Druk nr 2573

Warszawa, 13 września 2022 r.

SEJM
RZECZYPOSPOLITEJ POLSKIEJ
IX kadencja
Prezes Rady Ministrów
RM-06111-185-22

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 Królestwa Danii o wzajemnej ochronie informacji niejawnych w dziedzinie obronności, podpisaną w Warszawie dnia 8 czerwca 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 8 czerwca 2022 roku w Warszawie została podpisana Umowa między Rządem Rzeczypospolitej Polskiej a Rządem Królestwa Danii o wzajemnej ochronie informacji niejawnych w dziedzinie obronności, 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 2022 roku.

PREZYDENT
RZECZYPOSPOLITEJ POLSKIEJ

Andrzej Duda

PREZES RADY MINISTRÓW

Mateusz Morawiecki

UZASADNIENIE

I. Wyjaśnienie potrzeby i celu związania Rzeczypospolitej Polskiej umową międzynarodową

Intensywnie rozwijająca się współpraca gospodarcza w sferze obronnej między Rzecząpospolitą Polską a Królestwem Danii wymogła konieczność związania obu Stron umową międzynarodową, niezbędną do otwarcia perspektyw dla polskich i duńskich przedsiębiorców oraz stworzenia sprzyjających warunków rozwoju współpracy między krajami.

Podpisana w dniu 8 czerwca 2022 r. w Warszawie Umowa między Rządem Rzeczypospolitej Polskiej a Rządem Królestwa Danii o wzajemnej ochronie informacji niejawnych w dziedzinie obronności reguluje prawne aspekty współpracy polskich i duńskich podmiotów upoważnionych do przetwarzania informacji niejawnych, zgodnie ze swoim prawem krajowym. Po wejściu w życie Umowa będzie stanowić podstawę do nawiązania ściślejszej współpracy sektorów przemysłu zbrojeniowego obu krajów, a także w zakresie obronności i bezpieczeństwa wewnętrznego. Uregulowanie wspomnianych kwestii będzie przede wszystkim istotne dla rozwoju współpracy gospodarczej, gdyż stworzy polskim i duńskim przedsiębiorcom podstawy prawne do zawierania kontraktów, których realizacja wiąże się z dostępem do informacji niejawnych lub wytwarzaniem takich informacji w dziedzinie obronności.

II. Wskazanie różnic między dotychczasowym a projektowanym stanem prawnym

Umowa między Rządem Rzeczypospolitej Polskiej a Rządem Królestwa Danii o wzajemnej ochronie informacji niejawnych w dziedzinie obronności będzie pierwszą Umową tego rodzaju zawartą z tym partnerem zagranicznym.

Artykuł 1 Umowy określa cel jej zawarcia i stosowania. Charakter Umowy powoduje, iż po wejściu w życie będzie miała ona zastosowanie do działań lub kontraktów dotyczących informacji niejawnych w dziedzinie obronności zawieranych między Stronami, osobami fizycznymi, osobami prawnymi lub innymi jednostkami organizacyjnymi pozostającymi pod ich jurysdykcją.

W celu ujednolicenia terminów na użytek niniejszej Umowy w artykule 2 zdefiniowano kluczowe dla Umowy pojęcia. Na wniosek Strony duńskiej dodano definicję „Zasady ograniczonego dostępu” („Need-to-Know”).

W artykule 3 zestawiono odpowiadające sobie klauzule tajności celem usystematyzowania ich nazewnictwa oraz uszczegółowiono obowiązek klasyfikowania informacji niejawnych zgodnie z prawem krajowym Stron.

W artykule 4 wskazano właściwe organy, które są odpowiedzialne za realizację postanowień niniejszej Umowy wraz z danymi adresowymi reprezentowanych podmiotów. Uregulowano także kwestie informowania o ich zmianach.

Artykuł 5 Umowy określa zasady ochrony informacji niejawnych, które mają gwarantować właściwą ochronę przekazywanym informacjom niejawnym. Ustalono m.in., iż Strony zobowiążą się do stosowania zasady ograniczonego dostępu przy udostępnianiu informacji niejawnych, zgodnie z którą informacje niejawne będą udostępniane jedynie osobom, których zadania wymagają zapoznania się z nimi.

