SEJM
RZECZYPOSPOLITEJ POLSKIEJ
VIII kadencja
Prezes Rady Ministrów
RM-111-17-19

Druk nr 3391

Warszawa, 12 kwietnia 2019 r.

Pan
Marek Kuchciński
Marszałek Sejmu
Rzeczypospolitej Polskiej

Szanowny Panie Marszałku

Na podstawie art. 89 ust. 2 Konstytucji Rzeczypospolitej Polskiej, uprzejmie zawiadamiam Pana Marszałka, że Rada Ministrów zamierza przedstawić do ratyfikacji Prezydentowi Rzeczypospolitej Polskiej

- **Umowę między Rządem Rzeczypospolitej Polskiej a Rządem Republiki Estońskiej o wzajemnej ochronie informacji niejawnych, podpisaną w Warszawie dnia 27 listopada 2018 r.,**

której ratyfikacja - zdaniem Rady Ministrów - nie wymaga uprzedniej zgody wyrażonej w ustawie.

W załączeniu przekazuję tekst wymienionego dokumentu wraz z uzasadnieniem.

W razie niezgłoszenia, w terminie 30 dni - zgodnie z art. 15 ust. 4 ustawy o umowach międzynarodowych - negatywnej opinii, co do zasadności wyboru trybu ratyfikacji dokumentu, zostanie on przedstawiony Prezydentowi Rzeczypospolitej Polskiej do ratyfikacji.

Z poważaniem

(-) Mateusz Morawiecki

Projekt

W imieniu Rzeczypospolitej Polskiej
PREZYDENT RZECZYPOSPOLITEJ POLSKIEJ
podaje do powszechnej wiadomości:

Dnia 27 listopada 2018 r. w Warszawie została podpisana Umowa między Rządem Rzeczypospolitej Polskiej a Rządem Republiki Estońskiej o wzajemnej ochronie informacji niejawnych.

Po zaznajomieniu się z powyższą Umową, w imieniu Rzeczypospolitej Polskiej oświadczam, że:
– została ona uznana za słuszną zarówno w całości, jak i każde z postanowień w niej zawartych,
– jest przyjęta, ratyfikowana i potwierdzona,
– będzie niezmiennie zachowywana.

Na dowód czego wydany został Akt niniejszy, opatrzony pieczęcią Rzeczypospolitej Polskiej.

Dano w Warszawie dnia

PREZYDENT
RZECZYPOSPOLITEJ POLSKIEJ

Andrzej Duda

PREZES RADY MINISTRÓW

Mateusz Morawiecki

UMOWA

między Rządem Rzeczypospolitej Polskiej

a Rządem Republiki Estońskiej

o wzajemnej ochronie informacji niejawnych

Rząd Rzeczypospolitej Polskiej i Rząd Republiki Estońskiej,

zwane dalej „Stronami",

mając na uwadze konieczność zagwarantowania efektywnej ochrony informacji niejawnych wymienianych między Stronami lub wytwarzanych w wyniku współpracy,

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

z zastrzeżeniem poszanowania obowiązujących norm prawa międzynarodowego i prawa krajowego Stron,

uzgodniły, co następuje:

ARTYKUŁ 1
PRZEDMIOT UMOWY

1. Celem niniejszej Umowy jest zapewnienie ochrony informacjom niejawnym wytwarzanym w wyniku współpracy lub wymienianym między Stronami oraz osobami fizycznymi, osobami prawnymi lub innymi jednostkami organizacyjnymi podlegającymi ich jurysdykcji.
2. Niniejsza Umowa ma zastosowanie do wszelkich kontraktów lub umów dotyczących informacji niejawnych, zawieranych lub realizowanych między Stronami oraz osobami fizycznymi, osobami prawnymi lub innymi jednostkami organizacyjnymi podlegającymi ich jurysdykcji, oraz do wszelkich działań realizowanych między nimi.

ARTYKUŁ 2
DEFINICJE

W rozumieniu niniejszej Umowy następujące definicje oznaczają:

1) **informacje niejawne** – wszelkie informacje niezależnie od formy, nośnika i sposobu ich utrwalenia oraz przedmioty lub dowolne ich części, także będące w trakcie ich opracowywania, które wymagają ochrony przed nieuprawnionym ujawnieniem i zostały oznaczone klauzulą tajności zgodnie z prawem krajowym każdej ze Stron i niniejszą Umową;
2) **krajowa władza bezpieczeństwa** – organ, który zgodnie z prawem krajowym każdej ze Stron jest odpowiedzialny za realizację niniejszej Umowy;
3) **Strona wytwarzająca** – Stronę, jak również osobę fizyczną, osobę prawną lub inną jednostkę organizacyjną podlegającą jej jurysdykcji, która wytworzyła informacje niejawne;
4) **Strona otrzymująca** – Stronę, jak również osobę fizyczną, osobę prawną lub inną jednostkę organizacyjną podlegającą jej jurysdykcji, która otrzymuje informacje niejawne;

5) **kontrakt niejawny** – umowę, która zawiera informacje niejawne lub której realizacja jest związana z dostępem do informacji niejawnych;

6) **kontrahent** – osobę fizyczną, osobę prawną lub inną jednostkę organizacyjną, podlegającą prawu krajowemu jednej ze Stron, uprawnioną – zgodnie z prawem krajowym – do realizowania kontraktów niejawnych;

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

8) **strona trzecia** – organizację międzynarodową lub państwo, w tym również osobę fizyczną, osobę prawną lub inną jednostkę organizacyjną, podlegającą jego jurysdykcji, niebędące Stroną niniejszej Umowy;

9) **poświadczenie bezpieczeństwa** – dokument wydany zgodnie z prawem krajowym jednej ze Stron, który potwierdza, że osoba fizyczna jest uprawniona do dostępu do informacji niejawnych;

10) **świadectwo bezpieczeństwa przemysłowego** – dokument wydany zgodnie z prawem krajowym jednej ze Stron, który potwierdza, że kontrahent posiada zdolność do ochrony informacji niejawnych;

11) **zasada ograniczonego dostępu** – zasadę, zgodnie z którą informacje niejawne udostępniane są tylko tym osobom, których zadania służbowe wymagają zapoznania się z takimi informacjami lub ich posiadania;

12) **naruszenie regulacji dotyczących ochrony informacji niejawnych** – działanie lub zaniechanie sprzeczne z prawem krajowym, mogące prowadzić do nieuprawnionego ujawnienia, utraty, zniszczenia, przywłaszczenia lub jakiegokolwiek innego zagrożenia bezpieczeństwa 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. Klauzule tajności mogą być zmienione lub zniesione wyłącznie przez Stronę wytwarzającą. Strona otrzymująca jest informowana w formie pisemnej o każdym przypadku zmiany lub zniesienia klauzuli otrzymanych uprzednio informacji niejawnych.
3. Strony uzgadniają, że niżej wymienione klauzule tajności są równorzędne:

RZECZPOSPOLITA POLSKA	REPUBLIKA ESTOŃSKA	ODPOWIEDNIK W JĘZYKU ANGIELSKIM
ŚCIŚLE TAJNE	TÄIESTI SALAJANE	TOP SECRET
TAJNE	SALAJANE	SECRET
POUFNE	KONFIDENTSIAALNE	CONFIDENTIAL
ZASTRZEŻONE	PIIRATUD	RESTRICTED

4. Strona otrzymująca oznacza informacje niejawne równorzędną klauzulą tajności, zgodnie z postanowieniami ustępu 3.

ARTYKUŁ 4
KRAJOWE WŁADZE BEZPIECZEŃSTWA

1. Krajowymi władzami bezpieczeństwa Stron są:
    1) w Rzeczypospolitej Polskiej: Szef Agencji Bezpieczeństwa Wewnętrznego;

2) w Republice Estońskiej: Służba Wywiadu Zagranicznego Estonii, Departament Krajowej Władzy Bezpieczeństwa.

2. Strony informują się drogą dyplomatyczną o zmianach krajowych władz bezpieczeństwa, o których mowa w ustępie 1, lub zmianach ich właściwości.

