DZIENNIK USTAW
RZECZYPOSPOLITEJ POLSKIEJ

Warszawa, dnia 22 czerwca 2026 r.

Poz. 818

UMOWA

między Rządem Rzeczypospolitej Polskiej a Rządem Królestwa Szwecji o wzajemnej ochronie informacji niejawnych,

podpisana w Warszawie dnia 29 października 2025 r.

W imieniu Rzeczypospolitej Polskiej

PREZYDENT RZECZYPOSPOLITEJ POLSKIEJ

podaje do powszechnej wiadomości:

Dnia 29 października 2025 roku w Warszawie została podpisana Umowa między Rządem Rzeczypospolitej Polskiej a Rządem Królestwa Szwecji o wzajemnej ochronie informacji niejawnych, w następującym brzmieniu:

UMOWA

między Rządem Rzeczypospolitej Polskiej

a Rządem Królestwa Szwecji

o wzajemnej ochronie informacji niejawnych

Rząd Rzeczypospolitej Polskiej

i Rząd Królestwa Szwecji,

zwane dalej „Stronami”,

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

z zastrzeżeniem zobowiązań wynikających z prawa międzynarodowego i prawa krajowego Stron,

uzgodniły, co następuje:

ARTYKUŁ 1
CEL UMOWY

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

ARTYKUŁ 2
DEFINICJE

Dla celów niniejszej Umowy następujące terminy zostały zdefiniowane jako:

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 bezpieczeństwa** – organy, o których mowa w artykule 4 ustęp 1 niniejszej Umowy;
3) **Strona wytwarzająca** – Strona, osoba fizyczna, osoba prawna lub inna jednostka organizacyjna uprawniona do wytwarzania i udostępniania informacji niejawnych zgodnie z prawem krajowym swojej Strony;
4) **Strona otrzymująca** – Strona, osoba fizyczna, osoba prawna lub inna jednostka organizacyjna uprawniona do otrzymywania informacji niejawnych zgodnie z prawem krajowym swojej Strony;

5) **kontrakt niejawny** – umowa, której realizacja jest związana z dostępem do informacji niejawnych bądź z wytworzeniem takich informacji;

6) **kontrahent lub podwykonawca** – osoba fizyczna, osoba prawna albo inna jednostka organizacyjna, która posiada zdolność do realizacji kontraktów niejawnych zgodnie z prawem krajowym jednej ze Stron;

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

ARTYKUŁ 3
KLAUZULE TAJNOŚCI

1. Informacjom niejawnym przyznaje się odpowiednią do ich treści klauzulę tajności zgodnie z prawem krajowym Strony wytwarzającej. Strona otrzymująca gwarantuje co najmniej równorzędny poziom ochrony otrzymanych informacji niejawnych, zgodnie z postanowieniami 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 SZWECJI**	**ODPOWIEDNIK W JĘZYKU ANGIELSKIM**
ŚCIŚLE TAJNE	KVALIFICERAT HEMLIG	TOP SECRET
TAJNE	HEMLIG	SECRET
POUFNE	KONFIDENTIELL	CONFIDENTIAL
ZASTRZEŻONE	BEGRÄNSAT HEMLIG	RESTRICTED

ARTYKUŁ 4
WŁAŚCIWE ORGANY BEZPIECZEŃSTWA

1. W rozumieniu niniejszej Umowy właściwymi organami bezpieczeństwa są:
   1) w Rzeczypospolitej Polskiej: Szef Agencji Bezpieczeństwa Wewnętrznego;
   2) w Królestwie Szwecji: Szwedzkie Siły Zbrojne, Wywiad Wojskowy i Służba Bezpieczeństwa w sferze wojskowej, Szwedzka Służba Bezpieczeństwa w sferze cywilnej i Szwedzka Administracja Materiałów Obronnych w zakresie zamówień zbrojeniowych oraz bezpieczeństwa przemysłowego.
2. Strony informują się w drodze dyplomatycznej o zmianach właściwych organów bezpieczeństwa, o których mowa w ustępie 1, lub o zmianach ich właściwości.

ARTYKUŁ 5
ZASADY OCHRONY INFORMACJI NIEJAWNYCH

1. Strony podejmują wszelkie działania określone w niniejszej Umowie oraz zgodne ze swoim prawem krajowym w celu ochrony informacji niejawnych wymienianych lub wytwarzanych w wyniku wspólnej działalności Stron, w tym w związku z realizacją kontraktów niejawnych.
2. 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.
3. Strona otrzymująca podejmie wszelkie kroki prawne konieczne do ochrony informacji niejawnych przed ujawnieniem lub wykorzystaniem,

z wyłączeniem celów i w zakresie ograniczeń określonych przez Stronę wytwarzającą.

