Poz. 795

UMOWA

między Rządem Rzeczypospolitej Polskiej a Rządem Republiki Serbii o wzajemnej ochronie informacji niejawnych,

podpisana w Warszawie dnia 11 czerwca 2015 r.

W imieniu Rzeczypospolitej Polskiej

PREZYDENT RZECZYPOSPOLITEJ POLSKIEJ

podaje do powszechnej wiadomości:

Dnia 11 czerwca 2015 r. w Warszawie została podpisana Umowa między Rządem Rzeczypospolitej Polskiej a Rządem Republiki Serbii o wzajemnej ochronie informacji niejawnych, w następującym brzmieniu:

UMOWA

między Rządem Rzeczypospolitej Polskiej a Rządem Republiki Serbii o wzajemnej ochronie informacji niejawnych

Rząd Rzeczypospolitej Polskiej i Rząd Republiki Serbii,

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
CEL

Celem niniejszej Umowy jest ustanowienie zasad ochrony informacji niejawnych wymienianych pomiędzy Stronami lub wytworzonych w wyniku współpracy.

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 w trakcie ich opracowywania, które wymagają ochrony przed nieuprawnionym ujawnieniem, zgodnie z prawem krajowym każdej ze Stron i niniejszą Umową;
2) właściwe organy – organy, o których mowa w artykule 4 niniejszej Umowy;
3) upoważnione podmioty – organy administracji państwowej, osoby fizyczne, osoby prawne lub inne jednostki organizacyjne właściwe do wytwarzania, przekazywania, otrzymywania, przechowywania, ochrony i wykorzystywania informacji niejawnych zgodnie z prawem krajowym swojej Strony;
4) kontrakt niejawny – umowę, której realizacja wiąże się z dostępem do informacji niejawnych, bądź z wytworzeniem takich informacji;
5) kontrahent – osobę fizyczną, osobę prawną albo inną jednostkę organizacyjną, podlegającą prawodawstwu jednej ze Stron, która posiada zdolność do zawierania kontraktów niejawnych;
6) zlecający – organ administracji państwowej, osobę fizyczną, osobę prawną albo inną jednostkę organizacyjną, podlegającą prawodawstwu jednej ze Stron, która posiada zdolność do zlecania kontraktów niejawnych;

7) podmiot wytwarzający – Stronę, osobę fizyczną, osobę prawną albo inną jednostkę organizacyjną podlegającą prawodawstwu tej Strony, która wytwarza i przekazuje informacje niejawne podmiotowi otrzymującemu;

8) podmiot otrzymujący – Stronę, osobę fizyczną, osobę prawną albo inną jednostkę organizacyjną podlegającą prawodawstwu tej Strony, która otrzymuje informacje niejawne od podmiotu wytwarzającego;

9) strona trzecia – organizację międzynarodową lub państwo, nie będące Stroną niniejszej umowy, osobę fizyczną albo inny podmiot podlegający prawodawstwu tego państwa.

ARTYKUŁ 3
KLAUZULE TAJNOŚCI

1. Informacjom niejawnym przyznaje się odpowiednią do ich treści klauzulę tajności, zgodnie z prawem krajowym podmiotu wytwarzającego. Podmiot otrzymujący gwarantuje co najmniej równorzędny poziom ochrony otrzymanych informacji niejawnych, zgodnie z postanowieniami ustępu 3.
2. Klauzula tajności może być zmieniona lub zniesiona wyłącznie przez upoważniony podmiot, który ją nadał. Podmiot otrzymujący jest pisemnie informowany o każdym przypadku zmiany lub zniesienia klauzuli tajności wcześniej otrzymanych informacji niejawnych.
3. Strony uzgadniają, że niżej wymienione klauzule tajności są równorzędne:

RZECZPOSPOLITA POLSKA	REPUBLIKA SERBII	ODPOWIEDNIK W JĘZYKU ANGIELSKIM
ŚCIŚLE TAJNE	ДРЖАВНА ТАЈНА	TOP SECRET
TAJNE	СТРОГО ПОВЕРЉИВО	SECRET
POUFNE	ПОВЕРЉИВО	CONFIDENTIAL
ZASTRZEŻONE	ИНТЕРНО	RESTRICTED

ARTYKUŁ 4
WŁAŚCIWE ORGANY

1. W rozumieniu niniejszej Umowy właściwymi organami są:
   1) W Rzeczypospolitej Polskiej: Szef Agencji Bezpieczeństwa Wewnętrznego;
   2) W Republice Serbii: Biuro Rady Bezpieczeństwa Narodowego i Ochrony Informacji Niejawnych.
2. Strony informują się drogą dyplomatyczną o zmianach dotyczących właściwych organów, o których mowa w ustępie 1, lub zmianach ich właściwości.

ARTYKUŁ 5
ZASADY OCHRONY INFORMACJI NIEJAWNYCH

1. Strony podejmują wszelkie działania, zgodne z niniejszą Umową oraz swoim prawem krajowym, w celu ochrony informacji niejawnych przekazywanych lub wytwarzanych w wyniku wspólnej działalności Stron lub upoważnionych podmiotów, w tym także wytworzonych w związku z realizacją kontraktów niejawnych.
2. Podmiot otrzymujący wykorzystuje informacje niejawne wyłącznie w celach, dla których zostały one przekazane.
3. Informacje niejawne mogą być udostępniane tylko tym osobom, których zadania wymagają zapoznania się z nimi i które, zgodnie z prawem krajowym podmiotu otrzymującego, zostały upoważnione do dostępu do nich.
4. Podmiot otrzymujący nie udostępnia informacji, o których mowa w ustępie 1, stronie trzeciej, bez uprzedniej pisemnej zgody podmiotu wytwarzającego.