ARTYKUŁ 5
ZASADY OCHRONY INFORMACJI NIEJAWNYCH

1. Strony podejmują wszelkie określone w niniejszej Umowie oraz zgodne ze swoim prawem krajowym działania w celu ochrony informacji niejawnych przekazywanych lub wytwarzanych w wyniku wspólnej działalności Stron, w tym także wytworzonych w związku z realizacją kontraktów niejawnych.
2. Strona otrzymująca wykorzystuje informacje niejawne wyłącznie w celach, dla których zostały one przekazane.
3. Informacje niejawne udostępnia się wyłącznie według zasady ograniczonego dostępu i tylko tym osobom, które zgodnie z prawem krajowym Strony otrzymującej zostały upoważnione do dostępu do informacji niejawnych oznaczonych równorzędną klauzulą tajności.
4. Strona otrzymująca nie udostępnia informacji, o których mowa w ustępie 1, stronie trzeciej bez uprzedniej pisemnej zgody Strony wytwarzającej.

ARTYKUŁ 6
POŚWIADCZENIA BEZPIECZEŃSTWA ORAZ ŚWIADECTWA BEZPIECZEŃSTWA PRZEMYSŁOWEGO

1. W zakresie niniejszej Umowy Strony uznają poświadczenia bezpieczeństwa i świadectwa bezpieczeństwa przemysłowego wydane zgodnie z prawem krajowym drugiej Strony.

2. Krajowe władze bezpieczeństwa Stron współpracują ze sobą podczas przeprowadzania postępowań sprawdzających, na wniosek jednej z nich.
3. W zakresie niniejszej Umowy krajowe władze bezpieczeństwa niezwłocznie informują się o każdej zmianie w odniesieniu do wydanych poświadczeń bezpieczeństwa oraz świadectw bezpieczeństwa przemysłowego, w szczególności o przypadkach ich cofnięcia lub zmiany klauzuli tajności.
4. Na wniosek krajowej władzy bezpieczeństwa Strony wytwarzającej krajowa władza bezpieczeństwa Strony otrzymującej wydaje pisemne potwierdzenie, że osoba fizyczna jest uprawniona do dostępu do informacji niejawnych.

ARTYKUŁ 7
KONTRAKTY NIEJAWNE

1. Przed zawarciem kontraktu niejawnego związanego z dostępem do informacji niejawnych o klauzuli POUFNE / KONFIDENTSIAALNE / CONFIDENTIAL lub wyższej zlecający składa do krajowej władzy bezpieczeństwa swojej Strony wniosek o wystąpienie do krajowej władzy bezpieczeństwa drugiej Strony z prośbą o wydanie zaświadczenia, że kontrahent posiada ważne świadectwo bezpieczeństwa przemysłowego, odpowiednie do klauzuli informacji niejawnych, do których będzie miał dostęp.
2. Informacje niejawne nie są udostępniane kontrahentowi do czasu uzyskania zaświadczenia, o którym mowa w ustępie 1.
3. Zlecający przekazuje kontrahentowi instrukcję bezpieczeństwa przemysłowego niezbędną do realizacji kontraktu niejawnego, która stanowi integralną część każdego kontraktu niejawnego. Instrukcja bezpieczeństwa przemysłowego zawiera postanowienia dotyczące wymogów bezpieczeństwa, w szczególności:

1) wykaz rodzajów informacji niejawnych odnoszących się do danego kontraktu niejawnego, z uwzględnieniem ich klauzul tajności;

2) zasady przyznawania klauzul tajności informacjom wytworzonym podczas realizacji danego kontraktu niejawnego.

4. Zlecający przekazuje kopię instrukcji bezpieczeństwa przemysłowego krajowej władzy bezpieczeństwa swojej Strony, która przesyła ją krajowej władzy bezpieczeństwa Strony kontrahenta.

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 instrukcją bezpieczeństwa przemysłowego.

6. Każdy podwykonawca podlega tym samym obowiązkom ochrony informacji niejawnych, jakie nałożono dla kontrahenta.

ARTYKUŁ 8
PRZEKAZYWANIE INFORMACJI NIEJAWNYCH

1. Informacje niejawne są przekazywane drogą dyplomatyczną.

2. Informacje niejawne mogą być przekazywane za pomocą systemów bezpiecznej łączności, sieci lub innych środków elektromagnetycznych dopuszczonych do użytku zgodnie z prawem krajowym Stron. Krajowe władze bezpieczeństwa poinformują się wzajemnie o zatwierdzonych systemach.

3. Informacje niejawne o klauzuli ZASTRZEŻONE / PIIRATUD / RESTRICTED mogą być przekazywane również za pośrednictwem uprawnionych do tego przewoźników, zgodnie z prawem krajowym Strony wytwarzającej.

4. Krajowe władze bezpieczeństwa Stron mogą ustalić inne sposoby przekazywania informacji niejawnych, zapewniające ochronę przed ich nieuprawnionym ujawnieniem.

5. W razie konieczności organy bezpieczeństwa i porządku publicznego Stron mogą wymieniać informacje niejawne bezpośrednio.
6. Strona otrzymująca potwierdza pisemnie odbiór informacji niejawnych.

ARTYKUŁ 9
POWIELANIE LUB TŁUMACZENIE INFORMACJI NIEJAWNYCH

1. Powielanie lub tłumaczenie informacji niejawnych odbywa się w sposób zgodny z prawem krajowym każdej ze Stron. Powielone lub przetłumaczone informacje podlegają takiej samej ochronie jak oryginały. Liczbę kopii lub tłumaczeń należy ograniczyć do liczby wymaganej dla celów służbowych.
2. Informacje niejawne o klauzuli ŚCIŚLE TAJNE / TÄIESTI SALAJANE / TOP SECRET są powielane lub tłumaczone tylko po uprzednim uzyskaniu pisemnego zezwolenia wydanego przez Stronę wytwarzającą.

ARTYKUŁ 10
NISZCZENIE INFORMACJI NIEJAWNYCH

1. Informacje niejawne są niszczone zgodnie z prawem krajowym Strony otrzymującej w sposób uniemożliwiający ich częściowe lub całkowite odtworzenie.
2. Informacje niejawne o klauzuli ŚCIŚLE TAJNE / TÄIESTI SALAJANE / TOP SECRET nie są niszczone. Są one zwracane Stronie wytwarzającej.
3. W wyjątkowych okolicznościach, jeśli nie jest możliwe zapewnienie ochrony lub zwrócenie informacji niejawnych, o których mowa w ustępie 2, zostaną one niezwłocznie zniszczone. Krajowa władza bezpieczeństwa Strony otrzymującej poinformuje bez zbędnej zwłoki krajową władzę bezpieczeństwa Strony wytwarzającej o ich zniszczeniu.

ARTYKUŁ 11
WIZYTY

1. Wizyty związane z dostępem do informacji niejawnych odbywają się po uprzednim uzyskaniu zezwolenia wydanego przez krajową władzę bezpieczeństwa Strony przyjmującej.
2. Krajowa władza bezpieczeństwa Strony wysyłającej zwraca się do krajowej władzy 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 pilnych przypadkach w krótszym czasie.
3. Wniosek, o którym mowa w ustępie 2, zawiera datę, podpis oraz oficjalną pieczęć krajowej władzy bezpieczeństwa Strony wysyłającej, a także następujące informacje:
   1) cel wizyty oraz informację o najwyższej klauzuli tajności udostępnianych informacji niejawnych;
   2) termin i program wizyty;
   3) imię i nazwisko, datę i miejsce urodzenia, obywatelstwo i numer paszportu lub innego dokumentu tożsamości osoby przybywającej z wizytą;
   4) stanowisko służbowe osoby przybywającej z wizytą wraz z nazwą podmiotu, który reprezentuje;
   5) poziom i datę ważności poświadczenia bezpieczeństwa posiadanego przez osobę przybywającą z wizytą;
   6) nazwę i adres odwiedzanego podmiotu;
   7) imię i nazwisko oraz stanowisko służbowe osoby przyjmującej.
4. Krajowe władze 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 informacje określone w ustępie 3 i są

ważne przez okres dwunastu miesięcy. Po zatwierdzeniu takich wykazów przez krajowe władze bezpieczeństwa Stron terminy wizyt są uzgadniane bezpośrednio między podmiotem wysyłającym a podmiotem przyjmującym wizytę, zgodnie z ustalonymi warunkami.