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 bezpieczeństwa 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 związanego z dostępem do informacji niejawnych o klauzuli POUFNE / KONFIDENTIELL/ CONFIDENTIAL lub wyższej, podmiot zamawiający składa wniosek do właściwego organu bezpieczeństwa swojej Strony o wystąpienie do właściwego organu bezpieczeństwa w zakresie zamówień zbrojeniowych oraz bezpieczeństwa przemysłowego drugiej Strony z prośbą o wydanie pisemnego zaświadczenia, że kontrahent posiada ważne świadectwo bezpieczeństwa przemysłowego, odpowiednie do klauzuli informacji niejawnych, do których będzie miał dostęp.
2. Wydanie zaświadczenia, o którym mowa w ustępie 1, jest równoznaczne z gwarancją, że zostały przeprowadzone czynności niezbędne do stwierdzenia, że kontrahent spełnia warunki w zakresie ochrony informacji

niejawnych określone w prawie krajowym Strony, na terytorium Państwa której posiada siedzibę.

3. Informacje niejawne nie są udostępniane kontrahentowi do czasu uzyskania zaświadczenia, o którym mowa w ustępie 1.
4. Każdy kontrakt niejawny zawiera przepisy 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.
5. 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 przepisami dotyczącymi wymogów bezpieczeństwa, o których mowa w ustępie 4.
6. 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 bezpieczeństwa Stron. Strony mogą przekazywać informacje niejawne elektronicznie za pomocą urządzeń kryptograficznych zgodnie z procedurami zatwierdzonymi przez właściwe organy bezpieczeństwa.
2. Informacje niejawne o klauzuli ZASTRZEŻONE / BEGRÄNSAT HEMLIG / RESTRICTED i POUFNE / KONFIDENTIELL / CONFIDENTIAL 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, jeżeli spełnione są wymogi bezpieczeństwa określone prawem krajowym Strony wytwarzającej, dopuszczalny jest przewóz osobisty informacji niejawnych o klauzuli ZASTRZEŻONE / BEGRÄNSAT HEMLIG / RESTRICTED i POUFNE / KONFIDENTIELL / CONFIDENTIAL przez osoby do tego upoważnione.
4. Strona otrzymująca potwierdza pisemnie odbiór informacji niejawnych.
5. Organy uprawnione do wymiany informacji niejawnych na podstawie innych umów międzynarodowych zawartych między Stronami mogą wymieniać informacje niejawne bezpośrednio, zgodnie z warunkami określonymi w tych umowach.

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 niejawne 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 / KVALIFICERAT HEMLIG / 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 w sposób uniemożliwiający ich częściowe lub całkowite odtworzenie lub archiwizowane zgodnie z prawem krajowym.

2. Informacje niejawne o klauzuli ŚCIŚLE TAJNE / KVALIFICERAT HEMLIG / TOP SECRET nie są niszczone. Są one zwracane Stronie wytwarzającej lub archiwizowane zgodnie z prawem krajowym.

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 bezpieczeństwa drugiej Strony.
2. Właściwy organ bezpieczeństwa Strony wysyłającej zwraca się do właściwego organu bezpieczeństwa 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 czas składania wniosku może zostać skrócony.
3. Wniosek, o którym mowa w ustępie 2, zawiera następujące informacje:
   1) cel, termin i program wizyty, w tym 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 bezpieczeństwa Strony wysyłającej.

4. Właściwe organy bezpieczeństwa Stron mogą wyrazić zgodę na ustalenie wykazów osób upoważnionych do składania wielokrotnych wizyt związanych z realizacją konkretnego projektu, programu lub kontraktu niejawnego. Wykazy te zawierają dane określone w ustępie 3 i są ważne przez okres dwunastu miesięcy. Po zatwierdzeniu takich wykazów przez właściwe organy bezpieczeństwa Stron, terminy wizyt są uzgadniane bezpośrednio między podmiotem wysyłającym a podmiotem przyjmującym, zgodnie z ustalonymi warunkami.
5. Wizyty związane z dostępem do informacji niejawnych o klauzuli ZASTRZEŻONE / BEGRÄNSAT HEMLIG / RESTRICTED są uzgadniane bezpośrednio między podmiotem wysyłającym a podmiotem przyjmującym wizytę.
6. Strony zapewnią, zgodnie ze swoim prawem krajowym, ochronę danych osobowych 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 bezpieczeństwa Strony, na terytorium Państwa której miało miejsce lub zaistniało podejrzenie takiego naruszenia.
2. Każdy przypadek naruszenia lub podejrzenia naruszenia regulacji dotyczących ochrony informacji niejawnych wyjaśnia się zgodnie z prawem krajowym Strony, na terytorium Państwa której zdarzenie miało miejsce.
3. W przypadku naruszenia regulacji dotyczących ochrony informacji niejawnych właściwy organ bezpieczeństwa Strony, na terytorium Państwa

której naruszenie miało miejsce, pisemnie informuje właściwy organ bezpieczeństwa drugiej Strony o fakcie, okolicznościach naruszenia oraz wyniku czynności, o których mowa w ustępie 2.

