Warszawa, dnia 9 marca 2026 r.

Poz. 286

UMOWA

między Rządem Rzeczypospolitej Polskiej a Rządem Kanady o ochronie informacji niejawnych,

podpisana w Warszawie dnia 16 stycznia 2025 r.

W imieniu Rzeczypospolitej Polskiej

PREZYDENT RZECZYPOSPOLITEJ POLSKIEJ

podaje do powszechnej wiadomości:

Dnia 16 stycznia 2025 roku w Warszawie została podpisana Umowa między Rządem Rzeczypospolitej Polskiej a Rządem Kanady o ochronie informacji niejawnych, w następującym brzmieniu:

UMOWA
MIĘDZY
RZĄDEM RZECZYPOSPOLITEJ POLSKIEJ
A
RZĄDEM KANADY
O OCHRONIE INFORMACJI NIEJAWNYCH

Rząd Rzeczypospolitej Polskiej (Rzeczpospolita Polska)

i Rząd Kanady (Kanada),

zwane dalej „Stronami",

dążąc do zapewnienia ochrony informacjom niejawnym, które są przekazywane lub udostępniane przez Strony, w szczególności w zakresie bezpieczeństwa przemysłowego oraz obronności,

uznając znaczenie wzajemnej współpracy w zapewnieniu pokoju, bezpieczeństwa międzynarodowego oraz wzajemnego zaufania,

pragnąc stworzyć praktyki i procedury regulujące wzajemną ochronę informacji niejawnych obu Stron,

uzgodniły, co następuje:

ARTYKUŁ 1
DEFINICJE

W niniejszej Umowie:

a) **informacje niejawne** oznaczają wszelkie informacje, którym jedna ze Stron nadała klauzulę tajności oraz które, zgodnie z jej prawem krajowym, wymagają ochrony przed nieuprawnionym ujawnieniem, dostępem oraz zniszczeniem ze względu na interes bezpieczeństwa narodowego. Informacje te mogą mieć formę ustną, wizualną, elektroniczną, magnetyczną lub dokumentu, materiału, sprzętu, a także technologii i obejmują kopie, tłumaczenia oraz materiały w trakcie ich opracowywania. W niniejszej Umowie odniesienie do informacji niejawnych dotyczy również kanadyjskich informacji PROTECTED A / PROTÉGÉ A, PROTECTED B / PROTÉGÉ B lub PROTECTED C / PROTÉGÉ C, o ile nie stwierdzono inaczej;

b) **kontrakt niejawny** oznacza wiążącą umowę, która wymaga udzielenia kontrahentowi dostępu do informacji niejawnych Strony w celu dostarczenia towarów lub świadczenia usług. Termin ten odnosi się również do kontraktu podwykonawczego, jak i działań poprzedzających zawarcie kontraktu;

c) **właściwe organy** oznaczają wyznaczone przez każdą ze Stron organy odpowiedzialne, w ramach ich kompetencji oraz zgodnie z prawem krajowym, za przetwarzanie informacji niejawnych;

d) **narażenie na szwank bezpieczeństwa informacji niejawnych** oznacza nieuprawniony dostęp do informacji niejawnych, ich ujawnienie lub przekazanie, zniszczenie, usunięcie, modyfikację lub wykorzystanie;

e) **kontrahent** oznacza osobę fizyczną lub prawną posiadającą zdolność do zawierania kontraktów niejawnych. Termin ten odnosi się także do podwykonawcy;

f) **świadectwo bezpieczeństwa przemysłowego** oznacza dokument wydany przez jedną ze Stron, który potwierdza, że kontrahent spełnia wymogi

bezpieczeństwa do przetwarzania informacji niejawnych zgodnie z prawem krajowym tej Strony;

g) **zasada ograniczonego dostępu** oznacza, że dostęp do informacji niejawnych jest ograniczony do osób uprawnionych, które wymagają dostępu do tych informacji w celu wykonywania swoich obowiązków służbowych;

h) **Strona wytwarzająca** oznacza Stronę, która przekazuje informacje niejawne Stronie otrzymującej;

i) **poświadczenie bezpieczeństwa** oznacza dokument wydany przez jedną ze Stron, który potwierdza, że osoba jest uprawniona do dostępu do informacji niejawnych zgodnie z prawem krajowym tej Strony;

j) **instrukcja bezpieczeństwa programu/projektu** oznacza zbiór zasad i procedur bezpieczeństwa opartych na prawie krajowym Stron i przez nie zatwierdzonych, które mają zastosowanie do określonego programu lub projektu w celu ujednolicenia procedur bezpieczeństwa;

k) **Strona otrzymująca** oznacza Stronę, która otrzymuje informacje niejawne przekazane przez Stronę wytwarzającą;

l) **organ bezpieczeństwa** oznacza organ rządowy wyznaczony przez Stronę do nadzoru nad wykonywaniem niniejszej Umowy; oraz

m) **strona trzecia** oznacza państwo, w tym osoby fizyczne lub prawne, lub inne jednostki organizacyjne podlegające jego jurysdykcji, jak również organizację międzynarodową, niebędące stroną niniejszej Umowy.

ARTYKUŁ 2
CEL I ZAKRES

1. Celem niniejszej Umowy jest zapewnienie ochrony informacjom niejawnym wytwarzanym w wyniku współpracy lub wymienianym między Stronami.
2. Umowa niniejsza określa zasady i procedury ochrony informacji niejawnych przekazywanych lub udostępnianych w zakresie bezpieczeństwa przemysłowego lub obronności przez jedną Stronę drugiej Stronie lub przez

jedną Stronę kontrahentowi drugiej Strony lub przez kontrahenta jednej Strony kontrahentowi drugiej Strony.

3. Umowa niniejsza nie stanowi podstawy do obligatoryjnego przekazywania lub udostępnienia informacji niejawnych przez Strony.

ARTYKUŁ 3
ORGANY BEZPIECZEŃSTWA

1. Strony, jako swoje organy bezpieczeństwa, wyznaczają:
   a) w Rzeczypospolitej Polskiej:
      Szefa Agencji Bezpieczeństwa Wewnętrznego;
   b) w Kanadzie:
      Zarząd Międzynarodowego Bezpieczeństwa Przemysłowego,
      Sektor Bezpieczeństwa Przemysłowego,
      Usługi Rządowe i Publiczne Kanady (określane również jako Usługi i Zamówienia Publiczne Kanady)
   lub ich właściwych następców prawnych.
2. Dla celów niniejszej Umowy Strony informują się pisemnie o właściwych organach.

ARTYKUŁ 4
KLAUZULE TAJNOŚCI

1. Strona wytwarzająca nadaje informacjom niejawnym klauzulę tajności i oznacza je zgodnie ze swoim prawem krajowym.
2. Zgodnie ze swoim prawem krajowym Strona otrzymująca może oznaczyć przekazane lub udostępnione przez Stronę wytwarzającą informacje niejawne klauzulą tajności co najmniej równoważną klauzuli nadanej przez Stronę wytwarzającą, zgodnie z tabelą numer 1 oraz 2.
3. Tabela numer 1 określa równorzędne oznaczenia stosowane przez Strony w odniesieniu do klauzul tajności ich informacji niejawnych.

Tabela numer 1: Informacje niejawne

RZECZPOSPOLITA POLSKA (JĘZYK POLSKI)	KANADA (JĘZYK ANGIELSKI)	KANADA (JĘZYK FRANCUSKI)
ŚCIŚLE TAJNE	TOP SECRET	TRÈS SECRET
TAJNE	SECRET	SECRET
POUFNE	CONFIDENTIAL	CONFIDENTIEL
ZASTRZEŻONE (PATRZ USTĘP 4)	PROTECTED A	PROTÉGÉ A

4. Kanada może określić dodatkowe wymogi bezpieczeństwa w postanowieniach kontraktu dotyczących ochrony i przetwarzania informacji PROTECTED A / PROTÉGÉ A w celu wsparcia kontrahentów z Rzeczypospolitej Polskiej mających dostęp do takich informacji.