5. Wizyty związane z dostępem do informacji niejawnych o klauzuli ZASTRZEŻONE / PIIRATUD / RESTRICTED są uzgadniane bezpośrednio między podmiotem wysyłającym a podmiotem przyjmującym wizytę.
6. Strony odpowiadają, zgodnie ze swoim prawem krajowym, za 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 przekazanych przez Stronę wytwarzającą lub informacji niejawnych wytworzonych w wyniku wspólnego działania Stron przekazuje się niezwłocznie krajowej władzy bezpieczeństwa drugiej Strony.
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. Krajowa władza bezpieczeństwa jednej ze Stron pisemnie informuje krajową władzę bezpieczeństwa drugiej Strony o okolicznościach naruszenia oraz o wyniku przeprowadzonych czynności wyjaśniających.
3. Krajowe władze bezpieczeństwa Stron współpracują przy czynnościach, o których mowa w ustępie 2, na wniosek jednej z nich.

ARTYKUŁ 13
JĘZYKI

W zakresie stosowania postanowień niniejszej Umowy Strony używają języka angielskiego lub swoich języków urzędowych. W przypadku użycia języka urzędowego jednej ze Stron dołącza się tłumaczenie na język urzędowy drugiej Strony lub na język angielski.

ARTYKUŁ 14
KOSZTY

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

ARTYKUŁ 15
KONSULTACJE

1. Krajowe władze bezpieczeństwa Stron informują się wzajemnie o wszelkich zmianach w swoim prawie krajowym dotyczącym ochrony informacji niejawnych, w zakresie niezbędnym do wykonywania niniejszej Umowy.
2. W celu zapewnienia ścisłej współpracy przy realizacji postanowień niniejszej Umowy, krajowe władze bezpieczeństwa Stron konsultują się na wniosek jednego z tych organów.
3. W celu zapewnienia skutecznej współpracy wynikającej z postanowień niniejszej Umowy, krajowe władze bezpieczeństwa Stron mogą, w razie potrzeby, zawierać pisemne szczegółowe uzgodnienia techniczne lub organizacyjne w zakresie kompetencji przyznanych im ich prawem krajowym.

ARTYKUŁ 16
ROZSTRZYGANIE SPORÓW

1. Wszelkie sporne kwestie dotyczące stosowania niniejszej Umowy są rozstrzygane w drodze bezpośrednich negocjacji między krajowymi władzami bezpieczeństwa Stron.
2. Jeśli nie jest możliwe rozwiązanie sporu w sposób, o którym mowa w ustępie 1, jest on rozstrzygany drogą dyplomatyczną.

ARTYKUŁ 17
STOSUNEK DO WCZEŚNIEJSZYCH POROZUMIEŃ

Z dniem wejścia w życie niniejszej Umowy traci moc Umowa między Rządem Rzeczypospolitej Polskiej a Rządem Republiki Estońskiej w sprawie wzajemnej ochrony informacji niejawnych, podpisana w Warszawie w dniu 12 maja 2003 roku. Wcześniej wymienione informacje niejawne są chronione zgodnie z postanowieniami niniejszej Umowy.

ARTYKUŁ 18
POSTANOWIENIA KOŃCOWE

1. Niniejsza Umowa podlega przyjęciu zgodnie z prawem krajowym każdej ze Stron, co zostanie stwierdzone w drodze wymiany not. Umowa wejdzie w życie w pierwszym dniu drugiego miesiąca, który nastąpi po dniu otrzymania noty późniejszej.
2. Niniejsza Umowa może zostać zmieniona na podstawie wspólnej pisemnej zgody obu Stron. Takie zmiany wejdą w życie zgodnie z postanowieniami ustępu 1.
3. Niniejsza Umowa zawarta jest na czas nieokreślony. Może być ona wypowiedziana w drodze notyfikacji przez każdą ze Stron. W takim

przypadku utraci moc po upływie sześciu miesięcy po dniu otrzymania noty informującej o wypowiedzeniu.

4. W przypadku wypowiedzenia informacje niejawne przekazane lub wytworzone na podstawie niniejszej Umowy będą nadal chronione zgodnie z jej postanowieniami.

Sporządzono w WARSZAWIE dnia 27 listopada 2018 roku, w dwóch jednobrzmiących egzemplarzach, każdy w językach polskim, estońskim i angielskim, przy czym wszystkie teksty posiadają jednakową moc. W przypadku rozbieżności przy ich interpretacji za rozstrzygający uważa się tekst w języku angielskim.

Z UPOWAŻNIENIA	Z UPOWAŻNIENIA
RZĄDU	RZĄDU
RZECZYPOSPOLITEJ POLSKIEJ	REPUBLIKI ESTOŃSKIEJ

Poola Vabariigi valitsuse ja Eesti Vabariigi valitsuse salastatud teabe kaitse kokkulepe

Poola Vabariigi valitsus ja Eesti Vabariigi valitsus,

edaspidi *pooled*,

pöörates asjakohast tähelepanu poolte vahetatud või koostöö käigus loodud salastatud teabele tõhusa kaitse tagamise vajadusele;

juhindudes kavatsusest kehtestada mõlema poole salastatud teabe kaitse ühtsed eeskirjad;

austades rahvusvahelise õiguse siduvaid norme ja poolte riigisisest õigust,

on kokku leppinud järgmises.

ARTIKKEL 1
KOKKULEPPE KOHALDAMISALA

1. Kokkuleppe eesmärk on tagada poolte või nende jurisdiktsiooni alla kuuluvate füüsiliste või juriidiliste isikute või muude organisatsioonide loodud või vahetatud salastatud teabe kaitse.
2. Kokkulepet kohaldatakse mis tahes lepingu või kokkuleppe suhtes, mis hõlmab salastatud teavet ja mille on sõlminud või mida täidavad pooled või nende jurisdiktsiooni alla kuuluvad füüsilised või juriidilised isikud või muud organisatsioonid, ning eelnimetatute muu tegevuse suhtes.

ARTIKKEL 2
MÕISTED

Kokkuleppes kasutatakse järgmisi mõisteid:

1) ***salastatud teave*** – mis tahes teave, sõltumata selle vormist, teabekandjast ja salvestamise viisist, samuti esemed ja nende osad, ka need, mida alles luuakse, mis on asjakohaselt märgistatud ja mida peab kaitsma omavolilise avalikustamise eest kummagi poole riigisisese õiguse ja kokkuleppe kohaselt;
2) ***riigi julgeoleku volitatud esindaja*** – ametiasutus, mis vastutab kokkuleppe rakendamise eest kummagi poole riigisisese õiguse kohaselt;
3) ***päritolupool*** – pool või tema jurisdiktsiooni alla kuuluv füüsiline või juriidiline isik või muu organisatsioon, mis on loonud salastatud teabe;
4) ***vastuvõttev pool*** – pool või tema jurisdiktsiooni alla kuuluv füüsiline või juriidiline isik või muu organisatsioon, mis võtab salastatud teabe vastu;
5) ***salastatud leping*** – leping, mis sisaldab salastatud teavet või mille täitmine hõlmab juurdepääsu salastatud teabele;
6) ***lepinglane*** – füüsiline või juriidiline isik või muu poole õiguse alusel tegutsev organisatsioon, millel on riigisisese õiguse kohaselt õigus täita salastatud lepinguid;

7) ***vastutav isik*** – füüsiline või juriidiline isik või muu poole õiguse alusel tegutsev organisatsioon, millel on riigisisese õiguse kohaselt õigus algatada salastatud lepinguid;

8) ***kolmas isik*** – mis tahes riik, füüsiline või juriidiline isik või muu riigi jurisdiktsiooni alla kuuluv organisatsioon või rahvusvaheline organisatsioon, mis ei ole käesoleva kokkuleppe pool;

9) ***juurdepääsuluba*** – poole riigisisese õiguse kohaselt tehtud otsus, et füüsilisel isikul lubatud pääseda juurde salastatud teabele;

10) ***töötlemisluba*** – poole riigisisese õiguse kohaselt tehtud otsus, et lepinglane on võimeline salastatud teavet kaitsma;

11) ***teadmisvajadus*** – põhimõte, mille kohaselt võib lubada füüsilisele isikule salastatud teabele juurdepääsu vaid seoses tema teenistuskohustustega ja teatava ülesande täitmiseks;

12) ***salastatud teabe kaitse nõuete rikkumine*** – tegevus või tegevusetus, millega rikutakse riigisisest õigust ja mille tulemusel võib salastatud teave saada avalikuks, kaduda, hävineda, saada seadusevastaselt omastatud või muul viisil rikutud.