4. Właściwe organy bezpieczeństwa 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 bezpieczeństwa Stron informują się wzajemnie o wszelkich zmianach w swoim prawie krajowym dotyczących ochrony informacji niejawnych, w zakresie stosowania postanowień niniejszej Umowy.
2. W celu zapewnienia ścisłej współpracy przy realizacji postanowień niniejszej Umowy właściwe organy bezpieczeństwa Stron konsultują się, na wniosek jednego z nich.
3. Każda ze Stron zezwoli przedstawicielom właściwego organu bezpieczeństwa 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 bezpieczeństwa 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 bezpieczeństwa Stron.
2. Jeśli nie jest możliwe rozwiązanie sporu w sposób, o którym mowa w ustępie 1, jest on rozstrzygany w drodze dyplomatycznej.

ARTYKUŁ 17
STOSUNEK DO INNYCH UMÓW

Z dniem wejścia w życie niniejszej Umowy traci moc Umowa między Rządem Rzeczypospolitej Polskiej a Rządem Królestwa Szwecji o wzajemnej ochronie informacji niejawnych, podpisana w Warszawie dnia 6 września 2007 r. Informacje niejawne, które zostały wymienione albo mają być wymienione na podstawie wyżej wymienionej Umowy, będą chronione zgodnie z postanowieniami niniejszej Umowy.

ARTYKUŁ 18
POSTANOWIENIA KOŃCOWE

1. Każda Strona informuje drugą Stronę w drodze dyplomatycznej o zakończeniu procedur krajowych niezbędnych do wejścia w życie niniejszej Umowy.

Umowa wejdzie w życie w pierwszym dniu drugiego miesiąca, który nastąpi po dacie 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 jest zawarta na czas nieokreślony. Może być ona wypowiedziana w drodze notyfikacji przez każdą ze Stron. W takim przypadku niniejsza Umowa utraci moc po upływie sześciu miesięcy od daty otrzymania noty informującej o wypowiedzeniu.
4. W przypadku wypowiedzenia niniejszej Umowy informacje niejawne wymieniane lub wytworzone na jej podstawie będą chronione zgodnie z jej postanowieniami.

Podpisano w Warszawie dnia 29 października 2025 roku w dwóch jednobrzmiących egzemplarzach, każdy w językach polskim, szwedzkim 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 SZWECJI

AVTAL

mellan Republiken Polens regering

och Konungariket Sveriges regering

om ömsesidigt skydd av säkerhetsskyddsklassificerade uppgifter

Republiken Polens regering och
Konungariket Sveriges regering,
nedan kallade *parterna*,

som vägleds av sin föresats att anta enhetliga bestämmelser för båda parter när det gäller skydd av säkerhetsskyddsklassificerade uppgifter, och

som är underkastade de skyldigheter som följer av internationell lagstiftning och parternas nationella lagstiftning,

har kommit överens om följande.

ARTIKEL 1

SYFTE

1. Syftet med detta avtal är att säkerställa skydd av säkerhetsskyddsklassificerade uppgifter som utbyts eller genereras till följd av samarbete mellan parterna eller mellan fysiska eller juridiska personer eller andra sorters organisationer under deras jurisdiktion.
2. Detta avtal ska vara tillämpligt på all verksamhet och alla kontrakt eller andra typer av avtal som innebär tillgång till säkerhetsskyddsklassificerade uppgifter och som utförs eller ingås av parterna eller av fysiska eller juridiska personer eller andra sorters organisationer under deras jurisdiktion.

ARTIKEL 2

DEFINITIONER

I detta avtal gäller följande definitioner:

1) *säkerhetsskyddsklassificerade uppgifter*: alla uppgifter, oberoende av form, förmedlingssätt eller lagringsmedium, och föremål eller delar av föremål, inklusive sådana som håller på att genereras, som kräver skydd mot obehörigt röjande i enlighet med endera partens nationella lagstiftning och detta avtal.
2) *behöriga säkerhetsmyndigheter*: de myndigheter som anges i artikel 4.1 i detta avtal.
3) *ursprungspart*: part, fysisk eller juridisk person eller annan sorts organisation som har behörighet att generera och lämna ut säkerhetsskyddsklassificerade uppgifter i enlighet med den aktuella partens nationella lagstiftning.
4) *mottagande part*: part, fysisk eller juridisk person eller annan sorts organisation som har behörighet att ta emot säkerhetsskyddsklassificerade uppgifter i enlighet med den aktuella partens nationella lagstiftning.
5) *säkerhetsskyddsklassificerat kontrakt*: kontrakt vars genomförande innebär tillgång till eller generering av säkerhetsskyddsklassificerade uppgifter.

6) *uppdragstagare* eller *underleverantör*: fysisk eller juridisk person eller annan sorts organisation med rättskapacitet att utföra säkerhetsskyddsklassificerade kontrakt i enlighet med endera partens nationella lagstiftning.
7) *säkerhetsöverträdelse*: handling eller underlåtenhet som strider mot detta avtal eller mot parternas nationella lagstiftning som rör skydd av säkerhetsskyddsklassificerade uppgifter.

ARTIKEL 3

SÄKERHETSSKYDDSKLASSER

1. Säkerhetsskyddsklassificerade uppgifter ska delas in i säkerhetsskyddsklasser utifrån uppgifternas innehåll, i enlighet med ursprungspartens nationella lagstiftning.

