



DZIENNIK USTAW

RZECZYPOSPOLITEJ POLSKIEJ

Warszawa, dnia 9 lutego 2023 r.

Poz. 267

UMOWA

**między Rządem Rzeczypospolitej Polskiej a Rządem Republiki Turcji
o wzajemnej ochronie informacji niejawnych w dziedzinie przemysłu obronnego,**

sporządzona w Ankarze dnia 24 maja 2021 r.

W imieniu Rzeczypospolitej Polskiej

PREZYDENT RZECZYPOSPOLITEJ POLSKIEJ

podaje do powszechnej wiadomości:

Dnia 24 maja 2021 roku w Ankarze została sporządzona Umowa między Rządem Rzeczypospolitej Polskiej a Rządem Republiki Turcji o wzajemnej ochronie informacji niejawnych w dziedzinie przemysłu obronnego, w następującym brzmieniu:

UMOWA

**między Rządem Rzeczypospolitej Polskiej a Rządem Republiki Turcji
o wzajemnej ochronie informacji niejawnych
w dziedzinie przemysłu obronnego**

Rząd Rzeczypospolitej Polskiej i Rząd Republiki Turcji,
(zwane dalej pojedynczo „Stroną” lub łącznie „Stronami”),

kierując się zamiarem zapewnienia ochrony informacjom niejawnym
związanym z przemysłem obronnym, którym nadano klauzulę tajności
w Państwie jednej ze Stron i które przekazano do Państwa drugiej Strony
i/lub które wytworzono w wyniku współpracy Stron i/lub upoważnionych
podmiotów w Państwach Stron,

pragnąc ustalić procedury i zasady gwarantujące
ochronę informacji niejawnych związanych z kontraktami niejawnymi
zawieranymi w ramach współpracy przemysłów obronnych Stron
i/lub upoważnionych podmiotów w Państwach Stron,

mając na uwadze, że w sprawach nieuregulowanych niniejszą Umową
zastosowanie będą mieć postanowienia *Porozumienia między Rządem
Rzeczypospolitej Polskiej a Rządem Republiki Tureckiej o współpracy
w dziedzinie techniki i przemysłu obronnego,*
podpisanego w Ankarze dnia 19 lipca 1994 roku,

z zastrzeżeniem poszanowania prawa krajowego Stron,

potwierdzając, iż niniejsza Umowa nie wpłynie na obowiązki wynikające
z innych umów międzynarodowych, których Stroną jest którekolwiek z Państw,
oraz nie zostanie wykorzystana przeciwko interesom, bezpieczeństwu bądź
integralności terytorialnej innych państw,

uzgodniły, co następuje:

ARTYKUŁ 1

CEL I ZAKRES

Celem niniejszej Umowy jest ustanowienie procedur i zasad służących zapewnieniu ochrony informacjom niejawnym związanym z przemysłem obronnym, wymienianym w ramach współpracy właściwych organów bezpieczeństwa i/lub upoważnionych podmiotów w Państwach Stron, zgodnie z ich prawem krajowym.

ARTYKUŁ 2

DEFINICJE

1. **„Informacje niejawne”** – oznaczają wszelkie informacje związane z przemysłem obronnym, niezależnie od formy, nośnika i sposobu ich utrwalenia, w tym dokumenty i materiały, będące także w trakcie ich wytwarzania, które wymagają ochrony przed nieuprawnionym ujawnieniem zgodnie z prawem krajowym jednej ze Stron i niniejszą Umową.
2. **„Właściwy organ bezpieczeństwa”** – oznacza jeden z organów właściwy w dziedzinie przemysłu obronnego i odpowiedzialny za wykonywanie niniejszej Umowy, o których mowa w artykule 3 ustęp 1 niniejszej Umowy.
3. **„Kontrakt niejawny”** – oznacza umowę, której realizacja wiąże się z dostępem do informacji niejawnych, lub z wytworzeniem takich informacji, w szczególności taką, która obejmuje wszelkie działania, także przygotowawcze, związane z zakupem bądź sprzedażą wszelkiego typu pojazdów i elementów uzbrojenia, ich istotnych podzespołów lub części, w tym również związane z nimi prace badawczo-rozwojowe, produkcję oraz serwisowanie.
4. **„Kontrahent”** – oznacza osobę fizyczną, osobę prawną lub inną jednostkę organizacyjną podlegającą prawu krajowemu jednej ze Stron, posiadającą

- zdolność do realizowania kontraktów niejawnych zgodnie z postanowieniami niniejszej Umowy.
5. **„Zlecający”** – oznacza osobę fizyczną, osobę prawną lub inną jednostkę organizacyjną podlegającą prawu krajowemu jednej ze Stron, posiadającą zdolność do zlecania kontraktów niejawnych zgodnie z postanowieniami niniejszej Umowy.
 6. **„Świadectwo bezpieczeństwa przemysłowego”** – oznacza dokument wydany zgodnie z prawem krajowym jednej ze Stron przez właściwy organ bezpieczeństwa lub inny uprawniony podmiot, który potwierdza, że kontrahent posiada zdolność do ochrony informacji niejawnych; w przypadku kontrahentów będących osobami fizycznymi funkcję świadectwa bezpieczeństwa przemysłowego pełni poświadczenie bezpieczeństwa.
 7. **„Upoważnione podmioty”** – oznaczają Strony, w tym organy administracji rządowej, osoby prawne lub inne jednostki organizacyjne, jak również osoby fizyczne, właściwe do przetwarzania informacji niejawnych zgodnie ze swoim prawem krajowym.
 8. **„Strona wytwarzająca”** – oznacza Stronę, jak również osoby fizyczne, osoby prawne lub inne jednostki organizacyjne, uprawnione do wytwarzania i przekazywania informacji niejawnych zgodnie z prawem krajowym swojej Strony.
 9. **„Strona otrzymująca”** – oznacza Stronę, jak również osoby fizyczne, osoby prawne lub inne jednostki organizacyjne, uprawnione do otrzymywania informacji niejawnych zgodnie z prawem krajowym swojej Strony.
 10. **„Poświadczenie bezpieczeństwa”** – oznacza dokument wydany zgodnie z prawem krajowym jednej ze Stron przez właściwy organ bezpieczeństwa lub inny uprawniony podmiot, który potwierdza, że osoba fizyczna została poddana postępowaniu sprawdzającemu i jest uprawniona do dostępu do informacji niejawnych.

11. „Strona trzecia” – oznacza państwo, oraz osoby fizyczne, osoby prawne lub inne jednostki organizacyjne podlegające jego jurysdykcji lub organizację międzynarodową, niebędące Stronami niniejszej Umowy.

ARTYKUŁ 3

WŁAŚCIWE ORGANY BEZPIECZEŃSTWA

1. Właściwymi organami bezpieczeństwa, odpowiedzialnymi za stosowanie niniejszej Umowy, są:
 - 1) w Rzeczypospolitej Polskiej: Szef Agencji Bezpieczeństwa Wewnętrznego;
 - 2) w Republice Turcji: Ministerstwo Obrony Narodowej Republiki Turcji, Departament Techniczny.
2. Strony informują się w drodze dyplomatycznej o zmianach właściwych organów bezpieczeństwa lub zmianach ich właściwości.

ARTYKUŁ 4

KLAUZULE TAJNOŚCI

1. W ramach środków bezpieczeństwa przewidzianych swoim prawem krajowym, właściwe organy bezpieczeństwa i upoważnione podmioty zobowiązują się zapewnić odpowiednią ochronę informacjom niejawnym wymienianym lub wytworzonym w trakcie współpracy oraz uzgadniają, iż wymienione w poniższej tabeli w językach: polskim, tureckim i angielskim, klauzule tajności są równorzędne:

W RZECZYPOSPOLITEJ POLSKIEJ	W REPUBLICIE TURCJI	ODPOWIEDNIK W JĘZYKU ANGIELSKIM
ŚCIŚLE TAJNE	ÇOK GİZLİ	TOP SECRET
TAJNE	GİZLİ	SECRET
POUFNE	ÖZEL	CONFIDENTIAL
ZASTRZEŻONE	HİZMETE ÖZEL	RESTRICTED

2. Właściwy organ bezpieczeństwa oraz upoważnione podmioty zobowiązują się oznaczać informacje niejawne otrzymane od właściwego organu bezpieczeństwa lub upoważnionych podmiotów Państwa drugiej Strony równorzędną krajową klauzulą tajności oraz jej odpowiednikiem w języku angielskim, zgodnie z przedstawioną powyżej tabelą.
3. Właściwe organy bezpieczeństwa zobowiązują się informować wzajemnie o zmianach w klauzulach tajności.
4. Klauzula tajności informacji niejawnych może być zmieniona lub zniesiona wyłącznie przez Stronę wytwarzającą. Strona otrzymująca jest niezwłocznie powiadamiana przez Stronę wytwarzającą o każdym przypadku zmiany lub zniesienia klauzuli tajności.