W artykule 6 określono zasadę wzajemnego uznawania przez Strony poświadczeń bezpieczeństwa oraz świadectw bezpieczeństwa przemysłowego. Postanowienie zawarte w tym artykule przewiduje również możliwość współpracy właściwych organów przy przeprowadzaniu odpowiednich procedur sprawdzających.

Artykuł 7 reguluje możliwość zawierania kontraktów niejawnych, których realizacja wiąże się z dostępem do informacji niejawnych bądź z wytworzeniem takich informacji. Ze względu na to, że dostęp do informacji o klauzuli odpowiadającej polskiemu oznaczeniu „zastrzeżone" według duńskiego prawa wymaga posiadania stosownego poświadczenia bezpieczeństwa lub świadectwa bezpieczeństwa przemysłowego, zmodyfikowano treść ustępu 1 oraz dodano ustęp 2 o następującej treści: „W przypadku, gdy zlecający podlega prawu Królestwa Danii, przed zawarciem kontraktu niejawnego związanego z dostępem do informacji niejawnych o klauzuli ZASTRZEŻONE / TIL TJENESTEBRUG / RESTRICTED właściwy organ Rzeczypospolitej Polskiej potwierdza, że polski kontrahent spełnia wymagania bezpieczeństwa określone prawem krajowym".

W artykułach 8, 9 i 10 uregulowano kolejno: przekazywanie, powielanie, tłumaczenie oraz niszczenie informacji niejawnych.

W artykule 11 określono zasady i warunki organizacji wzajemnych wizyt związanych z dostępem do informacji niejawnych. Wprowadzono również regulację, zgodnie z którą Strony zapewnią, zgodnie ze swoim prawem krajowym, ochronę danych osób przybywających z wizytą.

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

W artykule 13 uregulowano kwestię języków, jakimi Strony będą się posługiwały w zakresie stosowania postanowień niniejszej Umowy. Zgodnie z sugestią Strony duńskiej, postanowiono, że w zakresie stosowania niniejszej Umowy, Strony używać będą wyłącznie języka angielskiego.

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

W artykule 15 wprowadzono tryb konsultacji właściwych organów Stron w celu współpracy przy realizacji postanowień Umowy, w tym w drodze wzajemnych wizyt służących omówieniu procedur regulujących ochronę informacji niejawnych.

Ponadto w Umowie przewidziano tryb rozstrzygania sporów (artykuł 16) oraz określono procedurę jej wejścia w życie, czas obowiązywania oraz tryb wypowiedzenia (artykuł 18), które to regulacje stanowią niezbędny element każdej umowy międzynarodowej o takim charakterze. Jednocześnie na wniosek Strony duńskiej w artykule 18 dodano nowy ustęp 4 o terytorialnym wyłączeniu stosowania Umowy na Wyspach Owczych oraz Grenlandii.

W artykule 17 zawarto postanowienie, zgodnie z którym z dniem wejścia w życie niniejszej Umowy traci moc obowiązujące Porozumienie między Ministerstwem Obrony Narodowej Rzeczypospolitej Polskiej a Ministerstwem Obrony Królestwa Danii w sprawie środków bezpieczeństwa dla ochrony wojskowych informacji niejawnych, podpisane dnia 2 maja 1998 r., co pozwoli na zachowanie spójności systemu prawnego.

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 niniejszej Umowy nie spowoduje znaczących skutków społecznych. Skutkiem o charakterze prawnym będzie określenie jednolitych zasad ochrony informacji niejawnych, wymienianych w ramach współdziałania w dziedzinie obronności między Rzecząpospolitą Polską a Królestwem Danii. Umowa stanowić będzie podstawę do nawiązania ściślejszej współpracy zarówno sektorów obronnych, jak również w zakresie bezpieczeństwa wewnętrznego.

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

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

IV. Tryb związania

Wejście w życie niniejszej Umowy nie będzie wiązało się z koniecznością wprowadzenia zmian w polskim prawie krajowym, ponieważ jej postanowienia nie odbiegają od obowiązującego w Rzeczypospolitej Polskiej porządku prawnego, a w szczególności rozwiązań przyjętych w ustawie z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2019 r. poz. 742 oraz z 2022 r. poz. 655). Umowa dotyczy wprawdzie ochrony przekazywanych za granicę i otrzymywanych z zagranicy informacji niejawnych, ale nie wprowadza żadnych dodatkowych zasad ochrony lub wymiany tych informacji – innych, aniżeli określone w ustawie z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych. Nie zostały zatem spełnione przesłanki wymienione w art. 89 ust. 1 Konstytucji Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz. U. poz. 483, z późn. zm.), zwanej dalej „Konstytucją”, a więc ratyfikacja przedmiotowej Umowy nie wymaga uprzedniej zgody wyrażonej w ustawie.