ARTIKKEL 3
SALASTATUSE TASEMED

1. Salastatud teabele antakse selle sisule vastav salastatuse tase päritolupoole riigisisese õiguse kohaselt. Lõike 3 järgi tagab vastuvõttev pool saadud salastatud teabele vähemalt samaväärse kaitse taseme.
2. Salastatuse taset võib muuta või salastatust kustutada vaid teabe päritolupool. Vastuvõtvat poolt teavitatakse kirjalikult vastuvõetud teabe salastatuse taseme muudatustest või salastatuse kustutamisest.
3. Pooled lepivad kokku, et järgmised salastatuse tasemed on samaväärsed:

POOLA VABARIIK	EESTI VABARIIK	INGLISKEELNE VASTE
ŚCIŚLE TAJNE	TÄIESTI SALAJANE	TOP SECRET
TAJNE	SALAJANE	SECRET
POUFNE	KONFIDENTSIAALNE	CONFIDENTIAL
ZASTRZEŻONE	PIIRATUD	RESTRICTED

4. Vastuvõttev pool tagab, et salastatud teabele on lisatud lõike 3 kohaselt samaväärse taseme salastusmärge.

ARTIKKEL 4
RIIGI JULGEOLEKU VOLITATUD ESINDAJA

1. Poolte riigi julgeoleku volitatud esindajad on:
   1) Poola Vabariigis: sisejulgeoleku ameti juht;
   2) Eesti Vabariigis: Välisluureamet, riigi julgeoleku volitatud esindaja osakond.
2. Pooled teavitavad teineteist diplomaatiliste kanalite kaudu lõikes 1 nimetatud riigi julgeoleku volitatud esindaja muutumisest või selle pädevuse muudatustest.

ARTIKKEL 5
SALASTATUD TEABE KAITSE PÕHIMÕTTED

1. Pooled rakendavad kõiki kokkuleppes toodud ja riigisiseses õiguses sätestatud meetmeid, et kaitsta salastatud teavet, mida edastatakse või luuakse pooltevahelise koostöö tulemusel, sealhulgas teavet, mis on loodud seoses salastatud lepingute täitmisega.
2. Vastuvõttev pool kasutab salastatud teavet vaid sel eesmärgil, milleks see edastati.

3. Salastatud teabele saavad juurdepääsu vaid need isikud, kellel on teadmisvajadus ning kellel on vastuvõtva poole riigisisese õiguse kohaselt juurdepääsuõigus samaväärse salastatuse tasemega teabele.
4. Vastuvõttev pool ei avalikusta päritolupoole kirjaliku nõusolekuta lõikes 1 nimetatud salastatud teavet mis tahes kolmandale isikule.

ARTIKKEL 6
JUURDEPÄÄSULOAD

1. Kokkuleppe kohaldamisel tunnustavad pooled teise poole riigisisese õiguse kohaselt väljastatud juurdepääsulube ja töötlemislube.
2. Poolte riigi julgeoleku volitatud esindajad abistavad teineteist julgeolekukontrolli tegemises, kui üks neist selleks soovi avaldab.
3. Kokkuleppe kohaldamisel teavitavad riigi julgeoleku volitatud esindajad üksteist viivitamata juurdepääsulubade ja töötlemislubade muudatustest, eriti lubade kehtetuks tunnistamisest või salastatuse taseme muutmisest.
4. Päritolupoole riigi julgeoleku volitatud esindaja taotlusel väljastab vastuvõtva poole riigi julgeoleku esindaja kirjaliku kinnituse selle kohta, et isikul on juurdepääsuõigus salastatud teabele.

ARTIKKEL 7
SALASTATUD LEPINGUD

1. Enne kui sõlmitakse salastatud leping, mis hõlmab juurdepääsu salastatud teabele, mille salastatuse tase on POUFNE / KONFIDENTSIAALNE / CONFIDENTIAL või kõrgem, esitab vastutav isik riigi julgeoleku volitatud esindajale taotluse, et teise poole riigi julgeoleku volitatud esindaja väljastaks tunnistuse, mille kohaselt on lepinglasel kehtiv töötlemisluba, mis vastab selle teabe salastatuse tasemele, millele lepinglane juurdepääsu saab.

2. Lepinglasele ei edastata salastatud teavet enne, kui saadakse lõikes 1 nimetatud tunnistus.
3. Vastutav isik edastab lepinglasele salastatud lepingu täitmiseks vajaliku salastatud teabe töötlemiseeskirja, mis on iga salastatud lepingu osa. Salastatud teabe töötlemiseeskiri käsitleb eelkõige järgmisi julgeolekunõudeid:
   1) salastatud teabe liigid, mis on salastatud lepinguga seotud, sealhulgas teabe salastatuse tasemed;
   2) salastatud lepingu täitmise ajal loodavale teabele salastatuse taseme määramise eeskirjad.
4. Vastutav isik annab ühe salastatud teabe töötlemiseeskirja eksemplari oma poole riigi julgeoleku volitatud esindajale, kes edastab selle lepinglase poole riigi julgeoleku volitatud esindajale.
5. Salastatud lepingu täitmine salastatud teabele juurdepääsu hõlmavas ulatuses on võimalik vaid tingimusel, et lepinglane vastab salastatud teabe töötlemiseeskirja kohaselt salastatud teabe kaitseks vajalikele kriteeriumitele.
6. Kõik all-lepinglased peavad vastama samadele salastatud teabe kaitse tingimustele, mis on kehtestatud lepinglasele.

ARTIKKEL 8
SALASTATUD TEABE EDASTAMINE

1. Salastatud teavet edastatakse diplomaatiliste kanalite kaudu.
2. Salastatud teavet võib edastada kaitstud sidesüsteemide, võrkude või muude riigisisese õiguse kohaselt heakskiidetud elektromagnetiliste vahendite kaudu. Riigi julgeoleku volitatud esindajad teavitavad teineteist, millist süsteemi kasutatakse.
3. Teavet, mille salastatuse tase on ZASTRZEŻONE / PIIRATUD / RESTRICTED, võib edastada ka volitatud postiteenuse osutaja kaudu päritolupoole riigisisese õiguse kohaselt.

4. Poolte riigi julgeoleku volitatud esindajad võivad kokku leppida, et salastatud teabe edastamiseks kasutatakse muid viise, mille puhul on tagatud teabe kaitse omavolilise avalikustamise eest.
5. Vajaduse korral võivad poolte julgeoleku- ja politseiteenistused vahetada salastatud teavet omavahel otse.
6. Vastuvõttev pool kinnitab kirjalikult, et on salastatud teabe kätte saanud.

ARTIKKEL 9
SALASTATUD TEABE PALJUNDAMINE VÕI TÕLKIMINE

1. Salastatud teavet paljundatakse või tõlgitakse kummagi poole riigisisese õiguse kohaselt. Paljundatud või tõlgitud teavet kaitstakse samal viisil nagu algset teavet. Koopiate või tõlgete arv peab piirduma ametlikuks kasutuseks vajalike koopiate või tõlgete arvuga.
2. Teavet, mille salastatuse tase on ŚCIŚLE TAJNE / TÄIESTI SALAJANE / TOP SECRET, võib paljundada või tõlkida vaid siis, kui on saadud päritolupoole eelnev kirjalik nõusolek.

ARTIKKEL 10
SALASTATUD TEABE HÄVITAMINE

1. Salastatud teave hävitatakse vastuvõtva poole riigisisese õiguse kohaselt viisil, mis tagab, et teavet pole võimalik osaliselt ega täielikult taastada.
2. Teavet, mille salastatuse tase on ŚCIŚLE TAJNE / TÄIESTI SALAJANE / TOP SECRET ei hävitata, vaid see tagastatakse päritolupoolele.
3. Erakorralistel asjaoludel, kui pole võimalik lõikes 2 nimetatud salastatud teavet kaitsta või tagastada, hävitatakse see viivitamatult. Vastuvõtva poole riigi julgeoleku volitatud esindaja teavitab hävitamisest esimesel võimalusel päritolupoole riigi julgeoleku volitatud esindajat.