   Den mottagande parten ska säkerställa att de säkerhetsskyddsklassificerade uppgifter som tas emot ges åtminstone ett likvärdigt skydd enligt punkt 3.
2. Endast ursprungsparten får ändra eller häva säkerhetsskyddsklassificeringen. Den mottagande parten ska omedelbart underrättas skriftligen varje gång säkerhetsskyddsklassificeringen för säkerhetskyddsklassificerade uppgifter som den tagit emot ändras eller hävs.
3. Parterna har kommit överens om att följande säkerhetsskyddsklasser motsvarar varandra:

REPUBLIKEN POLEN	KONUNGARIKET SVERIGE	MOTSVARIGHET PÅ ENGELSKA
ŚCIŚLE TAJNE	KVALIFICERAT HEMLIG	TOP SECRET
TAJNE	HEMLIG	SECRET
POUFNE	KONFIDENTIELL	CONFIDENTIAL
ZASTRZEŻONE	BEGRÄNSAT HEMLIG	RESTRICTED

ARTIKEL 4

BEHÖRIGA SÄKERHETSMYNDIGHETER

1. Följande myndigheter är behöriga säkerhetsmyndigheter vid tillämpningen av detta avtal:
   1) För Republiken Polen: chefen för inrikessäkerhetstjänsten (Agencja Bezpieczeństwa Wewnętrznego).
   2) För Konungariket Sverige: Militära underrättelse- och säkerhetstjänsten vid Försvarsmakten i militära frågor, Säkerhetspolisen i civila frågor och Försvarets materielverk i försvarsmateriel- och industrisäkerhetsfrågor.
2. Parterna ska på diplomatisk väg underrätta varandra om ändringar av de behöriga säkerhetsmyndigheterna i punkt 1 eller av deras behörighet.

ARTIKEL 5

PRINCIPER FÖR SKYDD AV SÄKERHETSSKYDDSKLASSIFICERADE UPPGIFTER

1. Parterna ska, om inte annat följer av deras nationella lagstiftning, vidta alla åtgärder som föreskrivs i detta avtal för att skydda säkerhetsskyddsklassificerade uppgifter som utbyts eller genereras till följd av samarbete mellan parterna, inklusive genomförande av säkerhetsskyddsklassificerade kontrakt.
2. Tillgång till säkerhetsskyddsklassificerade uppgifter får endast ges till enskilda personer som har ett tjänstebehov av det och som har fått behörighet till det i enlighet med den mottagande partens nationella lagstiftning.
3. Den mottagande parten ska vidta alla lagliga åtgärder som krävs för att förhindra att de utlämnade säkerhetsskyddsklassificerade uppgifterna röjs eller används annat än för de ändamål och med de begränsningar som ursprungsparten angett.

ARTIKEL 6

SÄKERHETSGODKÄNNANDEN

1. Parterna ska inom ramen för detta avtal erkänna personalsäkerhetsgodkännanden och säkerhetsgodkännanden av verksamhetsställen som utfärdats i enlighet med den andra partens nationella lagstiftning.
2. De behöriga säkerhetsmyndigheterna ska i enlighet med sin nationella lagstiftning och på begäran av någon av dem hjälpa varandra att göra prövningar för säkerhetsgodkännanden av verksamhetsställen och personalsäkerhetsgodkännanden.

ARTIKEL 7

SÄKERHETSSKYDDSKLASSIFICERADE KONTRAKT

1. Före tilldelningen av ett säkerhetsskyddsklassificerat kontrakt som innebär tillgång till uppgifter i säkerhetsskyddsklassen POUFNE / KONFIDENTIELL / CONFIDENTIAL eller högre ska den upphandlande enheten vända sig till sin behöriga säkerhetsmyndighet för att begära att den andra partens behöriga säkerhetsmyndighet i försvarsmateriel- och industrisäkerhetsfrågor utfärdar ett skriftligt intyg om att uppdragstagaren innehar ett giltigt säkerhetsgodkännande av verksamhetsställe som omfattar den säkerhetsskyddsklass som de uppgifter som uppdragstagaren ska få tillgång till är indelade i.
2. Ett utfärdande av ett sådant intyg som avses i punkt 1 ska vara liktydigt med en garanti om att nödvändiga åtgärder har vidtagits för att konstatera att uppdragstagaren uppfyller de kriterier avseende skydd av säkerhetsskyddsklassificerade uppgifter som anges i partens nationella lagstiftning i den stat inom vars territorium uppdragstagaren finns.
3. Säkerhetsskyddsklassificerade uppgifter får inte lämnas ut till uppdragstagaren förrän det intyg som avses i punkt 1 har tagits emot.
4. Varje säkerhetsskyddsklassificerat kontrakt ska innehålla bestämmelser om säkerhetsskyddskrav, i synnerhet

1) en förteckning över vilka typer av säkerhetsskyddsklassificerade uppgifter det säkerhetsskyddsklassificerade kontraktet avser, inklusive uppgifternas säkerhetsskyddsklass, och
2) regler för hantering av säkerhetsskyddsklassificerade uppgifter som överförs till uppdragstagaren eller genereras under genomförandet av det säkerhetsskyddsklassificerade kontraktet.