W Rzeczypospolitej Polskiej związanie przedmiotową Umową nastąpi przez jej ratyfikację w trybie art. 89 ust. 2 Konstytucji, zgodnie z postanowieniami art. 12 ust. 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 Umowy za źródło prawa powszechnie obowiązującego w Rzeczypospolitej Polskiej, gdyż jej postanowienia będą miały zastosowanie do szerokiego kręgu podmiotów (organy administracji państwowej, przedsiębiorcy). W związku z faktem, iż zgodnie z art. 87 Konstytucji 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 Umową powinno nastąpić w drodze ratyfikacji bez uprzedniej zgody wyrażonej w ustawie.

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

W związku z faktem, iż 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 (Dz. U. z 2019 r. poz. 1781) oraz określonej w art. 47 Konstytucji 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 art. 12 ust. 2 ustawy z dnia 14 kwietnia 2000 r. o umowach międzynarodowych.

Załącznik
do uchwały nr 181/2022
Rady Ministrów
z dnia 29 sierpnia 2022 r.

UMOWA

między Rządem Rzeczypospolitej Polskiej

a Rządem Królestwa Danii

o wzajemnej ochronie informacji niejawnych

w dziedzinie obronności

Rząd Rzeczypospolitej Polskiej
i Rząd Królestwa Danii,
zwane dalej „Stronami",

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
CEL UMOWY

1. Celem niniejszej Umowy jest zapewnienie ochrony informacjom niejawnym związanym z dziedziną obronności wytwarzanym w wyniku współpracy lub wymienianym między Stronami, osobami fizycznymi, osobami prawnymi lub innymi jednostkami organizacyjnymi znajdującymi się pod ich jurysdykcją.
2. Umowa niniejsza ma zastosowanie do wszelkich działań, kontraktów lub innych umów wiążących się z dostępem do informacji niejawnych związanych z dziedziną obronności, realizowanych bądź zawieranych między Stronami lub osobami fizycznymi, osobami prawnymi bądź innymi jednostkami organizacyjnymi znajdującymi się pod ich jurysdykcją.

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) **właściwe organy** – organy, o których mowa w artykule 4 ustęp 1 niniejszej Umowy;
3) **Strona wytwarzająca** – Stronę, osobę fizyczną, osobę prawną lub inną jednostkę organizacyjną uprawnioną do wytwarzania, przekazywania i ochrony informacji niejawnych zgodnie z prawem krajowym swojej Strony;

4) **Strona otrzymująca** – Stronę, osobę fizyczną, osobę prawną lub inną jednostkę organizacyjną uprawnioną do otrzymywania i ochrony 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, która posiada zdolność do realizacji kontraktów niejawnych zgodnie z prawem krajowym jednej ze Stron;

7) **zlecający** – osobę fizyczną, osobę prawną albo inną jednostkę organizacyjną uprawnioną do zlecania kontraktów niejawnych zgodnie z prawem krajowym jednej ze Stron;

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

9) **zasada ograniczonego dostępu** – zasadę, zgodnie z którą informacje niejawne udostępnia się osobie wyłącznie w celach realizacji obowiązków służbowych lub określonego zadania;

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

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 ustępu 3.
2. Klauzula tajności może być zmieniona lub zniesiona 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	KRÓLESTWO DANII	ODPOWIEDNIK W JĘZYKU ANGIELSKIM
ŚCIŚLE TAJNE	YDERST HEMMELIGT	TOP SECRET
TAJNE	HEMMELIGT	SECRET
POUFNE	FORTROLIGT	CONFIDENTIAL
ZASTRZEŻONE	TIL TJENESTEBRUG	RESTRICTED

ARTYKUŁ 4
WŁAŚCIWE ORGANY

1. W rozumieniu niniejszej Umowy właściwymi organami są:
   1) w Rzeczypospolitej Polskiej: Szef Agencji Bezpieczeństwa Wewnętrznego
      Rakowiecka 2a
      00-993 Warszawa
      Polska;
   2) w Królestwie Danii: Duńska Wojskowa Służba Wywiadowcza
      Kastellet 30
      DK-2100 Copenhagen Ø
      Dania.
2. W razie potrzeby, Strony niniejszej Umowy informują się pisemnie o zmianach danych dotyczących ich właściwych organów.