ARTYKUŁ 5

ZASADY OCHRONY INFORMACJI NIEJAWNYCH

1. Strony podejmą wszelkie działania przewidziane w niniejszej Umowie i ich prawie krajowym w celu ochrony informacji niejawnych przekazywanych lub wytwarzanych w ramach współpracy między Stronami, w tym w związku z realizacją kontraktów niejawnych.
2. Informacje niejawne przekazywane i/lub wytwarzane w ramach współpracy właściwych organów bezpieczeństwa i/lub upoważnionych podmiotów w Państwach Stron wykorzystywane są wyłącznie zgodnie z celem, dla którego zostały przekazane.
3. Informacje niejawne nie są udostępniane stronie trzeciej bez uprzedniej pisemnej zgody Strony wytwarzającej.
4. Informacje niejawne mogą być udostępniane tylko tym osobom, których zadania służbowe wymagają zapoznania się lub posiadania takich informacji i które zostały upoważnione do dostępu do nich zgodnie z prawem krajowym Strony otrzymującej.

5. W zakresie niniejszej Umowy, właściwe organy bezpieczeństwa uznają wzajemnie poświadczenia bezpieczeństwa i świadectwa bezpieczeństwa przemysłowego wydane zgodnie z prawem krajowym drugiej Strony.

ARTYKUŁ 6

PRZEKAZYWANIE INFORMACJI NIEJAWNYCH

1. Informacje niejawne są przekazywane w drodze dyplomatycznej lub za pośrednictwem attaché wojskowego.
2. Informacje niejawne o klauzuli ZASTRZEŻONE / HİZMETE ÖZEL / RESTRICTED mogą być przekazywane również za pośrednictwem uprawnionych do tego przewoźników, zgodnie z prawem krajowym Strony wytwarzającej.
3. W pilnych przypadkach, o ile nie można skorzystać z innej formy przekazania informacji niejawnych, jeżeli spełnione są wymogi bezpieczeństwa określone prawem krajowym Strony wytwarzającej, dopuszczalny jest przewóz osobisty informacji niejawnych o klauzuli ZASTRZEŻONE / HİZMETE ÖZEL / RESTRICTED przez osoby do tego upoważnione.
4. Właściwe organy bezpieczeństwa mogą, zgodnie ze swoim prawem krajowym, ustalić inne sposoby przekazywania informacji niejawnych zapewniające ich ochronę przed nieuprawnionym ujawnieniem.
5. Strona otrzymująca potwierdza pisemnie odbiór informacji niejawnych.

ARTYKUŁ 7

TŁUMACZENIE, POWIELANIE

I NISZCZENIE INFORMACJI NIEJAWNYCH

1. Informacje niejawne o klauzuli POUFNE / ÖZEL / CONFIDENTIAL lub wyższej są tłumaczone lub powielane tylko po uprzednim uzyskaniu

- pisemnego zezwolenia wydanego przez właściwy organ bezpieczeństwa Strony wytwarzającej.
2. Wszelkie tłumaczenia informacji niejawnych oznacza się odpowiednią klauzulą tajności oraz adnotacją wskazującą, iż dokument niejawny został otrzymany od Strony wytwarzającej. Przetłumaczone lub powielone informacje niejawne podlegają takiej samej kontroli i ochronie jak ich oryginały. Liczbę kopii lub tłumaczeń należy ograniczyć do liczby wymaganej dla celów służbowych.
 3. Informacje niejawne o klauzuli ZASTRZEŻONE / HİZMETE ÖZEL / RESTRICTED są niszczone zgodnie z prawem krajowym Strony otrzymującej w sposób uniemożliwiający ich częściowe lub całkowite odtworzenie. Informacje niejawne o klauzuli POUFNE / ÖZEL / CONFIDENTIAL lub wyższej nie są natomiast niszczone; są one, po wykorzystaniu, zwracane Stronie wytwarzającej.

ARTYKUŁ 8

KONTRAKTY NIEJAWNE

1. Przed zawarciem kontraktu niejawnego zlecający składa wniosek do właściwego organu bezpieczeństwa swojej Strony w celu wystąpienia do właściwego organu bezpieczeństwa drugiej Strony z prośbą o potwierdzenie, że kontrahent posiada ważne świadectwo bezpieczeństwa przemysłowego odpowiednie do klauzuli informacji niejawnych, do których będzie miał dostęp.
2. W przypadku, gdy zlecający podlega prawu Republiki Turcji, przed zawarciem kontraktu niejawnego związanego z dostępem do informacji niejawnych o klauzuli ZASTRZEŻONE / HİZMETE ÖZEL / RESTRICTED właściwy organ bezpieczeństwa Rzeczypospolitej Polskiej potwierdza, że polski kontrahent spełnia wymagania bezpieczeństwa określone prawem krajowym.

3. Potwierdzenie, o którym mowa w ustępach 1 lub 2, 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 kontrahent ma swoją siedzibę.
4. Informacje niejawne nie są udostępniane kontrahentowi do czasu uzyskania potwierdzenia, o którym mowa w ustępach 1 lub 2.
5. Zlecający przekazuje kontrahentowi instrukcję bezpieczeństwa przemysłowego niezbędną do realizacji kontraktu niejawnego związanego z dostępem do informacji niejawnych o klauzuli POUFNE / ÖZEL / CONFIDENTIAL lub wyższej, która stanowi integralną część kontraktu niejawnego. W instrukcji bezpieczeństwa przemysłowego zamieszcza się postanowienia dotyczące wymogów bezpieczeństwa, w szczególności:
 - 1) wykaz rodzajów informacji niejawnych odnoszących się do danego kontraktu niejawnego, z uwzględnieniem ich klauzul tajności;
 - 2) procedury postępowania z informacjami niejawnymi, które zostaną przekazane wykonawcy lub przez niego wytworzone podczas realizacji kontraktu niejawnego.
6. Zlecający przekazuje kopię instrukcji bezpieczeństwa przemysłowego właściwemu organowi bezpieczeństwa swojej Strony, który przekazuje ją właściwemu organowi bezpieczeństwa Strony kontrahenta.
7. Realizacja kontraktu niejawnego w części związanej z dostępem do informacji niejawnych jest możliwa po spełnieniu przez kontrahenta niezbędnych warunków zapewniających ochronę informacji niejawnych, zgodnie z instrukcją bezpieczeństwa przemysłowego.
8. Każdy podwykonawca podlega tym samym obowiązkom ochrony informacji niejawnych, jakie ustalono dla kontrahenta.
9. Prawa własności intelektualnej obejmujące informacje niejawne w ramach kontraktów niejawnych będą wzajemnie respektowane zgodnie z prawem krajowym. Szczegóły mogą być określone w kontraktach niejawnych.

ARTYKUŁ 9
NARUSZENIE REGULACJI DOTYCZĄCYCH
WZAJEMNEJ OCHRONY INFORMACJI NIEJAWNYCH

1. Naruszeniem regulacji dotyczących wzajemnej ochrony informacji niejawnych jest działanie lub zaniechanie sprzeczne z niniejszą Umową lub prawem krajowym Stron, dotyczącym ochrony informacji niejawnych.
2. Informację o każdym przypadku naruszenia lub podejrzeniu naruszenia regulacji dotyczących wzajemnej ochrony informacji niejawnych przekazanych przez Stronę wytwarzającą lub informacji niejawnych wytworzonych w wyniku wspólnego działania Stron przekazuje się niezwłocznie właściwemu organowi bezpieczeństwa Strony, na terytorium Państwa której miało miejsce naruszenie lub zaistniało podejrzenie takiego naruszenia.
3. Każdy przypadek naruszenia lub podejrzenia naruszenia regulacji dotyczących wzajemnej ochrony informacji niejawnych wyjaśnia się zgodnie z prawem krajowym Strony, na terytorium Państwa której zdarzenie miało miejsce.
4. W przypadku naruszenia regulacji dotyczących wzajemnej ochrony informacji niejawnych, właściwy organ bezpieczeństwa Strony, na terytorium Państwa której naruszenie miało miejsce, pisemnie powiadamia właściwy organ bezpieczeństwa drugiej Strony o tym zdarzeniu, okolicznościach naruszenia oraz wyniku czynności, o których mowa w ustępie 3.
5. Właściwe organy bezpieczeństwa współpracują przy czynnościach, o których mowa w ustępie 3, na wniosek jednego z nich.