5. Uppdragstagaren får genomföra de delar av ett säkerhetsskyddsklassificerat kontrakt som innebär tillgång till säkerhetsskyddsklassificerade uppgifter om den uppfyller de uppställda kriterierna för skydd av säkerhetsskyddsklassificerade uppgifter, i enlighet med bestämmelserna om säkerhetsskyddskrav i punkt 4.
6. Varje underleverantör ska uppfylla samma villkor för skydd av säkerhetsskyddsklassificerade uppgifter som uppställs för uppdragstagaren.

ARTIKEL 8

ÖVERFÖRING AV SÄKERHETSSKYDDSKLASSIFICERADE UPPGIFTER

1. Säkerhetsskyddsklassificerade uppgifter ska överföras på diplomatisk väg eller på ett annat sätt som parternas behöriga säkerhetsmyndigheter kommer överens om och som garanterar att uppgifterna skyddas mot obehörigt röjande. Parterna får på elektronisk väg överföra säkerhetsskyddsklassificerade uppgifter som skyddas med kryptering i enlighet med förfaranden som ska godkännas av de behöriga säkerhetsmyndigheterna.
2. Uppgifter i säkerhetsskyddsklasserna ZASTRZEŻONE / BEGRÄNSAT HEMLIG / RESTRICTED och POUFNE / KONFIDENTIELL / CONFIDENTIAL får även översändas med behörigt bud i enlighet med ursprungspartens nationella lagstiftning.
3. Uppgifter i säkerhetsskyddsklasserna ZASTRZEŻONE / BEGRÄNSAT HEMLIG / RESTRICTED och POUFNE / KONFIDENTIELL / CONFIDENTIAL får i brådskande fall överlämnas personligen av behöriga enskilda personer om det inte är möjligt att använda andra överföringssätt och om säkerhetsskyddskraven i ursprungspartens nationella lagstiftning är uppfyllda.

4. Den mottagande parten ska skriftligen bekräfta mottagandet av de säkerhetsskyddsklassificerade uppgifterna.
5. De myndigheter som är behöriga att utbyta säkerhetsskyddsklassificerade uppgifter med stöd av andra internationella överenskommelser som parterna ingått med varandra får utbyta säkerhetsskyddsklassificerade uppgifter direkt i enlighet med villkoren i de överenskommelserna.

ARTIKEL 9

ÅTERGIVNING OCH ÖVERSÄTTNING AV SÄKERHETSSKYDDSKLASSIFICERADE UPPGIFTER

1. Återgivning eller översättning av säkerhetsskyddsklassificerade uppgifter ska göras i enlighet med den mottagande partens nationella lagstiftning. Återgivningar och översättningar av säkerhetsskyddsklassificerade uppgifter ska ges samma skydd som de ursprungliga uppgifterna. Antalet kopior eller översättningar ska vara begränsat till vad som krävs för officiella ändamål.
2. Uppgifter i säkerhetsskyddsklassen ŚCIŚLE TAJNE / KVALIFICERAT HEMLIG / TOP SECRET får inte återges eller översättas förrän ursprungsparten har gett sitt skriftliga medgivande.

ARTIKEL 10

FÖRSTÖRING AV SÄKERHETSSKYDDSKLASSIFICERADE UPPGIFTER

1. Säkerhetsskyddsklassificerade uppgifter ska förstöras på ett sätt som gör att de varken helt eller delvis kan återskapas, alternativt arkiveras i enlighet med nationell lagstiftning.
2. Uppgifter i säkerhetsskyddsklassen ŚCIŚLE TAJNE / KVALIFICERAT HEMLIG / TOP SECRET får inte förstöras. Sådana uppgifter ska återsändas till ursprungsparten eller arkiveras i enlighet med nationell lagstiftning.

ARTIKEL 11

BESÖK

1. Personer som besöker den andra partens territorium får inte ges tillgång till säkerhetsskyddsklassificerade uppgifter förrän den andra partens behöriga säkerhetsmyndighet har gett sitt skriftliga medgivande.
2. Den besökande partens behöriga säkerhetsmyndighet ska göra en besöksförfrågan till värdpartens behöriga säkerhetsmyndighet senast 30 dagar före ett sådant besök som avses i punkt 1. I brådskande fall kan tidsfristen förkortas.
3. Den besöksförfrågan som avses i punkt 2 ska innehålla följande information:
    1) Besökets syfte, tidpunkt och program samt den högsta säkerhetsskyddsklassen för de uppgifter som besöket inbegriper.
    2) Besökarens för- och efternamn, födelsedatum, födelseort och nationalitet samt passnummer eller annat id-handlingsnummer.
    3) Besökarens befattning och namnet på den organisation som han eller hon företräder.
    4) Nivå på besökarens personalsäkerhetsgodkännande och dess giltighetstid.
    5) Namn på och adress till den organisation som ska besökas.
    6) Besöksmottagarens för- och efternamn och befattning.
    7) Datum, underskrift och officiell stämpel från den besökande partens behöriga säkerhetsmyndighet.
4. Parternas behöriga säkerhetsmyndigheter kan komma överens om att upprätta förteckningar över personer som är behöriga att göra återkommande besök i samband med genomförandet av ett specifikt projekt, program eller säkerhetsskyddsklassificerat kontrakt. Förteckningarna ska innehålla de uppgifter som avses i punkt 3 och ska vara giltiga i 12 månader. Efter att sådana förteckningar har godkänts av parternas behöriga säkerhetsmyndigheter ska tidpunkterna för besöken överenskommas direkt mellan den besökande organisationen och värdorganisationen i enlighet med de överenskomna villkoren.