5. Rzeczpospolita Polska zapewnia ochronę kanadyjskim informacjom oznaczonym jako PROTECTED B / PROTÉGÉ B lub PROTECTED C / PROTÉGÉ C zgodnie z poziomem równorzędności klauzul tajności określonym w tabeli numer 2:

Tabela numer 2: kanadyjskie informacje oznaczone jako PROTECTED i PROTÉGÉ:

RZECZPOSPOLITA POLSKA (język polski)	KANADA (język angielski)	KANADA (język francuski)
TAJNE	PROTECTED C	PROTÉGÉ C
POUFNE	PROTECTED B	PROTÉGÉ B

ARTYKUŁ 5
OCHRONA I WYKORZYSTANIE INFORMACJI NIEJAWNYCH

1. Strony zapewniają ochronę i wykorzystują informacje niejawne w następujący sposób:
   a) Strona otrzymująca zapewnia co najmniej równoważny poziom ochrony, jaki zapewnia swoim informacjom o równorzędnej klauzuli tajności;
   b) Strona otrzymująca wykorzystuje informacje niejawne wyłącznie do celów, do których zostały przekazane lub udostępnione, chyba że Strona wytwarzająca, za pośrednictwem swoich organów bezpieczeństwa lub właściwych organów, wyrazi uprzednio pisemną zgodę na inne postępowanie;
   c) Strona wytwarzająca może pisemnie określić ograniczenia w zakresie wykorzystania informacji niejawnych przez Stronę otrzymującą, która ma obowiązek zastosowania się do tych ograniczeń;
   d) Strona otrzymująca nie obniży ani nie zniesie klauzuli tajności informacji niejawnych bez uprzedniej pisemnej zgody Strony wytwarzającej przekazanej za pośrednictwem odpowiednich organów bezpieczeństwa lub właściwych organów;
   e) Strona wytwarzająca informuje Stronę otrzymującą o zmianie klauzuli tajności informacji niejawnych; oraz
   f) Strona otrzymująca stosuje wszelkie możliwe środki, aby zapobiec narażeniu na szwank bezpieczeństwa informacji niejawnych przekazanych przez Stronę wytwarzającą lub utracie takich informacji.
2. Strony mogą wspólnie ustalić pisemnie dodatkowe wymogi bezpieczeństwa dla ochrony informacji niejawnych.
3. Strony informują się o zmianach w swoich przepisach krajowych, które mogą mieć wpływ na ochronę informacji niejawnych przekazanych lub udostępnionych zgodnie z niniejszą Umową.

ARTYKUŁ 6
DOSTĘP DO INFORMACJI NIEJAWNYCH

1. Strony nie udzielają dostępu do informacji niejawnych jedynie na podstawie stopnia, stanowiska lub poświadczenia bezpieczeństwa, chyba że Strona wytwarzająca wyrazi na to zgodę kierując się wyjątkowymi okolicznościami. Dostęp do informacji niejawnych przyznaje się osobie:
   a) wobec której stosuje się zasadę ograniczonego dostępu;
   b) która posiada poświadczenie bezpieczeństwa do odpowiedniej klauzuli, jeśli jest to wymagane; oraz
   c) która została przeszkolona w zakresie ochrony informacji niejawnych zgodnie z prawem krajowym Stron.
2. Dla celów niniejszej Umowy organy bezpieczeństwa Stron uznają poświadczenia bezpieczeństwa i świadectwa bezpieczeństwa przemysłowego wydane zgodnie z prawem krajowym drugiej Strony.

ARTYKUŁ 7
PRZEKAZYWANIE INFORMACJI NIEJAWNYCH

1. Strony zapewniają, że informacje niejawne są przekazywane wyłącznie za pośrednictwem uprawnionego przewoźnika lub innych środków wspólnie uzgodnionych przez ich odpowiednie organy bezpieczeństwa lub właściwe organy, zgodnie z prawem krajowym Stron.
2. Na wniosek Strony wytwarzającej, Strona otrzymująca przedstawi pisemne potwierdzenie odbioru informacji niejawnych.
3. Strony, za pośrednictwem swoich odpowiednich organów bezpieczeństwa, informują kontrahenta o sposobie zabezpieczania przekazywanych materiałów niejawnych, który wspólnie uzgodniły.
4. Jeżeli rozmiar informacji niejawnych uniemożliwia ich przekazanie za pośrednictwem uprawnionego przewoźnika, Strony, poprzez swoje odpowiednie organy bezpieczeństwa lub właściwe organy, wspólnie opracowują plan transportu informacji niejawnych uzgadniając sposób ich

przekazania. Plan ten może uwzględniać środek transportu, trasę i rodzaj eskorty informacji niejawnych.

5. Strony zapewniają, że informacje niejawne w postaci sprzętu lub jego elementu są odpowiednio opakowane i chronione podczas przekazywania w sposób uniemożliwiający identyfikację ich zawartości oraz pozostają pod stałą kontrolą, aby zapobiec dostępowi do nich osobom nieuprawnionym.

6. Strony mogą wspólnie zezwolić na przekazywanie informacji niejawnych bezpieczną drogą elektroniczną. W tym celu wspólnie określą odpowiednie procedury bezpieczeństwa.

ARTYKUŁ 8
TŁUMACZENIE, KOPIOWANIE I NISZCZENIE INFORMACJI NIEJAWNYCH

1. Strony zapewniają, że informacje niejawne o klauzuli tajności POUFNE / CONFIDENTIAL / CONFIDENTIEL lub wyższej nie są tłumaczone ani powielane bez pisemnej zgody Strony wytwarzającej przekazanej za pośrednictwem ich organów bezpieczeństwa lub jednego z jej właściwych organów.

2. Strony zapewniają, że przetłumaczone lub powielone informacje niejawne zachowują taką klauzulę tajności oraz poziom ochrony, jak ich oryginały.

3. W przypadku, gdy Strona otrzymująca wykorzysta informacje niejawne a Strona wytwarzająca zezwoli na ich zniszczenie bądź zwrot lub w przypadku, gdy Strona wytwarzająca wystąpi o ich zniszczenie lub zwrot, Strona otrzymująca zniszczy lub zwróci te informacje zgodnie z wymogami ochrony, jakie stosuje względem swoich informacji niejawnych o równorzędnej klauzuli tajności.

4. W przypadku zakończenia kontraktu niejawnego przez kontrahenta lub gdy nie ma potrzeby dalszego wykorzystania przez niego informacji niejawnych, Strona otrzymująca zapewnia, że są one zwracane Stronie wytwarzającej,

chyba że ta poinformuje pisemnie kontrahenta o konieczności ich zniszczenia.

ARTYKUŁ 9
KONTRAKTY NIEJAWNE

1. Przed przekazaniem lub udostępnieniem informacji niejawnych kontrahentowi, Strona otrzymująca zapewnia, że:
   a) kontrahent oraz użytkowane przez niego obiekty spełniają wymogi bezpieczeństwa związane z ochroną informacji niejawnych, zgodnie z prawem krajowym Strony otrzymującej;
   b) kontrahent posiada ważne świadectwo bezpieczeństwa przemysłowego do przetwarzania informacji niejawnych o klauzuli POUFNE / CONFIDENTIAL / CONFIDENTIEL lub wyższej;
   c) dostęp do informacji niejawnych jest udzielany zgodnie z zasadą ograniczonego dostępu oraz na podstawie ważnego poświadczenia bezpieczeństwa do odpowiedniego poziomu;
   d) osoba, która ma dostęp do informacji niejawnych, została poinformowana
      o obowiązku ich ochrony, zgodnie z prawem krajowym Strony otrzymującej oraz postanowieniami niniejszej Umowy; oraz
   e) obiekty użytkowane przez kontrahenta, który posiada świadectwo bezpieczeństwa przemysłowego, są poddawane inspekcjom w celu stwierdzenia, czy spełniają wymogi w zakresie ochrony informacji niejawnych.
2. W przypadku, gdy w użytkowanych przez kontrahenta obiektach przetwarzane są informacje niejawne, Strona otrzymująca zapewnia, że kontrahent zatrudnia pełnomocnika ochrony z ważnym poświadczeniem bezpieczeństwa do odpowiedniego poziomu, w celu ochrony tych informacji.

ARTYKUŁ 10
POSTANOWIENIA DOTYCZĄCE WYMOGÓW BEZPIECZEŃSTWA KONTRAKTU

1. Każda ze Stron zapewnia, że:

a) kontrakt niejawny, który wiąże się z dostępem do informacji niejawnych, jest realizowany na podstawie postanowień dotyczących wymogów bezpieczeństwa, zgodnie z przepisami krajowymi tej Strony oraz niniejszej Umowy;

b) kontrakt niejawny zawiera opis wymogów bezpieczeństwa związanych z przetwarzaniem informacji niejawnych i obejmuje wykaz informacji niejawnych przekazywanych lub udostępnianych kontrahentowi lub przez niego wytwarzanych z uwzględnieniem ich klauzul tajności. Wymogi bezpieczeństwa w Kanadzie są zawarte w kontrolnej liście wymogów bezpieczeństwa, natomiast w przypadku Rzeczypospolitej Polskiej w instrukcji bezpieczeństwa przemysłowego;

c) w przypadku, gdy kontrakt niejawny jest realizowany na terytorium Państwa drugiej Strony, organ bezpieczeństwa lub właściwe organy Strony wytwarzającej przekażą organowi bezpieczeństwa drugiej Strony kopię opisu wymogów bezpieczeństwa;

d) postanowienia dotyczące wymogów bezpieczeństwa związanych z kontraktem niejawnym zawierają w szczególności:

i) wymóg, aby kontrahent przekazywał lub udostępniał informacje niejawne wyłącznie osobie, która posiada poświadczenie bezpieczeństwa, spełnia zasadę ograniczonego dostępu oraz została przeszkolona w zakresie ochrony informacji niejawnych zgodnie z prawem krajowym swojej Strony;

ii) środki stosowane do przekazywania informacji niejawnych;

iii) procedury wnioskowania o wizytę w obiektach przemysłowych lub rządowych na terytorium Państwa Strony, zgodnie z postanowieniami artykułu 13;

iv) procedury dla kontrahentów umożliwiające niezwłoczne powiadamianie organów bezpieczeństwa swojej Strony o możliwości utraty lub narażenia na szwank bezpieczeństwa informacji niejawnych;

v) wymóg, aby informacje niejawne przekazane lub udostępnione w ramach realizacji kontraktu niejawnego, zostały wykorzystane wyłącznie w tym celu;

vi) procedury niszczenia informacji niejawnych; oraz

vii) wymóg uzyskania pisemnej zgody organu bezpieczeństwa Strony wytwarzającej na przekazanie lub udostępnienie przez kontrahenta informacji niejawnych stronie trzeciej.

