochronę informacjom niejawnym, zgodnie z wymogami bezpieczeństwa, o których mowa w ustępie 3.

7. Właściwe organy zapewnią, że potencjalni podwykonawcy będą przestrzegać tych samych warunków ochrony informacji niejawnych jakie nałożono na kontrahenta.

ARTYKUŁ 6
PRZEKAZYWANIE I PRZESYŁANIE INFORMACJI NIEJAWNYCH

1. Informacje niejawne przekazywane są w drodze dyplomatycznej.

2. Właściwe organy mogą uzgodnić inne formy przekazywania informacji niejawnych zapewniające, zgodnie z ich prawem krajowym, ochronę przed nieuprawnionym ujawnieniem.
3. Informacje niejawne mogą być przesyłane za pomocą bezpiecznych systemów lub sieci teleinformatycznych, akredytowanych zgodnie z prawem krajowym każdej ze Stron.
4. Odbiór informacji niejawnych jest pisemnie potwierdzany przez odbiorcę.

ARTYKUŁ 7
POWIELANIE I TŁUMACZENIE INFORMACJI NIEJAWNYCH

1. Na wszystkie powielone lub przetłumaczone informacje niejawne jest nanoszona odpowiednia adnotacja w języku urzędowym stwierdzająca, że kopie lub tłumaczenia zawierają informacje niejawne pochodzące od Strony wytwarzającej i wymagają takiej samej ochrony ja ich oryginały.
2. Informacje niejawne oznaczone jako TAJNE/ GEHEIM/ SECRET/ SEGRETO/ SECRET są powielone lub tłumaczone wyłącznie po uzyskaniu uprzedniej pisemnej zgody Strony wytwarzającej.

ARTYKUŁ 8
NISZCZENIE INFORMACJI NIEJAWNYCH

1. Informacje niejawne oznaczone jako TAJNE/ GEHEIM/ SECRET/ SEGRETO/ SECRET nie są niszczone, lecz są one zwracane Stronie wytwarzającej.
2. Informacje niejawne oznaczone jako POUFNE/ VETRAULICH/ CONFIDENTIEL/ CONFIDENZIALE/ CONFIDENTIAL lub niższą są

niszczone zgodnie z prawem krajowym Strony otrzymującej w taki sposób, aby zapobiec ich częściowemu lub całkowitemu odtworzeniu.

ARTYKUŁ 9
WIZYTY

1. Osobom przybywającym z wizytą z terytorium jednej Strony na terytorium drugiej Strony zezwala się na dostęp do informacji niejawnych oznaczonych klauzulą POUFNE/ VETRAULICH/ CONFIDENTIEL/ CONFIDENZIALE/ CONFIDENTIAL lub wyższą wyłącznie po otrzymaniu pisemnej zgody wydanej przez właściwy organ Strony przyjmującej wizytę.
2. Przynajmniej dwadzieścia dni przed planowaną wizytą właściwy organ Strony przyjmującej otrzymuje wniosek o wizytę zgodnie z prawem krajowym i postanowieniami niniejszego artykułu. W nagłych przypadkach właściwe organy mogą uzgodnić krótszy czas informowania.
3. Wniosek o wizytę zawiera:
   1) cel, termin i program wizyty;
   2) imię i nazwisko, datę i miejsce urodzenia, obywatelstwo, numer paszportu lub dokumentu tożsamości osoby przybywającej z wizytą;
   3) stanowisko osoby przybywającej z wizytą oraz nazwę instytucji lub jednostki, którą reprezentuje;
   4) potwierdzenie posiadanego przez osobę przybywającą z wizytą poświadczenia bezpieczeństwa;
   5) nazwę i adres odwiedzanej jednostki;
   6) imię, nazwisko oraz stanowisko osoby przyjmującej wizytę.
4. Strona przyjmująca zapewni ochronę danych osobowych osób przybywających z wizytą zgodnie ze swoim prawem krajowym.

ARTYKYŁ 10

NARUSZENIE REGULACJI DOTYCZĄCYCH WZAJEMNEJ OCHRONY INFORMACJI NIEJAWNYCH

1. Wszelkie naruszenie regulacji dotyczących wzajemnej ochrony informacji niejawnych wymienianych lub wytworzonych w ramach realizacji niniejszej Umowy, jest wyjaśnianie zgodnie z prawem krajowym Strony, na terytorium której naruszenie miało miejsce.
2. Właściwe organy informują się niezwłocznie o każdym przypadku naruszenia regulacji dotyczących wzajemnej ochrony informacji niejawnych.
3. Jeśli naruszenie regulacji dotyczących wzajemnej ochrony informacji niejawnych miało miejsce na terytorium strony trzeciej, Strona, która przesłała lub przekazała informacje niejawne, podejmie we współpracy ze stroną trzecią działania, o których mowa w ustępach 1 i 2.
4. Właściwe organy niezwłocznie informują się o okolicznościach naruszenia regulacji dotyczących wzajemnej ochrony informacji niejawnych i wynikach podjętych czynności. Na wniosek właściwe organy współpracują przy czynnościach wyjaśniających.
5. W przypadku podejrzenia naruszenia regulacji dotyczących wzajemnej ochrony informacji niejawnych stosuje się postanowienia ustępów 1-4.

ARTYKUŁ 11

KOSZTY

Każda ze Stron pokrywa koszty własne wynikające z realizacji postanowień niniejszej Umowy.