5. Besök som innebär tillgång till uppgifter i säkerhetsskyddsklassen ZASTRZEŻONE / BEGRÄNSAT HEMLIG / RESTRICTED ska anordnas direkt mellan den besökande organisationen och värdorganisationen.
6. Vid besök som innebär tillgång till säkerhetsskyddsklassificerade uppgifter ska parterna i enlighet med sin nationella lagstiftning säkerställa skyddet av besökarnas personuppgifter.

ARTIKEL 12

SÄKERHETSÖVERTRÄDELSER

1. Information om varje säkerhetsöverträdelse eller misstänkt säkerhetsöverträdelse som rör säkerhetsskyddsklassificerade uppgifter från ursprungsparten eller säkerhetsskyddsklassificerade uppgifter som genererats till följd av samarbete mellan parterna ska omedelbart rapporteras till den behöriga säkerhetsmyndigheten i den part inom vars territorium säkerhetsöverträdelsen eller den misstänkta säkerhetsöverträdelsen skett.
2. Varje säkerhetsöverträdelse eller misstänkt säkerhetsöverträdelse ska utredas i enlighet med den nationella lagstiftningen i den part inom vars territorium den skett.
3. I händelse av en säkerhetsöverträdelse ska den behöriga säkerhetsmyndigheten i den part inom vars territorium överträdelsen skett skriftligen underrätta den andra partens behöriga säkerhetsmyndighet om överträdelsen, omständigheterna kring den och resultatet av de åtgärder som avses i punkt 2.
4. Parternas behöriga säkerhetsmyndigheter ska på begäran av någon av dem samarbeta kring de åtgärder som avses i punkt 2.

ARTIKEL 13

SPRÅK

Parterna ska använda engelska vid genomförandet av bestämmelserna i detta avtal.

ARTIKEL 14

UTGIFTER

Vardera parten ska stå för sina egna utgifter som uppstår i samband med genomförandet av bestämmelserna i detta avtal.

ARTIKEL 15

SAMRÅD

1. Parternas behöriga säkerhetsmyndigheter ska underrätta varandra om ändringar av deras nationella lagstiftning som rör skydd av säkerhetsskyddsklassificerade uppgifter och som har bäring på genomförandet av detta avtal.
2. Parternas behöriga säkerhetsmyndigheter ska på begäran av någon av dem samråda med varandra för att säkerställa ett nära samarbete kring genomförandet av bestämmelserna i detta avtal.
3. Vardera parten ska tillåta att företrädare för den andra partens behöriga säkerhetsmyndighet besöker dess territorium för att diskutera förfaranden för skydd av säkerhetsskyddsklassificerade uppgifter som överförs av den andra parten.
4. För att säkerställa ett effektivt samarbete, vilket är syftet med detta avtal, får de behöriga säkerhetsmyndigheterna vid behov och inom ramen för den behörighet som de har enligt sin nationella lagstiftning ingå närmare tekniska eller organisatoriska skriftliga överenskommelser.

ARTIKEL 16

TVISTLÖSNING

1. Eventuella tvister i fråga om tillämpningen eller tolkningen av detta avtal ska lösas genom direkta samråd mellan parternas behöriga säkerhetsmyndigheter.
2. Om en tvist inte kan lösas på det sätt som avses i punkt 1 ska den lösas på diplomatisk väg.

ARTIKEL 17

FÖRHÅLLANDE TILL ANDRA AVTAL

Den dag då detta avtal träder i kraft ska avtalet mellan Konungariket Sveriges regering och Republiken Polens regering om ömsesidigt skydd av hemliga uppgifter, undertecknat i Warszawa den 6 september 2007, upphöra att gälla. Säkerhetsskyddsklassificerade uppgifter som har utbytts eller ska utbytas med stöd av det avtalet ska skyddas i enlighet med bestämmelserna i det här avtalet.

ARTIKEL 18

SLUTBESTÄMMELSER

1. Vardera parten ska på diplomatisk väg underrätta den andra parten när de nationella förfaranden som krävs för att detta avtal ska träda i kraft är slutförda. Avtalet träder i kraft den första dagen i den andra månaden efter den dag då den sista noten togs emot.
2. Detta avtal får ändras efter skriftligt samtycke från parterna. Sådana ändringar ska träda i kraft i enlighet med bestämmelserna i punkt 1.
3. Detta avtal ingås på obestämd tid. Vardera parten får säga upp avtalet genom skriftligt meddelande till den andra parten. Detta avtal ska i så fall upphöra att gälla sex månader efter den dag då meddelandet om uppsägning togs emot.
4. Om detta avtal sägs upp ska säkerhetsskyddsklassificerade uppgifter som utbytts eller genererats med stöd av detta avtal skyddas i enlighet med bestämmelserna i det.