ARTYKUŁ 6
POŚWIADCZENIA BEZPIECZEŃSTWA ORAZ ŚWIADECTWA BEZPIECZEŃSTWA PRZEMYSŁOWEGO

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

ARTYKUŁ 7
KONTRAKTY NIEJAWNE

1. Przed zawarciem kontraktu niejawnego, związanego z dostępem do informacji niejawnych o klauzuli POUFNE/ПОВЕРЉИВО/ CONFIDENTIAL lub wyższej, zlecający składa wniosek do właściwego organu swojej Strony, o wystąpienie do właściwego organu drugiej Strony, z prośbą o wydanie zaświadczenia, że kontrahent posiada ważne świadectwo bezpieczeństwa przemysłowego odpowiednie do klauzuli informacji niejawnych, do których będzie miał dostęp.
2. Wydanie zaświadczenia, o którym mowa w ustępie 1, jest równoznaczne z gwarancją, że zostały przeprowadzone czynności niezbędne do stwierdzenia, że kontrahent spełnia warunki w zakresie ochrony informacji niejawnych określone w prawie krajowym Strony, na terytorium której posiada siedzibę.
3. Informacje niejawne nie są udostępniane kontrahentowi do czasu uzyskania zaświadczenia, o którym mowa w ustępie 1.
4. 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.

5. Zlecający przekazuje kopię instrukcji bezpieczeństwa przemysłowego właściwemu organowi swojej Strony, który przesyła ją właściwemu organowi Strony kontrahenta.
6. Realizacja kontraktu niejawnego w części związanej z dostępem do informacji niejawnych, będzie możliwa pod warunkiem, że kontrahent spełnia wymogi niezbędne do ochrony informacji niejawnych, zgodnie z instrukcją bezpieczeństwa przemysłowego.
7. Każdy podwykonawca podlega tym samym obowiązkom ochrony informacji niejawnych, jakie nałożono na kontrahenta.

ARTYKUŁ 8
PRZEKAZYWANIE INFORMACJI NIEJAWNYCH

1. Informacje niejawne są przekazywane drogą dyplomatyczną.
2. Informacje niejawne o klauzuli ZASTRZEŻONE/ИНТЕРНО/RESTRICTED oraz POUFNE/ПОВЕРЉИВО/CONFIDENTIAL mogą być przekazywane również za pośrednictwem uprawnionych do tego przewoźników, zgodnie z prawem krajowym Strony przekazującej.
3. W pilnych przypadkach, o ile nie można skorzystać z innej formy przekazania, jeżeli spełnione są wymogi bezpieczeństwa określone prawem krajowym Strony przekazującej, dopuszczalny jest przewóz osobisty informacji niejawnych o klauzuli ZASTRZEŻONE/ИНТЕРНО/ RESTRICTED i POUFNE/ПОВЕРЉИВО/CONFIDENTIAL.
4. Właściwe organy Stron mogą ustalić inne sposoby przekazywania informacji niejawnych zapewniające ochronę przed ich nieuprawnionym ujawnieniem.

5. Podmiot otrzymujący pisemnie potwierdza odbiór informacji niejawnych.

ARTYKUŁ 9
POWIELANIE I TŁUMACZENIE INFORMACJI NIEJAWNYCH

1. Powielanie i tłumaczenie informacji niejawnych odbywa się w sposób zgodny z prawem krajowym każdej ze Stron. Powielone i przetłumaczone informacje podlegają takiej samej ochronie jak oryginały. Liczba kopii i tłumaczeń będzie ograniczona do liczby wymaganej dla celów służbowych.
2. Informacje niejawne o klauzuli ŚCIŚLE TAJNE/ДРЖАВНА ТАЈНА/TOP SCERET są powielane i tłumaczone tylko po uprzednim uzyskaniu pisemnego zezwolenia wydanego przez podmiot wytwarzający.

ARTYKUŁ 10
NISZCZENIE INFORMACJI NIEJAWNYCH

1. Z zastrzeżeniem ustępu 2, informacje niejawne są niszczone zgodnie z prawem krajowym podmiotu otrzymującego w sposób uniemożliwiający ich częściowe lub całkowite odtworzenie.
2. Informacje niejawne o klauzuli ŚCIŚLE TAJNE/ ДРЖАВНА ТАЈНА/ TOP SCERET nie są niszczone; są one zwracane podmiotowi wytwarzającemu.

ARTYKUŁ 11
WIZYTY

1. Z zastrzeżeniem ustępów 5 i 6, osobom przybywającym z wizytą z terytorium jednej Strony na terytorium drugiej Strony, zezwala się na dostęp do informacji niejawnych, tylko po uprzednim uzyskaniu pisemnego zezwolenia wydanego przez właściwy organ drugiej Strony.

2. Co najmniej na trzydzieści dni przed planowaną wizytą, o której mowa w ustępie 1, a w pilnych przypadkach w krótszym czasie, właściwy organ Strony przyjmującej wizytę powinien otrzymać wniosek w sprawie wizyty od właściwego organu drugiej Strony.
3. Wniosek, o którym mowa w ustępie 2, powinien zawierać:
   1) cel, termin i program wizyty;
   2) imię i nazwisko, datę i miejsce urodzenia, obywatelstwo i numer paszportu osoby przybywającej z wizytą;
   3) stanowisko służbowe osoby przybywającej z wizytą wraz z nazwą podmiotu, który reprezentuje;
   4) poziom i datę ważności poświadczenia bezpieczeństwa posiadanego przez osobę przybywającą z wizytą;
   5) nazwę i adres odwiedzanego podmiotu;
   6) imię i nazwisko oraz stanowisko służbowe osoby przyjmującej;
   7) datę, podpis oraz oficjalną pieczęć właściwego organu.
4. W celu ochrony danych osobowych, o których mowa w ustępie 3, przekazywanych w związku z postanowieniami ustępu 1, 5 oraz 6, stosuje się następujące postanowienia, włączając w to prawo krajowe każdej ze Stron:
   1) otrzymane przez Stronę przyjmującą wizytę dane osobowe będą wykorzystane wyłącznie w celu i na warunkach określonych przez Stronę je przekazującą;
   2) Strona przyjmująca wizytę nie przechowuje danych osobowych dłużej, aniżeli jest to niezbędne dla osiągnięcia celu przetwarzania;
   3) w przypadku przekazania danych, których nie wolno było przekazać zgodnie z jej prawem krajowym, Strona przekazująca dane osobowe zawiadamia o tym Stronę przyjmującą wizytę, która jest zobowiązana do usunięcia tych danych w sposób uniemożliwiający ich częściowe lub całkowite odtworzenie;