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. Zgodnie ze swoim prawem krajowym, właściwe organy współpracują podczas procedur sprawdzających dotyczących poświadczenia bezpieczeństwa i świadectwa bezpieczeństwa przemysłowego, na wniosek jednego z nich.

ARTYKUŁ 7
KONTRAKTY NIEJAWNE

1. Przed zawarciem kontraktu niejawnego zlecający składa wniosek do właściwego organu swojej Strony o wystąpienie do właściwego organu 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. W przypadku, gdy zlecający podlega prawu Królestwa Danii, przed zawarciem kontraktu niejawnego związanego z dostępem do informacji niejawnych o klauzuli ZASTRZEŻONE / TIL TJENESTEBRUG / RESTRICTED właściwy organ Rzeczypospolitej Polskiej potwierdza, że polski kontrahent spełnia wymagania bezpieczeństwa określone prawem krajowym.
3. 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.
4. Informacje niejawne nie są udostępniane kontrahentowi do czasu uzyskania zaświadczenia, o którym mowa w ustępie 1 lub potwierdzenia, o którym mowa w ustępie 2.
5. 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 przetwarzania informacji niejawnych przekazanych kontrahentowi lub wytworzonych w związku z realizacją danego kontraktu.

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 właściwymi organami Stron.
2. Informacje niejawne o klauzuli ZASTRZEŻONE / TIL TJENESTEBRUG / RESTRICTED i POUFNE / FORTROLIGT / CONFIDENTIAL mogą być przekazywane również za pośrednictwem uprawnionych do tego przewoźników zgodnie z prawem krajowym Strony przekazującej.
3. Strona otrzymująca potwierdza pisemnie odbiór informacji niejawnych.
4. 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 ich oryginały. Liczbę kopii lub tłumaczeń należy ograniczyć do liczby wymaganej dla celów służbowych.

2. Informacje niejawne o klauzuli ŚCIŚLE TAJNE / YDERST HEMMELIGT / 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 / YDERST HEMMELIGT / TOP SECRET nie są niszczone; są one zwracane Stronie wytwarzającej.

ARTYKUŁ 11
WIZYTY

1. Osobom przybywającym z wizytą na terytorium Państwa drugiej Strony zezwala się na dostęp do informacji niejawnych tylko po uprzednim uzyskaniu pisemnego zezwolenia wydanego przez właściwy organ drugiej Strony.
2. Właściwy organ Strony wysyłającej zwraca się do właściwego organu Strony przyjmującej z wnioskiem o wyrażenie zgody na wizytę co najmniej trzydzieści dni przed planowanym terminem wizyty, o której mowa w ustępie 1, a w nagłych przypadkach w krótszym czasie.
3. Wniosek, o którym mowa w ustępie 2, zawiera następujące informacje:
   1) cel, termin i program wizyty uwzględniający najwyższą klauzulę tajności informacji z dostępem do których związana jest wizyta;

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

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) datę, podpis oraz pieczęć urzędową właściwego organu Strony wysyłającej.

4. Właściwe organy Stron mogą wyrazić zgodę na ustalenie wykazów osób upoważnionych do składania wielokrotnych wizyt związanych z realizacją konkretnego projektu, programu lub kontraktu niejawnego. Wykazy te zawierają dane określone w ustępie 3 i są ważne przez okres dwunastu miesięcy. Po zatwierdzeniu takich wykazów przez właściwe organy Stron, terminy wizyt są uzgadniane bezpośrednio między podmiotem wysyłającym a podmiotem przyjmującym, zgodnie z ustalonymi warunkami.

5. Strony zapewnią, zgodnie ze swoim prawem krajowym, ochronę danych osób przybywających z wizytą związaną z dostępem do informacji niejawnych.