ARTIKKEL 11
KÜLASTUSED

1. Külastustele, millega kaasneb juurdepääs salastatud teabele, peab saama eelneva loa võõrustava poole riigi julgeoleku volitatud esindajalt.
2. Külastava poole riigi julgeoleku volitatud esindaja esitab külastustaotluse võõrustava poole riigi julgeoleku volitatud esindajale vähemalt 30 päeva enne lõikes 1 nimetatud külastust, pakilistel juhtudel aga lühema aja jooksul.
3. Lõikes 2 nimetatud taotluses peavad olema külastava poole riigi julgeoleku volitatud esindaja märgitud kuupäev, allkiri ja ametlik pitser ning alljärgnev teave:
   1) külastuse eesmärk, sealhulgas külastusega seotud salastatud teabe kõrgeim salastatuse tase;
   2) külastuse kuupäev ja kava;
   3) külastaja ees- ja perekonnanimi, tema sünniaeg- ja koht, kodakondsus ja passi või muu isikut tõendava dokumendi number;
   4) külastaja ametinimetus ja selle üksuse nimi, mida ta esindab;
   5) külastaja juurdepääsuloa tase ja kehtivus;
   6) külastatava üksuse nimetus ja aadress;
   7) külastatava isiku ees- ja perekonnanimi ning ametinimetus.
4. Poolte riigi julgeoleku volitatud esindajad võivad kokku leppida, et koostavad nimekirjad isikutest, kellel on lubatud teha korduvaid külastusi seoses konkreetse projekti, programmi või salastatud lepingu rakendamisega. Nimekirjad peavad sisaldama lõikes 3 määratud teavet ja kehtivad 12 kuud. Kui nimekirjad on saanud poolte riigi julgeoleku volitatud esindaja heakskiidu, lepivad külastav ja võõrustav üksus omavahel kokku külastuste kuupäevad.
5. Külastusi, mis hõlmavad juurdepääsu ZASTRZEŻONE / PIIRATUD / RESTRICTED salastatuse tasemega teabele, korraldavad vahetult volitatud külastavad ja võõrustavad üksused.

6. Pooled tagavad oma riigisisese õiguse kohaselt salastatud teavet hõlmavale külastusele saabuvate isikute isikuandmete kaitse.

ARTIKKEL 12
SALASTATUD TEABE KAITSE NÕUETE RIKKUMINE

1. Teave päritolupoole edastatud või poolte koostöös loodud salastatud teabe kaitse nõuete rikkumise või rikkumise kahtluse kohta esitatakse viivitamata teise poole riigi julgeoleku volitatud esindajale.
2. Kõiki salastatud teabe kaitse nõuete rikkumisi või rikkumise kahtlusi uuritakse poole riigisisese õiguse kohaselt selle riigi territooriumil, kus juhtum toimus. Poole riigi julgeoleku volitatud esindaja teavitab teise poole riigi julgeoleku volitatud esindajat kirjalikult rikkumise asjaoludest ja uurimise tulemustest.
3. Poolte riigi julgeoleku volitatud esindajad teevad lõikes 2 nimetatud uurimises koostööd, kui üks neist selleks soovi avaldab.

ARTIKKEL 13
KEELED

Pooled kasutavad kokkuleppe rakendamisel inglise keelt või oma riigikeelt, lisades sel juhul tõlke teise poole riigikeelde või inglise keelde.

ARTIKKEL 14
KULUD

Kokkuleppe rakendamise kulud kannab see pool, kellel need on tekkinud.

ARTIKKEL 15
NÕUPIDAMINE

1. Poolte riigi julgeoleku volitatud esindajad teavitavad teineteist salastatud teabe kaitset käsitlevate riigisiseste õigusaktide muudatustest, mis seostuvad käesoleva kokkuleppe rakendamisega.
2. Poolte riigi julgeoleku volitatud esindajad peavad teineteisega nõu, et tagada tihe koostöö kokkuleppe rakendamisel, kui üks esindajatest selleks soovi avaldab.
3. Selleks, et tagada kokkuleppekohane tõhus koostöö, võivad riigi julgeoleku volitatud esindajad poolte riigisisese õigusega lubatud volituste piires vajaduse korral sõlmida kirjalikke ja üksikasjalikke tehnilisi või korralduslikke kokkuleppeid.

ARTIKKEL 16
VAIDLUSTE LAHENDAMINE

1. Kokkuleppe rakendamisega seotud vaidlused lahendatakse poolte riigi julgeoleku volitatud esindajate läbirääkimistel.
2. Kui vaidlust ei suudeta lahendada lõikes 1 nimetatud viisil, lahendatakse see diplomaatiliste kanalite kaudu.

ARTIKKEL 17
SEOS VARASEMATE KOKKULEPETEGA

Käesoleva kokkuleppe jõustumisel lõpeb 2003. aasta 12. mail Varssavis koostatud Poola Vabariigi valitsuse ja Eesti Vabariigi valitsuse vaheline salastatud teabe kaitse kokkulepe. Varem vahetatud salastatud teavet kaitstakse käesoleva kokkuleppe kohaselt.

ARTIKKEL 18
LÕPPSÄTTED

1. Kokkulepe jõustub pärast seda, kui on lõpetatud kummagi poole riigisisene menetlus, mida kinnitatakse nootide vahetamisega. Kokkulepe jõustub viimase noodi kättesaamisele järgneva teise kuu esimesel päeval.
2. Kokkulepet võib muuta mõlema poole kirjalikul nõusolekul. Muudatused jõustuvad lõike 1 kohaselt.
3. Kokkulepe sõlmitakse määramata ajaks. Pool võib kokkuleppe lõpetada kirjaliku teatega teisele poolele. Sellisel juhul lõpeb kokkulepe kuus kuud pärast lõpetamise teate kättesaamist.
4. Kui kokkulepe lõpetatakse, kaitstakse kokkuleppe põhjal vahetatud või loodud teavet kokkuleppe kohaselt.

Koostatud 27. NOVEMBRIL 2018 (kuupäev) VARSSAVIS (koht) kahes originaaleksemplaris poola, eesti ja inglise keeles; kõik tekstid on võrdselt autentsed. Tõlgendamiserinevuste korral lähtutakse ingliskeelsest tekstist.

POOLA VABARIIGI
VALITSUSE NIMEL

EESTI VABARIIGI
VALITSUSE NIMEL

AGREEMENT

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

The Government of the Republic of Poland

and the Government of the Republic of Estonia,

hereinafter referred to as the "Parties",

Having due regard for the necessity of guaranteeing the effective protection of Classified Information exchanged between the Parties or generated in the course of the cooperation,

Being guided by the intention to adopt uniform regulations for both Parties in the scope of the protection of Classified Information,

Subject to respect binding rules of the international law and the national law of the Parties,

Have agreed as follows:

ARTICLE 1
SCOPE OF THE AGREEMENT

1. The objective of this Agreement is to ensure the protection of Classified Information that is generated by or exchanged between the Parties or individuals, legal entities or other forms of organisations under their jurisdiction.
2. This Agreement shall be applicable to any contract or agreement involving Classified Information concluded or performed between the Parties, individuals, legal entities or other forms of organisations under their jurisdiction as well as to any activity conducted between them.