ARTYKUŁ 12
KONSULTACJE

1. Właściwe organy informują się wzajemnie o wszelkich zmianach w swoim prawie krajowym, które dotyczą postanowień niniejszej Umowy.
2. W celu zapewnienia ścisłej współpracy przy realizacji postanowień niniejszej Umowy właściwe organy konsultują się w razie potrzeby.
3. Każda ze Stron pozwoli przedstawicielom właściwych organów drugiej Strony na złożenie wizyty na swoim terytorium w celu omówienia procedur związanych z ochroną informacji niejawnych przesyłanych lub przekazywanych przez drugą Stronę.

ARTYKUŁ 13
POŚWIADCZENIA BEZPIECZEŃSTWA I ŚWIADECTWA BEZPIECZEŃSTWA PRZEMYSŁOWEGO

1. Każda ze Stron uznaje poświadczenia bezpieczeństwa i świadectwa bezpieczeństwa przemysłowego wydane przez drugą Stronę.
2. Właściwe organy informują się niezwłocznie o wszelkich zmianach dotyczących wzajemnie uznanych lub wydanych poświadczeń bezpieczeństwa lub świadectw bezpieczeństwa przemysłowego.
3. Na wniosek, właściwe organy informują się wzajemnie o świadectwach bezpieczeństwa przemysłowego wydanych kontrahentom, zgodnie ze swoim prawem krajowym.

ARTYKUŁ 14
ROZSTRZYGANIE SPORÓW

1. Wszelkie spory dotyczące realizacji lub interpretacji postanowień niniejszej Umowy są rozstrzygane w drodze bezpośrednich negocjacji pomiędzy właściwymi organami.
2. Jeśli rozstrzygnięcie sporu w sposób, o którym mowa w ustępie 1, nie jest możliwe, jest on rozstrzygany w drodze dyplomatycznej.

ARTYKUŁ 15
POSTANOWIENIA KOŃCOWE

1. Strony poinformują się pisemnie w drodze dyplomatycznej o zakończeniu krajowych procedur prawnych niezbędnych do wejścia w życie Umowy.
2. Umowa niniejsza wejdzie w życie pierwszego dnia drugiego miesiąca, który nastąpi po dniu otrzymania późniejszej z not.
3. Umowa niniejsza jest zawarta na czas nieokreślony. Może zostać wypowiedziana w drodze notyfikacji przez każdą ze Stron. W takim przypadku niniejsza Umowa traci moc po upływie sześciu miesięcy od otrzymania noty informującej o wypowiedzeniu.
4. W przypadku wypowiedzenia wszelkie informacje niejawne przekazane lub przesłane albo wytworzone w ramach realizacji postanowień niniejszej Umowy będą chronione zgodnie z jej postanowieniami.
5. Umowa niniejsza może zostać zmieniona na podstawie wspólnej pisemnej zgody obu Stron. Takie zmiany wejdą w życie zgodnie z postanowieniami ustępów 1 i 2.

Podpisano w Thun dnia 7 września 2022 r. w dwóch jednobrzmiących egzemplarzach, każdy w językach polskim, niemieckim i angielskim. W przypadku rozbieżności tekst w języku angielskim będzie uważany za rozstrzygający.

Z UPOWAŻNIENIA RZĄDU RZECZYPOSPOLITEJ POLSKIEJ

Z UPOWAŻNIENIA RADY FEDERALNEJ KONFEDERACJI SZWAJCARSKIEJ

Stwierdzam zgodność
fotokopii z oryginałem~~/odpisem~~

Warszawa, dnia 29 września 2022 r.

Sławomir Majszyk

Sławomir Majszyk
Zastępca Dyrektora
DEPARTAMENT PRAWNO-TRAKTATOWY

Agreement

between

The Government of the Republic of Poland

And

The Swiss Federal Council

On the mutual protection of Classified Information

The Government of the Republic of Poland and the Swiss Federal Council (hereinafter referred to as the „Parties"),

having due regard for guaranteeing the mutual protection of all information which has been classified pursuant to the national law of each of the Parties and conveyed to the other Party,

recognizing the need to establish mutually agreed rules and regulations for the safeguarding of Classified Information in relation to all mutual cooperation in connection with the exchange thereof,

have agreed as follows:

ARTICLE 1
DEFINITIONS

For the purpose of this Agreement:

1) "Classified Information" means any information irrespective of the form and manner of recording thereof, as well as objects or any parts thereof, which requires protection against unauthorized disclosure and is marked as such;

2) "Competent Authorities" means the authorities competent in the scope of the protection of Classified Information, referred to in Article 3 Paragraph 1 of this Agreement;

3) "Authorized Bodies" means individuals, legal entities or organizational units with no legal personality competent to generate, receive, store, protect and use Classified Information in accordance with the national law of their Party;

4) "Originating Party" means the Competent authorities and Authorized Bodies which generate, convey or transmit Classified Information;

5) "Recipient Party" means the Competent Authorities or Authorized Bodies to which Classified Information is conveyed or transmitted;

6) "Classified Contract" means a contract the performance of which involves access to Classified Information or that generates such information;

7) "Contractor" means an individual, legal entity or organizational unit that has legal capacity to conclude Classified Contracts;

8) "Principal" means an individual, legal entity or organizational unit that has the legal capacity to let Classified Contracts;

9) "Need-to-Know" means the necessity to have access to Classified Information in order to be able to perform official duties and tasks;

10) "Personnel Security Clearance" means a document confirming that an individual has been cleared and is authorized to have access to Classified Information marked as POUFNE/ VETRAULICH/ CONFIDENTIEL/ CONFIDENZIALE/ CONFIDENTIAL or above, issued in accordance with its national law;

11) "Facility Security Clearance" means a document confirming that a contractor has a capability to protect Classified Information marked as POUFNE/ VETRAULICH/ CONFIDENTIEL/ CONFIDENZIALE/ CONFIDENTIAL or above, issued in accordance with its national law;

12) „Third Party" means any state or public or private entity under its jurisdiction or an international organization that is not party to this Agreement.