ARTYKUŁ 12
NARUSZENIE REGULACJI DOTYCZĄCYCH OCHRONY INFORMACJI NIEJAWNYCH

1. Informację o każdym przypadku naruszenia lub o podejrzeniu naruszenia regulacji dotyczących ochrony informacji niejawnych Strony wytwarzającej lub informacji niejawnych wytworzonych w wyniku

wspólnego działania Stron przekazuje się niezwłocznie właściwemu organowi 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, właściwy organ Strony, na terytorium Państwa której naruszenie miało miejsce, pisemnie informuje właściwy organ drugiej Strony o fakcie, okolicznościach naruszenia oraz wyniku czynności, o których mowa w ustępie 2.
4. Jeśli naruszenie regulacji dotyczących ochrony informacji niejawnych miało miejsce na terytorium państwa strony trzeciej, właściwy organ Strony, która przekazała informacje niejawne, podejmuje we współpracy ze stroną trzecią działania, o których mowa w ustępach 1 – 3.
5. Właściwe organy Stron współpracują przy czynnościach, o których mowa w ustępie 2, na wniosek jednego z nich.

ARTYKUŁ 13
JĘZYKI

W zakresie stosowania postanowień niniejszej Umowy Strony posługują się językiem angielskim.

ARTYKUŁ 14
KOSZTY

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

ARTYKUŁ 15
KONSULTACJE

1. Właściwe organy Stron informują się wzajemnie o wszelkich zmianach w 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 właściwe organy Stron konsultują się, na wniosek jednego z nich.
3. Każda ze Stron zezwoli przedstawicielom właściwego organu drugiej Strony na składanie wizyt na terytorium swojego Państwa w celu omówienia procedur służących ochronie informacji niejawnych, które zostały jej przekazane przez drugą Stronę.
4. W celu zapewnienia skutecznej współpracy będącej przedmiotem niniejszej Umowy i w zakresie kompetencji przyznanych właściwym organom Stron ich prawem krajowym, organy te 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 są rozstrzygane w drodze bezpośrednich konsultacji między właściwymi organami Stron.
2. Jeśli nie jest możliwe rozwiązanie sporu w sposób, o którym mowa w ustępie 1, jest on rozstrzygany w drodze dyplomatycznej.

ARTYKUŁ 17
STOSUNEK DO INNYCH UMÓW

Z dniem wejścia w życie niniejszej Umowy traci moc Porozumienie między Ministerstwem Obrony Narodowej Rzeczypospolitej Polskiej a Ministerstwem Obrony Królestwa Danii w sprawie środków bezpieczeństwa dla ochrony wojskowych informacji niejawnych, podpisane dnia 2 maja 1998 roku. Informacje niejawne, które zostały przekazane albo mają być przekazywane na podstawie wyżej wymienionego Porozumienia, będą chronione zgodnie z postanowieniami niniejszej Umowy.

ARTYKUŁ 18
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 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 pisemnej notyfikacji przez każdą ze Stron. W takim przypadku utraci moc po upływie sześciu miesięcy po dniu otrzymania noty informującej o wypowiedzeniu.
4. Umowa niniejsza nie ma zastosowania do Wysp Owczych oraz Grenlandii. Obowiązywanie postanowień niniejszej Umowy może być rozszerzone na Wyspy Owcze i Grenlandię, co może zostać uzgodnione między Stronami w drodze wymiany not.
5. W przypadku wypowiedzenia niniejszej Umowy informacje niejawne wymieniane lub wytworzone na jej podstawie będą chronione zgodnie z jej postanowieniami.

Podpisano w Warszawie dnia 8 czerwca 2022 roku w dwóch jednobrzmiących egzemplarzach, każdy w językach polskim, duńskim 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 KRÓLESTWA DANII

Stwierdzam zgodność
fotokopii z oryginałem/~~odpisem~~

Warszawa, dnia 28.6.2022...

Konrad Marciniak
Dyrektor
DEPARTAMENT PRAWNO-TRAKTATOWY

AGREEMENT

between the Government of the Republic of Poland and the Government of the Kingdom of Denmark on the Mutual Protection of Classified Information in the Field of Defence

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

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
PURPOSE OF THE AGREEMENT

1. The purpose of this Agreement is to ensure the protection of Classified Information related to the field of defence that is generated as a result of cooperation or exchanged between the Parties, individuals, legal entities and other organizational units being under their jurisdiction.
2. This Agreement shall be applicable to any activities, contracts or other types of agreements involving access to Classified Information related to the field of defence that will be conducted or concluded between the Parties or individuals, legal entities or other organizational units being under their jurisdiction.