ARTICLE 2
DEFINITIONS

For the purpose of this Agreement, the following definitions mean:

1) **Classified Information** – any information, irrespective of its form, carrier and manner of recording, as well as objects or any parts thereof, also in the process of being generated, which requires protection against unauthorized disclosure in accordance with the national law of either Party and this Agreement and which has been duly designated as such;
2) **National Security Authority** – the authority which, in accordance with the national law of either Party, is responsible for the implementation of this Agreement;
3) **Originating Party** – the Party or an individual, a legal entity or other form of organisation under its jurisdiction, which has generated the Classified Information;
4) **Recipient Party** – the Party or an individual, a legal entity or other form of organisation under its jurisdiction, which receives the Classified Information;

5) **Classified Contract** – a contract that contains or the performance of which involves access to Classified Information;

6) **Contractor** – an individual, a legal entity or other form of organization under the law of one of the Parties, which in accordance with the national law is entitled to perform Classified Contracts;

7) **Principal** – an individual, a legal entity or other form of organisation under the law of one of the Parties, which in accordance with the national law is entitled to initiate Classified Contracts;

8) **Third Party** – any state or an individual, a legal entity or other form of organisation under the state's jurisdiction or an international organisation that is not a Party to this Agreement;

9) **Personnel Security Clearance** – a determination made in accordance with the national law of one of the Parties that an individual is authorised to access Classified Information;

10) **Facility Security Clearance** – a determination made in accordance with the national law of one of the Parties that a Contractor is capable to protect Classified Information;

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

12) **Breach of Security** – an act or an omission contrary to the national law, the result of which may lead to disclosure, loss, destruction, misappropriation or any other type of compromise of Classified Information.

ARTICLE 3
SECURITY CLASSIFICATION LEVELS

1. Classified Information is granted a security classification level in accordance to its content, pursuant to the national law of the Originating Party. The Recipient Party shall guarantee at least an equivalent level of

protection of the received Classified Information, pursuant to the provisions of paragraph 3.

2. The security classification level may be altered or revoked only by the Originating Party. The Recipient Party shall be notified in writing of every alteration or revocation 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 REPUBLIC OF ESTONIA	EQUIVALENT IN ENGLISH
ŚCIŚLE TAJNE	TÄIESTI SALAJANE	TOP SECRET
TAJNE	SALAJANE	SECRET
POUFNE	KONFIDENTSIAALNE	CONFIDENTIAL
ZASTRZEŻONE	PIIRATUD	RESTRICTED

4. The Recipient Party shall ensure that the Classified Information is marked with an equivalent classification marking in accordance with paragraph 3.

ARTICLE 4
NATIONAL SECURITY AUTHORITIES

1. The National Security Authorities of the Parties are:
   1) for the Republic of Poland: the Head of the Internal Security Agency;
   2) for the Republic of Estonia: Estonian Foreign Intelligence Service, National Security Authority Department.
2. The Parties shall inform each other via diplomatic channels about changes of the National 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 law in order to protect Classified Information transmitted or generated as a result of the cooperation between the Parties, including that generated in connection with the performance of Classified Contracts.
2. The Recipient Party shall use Classified Information exclusively for the purposes for which it has been transmitted.
3. Access to Classified Information shall be granted only to those individuals who have a Need-to-Know and who are authorised in accordance with the national law of the Recipient Party to have access to Classified Information of the equivalent security classification level.
4. The Recipient Party shall not release the Classified Information referred to in paragraph 1 to any Third Party without a prior written consent of the Originating Party.

ARTICLE 6
SECURITY CLEARANCES

1. Within the scope of this Agreement, the Parties shall recognise Personnel Security Clearances and Facility Security Clearances issued in accordance with the national law of the other Party.
2. The National Security Authorities of the Parties shall assist each other upon request of one of them in carrying out vetting procedures.
3. Within the scope of this Agreement, the National Security Authorities shall inform each other without delay about any alteration with regard to Personnel Security Clearances or Facility Security Clearances, in particular about their revocation or an alteration of the security classification level.

4. Upon request of the National Security Authority of the Originating Party, the National Security Authority of the Recipient Party shall issue a written confirmation that an individual has the right to access Classified Information.

ARTICLE 7
CLASSIFIED CONTRACTS

1. Before concluding a Classified Contract involving access to information classified as POUFNE / KONFIDENTSIAALNE / CONFIDENTIAL or above, the Principal shall apply to its National Security Authority to request that the National Security Authority of the other Party issue a 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. Classified Information shall not be released to the Contractor until the receipt of the certificate referred to in paragraph 1.
3. The Principal shall transmit to the Contractor a facility security instruction necessary to perform a Classified Contract, which is an integral part of every Classified Contract. The facility security instruction contains provisions on the security requirements, in particular:
   1) the list of types of Classified Information related to a given Classified Contract, including their security classification levels;
   2) the rules for granting security classification levels to information generated during the performance of a given Classified Contract.
4. The Principal shall put forward a copy of the facility security instruction to the National Security Authority of its Party, which shall transmit it to the National Security Authority of the Contractor's Party.
5. The performance of a Classified Contract in the part involving access to Classified Information shall be possible on condition that

the Contractor meets the criteria necessary for the protection of Classified Information, pursuant to the facility security instruction.

6. Every subcontractor shall comply with the same conditions for the protection of Classified Information as those laid down for the Contractor.

ARTICLE 8
TRANSMISSION OF CLASSIFIED INFORMATION

1. Classified Information shall be transmitted via diplomatic channels.
2. Classified Information may be transmitted through protected communications systems, networks, or other electromagnetic media approved in accordance with the national law of the Parties. The National Security Authorities shall inform each other about the systems to be used.
3. Information classified as ZASTRZEŻONE / PIIRATUD / RESTRICTED may be transmitted also through authorised carriers in accordance with the national law of the Originating Party.
4. The National Security Authorities of the Parties may agree on other forms of transmitting Classified Information which ensure its protection against unauthorized disclosure.
5. If necessary, the security and police services of the Parties may exchange Classified Information directly.
6. The Recipient Party shall confirm in writing the receipt of Classified Information.

ARTICLE 9
REPRODUCTION OR TRANSLATION OF CLASSIFIED INFORMATION

1. Reproduction or translation of Classified Information shall be conducted pursuant to the national law of each of the Parties. Reproduced or translated information shall be placed under the same protection as

the original information. The number of copies or translations shall be reduced to that required for official purposes.

2. Information classified as ŚCIŚLE TAJNE / TÄIESTI SALAJANE / TOP SECRET shall be reproduced or translated only after obtaining a prior written consent issued by the Originating Party.

ARTICLE 10
DESTRUCTION OF CLASSIFIED INFORMATION

1. Classified Information shall be destroyed in accordance with the national law of the Recipient Party in such a manner as to eliminate its partial or total reconstruction.
2. Information classified as ŚCIŚLE TAJNE / TÄIESTI SALAJANE / TOP SECRET shall not be destroyed, it shall be returned to the Originating Party.
3. In case of exceptional circumstances in which it is impossible to protect or return Classified Information referred to in paragraph 2, it shall be destroyed immediately. The National Security Authority of the Recipient Party shall inform the National Security Authority of the Originating Party about this destruction as soon as possible.

ARTICLE 11
VISITS

1. Visits involving access to Classified Information shall be subject to prior permission of the National Security Authority of the host Party.
2. The National Security Authority of the visiting Party shall apply with a request for a visit to the National Security Authority of the host Party at least 30 days prior to the planned visit referred to in paragraph 1, and in urgent cases in shorter time.

3. The request referred to in paragraph 2 shall include the date, signature and official seal of the National Security Authority of the visiting Party as well as the following information:
   1) purpose of the visit, including the highest security classification level of Classified Information involved;
   2) date and program of the visit;
   3) name and surname of the visitor, his date and place of birth, nationality and passport or other official identification document's number;
   4) position of the visitor together with the name of the entity which he represents;
   5) level and the validity date of Personnel Security Clearance held by the visitor;
   6) name and address of the entity to be visited;
   7) name, surname and position of the person to be visited.
4. The National 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 valid for a period of 12 months. Once such lists have been approved by the National 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 / PIIRATUD / RESTRICTED are arranged directly between authorised visiting and hosting entities.
6. The Parties shall ensure, pursuant to their national law, the protection of the personal data of the persons arriving on a visit involving access to Classified Information.

ARTICLE 12
BREACH OF SECURITY

1. Information on every Breach of Security or a suspicion of a Breach of Security concerning Classified Information of the Originating Party or Classified Information generated as a result of cooperation of the Parties shall be immediately reported to the National Security Authority of the other Party.
2. Every Breach of Security or a suspicion of a Breach of Security shall be investigated pursuant to the national law of the Party in the territory of the state of which it has occurred. The National Security Authority of one Party shall inform the National Security Authority of the other Party in writing about the circumstances of the breach and the outcome of the investigation.
3. The National Security Authorities of the Parties shall cooperate in the investigations referred to in paragraph 2, upon the request of one of them.