2. W przypadku, gdy skala lub złożoność programu lub projektu oraz związane z tym informacje niejawne wymagają zastosowania dodatkowych wymogów bezpieczeństwa, organy bezpieczeństwa Stron wspólnie opracują instrukcję bezpieczeństwa programu/projektu w formie załącznika do kontraktu.

ARTYKUŁ 11
POTWIERDZANIE UPRAWNIEŃ

1. Strona, działając za pośrednictwem swojego organu bezpieczeństwa, zapewnia, że przed zawarciem kontraktu niejawnego z kontrahentem drugiej Strony lub udostępnieniem mu informacji niejawnych, uzyska potwierdzenie organu bezpieczeństwa drugiej Strony, że kontrahent spełnia stosowne wymogi bezpieczeństwa.

2. Strona zapewnia, że na wniosek organu bezpieczeństwa drugiej Strony jej organ bezpieczeństwa potwierdzi pisemnie, że kontrahent posiada ważne poświadczenie bezpieczeństwa lub świadectwo bezpieczeństwa przemysłowego.

3. Strona zapewnia, że:

a) jeżeli jej organ bezpieczeństwa wydał świadectwo bezpieczeństwa przemysłowego lub poświadczenie bezpieczeństwa kontrahentowi, który zawarł kontrakt niejawny z drugą Stroną, organ ten może je cofnąć zgodnie z prawem krajowym swojej Strony i wówczas niezwłocznie informuje organ bezpieczeństwa drugiej Strony o tym fakcie;

b) jeżeli kontrahent nie posiada świadectwa bezpieczeństwa przemysłowego lub poświadczenia bezpieczeństwa, które spełnia wymogi bezpieczeństwa określone w kontrakcie niejawnym drugiej Strony, jego organ bezpieczeństwa, za zgodą i na wniosek przedsiębiorcy, dokona oceny bezpieczeństwa w celu ustalenia czy może wydać mu świadectwo bezpieczeństwa przemysłowego lub poświadczenie bezpieczeństwa, bądź poszerzyć ich dotychczasowy zakres, a także potwierdzić posiadane przez niego uprawnienia, zgodnie z ustępem 2; oraz

c) jeżeli jej organ bezpieczeństwa nie jest w stanie niezwłocznie potwierdzić uprawnień kontrahenta na wniosek drugiej Strony, organ ten informuje organ bezpieczeństwa drugiej Strony o statusie realizacji wniosku.

4. Organ bezpieczeństwa, który otrzymał wniosek o potwierdzenie uprawnień, odpowiada w terminie pięciu dni roboczych, chyba że Strony uzgodnią inaczej.

5. Na wniosek Strony, która przeprowadza postępowanie sprawdzające w celu wydania poświadczenia bezpieczeństwa lub świadectwa bezpieczeństwa przemysłowego, druga Strona udzieli pomocy w przeprowadzeniu takiego postępowania.

ARTYKUŁ 12

OCENA BEZPIECZEŃSTWA I KONSULTACJE

1. Strony mogą porozumieć się w zakresie składania obustronnych wizyt w celu oceny skuteczności wymogów bezpieczeństwa realizowanych

na mocy niniejszej Umowy, w tym również w odniesieniu do kontraktów niejawnych.

2. Strony mogą organizować spotkania w celu omówienia swojego prawa krajowego oraz procedur dotyczących niniejszej Umowy, aby zapewnić ich spójne stosowanie.

3. Strony wspólnie ustalą szczegóły spotkań i wizyt, o których mowa w ustępach 1 i 2.

ARTYKUŁ 13
WIZYTY MIĘDZYNARODOWE

Strona zapewnia, że:

a) jej organ bezpieczeństwa lub jeden z jej właściwych organów udzieli zgody na wizytę osoby zatrudnionej przez drugą Stronę lub przez kontrahenta drugiej Strony w obiekcie na terytorium swojego Państwa, jeżeli wizyta została zatwierdzona przez organ bezpieczeństwa lub jeden z właściwych organów drugiej Strony, a osoba przybywająca z wizytą posiada odpowiednie poświadczenie bezpieczeństwa oraz spełnia zasadę ograniczonego dostępu;

b) osoba zatrudniona przez tę Stronę lub przez kontrahenta tej Strony, która ubiega się o wizytę związaną z dostępem do informacji niejawnych na poziomie POUFNE / CONFIDENTIAL / CONFIDENTIEL lub wyższym w obiekcie kontrahenta na terytorium Państwa drugiej Strony, składa wniosek o wyrażenie na nią zgody za pośrednictwem swojego organu bezpieczeństwa i spełnia wymogi bezpieczeństwa drugiej Strony;

c) wniosek o wyrażenie zgody na wizytę zawiera imię i nazwisko osoby przybywającej z wizytą, datę i miejsce jej urodzenia, obywatelstwo, numer paszportu lub innego dokumentu tożsamości, stopień (jeśli ma to zastosowanie), stanowisko służbowe oraz poziom poświadczenia bezpieczeństwa, jak również nazwę podmiotu

wysyłającego, cel i datę wizyty, osoby do kontaktu po stronie wizytującego oraz nazwę odwiedzanego podmiotu;

d) jej organ bezpieczeństwa lub jeden z jej właściwych organów składa wniosek o wyrażenie zgody na wizytę do organu bezpieczeństwa lub jednego z właściwych organów drugiej Strony na co najmniej trzydzieści dni roboczych przed planowaną wizytą, chyba że Strony uzgodnią inaczej; oraz

e) dane osobowe związane z wizytami są chronione zgodnie z jej prawem krajowym.

ARTYKUŁ 14
OGRANICZENIA WOBEC STRONY TRZECIEJ

1. Strona otrzymująca nie przekazuje ani nie udostępnia informacji niejawnych stronie trzeciej bez uprzedniej pisemnej zgody organu bezpieczeństwa Strony wytwarzającej.
2. Strony zapewniają, że ich kontrahenci nie przekazują ani nie udostępniają informacji niejawnych kontrahentom strony trzeciej bez uprzedniej pisemnej zgody organów bezpieczeństwa obu Stron.
3. Do celów niniejszej Umowy osoba fizyczna, która posiada poświadczenie bezpieczeństwa lub kontrahent posiadający świadectwo bezpieczeństwa przemysłowego wydane przez którąkolwiek ze Stron nie jest uważany za stronę trzecią.

ARTYKUŁ 15
UTRATA LUB NARAŻENIE NA SZWANK BEZPIECZEŃSTWA INFORMACJI NIEJAWNYCH

1. W przypadku uzyskania informacji o możliwości utraty lub narażenia bezpieczeństwa informacji niejawnych na szwank, Strona otrzymująca niezwłocznie informuje o tym Stronę wytwarzającą oraz wszczyna postępowanie wyjaśniające. Wyniki postępowania wraz z informacją na

temat środków podjętych w celu uniknięcia podobnego zdarzenia w przyszłości są przekazywane Stronie wytwarzającej.

2. Strony, na wniosek jednej z nich, współpracują w ramach prowadzonego postępowania wyjaśniającego, o którym mowa w ustępie 1.

ARTYKUŁ 16
KOSZTY

Każda ze Stron pokrywa koszty własne ponoszone w związku z realizacją niniejszej Umowy.

ARTYKUŁ 17
POROZUMIENIA WYKONAWCZE

1. Organy bezpieczeństwa Stron mogą zawierać porozumienia wykonawcze na podstawie niniejszej Umowy.
2. W ramach swoich kompetencji, właściwe organy Stron mogą zawierać porozumienia wykonawcze określające dodatkowe środki postępowania z informacjami niejawnymi. Porozumienia te mają charakter wykonawczy w stosunku do niniejszej Umowy.

ARTYKUŁ 18
INNE UMOWY I POROZUMIENIA

Umowa niniejsza nie zmienia obowiązujących umów lub porozumień między Stronami, chyba że jej postanowienia stanowią inaczej.

ARTYKUŁ 19
ROZSTRZYGANIE SPORÓW

Kwestie sporne wynikające z niniejszej Umowy są rozstrzygane w drodze konsultacji między Stronami.