ARTYKUŁ 10**WIZYTY**

1. Wizyty w obiektach upoważnionych podmiotów w Państwie każdej ze Stron związane z dostępem do informacji niejawnych, organizowane w ramach współpracy właściwych organów bezpieczeństwa i/lub upoważnionych podmiotów w Państwach Stron, są możliwe tylko po uzyskaniu pisemnego zezwolenia wydanego przez właściwy organ bezpieczeństwa Strony przyjmującej.
2. Wnioski o wyrażenie zgody na wizytę składa się pisemnie właściwemu organowi bezpieczeństwa Strony przyjmującej, co najmniej 21 (dwadzieścia jeden) dni przed planowanym terminem wizyty. Wnioski przedkładane są w drodze dyplomatycznej lub za pośrednictwem attaché wojskowego.
3. We wniosku o wyrażenie zgody na wizytę każdorazowo umieszcza się następujące informacje:
 - a) imię i nazwisko, datę i miejsce urodzenia, obywatelstwo, numer paszportu oraz stanowisko służbowe osób przybywających z wizytą,
 - b) proponowany termin, program oraz przewidywany czas trwania wizyty,
 - c) poziom poświadczenia bezpieczeństwa posiadanego przez osoby przybywające z wizytą oraz rodzaj i klauzula tajności informacji niejawnych, z dostępem do których związana jest wizyta,
 - d) nazwy odwiedzanych obiektów i jednostek oraz cel wizyty,
 - e) imiona i nazwiska oraz stanowiska służbowe osób przyjmujących,
 - f) datę, podpis oraz oficjalną pieczęć właściwego organu bezpieczeństwa Strony wysyłającej.
4. Zgodę wydaje się wyłącznie na przeprowadzenie wizyty w określonym terminie. W celu ułatwienia współpracy możliwe jest jednak sporządzenie planu wizyty na okres nie dłuższy niż 12 (dwanaście) miesięcy.

W przypadku gdy planowana wizyta ma trwać dłużej niż na to zezwolono i konieczne jest przedłużenie okresu jej trwania, właściwy organ bezpieczeństwa Strony wysyłającej występuje z kolejnym wnioskiem o wyrażenie zgody na wizytę, co najmniej 21 (dwadzieścia jeden) dni przed upłynięciem ważności zezwolenia na aktualnie realizowaną wizytę.

5. Do ochrony danych osobowych, o których mowa w ustępie 3, stosuje się, z uwzględnieniem prawa krajowego Stron, następujące postanowienia:
- a) wykorzystanie danych osobowych przez Stronę przyjmującą wizytę jest dopuszczalne wyłącznie w celu określonym przez Stronę przekazującą dane osobowe oraz na warunkach określonych przez tę Stronę;
 - b) Strona przyjmująca wizytę nie przechowuje danych osobowych dłużej, aniżeli jest to niezbędne dla osiągnięcia celu przetwarzania;
 - c) w przypadku przekazania danych osobowych, których nie wolno było przekazać zgodnie z prawem krajowym Strony przekazującej dane osobowe, Strona ta zawiadamia o tym Stronę przyjmującą wizytę, która jest zobowiązana do usunięcia tych danych w sposób uniemożliwiający ich częściowe lub całkowite odtworzenie;
 - d) Strona przekazująca dane osobowe odpowiada za merytoryczną poprawność przekazywanych danych i jeśli okaże się, że przekazane zostały dane nieprawdziwe lub niekompletne, zawiadamia o tym Stronę przyjmującą wizytę, która jest zobowiązana do sprostowania lub usunięcia tych danych;
 - e) Strona przekazująca dane osobowe oraz Strona przyjmująca wizytę są zobowiązane do rejestrowania przekazywania, otrzymywania i usuwania danych osobowych;
 - f) Strona przekazująca dane osobowe oraz Strona przyjmująca wizytę są zobowiązane do skutecznej ochrony przetwarzanych danych przed ich udostępnieniem osobom nieupoważnionym,

nieuprawnionym dokonywaniem zmian tych danych, ich utratą, uszkodzeniem lub zniszczeniem.

ARTYKUŁ 11

JĘZYKI

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

ARTYKUŁ 12

KOSZTY

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

ARTYKUŁ 13

KONSULTACJE I ZMIANY

1. Każda ze Stron może przedstawić propozycję konsultacji i/lub zmian do niniejszej Umowy w drodze pisemnej notyfikacji złożonej drugiej Stronie.
2. Umowa niniejsza może zostać zmieniona na podstawie pisemnej zgody Stron. Takie zmiany wejdą w życie zgodnie z postanowieniami artykułu 16.
3. W celu zapewnienia skutecznej współpracy będącej przedmiotem niniejszej Umowy i w zakresie kompetencji przyznanych właściwym organom bezpieczeństwa w prawie krajowym każdej ze Stron, organy te mogą, w razie potrzeby, zawierać pisemne szczegółowe uzgodnienia techniczne.

4. Właściwe organy bezpieczeństwa informują się wzajemnie o wszelkich zmianach w swoim prawie krajowym dotyczącym ochrony informacji niejawnych, w zakresie niezbędnym do wykonywania niniejszej Umowy.

ARTYKUŁ 14

ROZSTRZYGANIE SPORÓW

1. Wszelkie sporne kwestie dotyczące stosowania i interpretacji niniejszej Umowy rozstrzygane będą w drodze bezpośrednich negocjacji między właściwymi organami bezpieczeństwa. Spory nie będą przekazywane do rozstrzygnięcia jakimkolwiek krajowym, międzynarodowym sądom lub stronie trzeciej.
2. Jeśli nie jest możliwe rozwiązanie sporu w sposób, o którym mowa w ustępie 1, jest on rozstrzygany w drodze dyplomatycznej. W przypadku braku możliwości osiągnięcia porozumienia, niniejsza Umowa może być wypowiedziana przez każdą ze Stron.

ARTYKUŁ 15

CZAS OBOWIĄZYWANIA I WYPOWIEDZENIE

1. Umowa niniejsza zawarta jest na okres pięciu lat i będzie automatycznie przedłużana na kolejne pięcioletnie okresy, o ile nie zostanie wypowiedziana z trzydziestodniowym wypowiedzeniem poprzez notyfikację w drodze dyplomatycznej. Może być również wypowiedziana w drodze pisemnej notyfikacji przez każdą ze Stron. W takim przypadku Umowa utraci moc po upływie trzech miesięcy od otrzymania notyfikacji.
2. W przypadku wypowiedzenia niniejszej Umowy, informacje niejawne przekazane lub wytworzone na jej podstawie będą nadal chronione zgodnie z jej postanowieniami.

ARTYKUŁ 16 WEJŚCIE W ŻYCIE

Umowa niniejsza wejdzie w życie w pierwszym dniu drugiego miesiąca, który nastąpi po dniu otrzymania w drodze dyplomatycznej ostatniej z not wymienionych przez Strony, informującej o zakończeniu wewnętrznych procedur niezbędnych do wejścia Umowy w życie.

Na dowód czego, niżej podpisani, odpowiednio upoważnieni przez swoje Rządy, podpisali niniejszą Umowę.

Sporządzono w Ankarze dnia 24 maja 2021 roku w dwóch jednobrzmiących egzemplarzach, każdy w językach polskim, tureckim i angielskim, przy czym wszystkie teksty mają jednakową moc. W przypadku rozbieżności przy interpretacji postanowień niniejszej Umowy, za rozstrzygający uważa się tekst w języku angielskim.