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) **Competent Authorities** – the authorities referred to in Article 4 Paragraph 1 of this Agreement;
3) **Originating Party** – the Party, an individual, a legal entity or other organizational unit, competent to originate, transmit and protect Classified Information in accordance with the national law of its Party;
4) **Recipient Party** – the Party, an individual, a legal entity or other organizational unit, competent to receive and protect 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 organizational unit which has legal capacity to perform Classified Contracts in accordance with the national law of one of the Parties;

7) **Principal** – an individual, a legal entity or other organizational unit authorized to award Classified Contracts in accordance with the national law of one of the Parties;

8) **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;

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

10) **Third Party** – any state, including individuals, legal entities or other organizational units under its jurisdiction or an international organization not being a Party to this Agreement.

ARTICLE 3
SECURITY CLASSIFICATION LEVELS

1. Classified Information is granted a security classification level in accordance to its content, pursuant to the 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 Paragraph 3.
2. The security classification level may be changed or removed only by the Originating Party. The Recipient Party shall be immediately notified in writing of every change or removal of 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 KINGDOM OF DENMARK	EQUIVALENT IN ENGLISH
ŚCIŚLE TAJNE	YDERST HEMMELIGT	TOP SECRET
TAJNE	HEMMELIGT	SECRET
POUFNE	FORTROLIGT	CONFIDENTIAL
ZASTRZEŻONE	TIL TJENESTEBRUG	RESTRICTED

ARTICLE 4
COMPETENT AUTHORITIES

1. For the purpose of this Agreement, the Competent Authorities shall be:
   1) for the Republic of Poland: the Head of the Internal Security Agency
      Rakowiecka 2a
      00-993 Warsaw
      Poland;
   2) for the Kingdom of Denmark: Danish Defence Intelligence Service
      Kastellet 30
      DK-2100 Copenhagen Ø
      Denmark.
2. The Parties to this Agreement shall update each other in writing about the details of their respective Competent Authorities as necessary.

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 Classified Contracts performance.

2. The Recipient Party shall use Classified Information exclusively for the purposes for which it has been transmitted.
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. In accordance with their national law, the Competent Authorities shall assist each other in carrying out Facility Security Clearance and Personnel Security Clearance investigations upon the request of one of them.

ARTICLE 7
CLASSIFIED CONTRACTS

1. Before concluding a Classified Contract, the Principal shall apply to its Competent Authority to request that the Competent Authority of the other Party issue a written 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. In case the Principal is under the legislation of the Kingdom of Denmark, before concluding a Classified Contract involving information classified

as ZASTRZEŻONE / TIL TJENESTEBRUG / RESTRICTED, the Competent Authority of the Republic of Poland shall confirm that a Polish Contractor meets security requirements under the national legislation.

3. 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.
4. Classified Information shall not be released to the Contractor until the receipt of the certificate referred to in Paragraph 1 or the confirmation referred to in Paragraph 2.
5. 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 handling Classified Information transmitted to the Contractor or originated during the performance of a given Classified Contract.
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 in other way agreed between the Competent Authorities of the Parties ensuring its protection against unauthorized disclosure.
2. Information classified as ZASTRZEŻONE / TIL TJENESTEBRUG / RESTRICTED and POUFNE / FORTROLIGT / CONFIDENTIAL may be transmitted also through authorized couriers in accordance with the national law of the transmitting Party.
3. The Recipient Party shall confirm in writing the receipt of Classified Information.
4. 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 Classified 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 / YDERST HEMMELIGT / 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 / YDERST HEMMELIGT / TOP SECRET shall not be destroyed, it shall be returned to the Originating Party.

ARTICLE 11
VISITS

1. Persons arriving on a visit in the territory of the State of the other Party shall be allowed access to Classified Information only after receiving a prior written consent issued by the Competent Authority of the other Party.
2. The Competent Authority of the visiting Party shall apply with a request for a visit to the Competent Authority of the hosting Party at least 30 days prior to the planned visit referred to in Paragraph 1, and in urgent cases in shorter time.
3. The request referred to in Paragraph 2 shall include information on:
   1) purpose, date and program of the visit, including the highest security classification level of the information the visit involves;
   2) name and surname of the visitor, their date and place of birth, nationality, passport number 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) date, signature and official seal of the Competent Authority of the visiting Party.