4) Strona przekazująca dane osobowe odpowiada za ich merytoryczną poprawność i jeśli okaże się, że przekazane zostały dane nieprawdziwe lub niekompletne, zawiadamia o tym Stronę przyjmującą wizytę, która jest zobowiązana do sprostowania lub usunięcia tych danych;

5) Strona przyjmująca wizytę oraz Strona przekazująca dane osobowe są zobowiązane do rejestrowania ich przekazywania, otrzymywania i usuwania;

6) Strona przekazująca dane osobowe oraz Strona przyjmująca wizytę są zobowiązane do skutecznego zabezpieczania przetwarzanych danych przed ich udostępnieniem osobom nieupoważnionym, nieuprawnionym dokonywaniem zmian tych danych, ich utratą, uszkodzeniem lub zniszczeniem.

5. Właściwe organy mogą wyrazić zgodę na ustalenie list osób upoważnionych do składania wielokrotnych wizyt związanych z realizacją konkretnego projektu, programu lub kontraktu niejawnego. Listy te zawierają dane określone w ustępie 3 i są ważne przez okres dwunastu miesięcy. Po zatwierdzeniu takich list przez właściwe organy, terminy wizyt uzgadniane są bezpośrednio między jednostką wysyłającą a jednostką przyjmującą wizytę, zgodnie z ustalonymi warunkami.

6. Wizyty związane z dostępem do informacji niejawnych o klauzuli ZASTRZEŻONE/ ИНТЕРНО/ RESTRICTED są uzgadniane bezpośrednio między jednostką wysyłającą a jednostką przyjmującą wizytę.

ARTYKUŁ 12
NARUSZENIE REGULACJI DOTYCZĄCYCH WZAJEMNEJ OCHRONY INFORMACJI NIEJAWNYCH

1. Naruszeniem regulacji dotyczących wzajemnej ochrony informacji niejawnych jest działanie lub zaniechanie sprzeczne z niniejszą Umową lub

prawem krajowym Stron, dotyczącym ochrony informacji niejawnych, w tym również nieuprawnione ujawnienie informacji niejawnych.

2. Informacja o każdym przypadku naruszenia lub o podejrzeniu naruszenia regulacji dotyczących wzajemnej ochrony informacji niejawnych podmiotu wytwarzającego lub informacji niejawnych wytworzonych w wyniku wspólnego działania Stron, będzie niezwłocznie przekazywana właściwemu organowi Strony, na terytorium której miało miejsce lub zaistniało podejrzenie takiego naruszenia.
3. Każdy przypadek naruszenia lub podejrzenia naruszenia regulacji dotyczących wzajemnej ochrony informacji niejawnych będzie wyjaśniany zgodnie z prawem krajowym Strony, na terytorium której zdarzenie miało miejsce.
4. W przypadku naruszenia regulacji dotyczących wzajemnej ochrony informacji niejawnych, o których mowa w ustępie 1, właściwy organ Strony na terytorium, której naruszenie miało miejsce, pisemnie informuje właściwy organ drugiej Strony o fakcie, okolicznościach naruszenia oraz wyniku czynności, o których mowa w ustępie 3.
5. Właściwe organy Stron współpracują przy czynnościach, o których mowa w ustępie 3, na wniosek jednego z nich.

ARTYKUŁ 13
JĘZYKI

W zakresie stosowania postanowień niniejszej Umowy, Strony używają języka angielskiego lub swoich języków urzędowych, dołączając wówczas 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. Właściwe organy informują się wzajemnie o wszelkich zmianach ich prawa krajowego w zakresie ochrony informacji niejawnych, które dotyczą postanowień niniejszej Umowy.
2. W celu zapewnienia ścisłej współpracy przy realizacji postanowień niniejszej Umowy właściwe organy konsultują się, na wniosek jednego z tych organów.
3. Każda ze Stron zezwoli przedstawicielom właściwego organu drugiej Strony na składanie wizyt na swoim terytorium, w celu omówienia procedur służących ochronie informacji niejawnych, które zostały jej przekazane przez drugą Stronę.
4. W celu zapewnienia skutecznej współpracy, będącej przedmiotem niniejszej Umowy, i w zakresie kompetencji przyznanych im prawem krajowym, właściwe organy mogą, w razie potrzeby, zawierać pisemne szczegółowe uzgodnienia techniczne lub organizacyjne.

ARTYKUŁ 16
ROZSTRZYGANIE SPORÓW

1. Wszelkie sporne kwestie dotyczące stosowania niniejszej Umowy będą rozstrzygane w drodze bezpośrednich konsultacji między właściwymi organami.

2. Jeśli nie jest możliwe rozwiązanie sporu w sposób, o którym mowa w ustępie 1, będzie on rozstrzygany drogą dyplomatyczną.

ARTYKUŁ 17
BEZPOŚREDNIA WYMIANA INFORMACJI NIEJAWNYCH

1. Służby wywiadowcze i kontrwywiadowcze Stron oraz służby właściwe do ochrony bezpieczeństwa i porządku publicznego mogą wymieniać informacje niejawne bezpośrednio.
2. Listę takich służb Strony przekażą drogą dyplomatyczną.