Z UPOWAŻNIENIA RZĄDU
RZECZYPOSPOLITEJ POLSKIEJ



Z UPOWAŻNIENIA RZĄDU
REPUBLIKI TURCJI



**POLONYA CUMHURİYETİ HÜKÜMETİ
İLE
TÜRKİYE CUMHURİYETİ HÜKÜMETİ
ARASINDA
SAVUNMA SANAYİNDE
GİZLİLİK DERECELİ BİLGİLERİN KARŞILIKLI
KORUNMASINA
İLİŞKİN
ANLAŞMA**

Polonya Cumhuriyeti Hükümeti ile Türkiye Cumhuriyeti Hükümeti (bundan böyle ferdi olarak Taraf, müştereken Taraflar şeklinde anılacaktır),

Bir Tarafın ülkesinde gizlilik derecesi verilmiş ve diğer Tarafın ülkesine gönderilmiş ve/veya Taraflar ve/veya Tarafların ülkelerindeki Yetkili Kuruluşlar arasındaki karşılıklı işbirliğiyle oluşturulmuş savunma sanayi ile ilgili Gizlilik Dereceli Bilgilerin güvenliğini sağlamayı niyet ederek,

Taraflar ve/veya Tarafların ülkelerindeki Yetkili Kuruluşlar arasındaki savunma sanayi işbirliği çerçevesinde akdedilen Gizlilik Dereceli Sözleşmelerle ilgili Gizlilik Dereceli Bilgilerin güvenliğini sağlamaya yönelik usul ve esasların oluşturulmasını arzu ederek,

Bu Anlaşmada hüküm bulunmayan hususlarda 19 Temmuz 1994'te Ankara'da imzalanan *Polonya Cumhuriyeti Hükümeti ile Türkiye Cumhuriyeti Hükümeti arasında Teknik ve Savunma Sanayi İşbirliğine Dair Anlaşma*'yı dikkate alarak ve uygulayarak,

Tarafların ulusal mevzuatlarına maruz olarak,

Bu Anlaşmanın; her iki ülkenin taraf olduğu diğer uluslararası anlaşmalardan doğan yükümlülükleri etkilemeyeceğini ve diğer devletlerin çıkarları, güvenliği ve toprak bütünlüğüne karşı kullanılmayacağını teyit ederek,

Aşağıdaki şekilde anlaşmışlardır:

MADDE 1

AMAÇ VE KAPSAM

İşbu Anlaşmanın amacı, kendi ilgili ulusal mevzuatına uygun olarak Tarafların ülkelerindeki Yetkili Güvenlik Makamları ve/veya Yetkili Kuruluşlar arasında gerçekleştirilen işbirliği faaliyetleri kapsamında savunma sanayiyle ilgili Gizlilik Dereceli Bilgilerin güvenliğinin sağlanması için usul ve esasları belirlemektir.

MADDE 2

TANIMLAR

1. **Gizlilik Dereceli Bilgi** – her iki Tarafın ulusal mevzuatına ve bu Anlaşmaya uygun olarak, şekli, taşıyıcısı ve kayıt yöntemine bakmaksızın, yetkisiz ifşaya karşı koruma gerektiren, üretilme sürecinde olan belgeler ve malzeme dahil, savunma sanayine ilişkin her tür bilgiyi ifade eder.
2. **Yetkili Güvenlik Makamı** – bu Anlaşmanın 3'üncü maddesinin 1'inci paragrafında belirtildiği şekilde, bu Anlaşmanın uygulanmasından sorumlu ve savunma sanayi konusunda yetkili olan otoriteyi ifade eder.
3. **Gizlilik Dereceli Sözleşme** – gerçekleştirilmesi Gizlilik Dereceli Bilgiye erişimi veya bu gibi bilgilerin oluşturulmasını kapsayan, özellikle, hazırlık faaliyetleri dâhil olmak üzere, her tür araç ve savaş ve silah teçhizatı ile önemli ve kritik alt sistemler ve bunların parçalarının alım ve satımı, araştırma ve geliştirme ile her tür üretim veya servisi ile ilgili her tür işi kapsayan bir sözleşmeyi ifade eder.
4. **Yüklenici** – bu Anlaşmanın hükümlerine uygun olarak Gizlilik Dereceli Sözleşmeler yapmak için hukuki ehliyete sahip, Taraflardan birinin kanunları kapsamındaki bir gerçek kişi, tüzel kişi veya diğer bir teşekkülü ifade eder.

5. **İdare** – bu Anlaşmanın hükümlerine uygun olarak Yüklenicilere Gizlilik Dereceli İhale vermek için hukuki ehliyete sahip, Taraflardan birinin kanunları kapsamındaki bir gerçek kişi, tüzel kişi veya diğer bir teşekkülü ifade eder.
6. **Tesis Güvenlik Belgesi** – bir Tarafın ulusal mevzuatına uygun olarak Yetkili Güvenlik Makamı veya başka bir yetkili kuruluş tarafından verilen, bir Yüklenicinin Gizlilik Dereceli Bilgiyi koruma kabiliyetine sahip olduğunu doğrulayan bir belgeyi ifade eder; Yüklenici sıfatıyla hareket eden tek malikler olması durumunda, Kişi Güvenlik Belgesi, Tesis Güvenlik Belgesi'nin eşiti olacaktır.
7. **Yetkili Kuruluşlar** – Gizlilik Dereceli Bilgiyi kendi ilgili ulusal mevzuatlarına uygun olarak kullanmaya yetkili gerçek kişiler ile hükümet kurumları, tüzel kişiler veya başka teşekküller dahil Tarafları ifade eder.
8. **Kaynak Taraf** – kendi Tarafının ulusal mevzuatına uygun olarak Gizlilik Dereceli Bilgi oluşturma ve göndermeye yetkili Taraf, gerçek kişiler, tüzel kişiler veya başka teşekkülleri ifade eder.
9. **Alan Taraf** – kendi Tarafının ulusal mevzuatına uygun olarak Gizlilik Dereceli Bilgi almaya yetkili Taraf, gerçek kişiler, tüzel kişiler veya başka teşekkülleri ifade eder.
10. **Kişi Güvenlik Belgesi** – bir Tarafın ulusal mevzuatına uygun olarak Yetkili Güvenlik Makamı veya diğer yetkili kuruluş tarafından verilen, bir kişinin güvenlik incelemesinden geçtiğini ve Gizlilik Dereceli Bilgiye erişim için uygun olduğunu doğrulayan bir belgeyi ifade eder.
11. **Üçüncü Taraf** – yetkisi altındaki gerçek kişi, tüzel kişi veya diğer bağlı teşekkülleri de dâhil olmak üzere bu Anlaşmaya Taraf olmayan herhangi bir ülke veya bir uluslararası teşkilatı ifade eder.

MADDE 3

YETKİLİ GÜVENLİK MAKAMLARI

1. Bu Anlaşmanın uygulanmasından sorumlu olan Yetkili Güvenlik Makamları aşağıdadır:

- 1) Polonya Cumhuriyeti için: İç Güvenlik Kurumu Başkanı;
- 2) Türkiye Cumhuriyeti için: Türkiye Cumhuriyeti Millî Savunma Bakanlığı,
Teknik Hizmetler Dairesi Başkanlığı.

2. Taraflar, Yetkili Güvenlik Makamlarının değişiklikleriyle veya yetkilerine yapılan değişikliklerle ilgili olarak diplomatik kanallarla birbirlerini bilgilendireceklerdir.

MADDE 4

GÜVENLİK SINIFLANDIRMALARI

1. İlgili ulusal mevzuatlarında belirtilen güvenlik önlemleri çerçevesinde, Yetkili Güvenlik Makamları ve Yetkili Kuruluşlar, aralarında mübadele edilen veya karşılıklı işbirliğiyle üretilen Gizlilik Dereceli Bilginin korunmasını gereğince sağlamayı taahhüt ederek, aşağıdaki tabloda gösterilen Lehçe, Türkçe ve İngilizce gizlilik derecesi seviyelerinin eşdeğerliğini kabul ederler:

Polonya Cumhuriyeti'nde	Türkiye Cumhuriyeti'nde	İngilizce karşılığı
“ŚCIŚLE TAJNE”	“ÇOK GİZLİ”	“TOP SECRET”
“TAJNE”	“GİZLİ”	“SECRET”
“POUFNE”	“ÖZEL”	“CONFIDENTIAL”
“ZASTRZEŻONE”	“HİZMETE ÖZEL”	“RESTRICTED”

2. Yetkili Güvenlik Makamı ve Yetkili Kuruluşları, diğer Tarafın devletinde Yetkili Güvenlik Makamı veya Yetkili Kuruluşlarından aldıkları Gizlilik Dereceli Bilgiyi yukarıdaki tabloya uygun olarak kendi ulusal sınıflandırma seviyesi ve İngilizce karşılığı ile işaretlemeyi taahhüt eder.

3. Yetkili Güvenlik Makamları, güvenlik sınıflandırmalarında yapılan değişiklikler hakkında birbirlerini karşılıklı olarak bilgilendirmeyi taahhüt ederler.

4. Gizlilik Dereceli Bilgiye verilen güvenlik sınıflandırması seviyesi sadece Kaynak Tarafça değiştirilebilir veya kaldırılabilir. Böyle bir değişiklik veya kaldırma kararı Kaynak Tarafça Alan Tarafa derhal bildirilecektir.