ARTICLE 2
SECURITY CLASSIFICATION LEVELS

1. Classified Information is granted a security classification level in accordance with its content, pursuant to the national law of the Originating Party. Received Classified Information shall be guaranteed an equivalent classification level, in accordance with the provisions of Paragraph 4.
2. The obligation referred to in Paragraph 1 also applies to Classified Information that is generated during the cooperation between the Parties, Authorized Bodies, and Competent Authorities as well as in connection with the performance of Classified Contracts.
3. The security classification level may be changed or removed only by the Originating Party which has granted it. The Recipient Party shall be notified promptly of any change or removal of the security classification level of Classified Information.
4. The Parties agree that the following classification levels are equivalent:

in the Republic of Poland	**in the Swiss Confederation**	**Equivalent in English**
TAJNE	GEHEIM/SECRET/SEGRETO	SECRET
POUFNE	VERTRAULICH/ CONFIDENTIEL/ CONFIDENZIALE	CONFIDENTIAL
ZASTRZEŻONE	INTERN/INTERNE/AD USO INTERNO	RESTRICTED

5. When conveying or transmitting and protecting Classified Information marked by the Polish side as „ŚCIŚLE TAJNE", special provision shall be arranged on a case by case basis between the Competent Authorities.

ARTICLE 3
COMPETENT AUTHORITIES

1. For the purpose of this Agreement, the Competent Authorities are:
   1) For the Republic of Poland:
      The Head of the Internal Security Agency;
   2) For the Swiss Confederation:
      The Directorate for Information Security and Facility Protection.
2. In order to ensure effective cooperation being the subject of this Agreement and within the scope of competences acknowledged by their national law, the Competent Authorities may, if necessary, make detailed technical or organizational arrangements in writing.

ARTICLE 4
PROTECTION OF CLASSIFIED INFORMATION

1. In accordance with this Agreement and their national law, the Parties shall adopt every measure necessary aimed at the protection of exchanged Classified Information.
2. The Parties shall guarantee at least the same protection of the Classified Information referred to in Paragraph 1 as applies to their own Classified Information with an equivalent classification level in accordance with Article 2 Paragraph 4.
3. The Classified Information referred to in Paragraph 1 shall be used exclusively for the purposes it was conveyed or transmitted for.
4. The Recipient Party shall not release the Classified Information referred to in Paragraph 1 to a Third Party without prior written consent of the Originating Party that has granted a classification level.

5. 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.

6. The exchange of Classified Information between the Intelligence Services and Police or Border Authorities shall be conducted pursuant to the provisions of this Agreement, unless other bilateral or multirateral Agreements stipulate otherwise.

ARTICLE 5
CLASSIFIED CONTRACT

1. When intending to conclude a Classified Contract including information classified as POUFNE/ VERTRAULICH/ CONFIDENTIEL CONFIDENZIALE/ CONFIDENTIAL or above, the Principal shall first obtain a written assurance from the Competent Authority of the potential contractor that it holds a valid Facility Security Clearance.

2. Before the assurance referred to in Paragraph 1 is obtained, Classified Information shall not be released to a Contractor.

3. The Principal shall notify the Contractor of the security requirements necessary to perform a Classified Contract, including the list of types of Classified Information and the rules for granting security classification levels to information generated during the performance of a Classified Contract.

4. A copy of the document referred to in Paragraph 3 shall be sent to the Competent Authorities of both Parties.

5. The Competent Authority of the Contractor shall ensure that Classified Information conveyed or transmitted to it or generated in connection with the performance of a Classified Contract shall be protected in accordance with the security requirements referred to in Paragraph 3 and its national law.

6. The performance of that part of a Classified Contract related to access to Classified Information shall be allowed only after all necessary measures

have been taken by the Contractor to ensure the protection of Classified Information in accordance with the security requirements referred to in Paragraph 3.

7. The Competent Authorities shall ensure that potential subcontractors comply with the same conditions for the protection of Classified Information as those laid down for the Contractor.

ARTICLE 6
CONVEYANCE AND TRANSMISSION OF CLASSIFIED INFORMATION

1. Classified Information shall be conveyed via diplomatic channels.
2. The Competent Authorities may agree on other forms of conveying Classified Information to ensure its protection under their national law against unauthorized disclosure.
3. Classified Information may be transmitted by protected telecommunication systems or networks that have been certified according to the national law of each Party.
4. The receipt of Classified Information shall be confirmed in writing by the recipient.

ARTICLE 7
REPRODUCTION AND TRANSLATION OF CLASSIFIED INFORMATION

1. Any reproduction or translation of Classified Information shall bear an appropriate note in the official language stating that it contains Classified Information received from the Originating Party and must be protected as if it were original Classified Information.
2. Classified Information marked as TAJNE/ GEHEIM/ SECRET/ SEGRETO/ SECRET may be copied or translated only after having obtained written consent from the Originating Party.