ARTYKUŁ 18
POSTANOWIENIA KOŃCOWE

1. Umowa niniejsza wchodzi w życie zgodnie z prawem krajowym każdej ze Stron, co zostanie stwierdzone w drodze wymiany not. Umowa wejdzie w życie w pierwszym dniu drugiego miesiąca, który nastąpi po dniu otrzymania noty późniejszej.
2. Umowa niniejsza może zostać zmieniona na podstawie wspólnej pisemnej zgody obu Stron. Takie zmiany wejdą w życie zgodnie z postanowieniami ustępu 1.
3. Umowa niniejsza zawarta jest na czas nieokreślony. Może być ona wypowiedziana w drodze notyfikacji przez każdą ze Stron. W takim przypadku utraci moc po upływie sześciu miesięcy od dnia otrzymania noty informującej o wypowiedzeniu.
4. W przypadku wypowiedzenia, Strony zastosują postanowienia artykułu 10 w czasie wskazanym w ustępie 3 powyżej, wobec wszystkich informacji niejawnych przekazanych lub wytworzonych na podstawie niniejszej Umowy.

Sporządzono w WARSZAWIE **dnia** 11 CZERWCA 2015 **roku w dwóch jednobrzmiących egzemplarzach, każdy w językach polskim, serbskim i angielskim, przy czym wszystkie teksty posiadają jednakową moc. W przypadku rozbieżności przy ich interpretacji, tekst w języku angielskim uważany będzie za rozstrzygający.**

Z UPOWAŻNIENIA RZĄDU RZECZYPOSPOLITEJ POLSKIEJ

Z UPOWAŻNIENIA RZĄDU REPUBLIKI SERBII

СПОРАЗУМ

ИЗМЕЂУ

ВЛАДЕ РЕПУБЛИКЕ ПОЉСКЕ

И

ВЛАДЕ РЕПУБЛИКЕ СРБИЈЕ

О УЗАЈАМНОЈ ЗАШТИТИ ТАЈНИХ ПОДАТАКА

Влада Републике Пољске и Влада Републике Србије,
(у даљем тексту: „стране”),

узимајући у обзир потребу за гарантовањем делотворне заштите тајних података који су размењени између страна или су настали у оквиру њихове сарадње,

у намери да усвоје јединствене прописе у области заштите тајних података,

поштујући обавезујућа правила међународног права и националног законодавства страна,

споразумеле су се следеће:

ЧЛАН 1.
ЦИЉ СПОРАЗУМА

Циљ овог споразума је да успостави правила за заштиту тајних података који се размењују између страна или настају у току сарадње.

ЧЛАН 2.
ДЕФИНИЦИЈЕ

Ради примене овог споразума наведени појмови имају следеће значење:

1) **тајни подаци** јесу сви подаци, без обзира на облик, средства за њихово записивање и начин на који су записани, као и сви предмети или њихови делови чија је израда у току и који захтевају заштиту од неовлашћеног откривања, у складу са националним законодавством страна и овим споразумом;

2) **надлежни органи** јесу органи који су наведени у члану 4. овог споразума;

3) **овлашћени органи** јесу органи јавне власти, физичка лица, правна лица или други органи надлежни да стварају, преносе, примају, чувају, штите и користе тајне податке, у складу са националним законодавством сваке стране;

4) **уговор са тајним подацима** јесте уговор чије извршење подразумева остваривање увида у тајне податке или стварање таквих података;

5) **уговарач - извршилац посла** јесте физичко лице, правно лице или други орган у оквиру правног система једне стране који поседују пословну способност да закључују уговоре са тајним подацима;

6) **уговарач - наручилац посла** јесте орган јавне власти, физичко лице, правно лице или други орган у оквиру правног система једне Стране који поседују пословну способност да закључују уговоре са тајним подацима;

7) **давалац** јесте страна, физичко лице, правно лице или други орган у оквиру правног система једне стране која ствара и доставља тајне податке примаоцу;

8) **прималац** јесте страна, физичко лице, правно лице или други орган у оквиру правног система једне од страна која прима тајне податке од даваоца;

9) **трећа страна** јесте међународна организација или држава која није страна у овом споразуму, физичко лице или други орган у оквиру правног система те државе.

ЧЛАН 3.
ОЗНАКЕ СТЕПЕНА ТАЈНОСТИ

1. Тајним подацима се додељују ознаке степена тајности у складу са њиховим садржајем и националним законодавством даваоца. Прималац гарантује да ће тајним подацима које прими обезбедити најмање еквивалентан степен заштите у складу са ставом 3. овог члана.

2. Ознаку степена тајности податка може изменити или скинути једино надлежни орган коју је ту ознаку доделио тајном податку. Прималац ће бити писмено обавештен о свакој промени или скидању ознаке степена тајности са података који је претходно примио.

3. Стране су сагласне да су следеће ознаке степена тајности еквивалентне:

РЕПУБЛИКА ПОЉСКА	РЕПУБЛИКА СРБИЈА	ЕКВИВАЛЕНТ НА ЕНГЛЕСКОМ
ŚCIŚLE TAJNE	ДРЖАВНА ТАЈНА	TOP SECRET
TAJNE	СТРОГО ПОВЕРЉИВО	SECRET
POUFNE	ПОВЕРЉИВО	CONFIDENTIAL
ZASTRZEŻONE	ИНТЕРНО	RESTRICTED

ЧЛАН 4.
НАДЛЕЖНИ ОРГАНИ

1. Надлежни органи за примену овог споразума су:

1) За Републику Пољску: директор Агенције за унутрашњу безбедност

2) За Републику Србију: Канцеларија Савета за националну безбедност и заштиту тајних података,

2. Стране се узајамно обавештавају дипломатским путем о свим променама у вези са надлежним органима наведеним у ставу 1. овог члана или о променама њихове надлежности.

ЧЛАН 5.
ПРИНЦИПИ ЗАШТИТЕ ТАЈНИХ ПОДАТАКА

1. Стране доносе потребне мере ради заштите тајних података који су достављени или створени као резултат сарадње између страна или овлашћених тела, укључујући податке који су настали у вези са извршењем уговора са тајним подацима, у складу са овим споразумом и националним законодавством страна.

2. Прималац ће користити тајне податке искључиво у сврхе у које су достављени.

3. Приступ тајним подацима биће одобрен само оним лицима која поступају у складу с принципом „потребно је да зна" и која су овлашћена да остваре увид у податке, у складу са националним законодавством примаоца.