MADDE 5

GİZLİLİK DERECELİ BİLGİYİ KORUMA USULLERİ

1. Taraflar, Gizlilik Dereceli Sözleşmelerin gerçekleştirilmesiyle bağlantılı olarak oluşturulan işbu belge dahil olmak üzere Taraflar arasındaki işbirliğinin sonucu olarak gönderilen veya oluşturulan Gizlilik Dereceli Bilgiyi korumak için bu Anlaşmada belirtilen ve kendi ulusal mevzuatlarına tabi her tedbiri kabul edeceklerdir.

2. Yetkili Güvenlik Makamları ve/veya Tarafların ülkelerindeki Yetkili Kuruluşlar arasında karşılıklı işbirliğiyle üretilen ve/veya mübadele edilen Gizlilik Dereceli Bilgi sadece transfer amacı doğrultusunda kullanılacaktır.

3. Gizlilik Dereceli Bilgi, Kaynak Tarafın önceden yazılı onayı olmadan bir Üçüncü Tarafa ifşa edilmeyecektir.

4. Gizlilik Dereceli Bilgi sadece resmi görev ve hizmetleri icra etmek için söz konusu bilgiye sahip olma gereksinimi bulunan ve Alan Tarafın ulusal mevzuatına uygun şekilde gereğince yetkilendirilmiş kişilere ifşa edilebilir.

5. Bu Anlaşmanın kapsamında, Yetkili Güvenlik Makamları, diğer Tarafın ulusal mevzuatına uygun olarak verilen Kişi Güvenlik Belgeleri ve Tesis Güvenlik Belgelerini kabul edecektir.

MADDE 6**GİZLİLİK DERECELİ BİLGİNİN TRANSFERİ**

1. Gizlilik Dereceli Bilgi diplomatik kanallar veya askeri atışe yoluyla gönderilecektir.
2. ZASTRZEŻONE / HİZMETE ÖZEL / RESTRICTED olarak sınıflandırılan bilgi ayrıca Kaynak Tarafın ulusal mevzuatına uygun olarak yetkili taşıyıcılar aracılığıyla da gönderilebilir.
3. Acil durumlarda, Gizlilik Dereceli Bilginin diğeri gönderim şekillerini kullanmak mümkün değılse, Kaynak Tarafın ulusal mevzuatı tarafından tanımlanan güvenlik şartlarının yerine getirilmesi durumunda ZASTRZEŻONE / HİZMETE ÖZEL / RESTRICTED olarak sınıflandırılan bilginin yetkili kişiler tarafından kişisel olarak taşınması kabul edilebilir.
4. Yetkili Güvenlik Makamları, kendi ilgili ulusal mevzuatlarına uygun olarak Gizlilik Dereceli Bilgiyi yetkisiz ifşaya karşı koruyan başka gönderim şekilleri üzerinde anlaşabilirler.
5. Alan Taraf, Gizlilik Dereceli Bilginin alındığını yazılı olarak doğrulayacaktır.

MADDE 7**GİZLİLİK DERECELİ BİLGİLERİN TERCÜME EDİLMESİ,
ÇOĞALTILMASI VE İMHA EDİLMESİ**

1. POUFNE / ÖZEL / CONFIDENTIAL veya üzeri güvenlik sınıflandırma seviyeleri ile işaretlenen gizlilik dereceli bilgiler sadece Kaynak Tarafın Yetkili Güvenlik Makamından önceden yazılı izin alınmak kaydı ile tercüme edilebilecek veya çoğaltılabilecektir.
2. Gizlilik Dereceli Bilgilerin bütün tercümeleri; gizlilik dereceli belgenin Kaynak Taraftan alındığını belirtecek şekilde, uygun bir güvenlik sınıflandırma işareti ve notları içerecektir. Bu şekilde tercüme edilmiş ya da çoğaltılmış bilgiler orijinali ile aynı kontrol ve korumaya tâbi tutulacaktır. Nüsha ve tercümelerin sayısı, resmi amaçlar için talep edilen miktar ile sınırlı olacaktır.

3. ZASTRZEŻONE / HİZMETE ÖZEL / RESTRICTED olarak tasnif edilen bilgilerin tamamen veya kısmen birleştirilmesini engelleyecek şekilde Alan Tarafın ulusal düzenlemelerine göre imha edilecektir. Ancak; POUFNE / ÖZEL / CONFIDENTIAL veya üzeri tasnif edilen bilgiler, süresi ya da kullanım amacı sona erdiğinde imha edilmek yerine Alan Tarafça Kaynak Tarafa iade edilecektir.

MADDE 8

GİZLİLİK DERECELİ SÖZLEŞMELER

1. Gizlilik Dereceli bir Sözleşme akdedilmeden önce İdare, kendi Yetkili Güvenlik Makamından, diğer Tarafın Yetkili Güvenlik Makamının Yüklenicinin erişmesi gereken Gizlilik Dereceli Bilginin güvenlik tasnif seviyesi ile ilgili olarak geçerli bir Tesis Güvenlik Kleransına sahip olduğunun onayını almasını ister.
2. İdare'nin Türkiye Cumhuriyeti mevzuatına tabi olması durumunda; ZASTRZEŻONE / HİZMETE ÖZEL / RESTRICTED olarak tasnif edilmiş olan Gizlilik Dereceli bir Sözleşme akdedilmeden önce Polonya Cumhuriyeti Yetkili Güvenlik Makamının, Polonyalı bir Yüklenicinin ulusal düzenlemeler ışığında güvenlik şartlarını karşılayacağını onaylayacaktır.
3. Paragraf 1 veya 2'de bahsi geçen onaylar, Yüklenicinin, topraklarında bulunduğu tarafın devletinin ulusal mevzuatında tanımlanan Gizlilik Dereceli Bilgilerin korunması bağlamındaki kriterleri karşıladığını beyan etmek için gerekli önlemlerin alındığının garantisi ile eşdeğer olacaktır.
4. Gizlilik Dereceli Bilgiler, Paragraf 1 veya 2'de bahsi geçen onaylar alınmadan Yükleniciye verilmeyecektir.
5. İdare, Yükleniciye Gizlilik Dereceli bir Sözleşmenin uygulanmasında gerekli olan ve bu tür sözleşmelerin ayrılmaz bir parçası olarak, POUFNE / ÖZEL / CONFIDENTIAL ya da daha üstü olarak tasnif edilmiş bilgilere erişimle ilgili bir proje güvenlik talimatı yayımlayacaktır. Proje güvenlik talimatı, başlıca şu güvenlik şartlarını ihtiva etmelidir:

- 1) Güvenlik sınıflandırma seviyeleri de dâhil olmak üzere, Gizlilik Dereceli Sözleşmeye ilişkin Gizlilik Dereceli Bilgi çeşitlerinin listesi;
- 2) Gizlilik dereceli bilginin icrasında ortaya çıkan veya yükleniciye sağlanan gizlilik dereceli bilginin taşınmasına ilişkin prosedürler.
6. İdare, Yüklenicinin Tarafının Yetkili Güvenlik Makamına ileilmek üzere kendi Tarafının Yetkili Güvenlik Makamına proje güvenlik talimatının bir kopyasını verecektir.
7. Gizlilik Dereceli bir Sözleşmenin uygulanmasında, Gizlilik Dereceli Bilgilere erişim ile ilgili kısım, Yüklenicinin, Gizlilik Dereceli Bilgilerin korunması için gerekli kriterleri proje güvenlik talimatına uygun olarak karşılaması şartıyla mümkün olacaktır.
8. Her bir altyüklenici de Yüklenici için konulan Gizlilik Dereceli Bilgilerin Korunması şartlarına aynen uymakla yükümlüdür.
9. Gizlilik Dereceli Sözleşmeler kapsamındaki Gizlilik Dereceli Bilgilere ilişkin fikri mülkiyet haklarına, ulusal mevzuatlar uyarınca karşılıklı olarak riayet edilecektir. Söz konusu detay Gizlilik Dereceli Sözleşmelerde belirtilecektir.

MADDE 9

GÜVENLİK İHLÂLİ

1. Güvenlik ihlali, Gizlilik Dereceli Bilgilerin korunmasına ilişkin Tarafların yasal mevzuatlarına ya da bu Anlaşmaya aykırı olarak yapılmış olan eylem ya da ihmallerdir.
2. Kaynak Tarafa ait olan veya Tarafların işbirliği sonucu ortaya çıkan Gizlilik Dereceli Bilgilere ilişkin her tür güvenlik ihlali ya da güvenlik ihlali şüphesi bilgileri, ihlalin ya da ihlal şüphesinin yer aldığı ülkedeki Taraf devletin Yetkili Güvenlik Makamına derhal rapor edilecektir.
3. Her tür güvenlik ihlali ya da güvenlik ihlali şüphesi, ortaya çıktığı Taraf ülkedeki devletin ulusal düzenlemelerine uygun olarak tahkik edilecektir.