ARTICLE 8

DESTRUCTION OF CLASSIFIED INFORMATION

1. Classified Information marked as TAJNE/ GEHEIM/ SECRET/ SEGRETO/ SECRET shall not be destroyed but must be returned to the Originating Party.
2. Classified Information marked as POUFNE/ VERTRAULICH/ CONFIDENTIEL/ CONFIDENZIALE/ CONFIDENTIAL or below shall be destroyed pursuant to the national law of the Recipient Party in such a manner as to prevent its partial or total reconstruction.

ARTICLE 9

VISITS

1. Individuals arriving on a visit from the territory of one Party to the territory of the other Party shall be allowed to access Classified Information marked as POUFNE/ VERTRAULICH/ CONFIDENTIEL/ CONFIDENZIALE/ CONFIDENTIAL or above only after having received a written permission issued by the Competent Authority of the hosting Party.
2. At least 20 (twenty) days before the planned date of the visit the request for visit shall be submitted to the Competent Authority of the hosting Party in accordance with national law and provisions laid down in this Article. In urgent cases the Competent Authorities may agree on a shorter period.
3. A request for visit shall include:
   1) the purpose, date and program of the visit;
   2) the first name(s) and surname, date and place of birth, nationality, passport or national ID card number of every visitor;
   3) the position of the visitor and the name of the institution or organizational unit represented;
   4) confirmation of the visitor's Personnel Security Clearance;
   5) the name and address of the organizational unit to be visited;

6) the first name(s) and surname as well as the position of the individual hosting the visit.

4. The hosting Party shall ensure, pursuant to its national law, the protection of the personal data of the individuals arriving on a visit.

ARTICLE 10
BREACH OF SECURITY

1. Any breach of security concerning the protection of Classified Information exchanged or generated under this Agreement shall be investigated pursuant to the national law of the Party in whose territory it has occurred.
2. The Competent Authorities shall promptly inform each other of any breach of security.
3. If a breach of security has occurred in the territory of a Third Party, the Party who transmitted or conveyed Classified Information shall take all the measures referred to in Paragraphs 1 and 2 in cooperation with the Third Party.
4. The Competent Authorities shall promptly inform each other of the circumstances of the breach of security and the outcome of the measures taken. Upon request, the Competent Authorities shall cooperate in investigations.
5. In the event of any suspicion of a breach of security, the provisions of Paragraphs 1-4 shall apply.

ARTICLE 11
EXPENSES

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

ARTICLE 12
CONSULTATIONS

1. The Competent Authorities shall inform each other of any amendments to their national law affecting the provisions of this Agreement.
2. In order to ensure close cooperation in the implementation of the provisions of this Agreement, the Competent Authorities may consult each other if necessary.
3. Each Party shall allow the representatives of the Competent authorities of the other Party to pay visits to its own territory to discuss the procedures related to the protection of Classified Information transmitted or conveyed by the other Party.

ARTICLE 13
PERSONNEL SECURITY CLEARANCES AND FACILITY SECURITY CLEARANCES

1. Each Party shall recognize Personnel Security Clearances and Facility Security Clearances issued by the other Party.
2. The Competent Authorities shall promptly inform each other of any changes concerning mutually recognized or issued Personnel Security Clearances and Facility Security Clearances.
3. On request, the Competent Authorities shall inform each other of Facility Security Clearances issued for contractors in accordance with their national law.

ARTICLE 14
SETTLEMENTS OF DISPUTES

1. Any dispute concerning the implementation or interpretation of the provisions of this Agreement shall be settled by direct negotiations between the Competent Authorities.

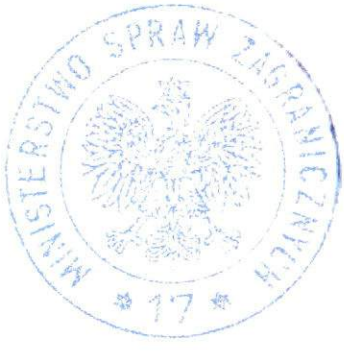
2. If a dispute cannot be settled according to Paragraph 1, it shall be settled through diplomatic channels.

ARTICLE 15
FINAL PROVISIONS

1. The Parties shall notify each other in writing of the completion of the national measures necessary for the entry into force of this Agreement.
2. This Agreement shall enter into force on the first day of the second month following the day of receipt of the latest notification.
3. This Agreement is concluded for an unlimited period of time. It may be terminated by either Party on giving notice to the other Party. In such a case, this Agreement shall expire six months following the receipt of the termination notice.
4. In the event of termination, any Classified Information conveyed, transmitted or generated under the provisions of this Agreement shall be protected pursuant to the provisions of this Agreement.
5. This Agreement may be amended by a mutual written consent. Such amendments shall enter into force in accordance with the provisions of Paragraphs 1 and 2.

Signed at Thun on 7 September 2022 in two original copies, each in the Polish, German as well as English language, all texts being equally authentic. In case of divergences, the English text shall prevail.

FOR THE GOVERNMENT OF THE REPUBLIC OF POLAND	FOR THE SWISS FEDERAL COUNCIL



Świadczam zgodność
fotokopii z oryginałem/~~odpisem~~

Warszawa, dnia 12/12/2022 r.