ARTYKUŁ 20
POSTANOWIENIA KOŃCOWE

1. Strony informują się pisemnie w drodze dyplomatycznej o zakończeniu procedur wewnętrznych niezbędnych do wejścia w życie niniejszej Umowy. Umowa niniejsza wejdzie w życie z datą noty późniejszej.
2. Umowa niniejsza może zostać zmieniona na podstawie pisemnej zgody Stron. Taka zmiana wejdzie w życie z datą noty późniejszej informującej o zakończeniu przez każdą ze Stron procedur wewnętrznych niezbędnych do wejścia w życie takiej zmiany.
3. Strona może wypowiedzieć niniejszą Umowę w drodze pisemnej notyfikacji skierowanej do drugiej Strony. Niniejsza Umowa traci moc w terminie sześciu miesięcy od daty otrzymania notyfikacji przez drugą Stronę.
4. Bez względu na wypowiedzenie niniejszej Umowy, wszystkie informacje niejawne przekazane lub udostępnione na jej podstawie będą nadal chronione zgodnie z jej postanowieniami, chyba że Strona wytwarzająca poinformuje o innych ustaleniach.
5. Strony dokonują wspólnie przeglądu niniejszej Umowy co najmniej raz na pięć lat w celu ustalenia, czy konieczne są jej zmiany.

Na dowód czego niżej podpisani, należycie do tego upoważnieni przez swoje Rządy, podpisali niniejszą Umowę.

Sporządzono w dwóch egzemplarzach w WARSZAWIE dnia 16 STYCZNIA 2025 r. w językach polskim, angielskim i francuskim, przy czym wszystkie teksty są jednakowo autentyczne.

Z UPOWAŻNIENIA RZĄDU RZECZYPOSPOLITEJ

Z UPOWAŻNIENIA RZĄDU KANADY

AGREEMENT
BETWEEN
THE GOVERNMENT OF THE REPUBLIC OF POLAND
AND THE GOVERNMENT OF CANADA
ON THE PROTECTION OF CLASSIFIED INFORMATION

The Government of the Republic of Poland (Republic of Poland)
and the Government of Canada (Canada),
hereinafter referred to as the "Parties",

Wishing to ensure the protection of classified information that is provided or disclosed between the Parties particularly in the context of industrial security and defence,

Recognizing the important role of their mutual co-operation in ensuring peace, international security, and mutual confidence,

Desiring to create practices and procedures to govern the reciprocal protection of classified information for both Parties,

Have agreed as follows:

ARTICLE 1

DEFINITIONS

In this Agreement:

(a) "classified information" means any information that is assigned a security classification level by a Party and which requires protection against unauthorised disclosure, access, or destruction in the interest of national security and in accordance with its national laws and regulations. This information may be in oral, visual, electronic, magnetic, or documentary form, or in the form of material, equipment, or technology, and includes reproductions, translations, and material in the process of development. A reference to classified information in this Agreement also includes Canadian information marked PROTECTED A/PROTÉGÉ A, PROTECTED B/PROTÉGÉ B or PROTECTED C/PROTÉGÉ C, unless otherwise specified;

(b) "classified contract" means a legally binding instrument that requires a contractor to access the classified information of a Party to provide a good or service. This term includes a sub-contract or a pre-contractual activity;

(c) "competent authorities" means organisations, which are designated by each Party as the authorities responsible, within their respective competence under the national laws and regulations, for the handling of classified information;

(d) "compromise" means the unauthorized access to, disclosure or provision of, destruction, removal, modification, or use of classified information;

(e) "contractor" means an individual or a legal entity that has the legal capacity to enter into a classified contract. This term includes a sub-contractor;

(f) "company security clearance" means a determination by a Party that a contractor meets the security requirements to handle classified information in accordance with the national laws and regulations of that Party;

(g) "need-to-know" means that access to classified information is limited

to authorised individuals who need to have access to that classified information in order to perform their official duties;

(h) "originating Party" means the Party which provides classified information to the receiving Party;

(i) "personnel security clearance" means a determination by a Party that an individual is eligible to access classified information in accordance with the national laws and regulations of that Party;

(j) "Program/Project Security Instruction" means a compilation of security regulations and procedures based on the national laws and regulations of the Parties, which are applied to a specific program or project in order to standardize security procedures and approved by both Parties;

(k) "receiving Party" means the Party which receives classified information provided by the originating Party;

(l) "security authority" means a governmental organisation designated by a Party to administer the implementation of this Agreement; and

(m) "third party" means any country, including individuals, legal entities or other forms of organisation under its jurisdiction, or an international organisation not being a party to this Agreement.

ARTICLE 2

OBJECTIVE AND SCOPE

1. The objective of this Agreement is to ensure the protection of classified information that is generated as a result of cooperation or exchanged between the Parties.

2. This Agreement sets out the standards and procedures for the protection of classified information that is provided or disclosed, in an industrial security or defence context, by one Party to the other Party, or by one Party to a contractor from the other Party, or by a contractor from one Party to a contractor from the other Party.

3. This Agreement cannot be construed to compel a Party to provide or disclose classified information.

ARTICLE 3

SECURITY AUTHORITIES

1. The Parties designate the following as their respective security authorities:

(a) for the Republic of Poland:

The Head of the Internal Security Agency

(b) for Canada:

International Industrial Security Directorate,

Industrial Security Sector,

Public Works and Government Services Canada

(also known as Public Services and Procurement Canada)

or their respective successors.

2. The Parties shall notify, in writing, each other of the competent authorities for this Agreement.

ARTICLE 4

SECURITY CLASSIFICATION LEVELS

1. The originating Party shall assign a security classification level to classified information and shall mark the classified information according to its national laws and regulations.

2. The receiving Party, in accordance with its national laws and regulations, may mark classified information that is provided or disclosed by the originating Party with a security classification level that is at least equivalent to the security classification level assigned by the originating Party, in accordance with Table 1 and Table 2.

3. Table 1 identifies the equivalent terms used by the respective Parties for their security classification levels of classified information:

Table 1: Classified Information

In the Republic of Poland (Polish)	In Canada (English)	In Canada (French)
ŚCIŚLE TAJNE	TOP SECRET	TRÈS SECRET
TAJNE	SECRET	SECRET
POUFNE	CONFIDENTIAL	CONFIDENTIEL
ZASTRZEŻONE (see paragraph 4)	PROTECTED A	PROTÉGÉ A

4. Canada may identify additional security requirements in contract clauses for the protection and handling of the PROTECTED A/PROTÉGÉ A information in support of the contractors from the Republic of Poland accessing such information.

5. The Republic of Poland shall protect Canadian information marked PROTECTED B/ PROTÉGÉ B or PROTECTED C/PROTÉGÉ C at the security classification level identified in Table 2:

Table 2: Canadian Information marked PROTECTED and PROTÉGÉ

In the Republic of Poland (Polish)	In Canada (English)	In Canada (French)
TAJNE	PROTECTED C	PROTÉGÉ C
POUFNE	PROTECTED B	PROTÉGÉ B

ARTICLE 5

PROTECTION AND USE OF CLASSIFIED INFORMATION

1. The Parties shall protect and use classified information as follows:

   (a) the receiving Party shall give protection that is at least equal to the protection that it gives to its own information of an equivalent security classification level;

   (b) the receiving Party shall use classified information only for the purpose for which it is provided or disclosed unless the originating Party gives prior consent in writing to do otherwise through the Parties' respective security authorities or competent authorities;

   (c) the originating Party may specify, in writing, limitations on the use of classified information by the receiving Party, and the receiving Party shall comply with such limitations;

   (d) the receiving Party shall not downgrade the security classification level of classified information or declassify classified information without the prior consent, in writing, of the originating Party through the Parties' respective security authorities or competent authorities;

   (e) the originating Party shall inform the receiving Party of a change in the security classification level of classified information; and

   (f) the receiving Party shall use every available means to prevent the loss or compromise of classified information provided by the originating Party.

2. The Parties may jointly determine, in writing, additional security requirements for the protection of classified information.

3. A Party shall notify the other Party of changes in its national laws and regulations that could affect the protection of classified information provided or disclosed under this Agreement.

ARTICLE 6

ACCESS TO CLASSIFIED INFORMATION

1. The Parties shall not give an individual access to classified information based only on that individual's rank, appointment, or personnel security clearance, unless the originating Party provides consent to such release in exceptional circumstances. The Parties shall give an individual access to classified information only if that individual:
   (a) has a need-to-know;
   (b) has a personnel security clearance to the appropriate level, as required; and
   (c) is briefed on the protection of classified information in accordance with the Parties' respective national laws and regulations.
2. For the purposes of this Agreement, the security authorities of each Party shall recognize personnel security clearances and company security clearances issued in accordance with the national laws and regulations of the other Party.

ARTICLE 7

TRANSMISSION OF CLASSIFIED INFORMATION

1. The Parties shall ensure that classified information is transmitted only by approved courier or by other means jointly approved by their respective security authorities or competent authorities, in accordance with the Parties' respective national laws and regulations.
2. At the request of the originating Party, the receiving Party shall provide the originating Party with confirmation, in writing, that it has received classified information.
3. The Parties, through their respective security authorities, shall advise a contractor of the means and the packaging standards that they have jointly approved for the transmission of classified information.
4. If classified information is too voluminous to be transmitted by approved

courier, the Parties, through their respective security authorities, shall jointly draft a transportation plan that describes how they intend to transmit the classified information. That plan may include the type of transport, the route, and the type of escort for the classified information.