4. Bir güvenlik ihlali halinde, ihlalin yer aldığı Taraf ülkenin Yetkili Güvenlik Makamı, diğer Tarafın devletinin Yetkili Güvenlik Makamını olay, ihlalin olduğu koşullar ve Paragraf 3'te değinilen eylemlerin sonucu hakkında yazılı olarak bilgilendirecektir.

5. Yetkili Güvenlik Makamları, birinin diğerinden talep etmesi halinde Paragraf 3'te değinilen eylemler üzerinde işbirliği yapacaktır.

MADDE 10

ZİYARETLER

1. Tarafların Yetkili Güvenlik Makamları ve/veya ülkesindeki Yetkili Kuruluşlar arasındaki iş birliği faaliyetleri kapsamında bir Tarafın ülkesindeki Yetkili Kuruluşların tesislerine yapılacak Gizlilik Dereceli Bilgilere erişim içerikli ziyaretler, Ev Sahibi Ülkenin Yetkili Güvenlik Makamının yazılı izninin alınmasını müteakip gerçekleştirilecektir.

2. Ziyarete yönelik talepler, önerilen ziyaret tarihinden en az 21 (yirmi bir) gün öncesinden yazılı olarak Ev Sahibi ülkenin Yetkili Güvenlik Makamına bildirilecektir. Bu talepler, diplomatik kanallar ya da askeri ataşeler aracılığıyla arz edilecektir.

3. Ziyarete yönelik talep biçimleri aşağıdaki müteakip bilgileri içerecek şekilde her bir ziyaret için hazırlanacaktır.

a. Konuk personelin adı ve soyadı, doğum yeri ve tarihi, uyruğu, pasaport numarası ve görevleri,

b. Öngörülen tarih, program ve tahmin edilen ziyaret süresi,

c. Konuk personelin sahip olacağı Kişi Güvenlik Belgesi düzeyi güvenlik sınıflandırma düzeyinin yanı sıra erişilecek gizlilik dereceli bilgilerin türü,

d. Ziyaret edilecek yer ve tesislerin adları ve ziyaretin amacı,

e. Konuk personeli kabul edecek kişilerin adları, soyadları ve resmi unvanları,

f. Konuk personeli gönderen ülkenin Yetkili Güvenlik Makamının resmi mühürü, imzası ve istek tarihi.

4. Ziyaret izni sadece belirlenen tarih ve süre için geçerli olacaktır. Ancak, işbirliğine kolaylık sağlamak amacıyla 12 ayı geçmeyen süreyi kapsayan bir ziyaret çizelgesi hazırlanabilir. Bu durumda, planlı ziyaretin izin verilen zaman süresi içerisinde sona ermeyeceği varsayıldığında bu tip ziyaretlerin süresini uzatmak gerekli olup, ziyaret talepleri Konuk Personeli gönderen ülkenin Yetkili Güvenlik Makamınca işlemdeki ziyaret izninin geçerliliğinin sona erme tarihinden en az 21 gün önce yenilenecektir.

5. 3'üncü Maddede bahsi geçen kişisel bilgileri muhafaza etmek amacıyla, Tarafların ulusal mevzuatlarına uygun olarak aşağıdaki hükümler uygulanacaktır:

a. Ev Sahibi Tarafça alınan kişisel bilgiler yalnızca bu bilgileri aktaran Tarafça tanımlanmak şart ve koşuluyla kullanılacaktır.

b. Kişisel bilgiler, amacı doğrultusunda işleme konması gerekli olduğu sürece Ev Sahibi Tarafça saklanacaktır.

c. İlgili Tarafın ulusal mevzuatlarına aykırı olarak kişisel bilgilerin aktarılması durumunda, bilgileri aktaran taraf kısmi ya da tamamen yeniden yapılandırmayı ortadan kaldıracak şekilde verilerin kaldırılmasından yükümlü olarak ev sahibi tarafı bilgilendirecektir.

d. Kişisel bilgileri aktaran taraf bu bilgilerin doğruluğundan sorumlu olacak ve bu bilgilerin eksik ya da doğru olmaması durumunda ise bilgilerin düzeltilmesi ya da çıkartılmasından yükümlü olacak olan ev sahibi tarafı bilgilendirecektir.

e. Ev sahibi Taraf ve kişisel bilgileri aktaran taraf bu bilgilerin iletilmesi, alınması ve çıkartılmasının kayıt altına alınmasından yükümlü olacaktır.

f. Kişisel bilgileri aktaran taraf ve ev sahibi taraf, işleme tabi tutulan kişisel bilgilerin yetkisiz kişilere ifşasına, yetki dışı olarak değiştirilmesine, kaybolmasına, zarar görmesine ya da tahribata uğramasına karşı etkin bir şekilde muhafazasından yükümlü olacaktır.

MADDE 11**DİLLER**

Bu Anlaşmanın hükümlerinin uygulanması kapsamında, tercümenin diğer Tarafın resmi dilinde ya da İngilizce olarak eklenmesi durumunda Taraflar ya İngilizce ya da kendi resmi dilini kullanacaktır.

MADDE 12**MALİ KONULAR**

Her iki Taraf da bu Anlaşmanın hükümlerinin uygulanmasından doğacak kendi masraflarını karşılayacaktır.

MADDE 13**İSTİŞARE VE TADİL**

1. Taraflardan biri diğer Tarafa yazılı bildirim göndererek bu Anlaşmaya istişare ve/veya tadil önerebilir.
2. Bu Anlaşma, Tarafların yazılı onayı ile tadil edilebilir. Bahse konu tadilatlar, Madde 16'da belirtilen aynı yasal prosedürler uyarınca yürürlüğe girecektir.
3. Bu Anlaşmanın amacı olan etkin bir işbirliği sağlayabilmek için, kendi Taraflarının ulusal mevzuatlarını kabul eden yetki kapsamında, Yetkili Güvenlik Kuruluşu, gerekli olması halinde, yazılı kapsamlı teknik anlaşmaları akdedebilir.
4. Tarafların Yetkili Güvenlik Kuruluşları, bu Anlaşmanın uygulanmasına yönelik olarak Gizlilik Dereceli Bilgilerin Korunması kapsamında kendi yasal düzenlemelerinde yapılacak herhangi bir tadilat hususunda birbirlerine haber verecektir.

MADDE 14**UYUŞMAZLIKLARIN ÇÖZÜMÜ**

1. Bu Anlaşmanın uygulanmasına ve yorumlanmasına yönelik herhangi bir uyuşmazlık Yetkili Güvenlik Kuruluşları arasında yürütülecek olan doğrudan müzakerelerle çözüme kavuşturulacaktır. Uyuşmazlıklar herhangi bir çözülmesi maksadıyla herhangi bir ulusal, uluslararası mahkemeye veya Üçüncü Tarafa intikal ettirilmeyecektir.
2. Madde 1'de bahsi geçen şekilde ihtilafa yönelik çözüm sağlanamaması halinde, uyuşmazlık diplomatik kanallarla çözümlenecektir. Çözüme ulaşılamaması halinde, her iki Taraf da bu Anlaşmayı fesih edebilir.

MADDE 15**YÜRÜRLÜK SÜRESİ VE SONA ERDİRME**

1. Bu Anlaşmanın yürürlük süresi beş yıldır ve otuz gün önceden diplomatik kanallardan sona erdirme talebinde bulunulmadığı sürece beş yıllık sürelerle otomatik olarak yenilenecektir. Taraflardan herhangi biri, işbu Anlaşmayı diğer Tarafa yazılı bildirimde bulunmak suretiyle sona erdirebilir. Böyle bir durumda, fesih bildirisi alındıktan üç ay sonra anlaşma sona erecektir.
2. Bu Anlaşmanın sona ermesi durumunda, bu Anlaşma temelinde mübadele edilen ya da oluşturulan Gizlilik Dereceli Bilgiler burada geçen hükümler uyarınca sürekli olarak korunacaktır.

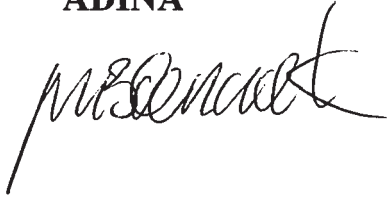
MADDE 16**YÜRÜRLÜĞE GİRİŞ**

Bu Anlaşma, Tarafların Anlaşmanın yürürlüğe girmesi için gerekli iç yasal usullerini tamamladığını birbirlerine diplomatik yollarla bildirdikleri son yazılı bildirim alındığı tarihi takip eden ikinci ayın ilk günü yürürlüğe girecektir.