Juchniewicz

Juliusz Juchniewicz
Zastępca Dyrektora
DEPARTAMENT PRAWNO-TRAKTATOWY

Abkommen

zwischen

der Regierung der Republik Polen

und

dem Schweizerischen Bundesrat

über den gegenseitigen Schutz

von klassifizierten Informationen

Die Regierung der Republik Polen und der Schweizerische Bundesrat (nachstehend «Vertragsparteien» genannt),

in Anerkennung der Notwendigkeit, den gegenseitigen Schutz aller Informationen, die gemäss nationalem Recht jeder Vertragspartei als klassifizierte Informationen eingestuft und der anderen Vertragspartei übermittelt werden, zu gewährleisten,

gegenseitig vereinbarte Regeln und Bestimmungen zum Schutz von klassifizierten Informationen festzulegen, welche für jegliche gemeinsame Zusammenarbeit im Zusammenhang mit deren Austausch gelten sollen,

sind wie folgt übereingekommen:

ARTIKEL 1

BEGRIFFSBESTIMMUNGEN

Im Sinne des vorliegenden Abkommens gelten die folgenden Begriffe:

1) «klassifizierte Informationen»: alle Informationen, ohne Rücksicht auf ihre Darstellungsform und deren Aufzeichnungsverfahren, sowie Gegenstände oder ihre beliebigen Bestandteile, die gegen eine unbefugte Preisgabe zu schützen und als solche gekennzeichnet sind;
2) «zuständige Sicherheitsbehörden»: die für den Schutz von klassifizierten Informationen zuständigen Behörden, die in Artikel 3 Absatz 1 dieses Abkommens aufgeführt sind;
3) «berechtigte Organisationen»: natürliche oder juristische Personen oder Dienststellen ohne Rechtspersönlichkeit, die zuständig für die Erzeugung, die Entgegennahme, die Aufbewahrung sowie den Schutz und den Gebrauch von klassifizierten Informationen gemäss nationalem Recht beider Vertragsparteien sind;
4) «übermittelnde Partei»: die zuständigen Sicherheitsbehörden und berechtigten Organisationen, die klassifizierte Informationen erzeugen, weitergeben oder übermitteln;
5) «empfangende Partei»: die zuständigen Sicherheitsbehörden und berechtigten Organisationen, an die klassifizierte Informationen weitergegeben oder übermittelt werden;
6) «klassifizierter Vertrag»: eine Vereinbarung, deren Verwirklichung klassifizierte Informationen enthält, die sich auf den Zugang zu klassifizierten Informationen oder deren Erzeugung bezieht;
7) «Auftragnehmer»: eine natürliche oder juristische Person oder eine Dienststelle, die die Rechtsfähigkeit besitzt, klassifizierte Verträge auszuführen;

8) «Auftraggeber»: eine natürliche oder juristische Person oder eine Dienststelle, die die Rechtsfähigkeit besitzt, klassifizierte Verträge abzuschliessen;

9) «Kenntnis nur wenn nötig»: Zugang zu klassifizierten Informationen nur für diejenigen Personen, die ihn zur Ausführung ihrer dienstlichen Pflichten und Aufgaben benötigen;

10) «Personensicherheitsermächtigung»: ein durch die zuständige Sicherheitsbehörde gemäss nationalem Recht herausgegebenes Dokument, das bestätigt, dass eine natürliche Person sicherheitsüberprüft und zum Zugang zu VERTRAULICH / CONFIDENZIALE / POUFNE / CONFIDENTIAL oder höher klassifizierten Informationen berechtigt ist;

11) «Betriebssicherheitserklärung»: ein durch die zuständige Sicherheitsbehörde gemäss nationalem Recht herausgegebenes Dokument, das bestätigt, dass ein Auftragnehmer über die Fähigkeit verfügt, VERTRAULICH / CONFIDENTIEL / CONFIDENZIALE / POUFNE / CONFIDENTIAL oder höher klassifizierte Informationen gemäss nationalem Recht zu schützen;

12) «Drittpartei»: jegliche öffentliche oder private Organisation eines Staates oder einer internationalen Organisation, die unter seiner oder ihrer Gerichtsbarkeit steht und die nicht Vertragspartei dieses Abkommens ist.

ARTIKEL 2

EINSTUFUNG VON KLASSIFIZIERTEN INFORMATIONEN

1. Klassifizierte Informationen werden entsprechend ihrem Inhalt nach dem nationalen Recht jeder Vertragspartei in eine Klassifizierungskategorie eingestuft. Den erhaltenen klassifizierten Informationen müssen den Bestimmungen in Absatz 4 entsprechend gleichwertige Klassifizierungskategorien gewährt werden.
2. Die in Absatz 1 genannte Pflicht gilt auch für klassifizierte Informationen, die sowohl infolge gemeinsamer Tätigkeit der Vertragsparteien,

der berechtigten Organisationen oder der zuständigen Sicherheitsbehörden als auch im Zusammenhang mit der Erfüllung eines klassifizierten Vertrags entstehen.