5. The Parties shall ensure that classified information in the form of or contained in equipment is securely packaged or protected for transmission in order to prevent identification of its contents and kept under continuous control to prevent access by unauthorized individuals.

6. The Parties may jointly authorize the transmission of classified information by protected electronic means and shall jointly determine the applicable security procedures.

ARTICLE 8

TRANSLATION, REPRODUCTION, AND DESTRUCTION OF CLASSIFIED INFORMATION

1. The Parties shall ensure that classified information at the level of POUFNE / CONFIDENTIAL / CONFIDENTIEL or above is not translated or reproduced without the written consent of the originating Party given through its security authority or one of its competent authorities.

2. The Parties shall ensure that a translation or a reproduction of classified information retains the security classification level of the original classified information and is given the same protection.

3. If the receiving Party no longer requires the classified information and the originating Party authorizes its destruction or return, or if the originating Party requests its destruction or return, the receiving Party shall destroy or return the classified information in accordance with the level of protection that the receiving Party gives to its own classified information at the equivalent security classification level.

4. If a contractor completes a classified contract or no longer needs to retain classified information, the receiving Party shall ensure that the classified

information is returned to the originating Party, unless the originating Party gives specific instructions, in writing, that the contractor needs to destroy the classified information.

ARTICLE 9

CLASSIFIED CONTRACTS

1. The receiving Party, prior to providing or disclosing classified information to a contractor, shall ensure that:
   (a) the contractor and the facility of that contractor meet the security requirements to protect the classified information in accordance with the national laws and regulations of the receiving Party;
   (b) the contractor has a valid company security clearance to handle classified information at the level of POUFNE / CONFIDENTIAL / CONFIDENTIEL or above;
   (c) an individual who has access to classified information has a need-to-know and a valid personnel security clearance to the appropriate level;
   (d) an individual who has access to classified information is informed of that individual's duty to protect the classified information in accordance with the national laws and regulations of the receiving Party and the provisions of this Agreement; and
   (e) the facility of the contractor that has a company security clearance is inspected to determine if it meets the security requirements to handle classified information.
2. The receiving Party shall ensure that if a facility of a contractor handles classified information, the contractor shall have a company security officer, holding a valid personnel security clearance to the appropriate level, to protect that classified information.

ARTICLE 10

CONTRACT SECURITY CLAUSES

1. A Party shall ensure that:

   (a) a classified contract that requires access to classified information is governed by security clauses in accordance with the national laws and regulations of that Party and the provisions of this Agreement;

   (b) a classified contract includes a description of the security requirements to handle classified information. The description of the security requirements shall indicate the classified information that is provided or disclosed to or generated by the contractor and the security classification level that is assigned to that classified information. For Canada, the security requirements are described in a Security Requirements Check List. For the Republic of Poland, the security requirements are described in the Industrial Security Instruction;

   (c) for a classified contract that is performed in the territory of the country of the other Party, the security authority or one of the competent authorities of the originating Party provides to the security authority of the other Party a copy of the description of the security requirements;

   (d) security clauses that govern a classified contract include at least:

      (i) a requirement that the contractor provide or disclose the classified information only to an individual who has a personnel security clearance, a need-to-know, and a briefing on the protection of classified information in accordance with that Party's national laws and regulations;

      (ii) the means to be used to transmit the classified information;

      (iii) the procedures to request an international visit to an industrial or a governmental facility in the territory of the country of a Party, in accordance with Article 13;

(iv) the procedures for a contractor to promptly notify the security authority of the Party where the contractor is based on the possibility that classified information is lost or compromised;

(v) a requirement that classified information provided or disclosed in the context of a classified contract only be used for the purpose of that classified contract;

(vi) the procedures for the final disposal of classified information; and

(vii) a requirement that a contractor not provide or disclose classified information to a third party without the consent, in writing, of the security authority of the originating Party.

2. When the Parties determine that the size or complexity of the program or project and the classified information involved require the application of additional security requirements, the security authorities of the Parties shall jointly prepare a Program/Project Security Instruction and include it in the contract as an annex.

ARTICLE 11

SECURITY ASSURANCES

1. A Party, through its security authority, shall take measures to ensure that a contractor from the other Party is not awarded a classified contract and does not receive classified information until the security authority of the other Party confirms that the contractor meets the requisite security requirements.

2. At the request of the security authority of the other Party, a Party shall ensure that its security authority provides a security assurance, in writing, that indicates whether a contractor has a valid personnel security clearance or company security clearance.

3. A Party shall ensure that:

(a) if its security authority grants a company security clearance

or personnel security clearance to a contractor that was awarded a classified contract from the other Party, that security authority may revoke that company security clearance or personnel security clearance in accordance with the national laws and regulations of that Party, and that security authority promptly informs the security authority of the other Party of that revocation;

(b) if a contractor does not have a company security clearance or personnel security clearance that meets the security requirements for a classified contract from the other Party, its security authority, with the consent and request of the company, conducts a security assessment to determine if it should grant or upgrade the company security clearance or personnel security clearance of that contractor and if it should provide a security assurance in accordance with paragraph 2; and

(c) if its security authority cannot promptly provide a security assurance in response to a request from the other Party, that security authority informs the security authority of the other Party of the status of the request.

4. The security authority that receives a request for a security assurance shall respond within five working days unless the Parties jointly determine otherwise.

5. At the request of the Party that conducts a security screening to determine if it should grant a personnel security clearance or company security clearance, the other Party shall assist it with that security screening.

ARTICLE 12

SECURITY ASSESSMENTS AND CONSULTATIONS

1. The Parties may jointly determine to conduct reciprocal visits to evaluate the effectiveness of the security requirements that are implemented under this

Agreement. This includes the security requirements that are implemented with respect to a classified contract.

2. The Parties may organize meetings to discuss their respective national laws, regulations, and procedures relevant to this Agreement to ensure that their application of those laws, regulations, and procedures is consistent.

3. The Parties shall jointly determine the details of meetings and visits referred in paragraphs 1 and 2.

ARTICLE 13

INTERNATIONAL VISITS

A Party shall ensure that:

(a) its security authority or one of its competent authorities approves a visit by an individual who works for the other Party or for a contractor from the other Party to a facility in the territory of its country if the visit is authorized by the security authority or one of the competent authorities of the other Party, if the visitor holds a valid personnel security clearance that meets the security requirements of that visit, and if the visitor has a need-to-know;

(b) if an individual who works for that Party or for a contractor from that Party requests a visit to a contractor's facility at the level of POUFNE / CONFIDENTIAL / CONFIDENTIEL or above in the country of the other Party, the individual submits that request through the security authority of that first Party and complies with the security requirements of the other Party;

(c) a request for a visit includes the visitor's first name and surname, date and place of birth, nationality, passport or identity card number, rank (if applicable), position, and personnel security clearance level, as well as the name of the organisation of the visitor, the purpose of the visit, the proposed date of the visit, the contact persons of the visitor, and the facility to be visited;

(d) its security authority or one of its competent authorities submits a request for a visit to the security authority or one of the competent authorities of the other Party at least 30 working days before the visit, unless the Parties jointly determine otherwise; and

(e) personal data related to visits is protected in accordance with its national laws and regulations.

ARTICLE 14

THIRD PARTY RESTRICTIONS

1. The receiving Party shall not provide or disclose classified information to a third party without the prior written consent of the security authority of the originating Party.
2. The Parties shall ensure that their respective contractors do not provide or disclose classified information to contractors from a third party without the prior written consent of both Parties' security authorities.
3. For the purposes of this Agreement, an individual who holds a personnel security clearance or a contractor who holds a company security clearance issued by either Party is not considered a third party.

ARTICLE 15

LOSS OR COMPROMISE

1. If the receiving Party becomes aware of the possibility that classified information is lost or compromised, it shall immediately inform the originating Party and initiate an investigation. The receiving Party shall forward the result of the investigation to the originating Party and inform the originating Party of the measures taken to prevent a recurrence.
2. The Parties shall cooperate in the investigation referred to in paragraph 1, upon the request of either Party.

ARTICLE 16

COSTS

Each Party shall bear its own costs to implement this Agreement.

ARTICLE 17

IMPLEMENTING ARRANGEMENTS

1. The security authorities of the Parties may conclude implementing arrangements pursuant to this Agreement.
2. The competent authorities of the Parties, in matters within their competence, may conclude implementing arrangements which specify supplementary measures regarding the handling of classified information. These arrangements are subordinate to this Agreement.

ARTICLE 18

OTHER AGREEMENTS OR ARRANGEMENTS

This Agreement does not alter existing agreements or arrangements between the Parties, unless otherwise specified in this Agreement.

ARTICLE 19

DISPUTE SETTLEMENT

The Parties shall resolve a dispute that arises with respect to this Agreement through consultation.