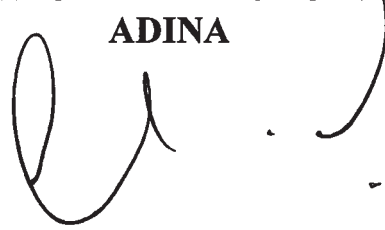
İşbu Anlaşma aşağıda imzası bulunan kendi Hükümetleri tarafından yetkilendirilmiş olan temsilciler tarafından imzalanmıştır.

..24 Mayıs 2024 tarihindeAnlaşma.. da her biri aynı derecede geçerli olmak üzere Lehçe, Türkçe ve İngilizce dillerinde ikişer asıl nüsha olarak oluşturulmuştur. Bu Anlaşma hükümlerinin yorumu ile ilgili olarak herhangi bir uyuşmazlık çıkması durumunda İngilizce metin esas alınacaktır.

**POLONYA
CUMHURİYETİ HÜKÜMETİ
ADINA**



**TÜRKİYE
CUMHURİYETİ HÜKÜMETİ
ADINA**



AGREEMENT**between****the Government of the Republic of Poland****and****the Government of the Republic of Turkey****on Mutual Protection of Classified Information in Defence Industry**

The Government of the Republic of Poland

and

The Government of the Republic of Turkey

(hereinafter referred to individually as Party, collectively as Parties),

Intending to ensure security of the Classified Information related to defence industry that has been classified in the country of one Party and transferred to the country of the other Party and/or generated by mutual cooperation between the Parties and/or the Authorized Entities in the countries of the Parties,

Desiring to lay down the procedures and principles for ensuring the security of the Classified Information related to the Classified Contracts concluded in the framework of defence industry cooperation between the Parties and/or the Authorized Entities in the countries of the Parties,

Noting that the provisions of the *Agreement between the Government of the Republic of Poland and the Government of the Republic of Turkey on Technical and Defence Industry Cooperation* signed in Ankara on 19 July 1994 apply in regard to the aspects not having provision in this Agreement,

Subject to the national legislations of the Parties,

Confirming that this Agreement shall not affect the obligations arising from other international agreements to which either country is a party and shall not be used against the interests, security and territorial integrity of other states,

Have agreed as follows:

ARTICLE 1

PURPOSE AND SCOPE

The purpose of this Agreement is to establish the procedures and principles for ensuring security of the Classified Information related to defence industry in the scope of cooperation activities carried out between the Competent Security Authorities and/or the Authorized Entities in the countries of the Parties in accordance with their respective national legislations.

ARTICLE 2

DEFINITIONS

1. **Classified Information** – means any information related to defence industry, irrespective of its form, carrier and manner of recording, including documents and material, also in the process of being generated, which require protection against unauthorized disclosure in accordance with the national legislation of either Party and this Agreement.
2. **Competent Security Authority** – means an authority competent in defence industry and responsible for implementation of this Agreement, as specified in Article 3 Paragraph 1 of this Agreement.
3. **Classified Contract** – means a contract, performance of which involves access to Classified Information or originating of such information, in particular one involving any kinds of works, including preparatory activities, related to the purchase and selling of all kinds of vehicles and equipment of war and arms, and important and critical subsystems and parts therein, research and development, and every kind of production or service thereof.
4. **Contractor** – means a natural person, a legal entity or other form of organization under the law of one of the Parties, which has legal capacity to perform Classified Contracts in accordance with the provisions of this Agreement.

5. **Principal** – means a natural person, a legal entity or other form of organization under the law of one of the Parties, which has legal capacity to let Classified Contracts to Contractors in accordance with the provisions of this Agreement.
6. **Facility Security Clearance** – means a document issued in accordance with the national legislation of a Party by the Competent Security Authority or other authorized entity confirming that a Contractor has capability to protect Classified Information; in case of sole proprietors acting as Contractors, a Personnel Security Clearance shall be an equivalent of a Facility Security Clearance.
7. **Authorized Entities** – means the Parties including the government agencies, legal entities or other forms of organizations, as well as natural persons, competent to handle Classified Information in accordance with their respective national legislations.
8. **Originating Party** – means the Party, as well as natural persons, legal entities or other forms of organizations, competent to originate and transmit Classified Information in accordance with the national legislation of its Party.
9. **Recipient Party** – means the Party, as well as natural persons, legal entities or other forms of organizations, competent to receive Classified Information in accordance with the national legislation of its Party.
10. **Personnel Security Clearance** – means a document issued in accordance with the national legislation of a Party by the Competent Security Authority or other authorized entity confirming that an individual has undergone security vetting and is eligible to have access to Classified Information.
11. **Third Party** – means any state, including natural persons, legal entities or other forms of organizations under its jurisdiction, or an international organization not being a Party to this Agreement.

ARTICLE 3
COMPETENT SECURITY AUTHORITIES

1. The Competent Security Authorities responsible for implementation of this Agreement are as follows:
 - 1) for the Republic of Poland: The Head of the Internal Security Agency;
 - 2) for the Republic of Turkey: Ministry of National Defence of the Republic of Turkey, Technical Services Department.
2. The Parties shall inform each other via diplomatic channels about changes of the Competent Security Authorities or amendments to their competences.

ARTICLE 4
SECURITY CLASSIFICATIONS

1. Within the framework of the security measures prescribed by their respective national legislations, the Competent Security Authorities and the Authorized Entities commit to duly ensure the protection of the Classified Information exchanged between each other or generated by mutual cooperation, and adopt the equivalence of levels of classification as shown in the table below, in Polish, Turkish and English:
- 2.

IN THE REPUBLIC OF POLAND	IN THE REPUBLIC OF TURKEY	EQUIVALENT IN ENGLISH
ŚCIŚLE TAJNE	ÇOK GİZLİ	TOP SECRET
TAJNE	GİZLİ	SECRET
POUFNE	ÖZEL	CONFIDENTIAL
ZASTRZEŻONE	HİZMETE ÖZEL	RESTRICTED

3. The Competent Security Authority and the Authorized Entities commit to mark the Classified Information they receive from the Competent Security Authority or the Authorized Entities of the state of the other Party, with its own level of national security classification and English equivalent in accordance with the above table.
4. The Competent Security Authorities commit to mutually inform each other about the changes made in the security classifications.
5. The level of security classifications given to the Classified Information can be changed or removed only by the Originating Party. Such a decision of change or removal shall be immediately notified by the Originating Party to the Recipient Party.

ARTICLE 5

PRINCIPLES OF CLASSIFIED INFORMATION PROTECTION

1. The Parties shall adopt every measure provided in this Agreement and subject to their national legislations in order to protect Classified Information transmitted or originated as a result of cooperation between the Parties, including this originated in connection with performance of Classified Contracts.
2. The Classified Information exchanged and/or generated by mutual cooperation between the Competent Security Authorities and/or the Authorized Entities in the countries of the Parties shall be only used in line with the purpose of transfer.
3. The Classified Information shall not be disclosed to a Third Party without prior written consent of the Originating Party.
4. The Classified Information may be disclosed only to persons who have a requirement for access to, knowledge of, or possession of information in order to perform official tasks or services and who are duly authorised in accordance with the national legislation of the Recipient Party.

5. In the scope of this Agreement, the Competent Security Authorities shall recognize Personnel Security Clearances and Facility Security Clearances issued in accordance with the national legislation of the other Party.

ARTICLE 6

TRANSFER OF THE CLASSIFIED INFORMATION

1. Classified Information shall be transmitted via diplomatic channels or military attaché.
2. Information classified as ZASTRZEŻONE / HİZMETE ÖZEL / RESTRICTED may be transmitted also through authorized carriers in accordance with the national legislation of the Originating Party.
3. In urgent cases, unless it is possible to use other forms of transmission of Classified Information, if the security requirements defined by the national legislation of the Originating Party are met, the personal carriage of information classified as ZASTRZEŻONE / HİZMETE ÖZEL / RESTRICTED by authorized individuals is admissible.
4. The Competent Security Authorities may agree on other forms of transmitting Classified Information which ensure its protection against unauthorized disclosure in accordance with their respective national legislation.
5. The Recipient Party shall confirm in writing the receipt of Classified Information.