4. Прималац неће уступити трећој страни податке који се наводе у ставу 1. овог члана, без претходног писаног одобрења даваоца.

ЧЛАН 6.
БЕЗБЕДНОСНИ СЕРТИФИКАТИ

У примени овог споразума, стране ће међусобно признати безбедносне сертификате за физичка лица и безбедносне сертификате за правна лица који су издати у складу са националним законодавством друге стране.

ЧЛАН 7.
УГОВОРИ СА ТАЈНИМ ПОДАЦИМА

1. Пре закључивања уговора са тајним подацима који се односи на остваривање увида у податке са ознаком степена тајности POUFNE/ПОВЕРЉИВО или више, уговарач-наручилац посла подноси захтев свом надлежном органу да од надлежног органа друге стране тражи издавање потврде да уговарач-извршилац посла поседује важећи сертификат за правна лица који одговара степену тајности података у које треба остварити увид.

2. Издавање сертификата из става 1. овог члана једнако је гаранцији да су спроведене потребне радње на основу којих се сматра да уговарач-извршилац испуњава критеријуме из области заштите тајних података који су утврђени националним законодавством стране на чијој територији је његово седиште.

3. Тајни подаци неће бити доступни уговарачу-извршиоцу посла док не добије сертификат који се наводи у ставу 1. овог члана.

4. Уговарач-наручилац посла доставља уговарачу-извршиоцу безбедносно упутство за правно лице које је потребно за извршење уговора са тајним подацима и чини саставни део сваког сваког уговора с тајним подацима. Безбедносно упутство за правно лице садржи одредбе о безбедносним захтевима, и то:

1) попис врста тајних података које се односе на уговор са тајним подацима, при чему се узимају у обзир њихови степени тајности;

2) правила за додељивање ознаке степена тајности подацима који су настали током извршења одређеног уговора са тајним подацима;

5. Уговарач-наручилац посла доставља примерак безбедносног упутства за правно лице свом надлежном органу који ће га проследити надлежном органу уговарача-извршиоца посла.

6. Извршење уговора са тајним подацима у делу који се односи на остваривање увида у тајне податке биће могуће под условом да уговарач-извршилац посла испуни критеријуме за заштиту тајних података, у складу са безбедносним упутством за правно лице.

7. Сваки подуговарач је дужан да испуни исте услове за заштиту тајних података, као и уговарач-извршилац посла.

ЧЛАН 8.

ПРЕНОС ТАЈНИХ ПОДАТАКА

1. Тајни подаци се преносе дипломатским путем.

2. Подаци са ознаком степена тајности ZASTRZEŻONE/ИНТЕРНО и POUFNE/ПОВЕРЉИВО могу се пренети преко овлашћених превозника у складу са националним законодавством стране преносиоца.

3. У хитним случајевима, осим ако није могуће користити друге начине преноса, уколико су испуњени безбедносни захтеви прописани националним законодавством Стране преносиоца, дозвољава се да пренос података степена тајности ZASTRZEŻONE/ИНТЕРНО и POUFNE/ ПОВЕРЉИВО изврши овлашћено лице.

4. Надлежни органи страна могу се договорити око других начина преноса тајних података који обезбеђују заштиту од неовлашћеног откривања.

5. Страна прималац писаним путем потврђује пријем тајних података.

ЧЛАН 9.

УМНОЖАВАЊЕ И ПРЕВОЂЕЊЕ ТАЈНИХ ПОДАТАКА

1. Умножавање и превођење тајних података врши се у складу са националним законодавством сваке стране. Умножени и преведени подаци биће заштићени на исти начин као оригинали. Број умножених примерака и превода треба свести на број који се захтева у службене сврхе.

2. Подаци са ознаком тајности ŚCIŚLE TAJNE/ДРЖАВНА ТАЈНА умножавају се и преводе само уз претходно прибављено одобрење даваоца.

ЧЛАН 10.

УНИШТЕЊЕ ТАЈНИХ ПОДАТАКА

1. Не доводећи у питање став 2. овог члана, тајни подаци се уништавају у складу са националним законодавством примаоца тако да се онемогући њихова делимична или потпуна реконструкција.

2. Подаци са ознаком степена тајности ŚCIŚLE TAJNE/ДРЖАВНА ТАЈНА не уништавају се него се враћају даваоцу.

ЧЛАН 11.

ПОСЕТЕ

1. Не доводећи у питање примену става 5 и 6 овог члана, лицима која долазе у посету са територије државе једне стране на територију државе друге стране, биће одобрен увид у тајне податке само по пријему писменог одобрења надлежног органа друге стране.

2. Надлежни орган стране домаћина прима захтев за посету од надлежног органа друге стране најмање 30 дана пре планиране посете из става 1. овог члана, а у хитним случајевима и у краћем року.

3. Захтев за посету из става 2. овог члана треба да садржи следеће:
1) сврху, датум и програм посете;

2) име и презиме, датум и место рођења, држављанство и број путне исправе посетиоца;

3) функцију посетиоца и назив органа чији је он представник;

4) степен тајности и датум важења безбедносног сертификата за физичка лица који поседује посетилац;

5) назив и адресу органа који се посећује;

6) име и презиме, функцију лица које ће бити посећено;

7) датум, потпис и службени печат надлежног органа.

4. Ради заштите личних података из става 3. овог члана који се достављају у вези са ст. 1, 5. и 6. овог члана, примењиваће се следеће одредбе овог споразума и национално законодавство сваке стране:

1) лични подаци које прими страна домаћин биће коришћени искључиво у сврху и под условима које је дефинисала страна доставилац,

2) страна домаћин чуваће личне податке онолико колико је потребно да се они обраде,

3) у случају да лични подаци буду достављени у супротности са националним законодавством страна, страна доставилац обавестиће о томе страну домаћина која ће бити обавезна да те податке уклони на начин да онемогући њихову делимичну или потпуну реконструкцију,

4) страна доставилац преузима одговорност за тачност личних података које доставља и, у случају да су они неистинити или непотпуни, обавештава о томе страну домаћина која ће бити обавезна да исправи или уклони те податке,

5) страна домаћин и страна доставилац су обавезне да воде евиденцију о достави, пријему и уклањању личних података,

6) страна доставилац и страна домаћин су обавезне да личне податке који су предмет обраде делотворно заштите од откривања неовлашћеним лицима, недозвољених измена, губитка, оштећења или уништења.