ARTICLE 20

FINAL PROVISIONS

1. The Parties shall notify each other in writing, through diplomatic channels, of the completion of the internal requirements for the entry into force of this Agreement. This Agreement enters into force on the date of the later notification.
2. The Parties may amend this Agreement by joint consent in writing. An amendment enters into force on the date of the later notification that each

Party has completed the internal requirements for entry into force of that amendment.

3. A Party may terminate this Agreement by notice, in writing, to the other Party. This Agreement terminates six months after the date that the notice is received by the other Party.

4. Notwithstanding the termination of this Agreement, all classified information provided or disclosed pursuant to this Agreement shall continue to be protected according to the provisions set forth in this Agreement unless the originating Party informs to do otherwise.

5. The Parties shall jointly review this Agreement at least once every five years to determine if amendments are required.

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

Done in duplicate at WARSAW on this 16TH day of JANUARY 2015 in the Polish, English and French languages, each version being equally authentic.

FOR THE GOVERNMENT OF THE REPUBLIC OF POLAND

FOR THE GOVERNMENT OF CANADA

ACCORD
ENTRE
LE GOUVERNEMENT DE LA RÉPUBLIQUE DE POLOGNE
ET LE GOUVERNEMENT DU CANADA
SUR LA PROTECTION DES INFORMATIONS CLASSIFIÉES

Le Gouvernement de la République de Pologne (la République de Pologne)
et le Gouvernement du Canada (le Canada),
ci-après dénommés les « Parties »,

Souhaitant assurer la protection des informations classifiées fournies ou communiquées par une Partie à l'autre Partie, en particulier dans un contexte de sécurité industrielle et de défense;

Reconnaissant l'importance de leur coopération mutuelle dans les efforts visant à garantir la paix et la sécurité internationale et à assurer une confiance réciproque;

Désirant mettre en place des pratiques et des procédures régissant la protection réciproque des informations classifiées des deux Parties,

Sont convenus de ce qui suit:

ARTICLE PREMIER
DÉFINITIONS

Aux fins du présent accord:

a) « informations classifiées » désigne toutes les informations auxquelles une Partie a attribué un niveau de classification de sécurité et qui requièrent une protection contre la divulgation, l'accès ou la destruction non autorisés dans l'intérêt de la sécurité nationale et conformément aux lois et règlements nationaux de cette Partie. Ces informations peuvent être orales, visuelles, électroniques, magnétiques ou documentaires, ou se présenter sous forme de matériel, d'équipement ou de technologie, et elles comprennent les reproductions, les traductions et le matériel en cours de développement. Toute mention d'informations classifiées dans le présent accord vise également les informations du Canada marquées PROTÉGÉ A/PROTECTED A, PROTÉGÉ B/PROTECTED B ou PROTÉGÉ C/PROTECTED C, sauf indication contraire;

b) « contrat classifié » désigne un instrument juridiquement contraignant en vertu duquel un contractant doit avoir accès à des informations classifiées d'une Partie pour fournir un produit ou un service. Ce terme vise également les contrats de sous-traitance et les activités préalables à l'attribution d'un contrat;

c) « autorités compétentes » désigne les organisations qui sont désignées par chacune des Parties comme autorités responsables, dans les limites de leurs compétences respectives en vertu des lois et règlements nationaux, du traitement des informations classifiées;

d) « compromission » désigne l'accès non autorisé à des informations classifiées, ou la divulgation, la fourniture, la destruction, la suppression, la modification ou l'utilisation non autorisées de ces informations;

e) « contractant » désigne une personne physique ou morale ayant la capacité juridique de conclure un contrat classifié. Ce terme vise également un sous-traitant;

f) « habilitation de sécurité d'installation » s'entend de la décision d'une Partie établissant qu'un contractant satisfait aux exigences de sécurité requises pour traiter des informations classifiées conformément aux lois et règlements nationaux de cette Partie;

g) « besoin d'en connaître » désigne le principe selon lequel l'accès aux informations classifiées est limité aux personnes autorisées à y avoir accès qui ont besoin de connaître ces informations pour s'acquitter de leurs fonctions officielles;

h) « Partie d'origine » désigne la Partie qui fournit des informations classifiées à la Partie destinataire;

i) « habilitation de sécurité du personnel » s'entend de la décision d'une Partie établissant qu'une personne physique peut avoir accès à des informations classifiées conformément aux lois et règlements nationaux de cette Partie;

j) « instructions de sécurité d'un programme/projet » désigne les règlements et procédures en matière de sécurité colligés à partir des lois et règlements nationaux des Parties, qui sont appliqués à un projet ou à un programme particulier afin d'uniformiser les procédures de sécurité, et qui sont approuvés par les deux Parties;

k) « Partie destinataire » désigne la Partie qui reçoit des informations classifiées fournies par la Partie d'origine;

l) « autorité de sécurité » désigne une organisation gouvernementale désignée par une Partie et chargée d'administrer la mise en œuvre du présent accord;

m) « tierce partie » désigne un pays, y compris les personnes physiques et morales ainsi que d'autres types d'organisations relevant de sa juridiction, ou une organisation internationale qui n'est pas partie au présent accord.

ARTICLE 2

OBJECTIF ET PORTÉE

1. Le présent accord vise à assurer la protection des informations classifiées qui sont générées dans le cadre de la coopération entre les Parties ou qui sont échangées entre ces dernières.
2. Le présent accord énonce les normes et les procédures régissant la protection des informations classifiées qui sont fournies ou communiquées, dans un contexte de sécurité industrielle ou de défense, par une Partie à l'autre Partie, ou par une Partie à un contractant de l'autre Partie, ou encore par un contractant d'une Partie à un contractant de l'autre Partie.
3. Le présent accord ne peut être interprété comme obligeant une Partie à fournir ou à communiquer des informations classifiées.

ARTICLE 3

AUTORITÉS DE SÉCURITÉ

1. Les autorités suivantes sont désignées comme autorités de sécurité respectives des Parties:

   a) pour la République de Pologne:
   Chef de l'Agence de sécurité intérieure

   b) pour le Canada:
   Direction de la sécurité industrielle internationale,
   Secteur de la sécurité industrielle,
   Travaux publics et Services gouvernementaux Canada
   (aussi connu sous le nom de Services publics et Approvisionnement Canada)

   ou leurs successeurs respectifs.
2. Les Parties se notifient mutuellement, par écrit, le nom des autorités compétentes au titre du présent accord.

ARTICLE 4

NIVEAUX DE CLASSIFICATION DE SÉCURITÉ

1. La Partie d'origine attribue un niveau de classification de sécurité aux informations classifiées et y appose les marques de classification de sécurité requises en vertu de ses lois et règlements nationaux.
2. La Partie destinataire, conformément à ses lois et règlements nationaux, peut apposer sur les informations classifiées fournies ou communiquées par la Partie d'origine des marques correspondant à un niveau de classification de sécurité qui équivaut, au minimum, au niveau de classification de sécurité attribué par la Partie d'origine, conformément aux tableaux 1 et 2.
3. Le tableau 1 énonce les termes utilisés respectivement par les Parties pour désigner des niveaux de classification de sécurité équivalents applicables aux informations classifiées:

Tableau 1: Informations classifiées

EN RÉPUBLIQUE DE POLOGNE (POLONAIS)	AU CANADA (FRANÇAIS)	AU CANADA (ANGLAIS)
ŚCIŚLE TAJNE	TRÈS SECRET	TOP SECRET
TAJNE	SECRET	SECRET
POUFNE	CONFIDENTIEL	CONFIDENTIAL
ZASTRZEŻONE (VOIR LE PARAGRAPHE 4)	PROTÉGÉ A	PROTECTED A

4. Le Canada peut spécifier des exigences de sécurité supplémentaires dans les clauses contractuelles concernant la protection et le traitement des informations portant la mention PROTÉGÉ A/PROTECTED A afin

de faciliter l'accès des contractants de la République de Pologne auxdites informations.

5. La République de Pologne protège les informations du Canada marquées PROTÉGÉ B/ PROTECTED B ou PROTÉGÉ C/PROTECTED C selon le niveau de classification de sécurité indiqué dans le tableau 2:

Tableau 2: Informations du Canada marquées PROTÉGÉ et PROTECTED

EN RÉPUBLIQUE DE POLOGNE (POLONAIS)	AU CANADA (FRANÇAIS)	AU CANADA (ANGLAIS)
TAJNE	PROTÉGÉ C	PROTECTED C
POUFNE	PROTÉGÉ B	PROTECTED B

ARTICLE 5

PROTECTION ET UTILISATION DES INFORMATIONS CLASSIFIÉES

1. Les Parties protègent et utilisent les informations classifiées comme suit:

   a) la Partie destinataire assure une protection au moins égale à celle qu'elle accorde à ses propres informations d'un niveau de classification de sécurité équivalent;

   b) la Partie destinataire n'utilise les informations classifiées qu'aux fins pour lesquelles celles-ci ont été fournies ou communiquées, sauf avec le consentement préalable écrit de la Partie d'origine, donné par l'entremise des autorités de sécurité ou des autorités compétentes respectives des Parties;

   c) la Partie d'origine peut indiquer, par écrit, que l'utilisation des informations classifiées par la Partie destinataire est soumise à des restrictions, auquel cas la Partie destinataire respecte ces restrictions;

d) la Partie destinataire ne peut abaisser le niveau de classification de sécurité des informations classifiées ou déclassifier les informations classifiées, sauf avec le consentement préalable écrit de la Partie d'origine, donné par l'entremise des autorités de sécurité ou des autorités compétentes respectives des Parties;

e) la Partie d'origine informe la Partie destinataire de toute modification apportée au niveau de classification de sécurité des informations classifiées;

f) la Partie destinataire emploie tous les moyens à sa disposition pour empêcher la perte ou la compromission des informations classifiées fournies par la Partie d'origine.