Undertecknat i Warszawa den 29 oktober 2025 i två original på svenska, polska och engelska språken, vilka alla texter är lika giltiga. Vid skiljaktiga tolkningar ska den engelska texten ha företräde.

FÖR REPUBLIKEN POLENS REGERING

FÖR KONUNGARIKET SVERIGES REGERING

AGREEMENT

between the Government of the Republic of Poland and the Government of the Kingdom of Sweden on the Mutual Protection of Classified Information

The Government of the Republic of Poland
and the Government of the Kingdom of Sweden,
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 obligations imposed by international legislation and the national legislation 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 that is exchanged or originated as a result of cooperation between the Parties, individuals, legal entities and other forms of organisations being under their jurisdiction.
2. This Agreement shall be applicable to any activities, contracts or other types of agreements involving access to Classified Information that will be conducted or concluded between the Parties or individuals, legal entities or other forms of organisations being under their jurisdiction.

ARTICLE 2
DEFINITIONS

For the purpose of this Agreement, the following terms are defined as follows:

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 originated, which require protection against unauthorised disclosure in accordance with the national legislation of either Party and this Agreement;
2) **Competent Security 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 form of organisation, competent to originate and release Classified Information in accordance with the national legislation of its Party;
4) **Recipient Party** – the Party, an individual, a legal entity or other form of organisation, competent to receive Classified Information in accordance with the national legislation of its Party;
5) **Classified Contract** – a contract, performance of which involves access to Classified Information or originating of such information;

6) **Contractor or Sub-Contractor** – an individual, a legal entity or other form of organisation which has legal capacity to undertake Classified Contracts in accordance with the national legislation of one of the Parties;

7) **Breach of Security** – an action or an omission which is contrary to this Agreement or the national legislation of the Parties concerning Classified Information protection.

ARTICLE 3
SECURITY CLASSIFICATION LEVELS

1. Classified Information is granted a security classification level based on its content, pursuant to the national legislation 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 SWEDEN	EQUIVALENT IN ENGLISH
ŚCIŚLE TAJNE	KVALIFICERAT HEMLIG	TOP SECRET
TAJNE	HEMLIG	SECRET
POUFNE	KONFIDENTIELL	CONFIDENTIAL
ZASTRZEŻONE	BEGRÄNSAT HEMLIG	RESTRICTED

ARTICLE 4
COMPETENT SECURITY AUTHORITIES

1. For the purpose of this Agreement, the Competent Security Authorities shall be:
   1) for the Republic of Poland: the Head of the Internal Security Agency;
   2) for the Kingdom of Sweden: the Swedish Armed Forces, Military Intelligence and Security Service in respect of military matters, the Swedish Security Service in respect of civilian matters and the Swedish Defence Materiel Administration in respect of defence material and industrial security matters.
2. The Parties shall inform each other via diplomatic channels about changes of the Competent Security Authorities referred to in Paragraph 1 or amendments to their competences.

ARTICLE 5
PRINCIPLES OF CLASSIFIED INFORMATION PROTECTION

1. The Parties shall adopt every measure provided in this Agreement and subject to their national legislation in order to protect Classified Information exchanged or originated as a result of cooperation between the Parties, including Classified Contracts performance.
2. Access to Classified Information shall be granted only to those individuals who have a need-to-know and who have been authorised to access such information in accordance with the national legislation of the Recipient Party.
3. The Recipient Party shall take all lawful steps required to prevent the disclosure or use of Classified Information released, except for the purposes and within limitations stated by the Originating Party.

ARTICLE 6
SECURITY CLEARANCES

1. In the scope of this Agreement, the Parties shall recognise Personnel Security Clearances and Facility Security Clearances issued in accordance with the national legislation of the other Party.
2. In accordance with their national legislation, the Competent Security Authorities shall assist each other in carrying out Facility Security Clearance and Personnel Security Clearance investigations upon request by one of them.

ARTICLE 7
CLASSIFIED CONTRACTS

1. Before concluding a Classified Contract connected with access to information classified as POUFNE / KONFIDENTIELL / CONFIDENTIAL or above, the contracting entity shall apply to its Competent Security Authority to request that the Competent Security Authority of the other Party in respect of defence material and industrial security matters 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. 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 legislation of the Party in the territory of the State in which it is located.
3. Classified Information shall not be released to the Contractor until the receipt of the certificate referred to in Paragraph 1.
4. Every Classified Contract shall contain 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.

5. The performance of a Classified Contract in the part connected with access to Classified Information shall be possible on the condition that the Contractor meets the criteria necessary for the protection of Classified Information, pursuant to the provisions on the security requirements referred to in Paragraph 4.