5. Надлежни орган може саставити спискове лица овлашћених да реализују периодичне посете у вези са извршењем одређеног пројекта, програма или уговора. Ти спискови садрже податке који су предвиђени у ставу 3. овог члана с роком важења од 12 месеци. Када надлежни органи одобре такве спискове, датуме посета ће договорити непосредно орган који шаље посетиоце и орган који их прима у складу са договореним условима.

6. Орган који шаље посетиоце и орган који их прима ће непосредно организовати посете које се односе на остваривање увида у податке са ознаком степена тајности ZASTRZEŻONE/ИНТЕРНО.

ЧЛАН 12.
ПОВРЕДА ПРОПИСА О БЕЗБЕДНОСТИ У ВЕЗИ СА УЗАЈАМНОМ ЗАШТИТОМ ТАЈНИХ ПОДАТАКА

1. Повреда безбедности тајних података је радња или пропуст у супротности са одредбама овог споразума или националним законодавством страна, укључујући и недозвољено откривање тајних података.

2. О повреди безбедности тајних података даваоца или тајних података насталих као резултат сарадње страна, односно о постојању сумње да је повреда наступила, одмах се извештава надлежни орган стране на чијој територији се догодила повреда безбедности или постоји сумња да је та повреда наступила.

3. Свака повреда безбедности или постојање сумње о наступању повреде биће истражени, у складу са националним законодавством стране на чијој територији се то догодило.

4. У случају повреде безбедности из става 1. овог члана, надлежни орган стране на чијој територији је повреда наступила, обавестиће писаним путем другу страну о тој чињеници, околностима и резултатима радњи из става 3. овог члана.

5. Надлежни органи страна, на захтев једног од њих, дужни су да сарађују у спровођењу радњи које су предвиђене у ставу 3. овог члана.

ЧЛАН 13.

ЈЕЗИЦИ

У примени одредаба овог споразума, стране ће користити енглески језик, односно своје службене језике, с тим што ће обезбедити превод на службени језик друге стране, односно превод на енглески језик.

ЧЛАН 14.

ТРОШКОВИ

Свака страна сноси́ће трошкове који настану у примени одредаба овог споразума.

ЧЛАН 15.

КОНСУЛТАЦИЈЕ

1. Надлежни органи страна обавестиће се узајамно о свим изменама и допунама националног законодавства у вези са заштитом тајних података које утичу на примену одредаба овог споразума.

2. Надлежни органи ће се, на захтев једног од њих, консултовати како би остварили блиску сарадњу у примени одредаба овог споразума.

3. Свака страна омогућиће представницима надлежног органа друге стране да дођу у посету на њену територију, како би се размотриле процедуре за заштиту тајних података које је доставила друга страна.

4. Ради остваривања успешне сарадње у области која је предмет овог споразума, надлежни органи страна могу, у оквиру својих овлашћења утврђених националним законодавством закључити детаљније техничке или организационе споразуме.

ЧЛАН 16.

РЕШАВАЊЕ СПОРОВА

1. Сви спорови у вези са применом овог споразума решаваће се непосредним преговорима између надлежних органа страна.

2. Уколико решење спора не може бити постигнуто на начин наведен у ставу 1. овог члана, спор ће бити решен дипломатским путем.

ЧЛАН 17.

НЕПОСРЕДНА РАЗМЕНА ТАЈНИХ ПОДАТАКА

1. Обавештајне и контраобавештајне службе страна, као и службе које се баве полицијским пословима могу непосредно да размењују тајне податке.

2. Списак тих служби и тела страна биће достављене дипломатским путем.

ЧЛАН 18

ЗАВРШНЕ ОДРЕДБЕ

1. Овај споразум ступа на снагу у складу са националним законодавством сваке Стране, што ће бити потврђено узајамном разменом нота. Споразум ступа на снагу првог дана другог месеца након пријема последње ноте.

2. Овај споразум може бити измењен на основу писмене сагласности обе стране. Такве измене ступају на снагу у складу са одредбама става 1. овог члана.

3. Овај споразум се закључује на неодређено време. Свака страна може отказати овај споразум достављањем писаног обавештења о отказу другој страни. У том случају важење овог споразума истиче након шест месеци од пријема обавештења о отказу.

4. У случају отказа, на све тајне податке који су размењени или настали на основу овог споразума, стране ће применити све одредбе дефинисане у члану 10 у року наведеном у ставу 3. овог члана.

Сачињено у ВАШИНГТОНУ **дана** 11 ЈУНА 2015 г. **у два оригинална примерка, сваки на пољском, српском и енглеском језику, при чему су сви текстови подједнако веродостојни. У случају неслагања у тумачењу, биће меродаван текст Споразума на енглеском језику.**

ЗА ВЛАДУ
РЕПУБЛИКЕ ПОЉСКЕ

ЗА ВЛАДУ
РЕПУБЛИКЕ СРБИЈЕ

AGREEMENT

between the Government of the Republic of Poland and the Government of the Republic of Serbia on the mutual protection of classified information

The Government of the Republic of Poland and the Government of the Republic of Serbia

hereinafter referred to as the "Parties",

having due regard for necessity of guaranteeing the effective protection of classified information which has been exchanged between the Parties or originated during the cooperation course,

being guided by the adoption of uniform regulations for both Parties in the scope of the protection of classified information,

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

have agreed as follows:

ARTICLE 1
OBJECTIVE

The objective of this Agreement is to establish the rules for the protection of classified information exchanged between the Parties or originated in the course of cooperation.