2. Les Parties peuvent définir conjointement, par écrit, des exigences de sécurité supplémentaires concernant la protection des informations classifiées.

3. Une Partie notifie à l'autre Partie toute modification apportée à ses lois et règlements nationaux qui est susceptible d'avoir une incidence sur la protection des informations classifiées fournies ou communiquées au titre du présent accord.

ARTICLE 6

ACCÈS AUX INFORMATIONS CLASSIFIÉES

1. Les Parties ne peuvent autoriser une personne à avoir accès à des informations classifiées uniquement en raison de son rang, d'une nomination ou d'une habilitation de sécurité du personnel, à moins que la Partie d'origine ne consente à une telle diffusion dans des circonstances exceptionnelles. Les Parties ne peuvent autoriser l'accès aux informations classifiées qu'à une personne qui, à la fois:

a) a le besoin d'en connaître;

b) possède une habilitation de sécurité du personnel du niveau approprié, selon le cas;

c) est informée des exigences des lois et règlements nationaux respectifs des Parties concernant la protection des informations classifiées.

2. Aux fins du présent accord, les autorités de sécurité de chaque Partie reconnaissent les habilitations de sécurité du personnel et les habilitations de sécurité d'installation délivrées conformément aux lois et règlements nationaux de l'autre Partie.

ARTICLE 7

TRANSMISSION DES INFORMATIONS CLASSIFIÉES

1. Les Parties font en sorte que les informations classifiées ne soient transmises que par un service de messagerie autorisé à cette fin, ou par tout autre moyen approuvé conjointement par leurs autorités de sécurité ou autorités compétentes respectives, conformément aux lois et règlements nationaux respectifs des Parties.
2. À la demande de la Partie d'origine, la Partie destinataire accuse réception, par écrit, des informations classifiées.
3. Par l'entremise de leurs autorités de sécurité respectives, les Parties informent le contractant des moyens de transmission et des normes d'emballage qu'elles ont approuvés conjointement pour la transmission des informations classifiées.
4. Si les informations classifiées sont trop volumineuses pour être transmises par un service de messagerie autorisé à cette fin, les Parties, par l'entremise de leurs autorités de sécurité respectives, rédigent conjointement une ébauche de plan de transport décrivant de quelle manière elles entendent procéder à la transmission des informations classifiées. Le plan en question peut notamment préciser le moyen de transport, l'itinéraire et le type d'escorte retenus pour la transmission des informations classifiées.
5. Les Parties font en sorte que les informations classifiées qui se présentent sous forme d'équipement ou qui sont contenues dans un équipement soient

emballées de manière à garantir leur sécurité ou à les protéger pendant la transmission pour éviter que leur contenu ne soit visible, et qu'elles fassent l'objet d'une surveillance continue pour empêcher tout accès non autorisé.

6. Les Parties peuvent autoriser conjointement la transmission des informations classifiées par des moyens électroniques sécurisés, auquel cas elles déterminent conjointement les procédures de sécurité applicables.

ARTICLE 8

TRADUCTION, REPRODUCTION ET DESTRUCTION DES INFORMATIONS CLASSIFIÉES

1. Les Parties font en sorte que les informations classifiées de niveau POUFNE/ CONFIDENTIEL/CONFIDENTIAL ou d'un niveau de classification supérieur ne soient pas traduites ou reproduites sans le consentement écrit de la Partie d'origine, donné par l'entremise de son autorité de sécurité ou de l'une de ses autorités compétentes.
2. Les Parties font en sorte que toute traduction ou reproduction des informations classifiées conserve le niveau de classification de sécurité qui a été attribué aux informations classifiées d'origine, et se voie accorder la même protection.
3. Si la Partie destinataire n'a plus besoin des informations classifiées et que la Partie d'origine autorise leur destruction ou leur renvoi dans le pays d'origine, ou que la Partie d'origine demande leur destruction ou leur renvoi, la Partie destinataire détruit ou renvoie les informations classifiées conformément au niveau de protection qu'elle attribue à ses propres informations classifiées de niveau de classification de sécurité équivalent.
4. Si un contractant achève l'exécution d'un contrat classifié ou qu'il n'a plus besoin de conserver les informations classifiées, la Partie destinataire fait en sorte que les informations classifiées soient renvoyées à la Partie d'origine, à moins que cette dernière ne demande expressément, par écrit, que le contractant détruise les informations classifiées.

ARTICLE 9

CONTRATS CLASSIFIÉS

1. Avant de fournir ou de communiquer des informations classifiées à un contractant, la Partie destinataire fait en sorte que:

   a) le contractant et l'installation de celui-ci satisfassent aux exigences de sécurité requises pour protéger les informations classifiées conformément aux lois et règlements nationaux de la Partie destinataire;

   b) le contractant fasse l'objet d'une habilitation de sécurité d'installation en cours de validité du niveau approprié pour traiter des informations classifiées de niveau POUFNE/CONFIDENTIEL/CONFIDENTIAL ou d'un niveau de classification supérieur;

   c) toute personne physique ayant accès aux informations classifiées ait le besoin d'en connaître et possède une habilitation de sécurité du personnel en cours de validité du niveau approprié;

   d) toute personne physique ayant accès aux informations classifiées soit informée de l'obligation qui lui incombe de protéger les informations classifiées conformément aux lois et règlements nationaux de la Partie destinataire et aux dispositions du présent accord;

   e) l'installation du contractant faisant l'objet d'une habilitation de sécurité d'installation soit inspectée pour vérifier si elle satisfait aux exigences de sécurité requises pour traiter des informations classifiées.

2. Si une installation d'un contractant traite des informations classifiées, la Partie destinataire fait en sorte que le contractant dispose d'un agent de sécurité d'installation qui possède une habilitation de sécurité

du personnel en cours de validité du niveau approprié pour protéger ces informations classifiées.

ARTICLE 10

CLAUSES CONTRACTUELLES RELATIVES À LA SÉCURITÉ

1. Une Partie fait en sorte:

   a) qu'un contrat classifié exigeant l'accès à des informations classifiées soit régi par des clauses de sécurité conformément aux lois et règlements nationaux de cette Partie et aux dispositions du présent accord;

   b) qu'un contrat classifié comporte une description des exigences de sécurité requises pour traiter des informations classifiées. La description des exigences de sécurité précise quelles informations classifiées sont fournies ou communiquées au contractant, ou générées par celui-ci, ainsi que le niveau de classification de sécurité attribué à ces informations classifiées. En ce qui concerne le Canada, les exigences de sécurité sont décrites dans une Liste de vérification des exigences relatives à la sécurité. En ce qui concerne la République de Pologne, les exigences de sécurité sont décrites dans les Instructions en matière de sécurité industrielle;

   c) s'agissant d'un contrat classifié exécuté sur le territoire du pays de l'autre Partie, que l'autorité de sécurité ou l'une des autorités compétentes de la Partie d'origine fournisse à l'autorité de sécurité de l'autre Partie une copie de la description des exigences de sécurité;

   d) que les clauses de sécurité régissant un contrat classifié prévoient au minimum:

      (i) une disposition stipulant que le contractant ne peut fournir ou communiquer les informations classifiées qu'à une

personne qui possède une habilitation de sécurité du personnel, qui a le besoin d'en connaître, et qui a été informée des exigences relatives à la protection des informations classifiées des lois et règlements nationaux de cette Partie;

(ii) les moyens à utiliser pour transmettre les informations classifiées;

(iii) la procédure à suivre pour demander une visite internationale d'une installation industrielle ou gouvernementale située sur le territoire du pays d'une Partie, conformément à l'article 13;

(iv) la procédure à suivre par un contractant pour informer promptement l'autorité de sécurité de la Partie sur le territoire de laquelle il est établi de la perte ou de la compromission possible des informations classifiées;

(v) une disposition stipulant que les informations classifiées fournies ou communiquées au titre d'un contrat classifié ne peuvent être utilisées qu'aux fins de ce contrat;

(vi) la procédure relative à l'élimination définitive des informations classifiées;

(vii) une disposition interdisant au contractant de fournir ou de communiquer des informations classifiées à une tierce partie sans le consentement écrit de l'autorité de sécurité de la Partie d'origine.

2. Si les Parties jugent que l'ampleur ou la complexité du programme ou du projet et les informations classifiées concernées nécessitent l'application d'exigences de sécurité supplémentaires, les autorités de sécurité des Parties élaborent conjointement des instructions de sécurité d'un programme/projet et les annexent au contrat.