ARTICLE 7

TRANSLATION, REPRODUCTION AND DESTRUCTION OF THE CLASSIFIED INFORMATION

1. Classified Information marked with the level of security classification of POUFNE / ÖZEL / CONFIDENTIAL or above shall be translated

- or reproduced only by prior written consent of the Competent Security Authority of the Originating Party.
2. All translations of Classified Information shall involve an appropriate security classification marking and annotations indicating that the classified document is received from the Originating Party. The translated or reproduced Classified Information shall be subject to the same control and protection as the original information. The number of copies and translations shall be limited to the extent required for official purposes.
 3. The information classified as ZASTRZEŻONE / HİZMETE ÖZEL / RESTRICTED shall be destroyed in accordance with the national legislation of the Recipient Party in a way to prevent re-gathering of the parts either partially or totally. However, the information classified as POUFNE / ÖZEL / CONFIDENTIAL or above shall be returned by the Recipient Party to the Originating Party instead of being destroyed, when its term or the purpose of usage is ended.

ARTICLE 8

CLASSIFIED CONTRACTS

1. Before concluding a Classified Contract, the Principal shall apply to its Competent Security Authority to request that the Competent Security Authority of the other Party confirm 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 Republic of Turkey, before concluding a Classified Contract involving information classified as ZASTRZEŻONE / HİZMETE ÖZEL / RESTRICTED, the Competent Security Authority of the Republic of Poland shall confirm that a Polish Contractor meets security requirements under the national legislation.

3. The confirmation referred to in Paragraphs 1 or 2 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 legislation 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 confirmation referred to in Paragraphs 1 or 2.
5. The Principal shall transmit to the Contractor a project security instruction necessary to perform a Classified Contract connected with access to information classified as POUFNE / ÖZEL / CONFIDENTIAL or above, which is an integral part of such Classified Contract. The project 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 procedures for handling Classified Information provided to the Contractor or generated during performance of a Classified Contract.
6. The Principal shall put forward a copy of the project security instruction to the Competent Security Authority of its Party, which shall transmit it to the Competent Security Authority of the Contractor's Party.
7. 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 project security instruction.
8. Every subcontractor shall comply with the same conditions for the protection of Classified Information as those laid down for the Contractor.

9. Intellectual property rights concerning the Classified Information within the Classified Contracts shall be respected reciprocally in accordance with national legislations. Details may be specified in the Classified Contracts.

ARTICLE 9

BREACH OF SECURITY

1. Breach of security is an action or an omission which is contrary to this Agreement or the national legislation of the Parties concerning Classified Information protection.
2. Information on every breach of security or a suspicion of a breach of security concerning Classified Information of the Originating Party or Classified Information originated as a result of cooperation of the Parties shall be immediately reported to the Competent Security Authority of the Party in the territory of the state of which the breach or suspicion of the breach has occurred.
3. Every breach of security or a suspicion of a breach of security shall be investigated pursuant to the national legislation of the Party in the territory of the state of which it has occurred.
4. In case of a breach of security the Competent Security Authority of the Party in the territory of the state of which the breach has occurred shall inform the Competent Security Authority of the other Party in writing about the fact, circumstances of the breach and the outcome of the actions referred to in Paragraph 3.
5. The Competent Security Authorities shall cooperate in the actions referred to in Paragraph 3, upon the request of one of them.

ARTICLE 10**VISITS**

1. The visits to the facilities of the Authorized Entities in the country of each Party involving access to Classified Information within the scope of cooperation activities between the Competent Security Authorities and/or the Authorized Entities in the countries of the Parties shall be made upon receiving the written authorisation of the Competent Security Authority of the Host Country.
2. The requests for visits shall be notified to the Competent Security Authority of the Host Country in writing, at least 21 (twenty-one) days prior to the proposed date of visit. These requests shall be submitted through the diplomatic channels or military attaché.
3. The form of request for visit shall be prepared for each visit to include the following information below:
 - a. The Guest Personnel's name and surname, date and place of birth, nationality, passport number and position,
 - b. The proposed date, programme and anticipated length of visit,
 - c. The level of the Personnel Security Clearance held by the Guest Personnel and type of Classified Information to be accessed as well as the level of security classification,
 - d. The names of the facilities, premises and places to be visited and the purpose of visit,
 - e. The names, surnames and official titles of the persons who will receive the Guest Personnel,
 - f. The date of request, signature and official stamp of the Competent Security Authority of the country sending the Guest Personnel.
4. A visit permission shall be valid only for the specified date or period. However, in order to facilitate cooperation, a schedule of a visit covering a period not exceeding 12 (twelve) months may be drawn up. In this case, if it is assumed that a planned visit will not end within the allowed period

of time and it is necessary to extend the period of such kind of visits, the request for visit shall be renewed by the Competent Security Authority of the country sending the Guest Personnel, at least 21 (twenty-one) days prior to the expiry of the validity of the visit permission in progress.

5. In order to protect personal data referred to in Paragraph 3, the following provisions shall apply, pursuant to the national legislation of the Parties:
 - a. personal data received by the hosting party shall be used exclusively for the purpose and on condition defined by the party transmitting it;
 - b. personal data shall be stored by the hosting party no longer than it is necessary for achieving the purpose of its processing;
 - c. in case of personal data transmitted against the national legislation of the Party, the party transmitting it shall notify the hosting party, which shall be obliged to remove the data in such a manner as to eliminate its partial or total reconstruction;
 - d. the party transmitting personal data shall take responsibility for its correctness and, in a case the data appears to be untrue or incomplete, shall notify the hosting party, which shall be obliged to correct or remove the data;
 - e. the hosting party and the party transmitting personal data shall be obliged to register its transmission, receipt and removal;
 - f. the party transmitting personal data and the hosting party shall be obliged to protect processed personal data efficiently against its disclosure to unauthorized persons, unauthorized modifications of the data, its loss, damage or destruction.

ARTICLE 11

LANGUAGES

In the scope of the implementation of the provisions of this Agreement, the Parties shall use English or their official languages, in case of which the

translation into the official language of the other Party or English shall be attached.

ARTICLE 12

FINANCIAL MATTERS

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

ARTICLE 13

CONSULTATION AND AMENDMENT

1. Either Party may propose consultation and/or amendment to this Agreement by sending a written notification to the other Party.
2. This Agreement may be amended by written consent of the Parties. The amendments shall enter into force in accordance with the same legal procedure as prescribed under Article 16.
3. In order to ensure effective cooperation, which is the objective of this Agreement, and in the scope of authority acknowledged by the national legislation of their Parties, the Competent Security Authorities may, if necessary, conclude written detailed technical arrangements.
4. The Competent Security Authorities of the Parties shall notify each other of any amendments to their national legislation on the protection of Classified Information concerning implementation of this Agreement.

ARTICLE 14

SETTLEMENT OF DISPUTES

1. Any disputes concerning the implementation and interpretation of this Agreement shall be settled by direct negotiations between

the Competent Security Authorities. The disputes shall not be referred to any national, international tribunal or to a Third Party for settlement.

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. If a solution is not reached, each Party may terminate this Agreement.

ARTICLE 15

EFFECTIVENESS PERIOD AND TERMINATION

1. This Agreement is concluded for five years and shall be then automatically renewed for five-year-periods unless terminated with thirty days advance notice through diplomatic channels. It may also be terminated by either Party by giving written notice to the other Party, and in such case it shall expire after three months following the receipt of the termination notice.
2. 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 continuously.

ARTICLE 16

ENTRY INTO FORCE

This Agreement shall enter into force on the first day of the second month following the day of receipt of the last written notification by which the Parties notify each other, through diplomatic channels, of the completion of their internal legal procedures required for the entry into force of the Agreement.

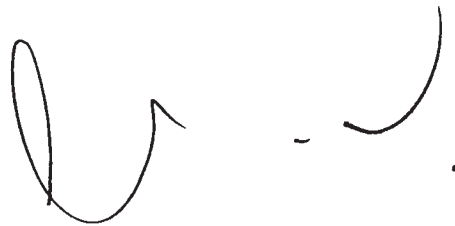
In witness whereof, the undersigned, being duly authorized by their respective Governments, have signed this Agreement.

Done in Ankara, on May 24, 2021, in two original copies in Polish, Turkish and English languages, each copy being equally authentic. In case of any dispute regarding the interpretation of provisions of this Agreement, the English text shall prevail.

FOR THE GOVERNMENT OF
THE REPUBLIC OF POLAND



FOR THE GOVERNMENT OF
THE REPUBLIC OF TURKEY



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 9 lutego 2022 roku.

Prezydent Rzeczypospolitej Polskiej: *A. Duda*

L.S.

Prezes Rady Ministrów: *M. Morawiecki*