ARTICLE 2
DEFINITIONS

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

1) classified information – any information, irrespective of the form, carrier and manner of recording thereof, as well as objects or any parts of thereof, also in the process of being generated, which requires protection against unauthorized disclosure in accordance with the national law of each of the Parties and this Agreement;
2) competent authorities – authorities referred to in Article 4 of this Agreement;
3) authorized bodies – public authorities, individuals, legal entities or other organizational units, competent to originate, transmit, receive, store, protect and use classified information in accordance with the national law of their Party;
4) classified contract - a contract, performance of which involves access to classified information or originating of such information;
5) contractor – an individual, a legal entity or other organizational unit coming under the law of one of the Party, which has legal capacity to conclude classified contracts;
6) principal – public authority, an individual, a legal entity or other organizational unit coming under the law of one of the Party, which has legal capacity to let classified contracts;

7) originating body – the Party, an individual, a legal entity or other organizational unit coming under the law of this Party, which originates and transmits classified information to the recipient body;

8) recipient body – the Party, an individual, a legal entity or other organizational unit coming under the law of this Party, which receives classified information from the originating body;

9) third party – an international organization or a State not being a Party of this Agreement, an individual or other entity coming under the law of the State.

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 body. The recipient body shall guarantee at least an equivalent level of protection of the received classified information, according to the provisions of Paragraph 3.

2 The security classification level may be changed or removed only by the authorized body, which has granted it. The recipient body shall be notified in writing of every change or removal of the security classification level of previously received classified information.

3 The Parties agree that the following security classification levels are equivalent:

REPUBLIC OF POLAND	REPUBLIC OF SERBIA	EQUIVALENT IN ENGLISH
ŚCIŚLE TAJNE	ДРЖАВНА ТАЈНА	TOP SECRET
TAJNE	СТРОГО ПОВЕРЉИВО	SECRET
POUFNE	ПОВЕРЉИВО	CONFIDENTIAL
ZASTRZEŻONE	ИНТЕРНО	RESTRICTED

ARTICLE 4
COMPETENT AUTHORITIES

1. For the purpose of this Agreement, the competent authorities shall be:
   1) for the Republic of Poland: the Head of the Internal Security Agency;
   2) for the Republic of Serbia: the Office of the Council on National Security and Classified Information Protection.
2. The Parties shall inform each other via diplomatic channels about amendments regarding competent authorities, referring to in Paragraph 1, or about amendments to their competences.

ARTICLE 5
PRINCIPLES OF CLASSIFIED INFORMATION PROTECTION

1. In accordance with this Agreement and their national law, the Parties shall adopt every measures aimed at the protection of classified information which has been transmitted or originated as a result of the mutual cooperation of the Parties or authorized bodies, including this originated in connection with performance of classified contracts.
2. The recipient body shall use classified information exclusively for the purposes it was transmitted.
3. Access to classified information shall be granted only to those individuals who have a need-to-know and who have been authorized to access to such information according to the national law of the recipient body.
4. The recipient body shall not release the information, referred to in Paragraph 1, to the third party without a prior written consent of the originating body.

ARTICLE 6
SECURITY CLEARANCES

In the scope of this Agreement, the Parties shall recognize Personnel Security Clearances and Facility Security Clearances issued in accordance with the national law of the other Party.

ARTICLE 7
CLASSIFIED CONTRACTS

1. Before concluding a classified contract, connected to access to information classified as POUFNE/ ПОВЕРЉИВО/CONFIDENTIAL or above, the principal shall apply to its competent authority to request the competent authority of the other Party to 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 having access to.
2. Issuing the certificate, referred to in Paragraph 1, shall be tantamount to a guarantee that the necessary actions have been conducted to declare that the contractor fulfills the criteria in the scope of the protection of classified information, defined in the national law of the Party, in whose territory it is located.
3. Classified information shall not be accessible to the contractor until the receipt of the certificate referred to in Paragraph 1.
4. The principal shall transmit to the contractor a facility security instruction necessary to perform the 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, taking into consideration their security classification levels;
   2) the rules for granting security classification levels to information originated during the performance of a given classified contract.

5. The principal shall put forward a copy of the facility security instruction to its competent authority, which shall transmit it to the competent authority of the contractor.
6. The performance of the classified contract in the part connected with access to classified information shall be possible on condition that the contractor fulfills the criteria necessary for the protection of Classified Information, according to the facility security instruction.
7. Every subcontractor shall comply with the same conditions for the protection of classified information as those laid down for the contractor.

ARTICLE 8
TRANSMISSION OF CLASSIFIED INFORMATION

1. Classified information shall be transmitted via diplomatic channels.
2. Information classified as ZASTRZEŻONE/ИНТЕРНО/RESTRICTED and POUFNE/ПОВЕРЉИВО/CONFIDENTIAL may be transmitted also through the authorized carriers, according to the national law of the transmitting Party.
3. In urgent cases, unless it is possible to use other forms of transmitting, if the security requirements defined by the national law of the transmitting Party are met, the personal carriage of information classified as ZASTRZEŻONE/ ИНТЕРНО/RESTRICTED and POUFNE/ПОВЕРЉИВО/CONFIDENTIAL is admissible.
4. The competent authorities of the Parties may agree on the other forms of transmitting classified information ensuring its protection against unauthorized disclosure.
5. The recipient body shall confirm in writing the receipt of classified information.

ARTICLE 9
REPRODUCTION AND TRANSLATION OF CLASSIFIED INFORMATION

1. Reproduction and translation of classified information shall be pursuant to the national law of each of the Parties. Reproduced and translated information shall be placed under the same protection as the originals. Number of copies and translations shall be reduced to that required for official purposes.
2. Information classified as ŚCIŚLE TAJNE/ДРЖАВНА ТАЈНА/TOP SECRET shall be reproduced and translated only after obtaining a prior written consent issued by the originating body.