ARTICLE 13
LANGUAGES

In the scope of the implementation of the provisions of this Agreement, the Parties shall use English or their official languages, in case of which the translation into the official language of the other Party or English shall be attached.

ARTICLE 14
EXPENSES

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

ARTICLE 15
CONSULTATIONS

1. The National Security Authorities of the Parties shall notify each other of any amendments to their national law on the protection of Classified Information concerning the implementation of this Agreement.
2. The National Security Authorities of the Parties shall consult each other, upon the request of one of them, in order to ensure close cooperation in the implementation of the provisions of this Agreement.
3. In order to ensure effective cooperation resulting from the provisions of this Agreement, and in the scope of authority acknowledged by the national law of their Parties, the National Security Authorities may, if necessary, conclude written detailed technical or organisational arrangements.

ARTICLE 16
SETTLEMENT OF DISPUTES

1. Any disputes concerning the implementation of this Agreement shall be settled by direct negotiations between the National Security Authorities of the Parties.
2. If settlement of a dispute cannot be reached in the manner referred to in paragraph 1, such a dispute shall be settled through diplomatic channels.

ARTICLE 17
RELATION TO PREVIOUS AGREEMENTS

Upon entry into force of this Agreement, the *Agreement between the Government of the Republic of Poland and the Government of the Republic of Estonia on Mutual Protection of Classified Information,* done in Warsaw on 12 May 2003, hall terminate. Previously exchanged Classified Information shall be protected in accordance with the provisions of this Agreement.

ARTICLE 18

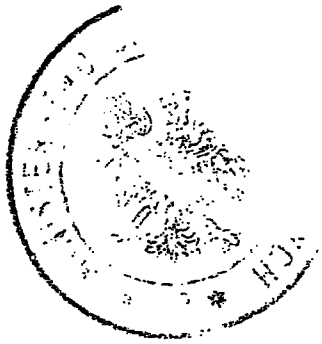
FINAL PROVISIONS

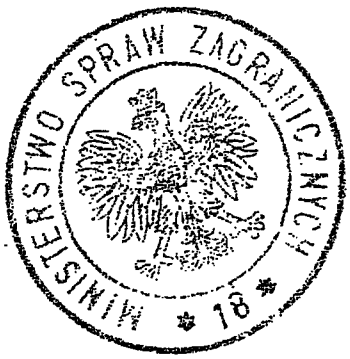
1. This Agreement shall enter into force after the completion of the national procedures of each of the Parties, which shall be confirmed by an exchange of notes. The Agreement shall enter into force on the first day of the second month following the receipt of the latter note.
2. This Agreement may be amended on the basis of mutual written consent of both Parties. Such amendments shall enter into force in accordance with the provisions of paragraph 1.
3. This Agreement is concluded for an unlimited period of time. It may be terminated by either Party by giving written notice to the other Party. In such case, this Agreement shall expire after six months following the receipt of the termination notice.
4. In case of termination, Classified Information exchanged or generated on the basis of this Agreement shall be protected in accordance with the provisions thereof.

Done at WARSAW ..... on 27 NOVEMBER 2018 ..... in two original copies, each in the Polish, Estonian 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 REPUBLIC OF ESTONIA





Stwierdzam zgodność
fotokopii z oryginałem/odpisem

Warszawa, dnia 20.12.2018r..

Piotr Rychlik

Piotr Rychlik
Dyrektor
DEPARTAMENT PRAWNO-TRAKTATOWY

UZASADNIENIE

I. Wyjaśnienie potrzeby i celu związania Rzeczypospolitej Polskiej Umową

Dotychczas obowiązująca *Umowa między Rządem Rzeczypospolitej Polskiej a Rządem Republiki Estońskiej w sprawie wzajemnej ochrony informacji niejawnych* podpisana w Warszawie dnia 12 maja 2003 r. (Dz. U. z 2005 r. poz. 1585) została zawarta ponad piętnaście lat temu. Mając zatem na uwadze rozwijającą się współpracę polityczną i gospodarczą, a przede wszystkim zmiany, jakie zaszły w tym czasie w prawie wewnętrznym Stron, należy wskazać, iż postanowienia obowiązującej Umowy okazują się dziś niewystarczające i nieprzystające do aktualnych potrzeb współpracy w zakresie wzajemnej ochrony informacji niejawnych.

Podpisana w dniu 27 listopada 2018 r. *Umowa między Rządem Rzeczypospolitej Polskiej a Rządem Republiki Estońskiej o wzajemnej ochronie informacji niejawnych* w sposób kompleksowy i wyczerpujący ureguluje kwestie dotyczące wymiany i wzajemnej ochrony informacji niejawnych, a po wejściu w życie, przedmiotowa Umowa będzie stanowić podstawę do nawiązania ściślejszej współpracy politycznej i ekonomicznej, a także współpracy w zakresie obronności i bezpieczeństwa wewnętrznego.

II. Wskazanie różnic między dotychczasowym a projektowanym stanem prawnym

Niniejsza Umowa w znacznym stopniu modyfikuje postanowienia dotychczas obowiązującej *Umowy między Rządem Rzeczypospolitej Polskiej a Rządem Republiki Estońskiej w sprawie wzajemnej ochrony informacji niejawnych*, podpisanej w Warszawie w dniu 12 maja 2003 r., dostosowując ją nie tylko do przepisów odnoszących się do ochrony informacji niejawnych obowiązujących obecnie w prawie wewnętrznym Stron, ale również do aktualnych standardów współpracy bilateralnej.

Artykuł 1 Umowy określa przedmiot i zakres jej stosowania. Kompleksowy charakter Umowy powoduje, iż będzie miała ona zastosowanie do wszelkich działań, kontraktów lub umów dotyczących informacji niejawnych zawieranych między Stronami, osobami fizycznymi, osobami prawnymi lub innymi jednostkami organizacyjnymi pozostającymi pod ich jurysdykcją.

W artykule 2 zdefiniowano kluczowe pojęcia, w tym przede wszystkim termin „informacje niejawne", w celu ujednolicenia pojęć na użytek przedmiotowej Umowy. Kolejne

definicje precyzują m.in. takie terminy, jak „kontrakt niejawny", „strona wytwarzająca" czy „strona otrzymująca".

W artykule 3 zestawiono odpowiadające sobie klauzule tajności celem usystematyzowania ich nazewnictwa oraz uszczegółowiono obowiązek klasyfikowania informacji niejawnych zgodnie z obowiązującym prawem krajowym Stron. W rezultacie zmian, jakie zaszły w estońskim prawie wewnętrznym od czasu wejścia w życie poprzedniej Umowy, aktualizacji poddano estońskie klauzule tajności. Ponadto w tabeli ekwiwalencji umieszczono, oprócz polskich i estońskich klauzul tajności, ich odpowiedniki w języku angielskim.

W artykule 4 wskazano krajowe władze bezpieczeństwa, które są odpowiedzialne za realizację postanowień niniejszej Umowy. Organami tymi są Szef Agencji Bezpieczeństwa Wewnętrznego w Rzeczypospolitej Polskiej oraz Departament Krajowej Władzy Bezpieczeństwa Służby Wywiadu Zagranicznego w Republice Estońskiej.

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

Istotną zmianą w stosunku do obowiązującej Umowy jest treść artykułu 6, zgodnie z którym Strony uznają wzajemnie poświadczenia bezpieczeństwa oraz świadectwa bezpieczeństwa przemysłowego. Krajowe władze bezpieczeństwa zobowiązały się ponadto, iż w razie konieczności udzielą sobie pomocy przy przeprowadzaniu postępowań sprawdzających.

Artykuł 7 reguluje możliwość zawierania kontraktów niejawnych, a więc takich, których realizacja wiąże się z dostępem do informacji niejawnych bądź z wytworzeniem takich informacji. Zgodnie z postanowieniami ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2018 r. poz. 412, z późn. zm.) do posiadania świadectwa bezpieczeństwa przemysłowego zostali zobligowani jedynie przedsiębiorcy ubiegający się o kontrakty związane z dostępem do informacji niejawnych o klauzuli „poufne" lub wyższej.