3. Die Klassifizierungskategorie darf ausschliesslich von der übermittelnden Partei, die die Einstufung veranlasst hat, geändert oder aufgehoben werden. Die empfangende Partei ist unverzüglich über jegliche Änderung oder Aufhebung der Klassifizierungskategorie zu unterrichten.
4. Die Vertragsparteien vereinbaren die Gleichwertigkeit der folgenden Klassifizierungskategorien:

IN POLEN	**IN DER SCHWEIZ**	**ENTSPRECHENDER BEGRIFF IN ENGLISCH**
TAJNE	GEHEIM / SECRET / SEGRETO	SECRET
POUFNE	VERTRAULICH / CONFIDENTIEL / CONFIDENZIALE	CONFIDENTIAL
ZASTRZEŻONE	INTERN / INTERNE / AD USO INTERNO	RESTRICTED

5. Für die Weitergabe oder Übermittlung und den Schutz von polnisch «ŚCIŚLE TAJNE» (TOP SECRET) klassifizierten Informationen werden zwischen den zuständigen Sicherheitsbehörden der Vertragsparteien im Einzelfall Sonderregelungen getroffen.

ARTIKEL 3
ZUSTÄNDIGE SICHERHEITSBEHÖRDEN

1. Die zuständigen Sicherheitsbehörden im Sinne dieses Abkommens sind:

1) seitens der Republik Polen:
der Leiter der Agentur für Innere Sicherheit;

2) seitens der Schweizerischen Eidgenossenschaft:
der Bereich Informations- und Objektsicherheit VBS.

2. Bei Bedarf können die zuständigen Sicherheitsbehörden der Vertragsparteien, im Rahmen der ihnen kraft innerstaatlicher Gesetzgebung übertragenen Befugnisse, detaillierte technische oder organisatorische Vereinbarungen in Schriftform treffen, um eine wirksame Zusammenarbeit im Sinne dieses Abkommens zu gewährleisten.

ARTIKEL 4
SCHUTZ VON KLASSIFIZIERTEN INFORMATIONEN

1. Die Vertragsparteien treffen gemäss diesem Abkommen und ihrem nationalen Recht alle geeigneten Massnahmen zum Schutz der ausgetauschten klassifizierten Informationen.
2. Die Vertragsparteien gewährleisten den Informationen nach Absatz 1 mindestens denselben Schutz, der bei eigenen klassifizierten Informationen der entsprechenden Klassifizierungskategorie gemäss Artikel 2 Absatz 4 gilt.
3. Die gemäss Absatz 1 erhaltenen klassifizierten Informationen werden ausschliesslich für die bei der Weitergabe oder Übermittlung festgelegten Zwecke verwendet.
4. Ohne vorherige schriftliche Zustimmung der übermittelnden Partei, die die Einstufung veranlasst hat, darf die empfangende Partei keine der Informationen gemäss Absatz 1 Dritten zugänglich machen.
5. Die erhaltenen klassifizierten Informationen dürfen nur Personen zugänglich gemacht werden, deren dienstliche Aufgaben die Kenntnis dieser Informationen notwendig machen und die gemäss nationalem Recht der empfangenden Partei zum Zugang berechtigt sind.
6. Der Austausch klassifizierter Informationen zwischen den Nachrichtendiensten und den Polizei- und Grenzbehörden richtet sich nach

diesem Abkommen, insofern keine sonstigen bilateralen oder multilateralen Vereinbarungen bestehen.

ARTIKEL 5
KLASSIFIZIERTE VERTRÄGE

1. Wird der Abschluss eines klassifizierten Vertrags beabsichtigt, der VERTRAULICH/CONFIDENTIEL/CONFIDENZIALE/POUFNE/CONFIDENTIAL oder höher klassifizierte Informationen einschliesst, erhält der Auftraggeber vorgängig eine schriftliche Zusicherung der zuständigen Sicherheitsbehörde des potenziellen Auftragnehmers, dass der vorgeschlagene Auftragnehmer über eine entsprechende Betriebssicherheitserklärung verfügt.
2. Bis zur Einholung der in Absatz 1 vermerkten Zusicherung dürfen dem Auftragnehmer keine klassifizierten Informationen zugänglich gemacht werden.
3. Der Auftraggeber informiert den Auftragnehmer über die zur Erfüllung des klassifizierten Vertrags nötigen Sicherheitsanforderungen, darunter eine Klassifizierungsliste und Regeln zur Einstufung von Informationen, die im Laufe der Erfüllung eines klassifizierten Vertrags entstehen.
4. Eine Kopie des Dokuments gemäss Absatz 3 wird den zuständigen Sicherheitsbehörden beider Vertragspartner zugestellt.
5. Die zuständige Sicherheitsbehörde des Auftragnehmers gewährleistet, dass die weitergegebenen oder übermittelten oder im Zusammenhang mit der Erfüllung des klassifizierten Vertrags entstandenen klassifizierten Informationen gemäss den Sicherheitsanforderungen nach Absatz 3 und den eigenen nationalen Rechtsvorschriften geschützt werden.
6. Die Erfüllung des Teils des klassifizierten Vertrags, mit dem der Zugang zu klassifizierten Informationen verbunden ist, ist erst dann erlaubt, wenn beim Auftragnehmer alle erforderlichen Massnahmen zum Schutz von

klassifizierten Informationen gemäss den Sicherheitsanforderungen nach Absatz 3 getroffen worden sind.

7. Die zuständigen Sicherheitsbehörden gewährleisten, dass potenzielle Subunternehmer dieselben Bedingungen für den Schutz von klassifizierten Informationen erfüllen, die für den Auftragnehmer festgelegt worden sind.