ARTICLE 10
DESTRUCTION OF CLASSIFIED INFORMATION

1. Without prejudice to Paragraph 2, classified information shall be destroyed according to the national law of the recipient body, in such a manner as to eliminate its partial or total reconstruction.
2. Information classified as ŚCIŚLE TAJNE/ДРЖАВНА ТАЈНА/TOP SECRET shall not be destroyed, it shall be returned to the originating body.

ARTICLE 11
VISITS

1. Without prejudice to Paragraphs 5 and 6, persons arriving on a visit from the territory of one of the Party to the territory of the other Party shall be allowed access to classified information only after receiving a prior written consent issued by the competent authority of the other Party.
2. At least 30 days prior to the planned visit, referred to in Paragraph 1, and in urgent cases in shorter time, the competent authority of the hosting Party shall receive a request for a visit from the competent authority of the other Party.

3 Request for a visit, referred to in Paragraph 2 shall include:

1) purpose, date and program of the visit;

2) name and surname, date and place of birth, nationality and passport number of the visitor;

3) position of the visitor together with the name of the entity which he or she represents;

4) level and the date of validity of Personnel Security Clearance held by the visitor;

5) name and address of the entity to be visited;

6) name, surname and position of the individual to be visited;

7) the date, signature and the official seal of the competent authority.

4. In order to protect personal data, referred to in Paragraph 3, transmitted in connection with the provisions of Paragraphs 1, 5 and 6, the following provisions shall apply, including the national law of each of the Party:

1) personal data received by the hosting Party shall be used exclusively for the purpose and on conditions defined by the Party transmitting it;

2) personal data shall be stored by the hosting Party no longer than it is necessary for the purpose of its processing;

3) in case of personal data transmitted against the national law of the Party, the Party transmitting it, shall notify the hosting Party, which is obliged to remove the data, in such a manner as to eliminate its partial or total reconstruction;

4) the Party transmitting personal data shall take the responsibility for its correctness and, in a case the data appears to be untrue or incomplete, shall inform the hosting Party, which is obliged to correct or remove the data;

5) the hosting Party and the Party transmitting personal data are obliged to register transmission, receiving and removing it;

6) the Party transmitting personal data and the hosting Party are obliged to protect processing personal data efficiently against its disclosure to unauthorized persons, unauthorized modifications of the data, its loss, damage or destruction.

5. The competent authority may agree to establish lists of authorized persons to make recurring visits connected to realization of specific project, program or classified contract. Those lists shall contain the data defined in Paragraph 3 and are valid for a period of 12 months. Once such lists have been approved by the competent authorities, the dates of the visits shall be arranged directly between the sending entity and the hosting entity, in accordance with the conditions agreed upon.

6. Visits connected to access to information classified as ZASTRZEŻONE/ИНТЕРНО/RESTRICTED are arranged directly between the sending entity and the hosting entity.

ARTICLE 12
BREACH OF SECURITY REGULATIONS CONCERNING MUTUAL PROTECTION OF CLASSIFIED INFORMATION

1. Breach of security is an action or an omission which is contrary to this Agreement or the national law of the Parties, including also unauthorized disclosure of classified information.

2. Information regarding every breach of security or a suspicion of the breach of security concerning classified information of the originating body or classified information originated as a result of mutual cooperation of the Parties shall be immediately reported to the competent authority of the Party in whose territory the breach or suspicion of the breach has occurred.

3. Every breach of security or a suspicion of a breach of security shall be investigated pursuant to the national law of the Party in whose territory it has occurred.

4. In case of a breach of security, referred to in Paragraph 1, the competent authority of the Party in whose territory the breach has occurred shall inform the competent authority of the other Party in writing about the fact, circumstances and the outcome of the actions referred to in Paragraph 3.
5. The competent authorities of the Parties shall cooperate in the actions referred to in Paragraph 3, upon the request of one of them.

ARTICLE 13
LANGUAGES

In the scope of the implementation of the provisions of this Agreement, the Parties shall use the English language or their official languages, attaching then the translation into the official language of the other Party or into English.

ARTICLE 14
EXPENSES

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

ARTICLE 15
CONSULTATIONS

1. The competent authorities shall notify each other of any amendments to its national law concerning the protection of classified information that affect the provisions of this Agreement.
2. The competent authorities shall consult each other, upon the request of one of them, in order to ensure a close cooperation in the implementation of the provisions of this Agreement.

3. Each Party shall allow the representatives of the competent authority of the other Party to pay visits to its own territory to discuss the procedures for protection of classified information transmitted by the other Party.

4. In order to ensure the effective cooperation being the subject matter of this Agreement and in the scope of authority acknowledged by their national law, the competent authorities may, if necessary, conclude written detailed technical or organizational arrangements.

ARTICLE 16
SETTLEMENT OF DISPUTES

1. Any disputes concerning the application of this Agreement shall be settled by direct negotiations between the competent authorities of the Parties.
2. If the 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
DIRECT EXCHANGE OF CLASSIFIED INFORMATION

1. The intelligence and counter – intelligence services of the Parties as well as the services competent to protect public safety and order may exchange classified information directly.
2. The list of such services and bodies of the Parties shall transmit via diplomatic channels.

ARTICLE 18
FINAL PROVISIONS

1. This Agreement shall enter into force in accordance with the national law of each of the Parties, what shall be confirmed by exchange of the 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 by 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 a case, this Agreement shall expire after six months following the receipt of the termination notice.
4. In case of termination, the Parties shall apply all regulations defined in Article 10 in time indicated in Paragraph 3 above, to any classified information exchanged or originated on the basis of this Agreement.

Done at.....WARSAW.....on.....11 JUNE 2015.....in two original copies, each in the Polish, Serbian and English languages, all texts being equally authentic. In case of divergences of interpretation, the English text shall prevail.

ON BEHALF OF
THE GOVERNMENT OF
THE REPUBLIC OF POLAND

ON BEHALF OF
THE GOVERNMENT OF
THE REPUBLIC OF SERBIA

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 12 marca 2016 r.

Prezydent Rzeczypospolitej Polskiej: *A. Duda*

L.S.

Prezes Rady Ministrów: *B. Szydło*