6. Every Sub-Contractor 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 Security Authorities of the Parties ensuring its protection against unauthorised disclosure. The Parties may electronically transmit Classified Information protected by cryptographic functions in accordance with procedures to be approved by the Competent Security Authorities.

2. Information classified as ZASTRZEŻONE /BEGRÄNSAT HEMLIG / RESTRICTED and POUFNE / KONFIDENTIELL / CONFIDENTIAL may be transmitted also through authorised couriers in accordance with the national legislation of the Originating Party.

3. In urgent cases, unless it is possible to use other forms of transmission, if the security requirements defined by the national legislation of the Originating Party are met, the hand carriage of information classified

as ZASTRZEŻONE / BEGRÄNSAT HEMLIG / RESTRICTED and POUFNE / KONFIDENTIELL / CONFIDENTIAL by authorised individuals is admissible.

4. The Recipient Party shall confirm in writing the receipt of Classified Information.
5. The authorities authorised to exchange Classified Information on the basis of other international agreements concluded between the Parties may exchange Classified Information directly in accordance with the terms of such agreements.

ARTICLE 9
REPRODUCTION OR TRANSLATION OF CLASSIFIED INFORMATION

1. Reproduction or translation of Classified Information shall be conducted pursuant to the national legislation of the Recipient Party. Reproduced or translated Classified Information shall be subject to 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 / KVALIFICERAT HEMLIG / TOP SECRET shall be reproduced or translated only after obtaining prior written consent issued by the Originating Party.

ARTICLE 10
DESTRUCTION OF CLASSIFIED INFORMATION

1. Classified Information shall be destroyed in a manner that prevents reconstruction of it in whole or in part, or filed according to national legislation.

2. Information classified as ŚCIŚLE TAJNE / KVALIFICERAT HEMLIG / TOP SECRET shall not be destroyed. It shall be returned to the Originating Party or filed according to national legislation.

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 prior written consent issued by the Competent Security Authority of the other Party.
2. The Competent Security Authority of the visiting Party shall apply for a visit to the Competent Security Authority of the hosting Party at least 30 days prior to the planned visit referred to in Paragraph 1, and in urgent cases the application period may be reduced.
3. The application referred to in Paragraph 2 shall include information on:
   1) purpose, date of and program for 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 number;
   3) position of the visitor along with the name of the entity that 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 Security Authority of the visiting Party.
4. The Competent Security Authorities of the Parties may agree to establish lists of persons authorised to make recurring visits connected

with the implementation of a specific project, program or Classified Contract. The lists shall contain the data specified in Paragraph 3 and are to be valid for a period of 12 months. Once such lists have been approved by the Competent Security 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. Visits involving access to information classified as ZASTRZEŻONE / BEGRÄNSAT HEMLIG / RESTRICTED shall be arranged directly between visiting and hosting entities.
6. The Parties shall ensure, pursuant to their national legislation, 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 between the Parties shall be immediately reported to the Competent Security Authority of the Party in the territory of the State in 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 legislation of the Party in the territory of the State in which it has occurred.
3. In case of a Breach of Security the Competent Security Authority of the Party in the territory of the State in 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 2.

4. The Competent Security Authorities of the Parties shall cooperate in the actions referred to in Paragraph 2, upon request by one of them.

ARTICLE 13
LANGUAGES

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

ARTICLE 14
EXPENSES

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

ARTICLE 15
CONSULTATIONS

1. The Competent Security Authorities of the Parties shall notify each other of any amendments to their national legislation concerning the protection of Classified Information in relation to the implementation of this Agreement.
2. The Competent Security Authorities of the Parties shall consult each other, upon request by 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 Security Authority of the other Party to pay visits to territory in 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 legislation of their Parties, the Competent Security Authorities may, if necessary, conclude written detailed technical or organisational arrangements.

ARTICLE 16
SETTLEMENT OF DISPUTES

1. Any disputes concerning the implementation or interpretation of this Agreement shall be settled through direct consultation between the Competent Security Authorities of the Parties.
2. If settlement of a dispute cannot be achieved 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 Agreement between the Government of the Republic of Poland and the Government of the Kingdom of Sweden on Mutual Protection of Classified Information, signed in Warsaw on 6 September 2007, shall cease to be binding. Classified Information that has been or is to be exchanged on the basis of the Agreement mentioned above, shall be protected according to the provisions of this Agreement.

ARTICLE 18
FINAL PROVISIONS

1. Each Party shall notify the other Party through diplomatic channels once the national procedures necessary for entering into force of this Agreement have been completed. The Agreement shall enter into

force on the first day of the second month following the date 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 indefinite period of time. It may be terminated by either Party by giving written notice to the other Party. In that case, this Agreement shall expire six months after the date of receipt of the termination notice.
4. In case of termination of this Agreement, Classified Information exchanged or originated on the basis of this Agreement shall be protected in accordance with the provisions thereof.

Signed in Warsaw on 29 October 2025 in two original copies, each in the Polish, Swedish 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 SWEDEN

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 15 maja 2026 roku.

Prezydent Rzeczypospolitej Polskiej: *K. Nawrocki*

L.S.

Prezes Rady Ministrów: *D. Tusk*