ARTIKEL 6
WEITERGABE UND ÜBERMITTLUNG VON KLASSIFIZIERTEN INFORMATIONEN

1. Klassifizierte Informationen werden auf diplomatischem Weg übermittelt.
2. Mit gegenseitigem Einverständnis beider zuständigen Sicherheitsbehörden und zu deren Schutz vor unbefugter Preisgabe unter den jeweiligen nationalen Sicherheitsbestimmungen können klassifizierte Informationen auch auf einem anderen Weg übermittelt werden.
3. Klassifizierte Informationen können über gesicherte Kommunikationssysteme und -netze übermittelt werden, die gemäss dem nationalen Recht der Vertragsparteien zur Nutzung zugelassen sind.
4. Der Empfang von klassifizierten Informationen erfordert eine schriftliche Bestätigung des Empfängers.

ARTIKEL 7
VERVIELFÄLTIGUNG UND ÜBERSETZUNG VON KLASSIFIZIERTEN INFORMATIONEN

1. In allen Vervielfältigungen und Übersetzungen wird in der Zielsprache darauf hingewiesen, dass sie klassifizierte Informationen enthalten, die von der übermittelnden Partei stammen; die Vervielfältigungen und Übersetzungen sind wie die Originale zu schützen.

2. Klassifizierte Informationen der Klassifizierungskategorie GEHEIM/SECRET/SEGRETO/ TAJNE/SECRET dürfen nur nach vorheriger Einholung der schriftlichen Zustimmung der übermittelnden Partei vervielfältigt oder übersetzt werden.

ARTIKEL 8
VERNICHTUNG VON KLASSIFIZIERTEN INFORMATIONEN

1. Klassifizierte Informationen der Klassifizierungskategorie GEHEIM/SECRET/SEGRETO/TANJE/SECRET dürfen nicht vernichtet werden, sondern sind der übermittelnden Partei zurückzugeben.
2. Klassifizierte Informationen bis zur Klassifizierungskategorie VERTRAULICH/CONFIDENTIEL/CONFIDENZIALE/POUFNE/CONFIDENTIAL sind gemäss dem nationalen Recht der empfangenden Partei so zu vernichten, dass eine partielle oder vollständige Wiederherstellung ausgeschlossen ist.

ARTIKEL 9
BESUCHE

1. Besucherinnen und Besuchern aus dem Hoheitsgebiet einer Vertragspartei wird im Hoheitsgebiet der anderen Vertragspartei nur nach vorgängiger schriftlicher Erlaubnis der zuständigen Sicherheitsbehörden der anderen Vertragspartei Zugang zu VERTRAULICH / CONFIDENTIEL / CONFIDENZIALE / POUFNE / CONFIDENTIAL oder höher klassifizierten Informationen gewährt.
2. Der Besuchsantrag muss der zuständigen Sicherheitsbehörde der empfangenden Vertragspartei spätestens 20 (zwanzig) Tage vor dem geplanten Besuch gemäss nationalem Recht und den in diesem Artikel festgelegten Bestimmungen unterbreitet werden. In dringenden Fällen

können die zuständigen Sicherheitsbehörden eine kürzere Meldefrist vereinbaren.

3. Besuchsanträge müssen folgende Angaben enthalten:
    1) Besuchszweck, -datum und -programm;
    2) Vorname(n) und Nachname, Geburtsdatum und -ort, Staatsangehörigkeit, Reisepass- oder ID-Kartennummer jeder Besucherin/jedes Besuchers;
    3) Funktion mit dem Namen der Einrichtung oder der Dienststelle jeder Besucherin/jedes Besuchers;
    4) Bestätigung der Personensicherheitsermächtigung jeder Besucherin/jedes Besuchers;
    5) Name und Adresse der zu besuchenden Dienststelle;
    6) Vorname(n), Nachname und Funktion des Gastgebers.
4. Die empfangende Partei gewährleistet den Schutz personenbezogener Daten von Besucherinnen und Besuchern gemäss ihrem nationalen Recht.

ARTIKEL 10
VERLETZUNG VON SICHERHEITSBESTIMMUNGEN

1. Alle Verletzungen der Bestimmungen über den Schutz von unter dieses Abkommen fallenden klassifizierten Informationen werden nach nationalem Recht der Vertragspartei, in deren Hoheitsgebiet es zur Verletzung gekommen ist, untersucht.
2. Die zuständigen Sicherheitsbehörden informieren einander umgehend über jegliche Verletzung von Sicherheitsbestimmungen.
3. Hat die Regelverletzung im Hoheitsgebiet einer Drittpartei stattgefunden, trifft die Vertragspartei, die die klassifizierten Informationen weitergegeben oder übermittelt hat, die in den Absätzen 1 und 2 genannten Massnahmen in Zusammenarbeit mit der Drittpartei.

4. Die zuständigen Sicherheitsbehörden der Vertragsparteien informieren sich gegenseitig unverzüglich über den Hintergrund der Verletzung der Sicherheitsbestimmungen und über das Ergebnis der ergriffenen Massnahmen. Auf Anfrage arbeiten die zuständigen Sicherheitsbehörden bei der Untersuchung zusammen.
5. Wird eine Verletzung von Sicherheitsbestimmungen vermutet, gelten die Bestimmungen der Absätze 1–4.

ARTIKEL 11
KOSTEN

Jede Vertragspartei trägt die eigenen Kosten, die ihr aufgrund der Umsetzung dieses Abkommens entstehen.