ARTICLE 11

GARANTIES DE SÉCURITÉ

1. Une Partie prend, par l'entremise de son autorité de sécurité, les mesures nécessaires pour faire en sorte qu'aucun contrat classifié ne soit attribué à un contractant de l'autre Partie, et que ce dernier ne reçoive aucune information classifiée, tant que l'autorité de sécurité de l'autre Partie n'a pas confirmé que

   le contractant satisfait aux exigences de sécurité requises.

2. À la demande de l'autorité de sécurité de l'autre Partie, une Partie fait en sorte que son autorité de sécurité fournisse, par écrit, une garantie de sécurité qui précise si un contractant possède une habilitation de sécurité du personnel ou une habilitation de sécurité d'installation en cours de validité.

3. Une Partie fait en sorte:

   a) si son autorité de sécurité délivre une habilitation de sécurité d'installation ou une habilitation de sécurité du personnel à un contractant qui s'est vu attribuer un contrat classifié par l'autre Partie, que l'autorité de sécurité en question puisse révoquer cette habilitation de sécurité d'installation ou habilitation de sécurité du personnel conformément aux lois et règlements nationaux de cette Partie, et que l'autorité de sécurité en question informe promptement l'autorité de sécurité de l'autre Partie de cette révocation;

   b) si un contractant ne possède pas d'habilitation de sécurité d'installation ou d'habilitation de sécurité du personnel qui satisfait aux exigences de sécurité applicables à un contrat classifié de l'autre Partie, que son autorité de sécurité, avec le consentement et à la demande de l'entreprise, mène une enquête de sécurité pour décider si elle devrait délivrer une habilitation de sécurité d'installation ou une habilitation de sécurité du personnel à cet contractant, ou relever le niveau de l'habilitation de sécurité d'installation ou de l'habilitation de sécurité du personnel dont il fait l'objet, et si elle

devrait fournir une garantie de sécurité conformément au paragraphe 2;

c) si son autorité de sécurité n'est pas en mesure de fournir promptement la garantie de sécurité demandée par l'autre Partie, que l'autorité de sécurité en question informe l'autorité de sécurité de l'autre Partie de l'état d'avancement de la demande.

4. L'autorité de sécurité qui reçoit une demande de garantie de sécurité y répond dans un délai de cinq jours ouvrables, ou dans tout autre délai déterminé conjointement par les Parties.

5. À la demande de la Partie qui mène une évaluation de sécurité pour décider si elle devrait délivrer une habilitation de sécurité du personnel ou une habilitation de sécurité d'installation, l'autre Partie lui apporte son concours dans le cadre de cette évaluation.

ARTICLE 12

ENQUÊTES DE SÉCURITÉ ET CONSULTATIONS

1. Les Parties peuvent décider conjointement de procéder à des visites réciproques pour évaluer l'efficacité des exigences de sécurité mises en œuvre au titre du présent accord. Celles-ci englobent les exigences de sécurité mises en œuvre en lien avec un contrat classifié.

2. Les Parties peuvent organiser des réunions pour discuter de leurs lois, réglementations et procédures nationales respectives pertinentes au regard du présent accord, afin de faire en sorte que ces lois, réglementations et procédures soient appliquées de manière cohérente.

3. Les Parties déterminent conjointement les modalités des réunions et des visites visées aux paragraphes 1 et 2.

ARTICLE 13

VISITES INTERNATIONALES

Une Partie fait en sorte:

a) que son autorité de sécurité ou l'une de ses autorités compétentes autorise la visite d'une personne qui travaille pour l'autre Partie, ou pour un contractant de l'autre Partie, dans une installation située sur le territoire de son pays, si la visite est autorisée par l'autorité de sécurité ou l'une des autorités compétentes de l'autre Partie, que le visiteur possède une habilitation de sécurité du personnel en cours de validité qui satisfait aux exigences de sécurité applicables à cette visite, et qu'il a le besoin d'en connaître;

b) si une personne travaillant pour cette Partie ou pour un contractant de cette Partie demande à visiter une installation d'un contractant de niveau POUFNE/ CONFIDENTIEL/CONFIDENTIAL ou d'un niveau de classification supérieur située dans le pays de l'autre Partie, que la personne en question présente sa demande par l'entremise de l'autorité de sécurité de la première Partie, et qu'elle se conforme aux exigences de sécurité de l'autre Partie;

c) qu'une demande de visite comporte le prénom et le nom de famille du visiteur, sa date et son lieu de naissance, sa nationalité, son numéro de passeport ou de carte d'identité, son grade (le cas échéant), son poste, le niveau de son habilitation de sécurité du personnel, ainsi que le nom de l'organisation dont il relève, l'objet de sa visite, la date de visite proposée, les personnes-ressources du visiteur et l'installation devant faire l'objet de la visite;

d) que son autorité de sécurité ou l'une de ses autorités compétentes présente une demande de visite à l'autorité de sécurité ou à l'une des autorités compétentes de l'autre Partie au moins 30 jours ouvrables

avant la visite, ou dans tout autre délai déterminé conjointement par les Parties;

e) que les données personnelles relatives aux visites soient protégées conformément à ses lois et règlements nationaux.

ARTICLE 14

RESTRICTIONS APPLICABLES AUX TIERCES PARTIES

1. La Partie destinataire ne peut fournir ou communiquer des informations classifiées à une tierce partie sans le consentement écrit préalable de l'autorité de sécurité de la Partie d'origine.
2. Les Parties font en sorte que leurs contractants respectifs s'abstiennent de fournir ou de communiquer des informations classifiées aux contractants d'une tierce partie sans le consentement écrit préalable des autorités de sécurité des deux Parties.
3. Aux fins du présent accord, une personne qui possède une habilitation de sécurité du personnel ou un contractant qui possède une habilitation de sécurité d'installation délivrée par l'une ou l'autre Partie n'est pas considéré comme une tierce partie.

ARTICLE 15

PERTE OU COMPROMISSION

1. Si la Partie destinataire prend connaissance d'une perte ou d'une compromission possible des informations classifiées, elle en informe immédiatement la Partie d'origine et ouvre une enquête. La Partie destinataire fait part du résultat de l'enquête à la Partie d'origine, et informe cette dernière des mesures prises pour empêcher que la perte ou la compromission ne se reproduise.
2. Les Parties coopèrent à l'enquête mentionnée au paragraphe 1, à demande de l'une ou l'autre Partie.

ARTICLE 16

COÛTS

Chaque Partie supporte les coûts qu'elle a engagés pour la mise en œuvre du présent accord.

ARTICLE 17

ARRANGEMENTS DE MISE EN ŒUVRE

1. Les autorités de sécurité des Parties peuvent conclure des arrangements de mise en œuvre au titre du présent accord.
2. Les autorités compétentes des Parties peuvent, dans les domaines relevant de leur compétence, conclure des arrangements de mise en œuvre spécifiant des mesures complémentaires concernant le traitement des informations classifiées. Ces arrangements sont subordonnés au présent accord.

ARTICLE 18

AUTRES ACCORDS OU ARRANGEMENTS

Le présent accord n'a pas pour effet de modifier des accords ou arrangements existants entre les Parties, sauf disposition contraire du présent accord.

ARTICLE 19

RÈGLEMENT DES DIFFÉRENDS

Les Parties règlent tout différend découlant du présent accord par la voie de consultations.

ARTICLE 20

DISPOSITIONS FINALES

1. Les Parties se notifient par écrit, par la voie diplomatique, l'accomplissement des formalités internes requises pour l'entrée en vigueur du présent accord. Le présent accord entre en vigueur à la date de la dernière de ces notifications.
2. Les Parties peuvent amender le présent accord par consentement mutuel écrit. L'amendement entre en vigueur à la date de la dernière des notifications

échangées entre les Parties pour confirmer l'accomplissement des formalités internes requises pour l'entrée en vigueur dudit amendement.

3. Une Partie peut dénoncer le présent accord par voie de notification écrite adressée à l'autre Partie. Le présent accord prend fin six mois après la date de réception de la notification par l'autre Partie.

4. Nonobstant la dénonciation du présent accord, toutes les informations classifiées fournies ou communiquées au titre du présent accord continuent d'être protégées conformément aux dispositions du présent accord, sauf instruction contraire de la Partie d'origine.

5. Les Parties procèdent à un examen conjoint du présent accord au moins une fois tous les cinq ans pour décider si des amendements s'imposent.

EN FOI DE QUOI, les soussignés, dûment autorisés par leurs gouvernements respectifs, ont signé le présent accord.

FAIT en double exemplaire à VARSOVIE, ce 16TH jour de janvier 2025, en langues polonaise, française et anglaise, chaque version faisant également foi.

POUR LE GOUVERNEMENT DE LA RÉPUBLIQUE DE POLOGNE

POUR LE GOUVERNEMENT DU CANADA

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 8 lipca 2025 roku.

Prezydent Rzeczypospolitej Polskiej: *A. Duda*

L.S.

Prezes Rady Ministrów: *D. Tusk*