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

ARTICLE 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 Competent 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 Competent Authority of the Party in the territory of the State of which the breach has occurred shall inform the Competent Authority of the other Party in writing about the fact, circumstances of the breach and the outcome of the actions referred to in Paragraph 2.

4. In case the breach of security has occurred in the territory of the State of the Third Party, the Competent Authority of the Party which transmitted Classified Information shall take all the measures referred to in Paragraphs 1 – 3 in cooperation with the Third Party.
5. The Competent Authorities of the Parties shall cooperate in the actions referred to in Paragraph 2, upon the request of one of them.

ARTICLE 13
LANGUAGES

In the scope of the implementation of the provisions of this Agreement, the Parties shall use the English language.

ARTICLE 14
EXPENSES

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

ARTICLE 15
CONSULTATIONS

1. The Competent Authorities of the Parties shall notify each other of any amendments to their national law on the protection of Classified Information concerning implementation of this Agreement.
2. The Competent Authorities of the Parties shall consult each other, upon the request of one of them, in order to ensure close cooperation in the implementation of the provisions of this Agreement.
3. Each Party shall allow the representatives of the Competent Authority of the other Party to pay visits to territory of its State to discuss

the procedures for the protection of Classified Information transmitted by the other Party.

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

ARTICLE 17
RELATION TO OTHER AGREEMENTS

From the date this Agreement enters into force, the Memorandum of Understanding between the Ministry of National Defence of the Republic of Poland and the Ministry of Defence of the Kingdom of Denmark Concerning Security Measures for the Protection of Classified Information in the Military Sphere, signed on 2 May 1998, shall cease to be binding. Classified Information which has been or is to be exchanged on the basis of the Memorandum of Understanding mentioned above, shall be protected according to the provisions of this Agreement.

ARTICLE 18

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 the notes. The Agreement shall enter into force on the first day of the second month following the day of receipt of the latter note.
2. This Agreement may be amended on the basis of written consent of the 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 day of receipt of the termination notice.
4. This Agreement shall not apply to the Faroe Islands and Greenland. The provisions of this Agreement may be extended to the Faroe Island and Greenland as may be agreed between the Parties in an exchange of notes.
5. 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.

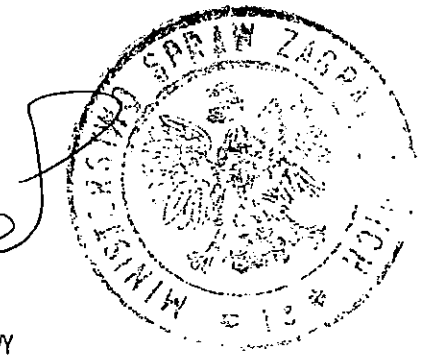
Signed in Warsaw on 8 June 2022 in two original copies, each in the Polish, Danish and English languages, all texts being equally authentic. In case of divergences of interpretation, the English text shall prevail.

FOR THE GOVERNMENT OF THE REPUBLIC OF POLAND

FOR THE GOVERNMENT OF THE KINGDOM OF DENMARK

Stwierdzam zgodność
fotokopii z oryginałem ~~/odpisem~~

Warszawa, dnia 28.6.2022



Konrad Marciniak
Dyrektor
DEPARTAMENT PRAWNO-TRAKTATOWY

Warszawa, 30 sierpnia 2022 r.

MINISTER DO SPRAW UNII EUROPEJSKIEJ

Konrad Szymański

Sygn. DPUE.920.186.2022.EBK(8)
dot.: RM-06111-185-22 z 24.08.2022 r.

Pan Łukasz Schreiber
Sekretarz Rady Ministrów

Opinia
o zgodności z prawem Unii Europejskiej *Umowy między Rządem Rzeczypospolitej Polskiej a Rządem Królestwa Danii o wzajemnej ochronie informacji niejawnych w dziedzinie obronności, podpisanej w Warszawie dnia 8 czerwca 2022 r.,* wyrażona przez ministra właściwego do spraw członkostwa Rzeczypospolitej Polskiej w Unii Europejskiej

Szanowny Panie Ministrze,

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

Umowa nie jest sprzeczna z prawem Unii Europejskiej.

Z poważaniem

Konrad Szymański
Minister do Spraw Unii Europejskiej
/podpisano kwalifikowanym podpisem elektronicznym/

Do wiadomości:
Pan Zbigniew Rau
Minister Spraw Zagranicznych