Artykuł 8 Umowy określa zasady przekazywania informacji niejawnych; kolejne dwa artykuły dotyczą natomiast kwestii, które zostały pominięte w dotychczas obowiązującej Umowie. W artykule 9 i 10 uregulowano kwestie powielania, tłumaczenia oraz niszczenia informacji niejawnych, co pozwoli na ujednolicenie postępowania z informacjami niejawnymi w stosunkach bilateralnych.

W artykule 11 określono zasady i warunki wzajemnych wizyt związanych z dostępem do informacji niejawnych. W stosunku do obowiązującej Umowy znacznie uszczegółowiono zakres danych, które powinien zawierać wniosek o wyrażenie zgody na wizytę. Ponadto zgodnie z międzynarodową praktyką ustalono, iż wizyty związane z dostępem do informacji niejawnych o klauzuli „zastrzeżone" będą uzgadniane bezpośrednio między zainteresowanymi podmiotami, tj. bez pośrednictwa właściwych organów. Wprowadzono również przepis stanowiący, iż Strony zapewnią, zgodnie z prawem wewnętrznym Stron, ochronę danych osobowych osób przybywających z wizytą.

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

W artykule 13 uregulowano kwestię języków, jakimi Strony będą się posługiwały w zakresie stosowania postanowień Umowy.

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

W artykule 15 wprowadzono tryb konsultacji właściwych organów państw Stron w celu współpracy przy realizacji postanowień Umowy.

Ponadto w Umowie przewidziano tryb rozstrzygania sporów (artykuł 16), określono stosunek Umowy do wcześniejszych porozumień regulujących kwestię wzajemnej ochrony informacji niejawnych (artykuł 17) oraz uregulowano procedurę wejścia w życie Umowy, czas jej obowiązywania oraz tryb wypowiedzenia (artykuł 18), które to regulacje stanowią niezbędny element każdej umowy międzynarodowej o takim charakterze.

III. Wskazanie przewidywanych skutków społecznych, gospodarczych, finansowych, politycznych i prawnych, związanych z wejściem w życie Umowy, wraz z określeniem źródeł finansowania

Wejście w życie niniejszej Umowy nie spowoduje znaczących skutków społecznych. Skutkiem o charakterze prawnym będzie określenie jednolitych zasad ochrony informacji niejawnych, wymienianych w ramach szeroko rozumianej współpracy między Rzecząpospolitą Polską a Republiką Estońską. Umowa będzie też stanowić podstawę do nawiązania ściślejszej współpracy w zakresie bezpieczeństwa wewnętrznego oraz w zwalczaniu najgroźniejszych form przestępczości.

Umowa o wzajemnej ochronie informacji niejawnych, poza kompleksowym uregulowaniem kwestii związanych z wymianą, warunkami i środkami ochrony informacji niejawnych, będzie stanowić również podstawę prawną do zawierania pisemnych szczegółowych uzgodnień technicznych lub organizacyjnych.

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

Wejście w życie Umowy nie spowoduje skutków finansowych dla podmiotów sektora finansów publicznych w postaci zmniejszenia ich dochodów lub zwiększenia ich wydatków ani dodatkowych skutków dla budżetu państwa innych, aniżeli przewidziane w ramach właściwej części tego budżetu.

IV. Wyjaśnienie trybu związania Rzeczypospolitej Polskiej Umową

Wejście w życie niniejszej Umowy nie spowoduje konieczności wprowadzenia zmian w ustawodawstwie wewnętrznym, ponieważ jej postanowienia nie odbiegają od obowiązującego w Rzeczypospolitej Polskiej porządku prawnego, a w szczególności rozwiązań przyjętych w ustawie z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych. Umowa ta dotyczy wprawdzie ochrony przekazywanych za granicę i otrzymywanych z zagranicy informacji niejawnych, nie wprowadza jednak żadnych dodatkowych zasad ochrony lub wymiany tych informacji – innych, aniżeli określone w ustawie z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych. Nie zostały zatem spełnione przesłanki wymienione w artykule 89 ustęp 1 Konstytucji Rzeczypospolitej Polskiej (Dz. U. z 1997 r. poz. 483, z późn. zm.), a więc ratyfikacja przedmiotowej Umowy nie wymaga uprzedniej zgody wyrażonej w ustawie.

Umowa niniejsza dotyczy takich podmiotów prawa wewnętrznego Rzeczypospolitej Polskiej, jak osoby fizyczne, osoby prawne oraz jednostki organizacyjne w rozumieniu ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych. W odniesieniu do zakresu, w jakim przedmiotowa Umowa dotyczy osób fizycznych, prawnych oraz jednostek organizacyjnych, należy wskazać na przewidzianą w Umowie możliwość zawierania kontraktów niejawnych związanych z dostępem do informacji niejawnych, w tym występowania w roli zlecającego, kontrahenta oraz podwykonawcy. Ponadto Umowa

przewiduje w odniesieniu do osób fizycznych także możliwość przeprowadzania wizyt na terytorium państwa drugiej Strony związanych z dostępem do informacji niejawnych. Umowa dotyczy spraw uregulowanych w prawie wewnętrznym Rzeczypospolitej Polskiej, objętych przepisami ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych oraz ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. poz. 1000 i 1669) w zakresie regulacji artykułu 11 Umowy.

W Rzeczypospolitej Polskiej związanie przedmiotową Umową powinno nastąpić przez jej ratyfikację w trybie artykułu 89 ustęp 2 Konstytucji Rzeczypospolitej Polskiej, zgodnie z postanowieniami artykułu 12 ustęp 2 ustawy z dnia 14 kwietnia 2000 r. o umowach międzynarodowych (Dz. U. poz. 443, z późn zm.).

Wybór trybu tzw. małej ratyfikacji jest poparty potrzebą uznania przedmiotowej Umowy za źródło powszechnie obowiązującego prawa w Rzeczypospolitej Polskiej, gdyż jej postanowienia będą miały zastosowanie do szerokiego kręgu podmiotów (organy administracji państwowej, przedsiębiorcy). W związku z faktem, iż zgodnie z artykułem 87 Konstytucji Rzeczypospolitej Polskiej źródłem powszechnie obowiązującego prawa w Rzeczypospolitej Polskiej są wyłącznie ratyfikowane umowy międzynarodowe, a nie zaistniały przesłanki ratyfikacji Umowy za uprzednią zgodą wyrażoną w ustawie, związanie Strony polskiej przedmiotową Umową powinno nastąpić w drodze ratyfikacji bez uprzedniej zgody wyrażonej w ustawie.

Zawarcie Umowy jest zgodne z innymi działaniami podejmowanymi przez Rzeczpospolitą Polską na arenie międzynarodowej i nie jest sprzeczne z Umową między Stronami Traktatu Północnoatlantyckiego o ochronie informacji, sporządzoną w Brukseli dnia 6 marca 1997 r. (Dz. U. z 2000 r. poz. 740) ani prawem Unii Europejskiej.

Przedmiotowa Umowa zawiera postanowienia kwalifikujące się do bezpośredniego stosowania, które po dokonaniu ratyfikacji Umowy oraz jej ogłoszeniu w Dzienniku Urzędowym Rzeczypospolitej Polskiej staną się częścią krajowego porządku prawnego.

Z uwagi na ww. przesłanki uzasadniające proponowany tryb związania Rzeczypospolitej Polskiej przedmiotową Umową, zostanie ona ratyfikowana.

Warszawa, 13 lutego 2019 r.

[redacted]

Minister
Spraw Zagranicznych

DPUE.920.1132.2014/bc/9

dot.: P-1228/2019/8304/2014/JS z 25.01.2019 r.

Pan Piotr Pogonowski
Szef Agencji Bezpieczeństwa
Wewnętrznego

Opinia
o zgodności z prawem Unii Europejskiej *Umowy między Rządem Rzeczypospolitej Polskiej a Rządem Republiki Estońskiej o wzajemnej ochronie informacji niejawnych*, wyrażona przez ministra właściwego do spraw członkostwa Rzeczypospolitej Polskiej w Unii Europejskiej

Szanowny Panie Ministrze,

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

Umowa nie jest sprzeczna z prawem Unii Europejskiej.

Z poważaniem

z up. Ministra Spraw Zagranicznych
SEKRETARZ STANU
Konrad Szymański