ARTIKEL 12
KONSULTATIONEN

1. Die zuständigen Sicherheitsbehörden informieren sich gegenseitig über Änderungen in ihrem nationalen Recht, soweit sie dieses Abkommen tangieren.
2. Um eine enge Zusammenarbeit bei der Umsetzung des vorliegenden Abkommens zu gewährleisten, konsultieren sich die zuständigen Sicherheitsbehörden nach Bedarf.
3. Jede Vertragspartei erlaubt den Vertretern der zuständigen Sicherheitsbehörde der anderen Vertragspartei, Besuche auf ihrem Hoheitsgebiet abzustatten, um sich über die Verfahren zum Schutz von klassifizierten Informationen, die ihr von der anderen Vertragspartei weitergegeben oder übermittelt wurden, zu informieren.

ARTIKEL 13

PERSONENSICHERHEITSBESCHEINIGUNGEN UND BETRIEBSSICHERHEITSERKLÄRUNGEN

1. Jede Vertragspartei anerkennt die von der anderen Vertragspartei ausgestellten Personensicherheitsermächtigungen und Betriebssicherheitserklärungen.
2. Die zuständigen Sicherheitsbehörden informieren sich gegenseitig umgehend über Änderungen der beiderseitig anerkannten oder ausgestellten Personensicherheitsermächtigungen und Betriebssicherheitserklärungen.
3. Auf Anfrage informieren sich die zuständigen Sicherheitsbehörden gegenseitig über ausgestellte Betriebssicherheitserklärungen von Firmen gemäss nationalem Recht.

ARTIKEL 14

BEILEGUNG VON STREITIGKEITEN

1. Alle Streitigkeiten über die Umsetzung oder Auslegung dieses Abkommens werden durch direkte Verhandlungen zwischen den zuständigen Sicherheitsbehörden der Vertragsparteien beigelegt.
2. Ist die Beilegung von Streitigkeiten gemäss Absatz 1 nicht möglich, erfolgt die Schlichtung auf diplomatischem Weg.

ARTIKEL 15

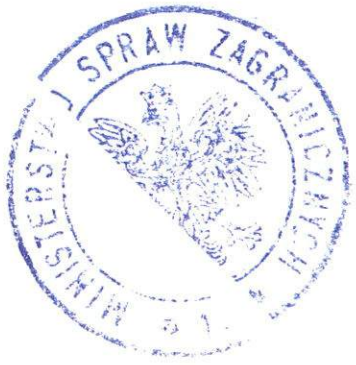
SCHLUSSBESTIMMUNGEN

1. Die Vertragsparteien informieren sich gegenseitig auf diplomatischem Weg über die Erfüllung aller nationalen Erfordernisse, die zur Inkraftsetzung dieses Abkommens anfallen.
2. Dieses Abkommen tritt am ersten Tag des zweiten Monats, der auf den Empfang der letzten Note folgt, in Kraft.

3. Dieses Abkommen wird auf unbestimmte Zeit abgeschlossen. Es kann jederzeit von einer Vertragspartei durch eine an die andere Vertragspartei gerichtete Kündigung beendet werden. In diesem Fall erlischt das vorliegende Abkommen sechs Monate nach Erhalt der Kündigung.
4. Im Kündigungsfall sind die aufgrund des vorliegenden Abkommens weitergegebenen, übermittelten oder erzeugten klassifizierten Informationen weiterhin nach den Bestimmungen dieses Abkommens zu schützen.
5. Dieses Abkommen kann in beiderseitigem schriftlichem Einvernehmen der Vertragsparteien geändert werden. In diesem Fall finden die Bestimmungen gemäss den Absätzen 1 und 2 Anwendung.

Unterschrieben in Thun am 7 September 2022 in zwei Urschriften in deutscher, polnischer und englischer Sprache, wobei jeder Wortlaut gleichermassen verbindlich ist. Im Falle unterschiedlicher Auslegung ist der englische Wortlaut massgebend.

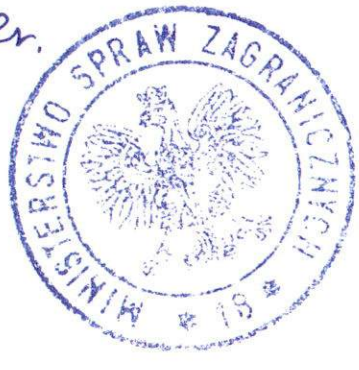
FÜR	FÜR
DIE REGIERUNG	DEN SCHWEIZERISCHEN
DER REPUBLIK POLEN	BUNDESRAT



Świadczam zgodność
fotokopii z oryginałem/~~odpisem~~.

Warszawa, dnia 29 września 2022r.

Sławomir Majszyk
Zastępca Dyrektora
DEPARTAMENT PRAWNO-TRAKTATOWY



Minister do Spraw
Unii Europejskiej

DPUE.920.1699.2022. EBK(3)
Warszawa, 29 listopada 2022 r.
Dot.:P-12435/2022 z 07.11.2022 r.

Pan Krzysztof Wacławek
Szef Agencji Bezpieczeństwa Wewnętrznego

Opinia
o zgodności z prawem Unii Europejskiej *umowy między Rządem Rzeczypospolitej Polskiej a Radą Federalną Konfederacji Szwajcarskiej o wzajemnej ochronie informacji niejawnych, podpisanej w Thun dnia 7 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 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