Warszawa, dnia 30 września 2016 r.

Poz. 1587

UMOWA

między Rządem Rzeczypospolitej Polskiej a Rządem Gruzji o wymianie i wzajemnej ochronie informacji niejawnych,

podpisana w Tbilisi dnia 8 października 2015 r.

W imieniu Rzeczypospolitej Polskiej

PREZYDENT RZECZYPOSPOLITEJ POLSKIEJ

podaje do powszechnej wiadomości:

Dnia 8 października 2015 r. w Tbilisi została podpisana Umowa między Rządem Rzeczypospolitej Polskiej a Rządem Gruzji o wymianie i wzajemnej ochronie informacji niejawnych, w następującym brzmieniu:

UMOWA

między Rządem Rzeczypospolitej Polskiej a Rządem Gruzji o wymianie i wzajemnej ochronie informacji niejawnych

Rząd Rzeczypospolitej Polskiej i Rząd Gruzji,

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 państw Stron,

uzgodniły, co następuje:

ARTYKUŁ 1
DEFINICJE

Dla celów niniejszej Umowy następujące definicje oznaczają:

a) **informacje niejawne** – wszelkie informacje, niezależnie od formy, nośnika i sposobu ich utrwalenia, oraz przedmioty lub dowolne ich części, będące także w trakcie ich opracowywania, które wymagają ochrony przed nieuprawnionym ujawnieniem zgodnie z prawem krajowym państwa Strony i niniejszą Umową;

b) **właściwy organ** – organ, o którym mowa w artykule 3 niniejszej Umowy;

c) **upoważniony podmiot** – osobę fizyczną, osobę prawną lub inną jednostkę organizacyjną właściwą do przetwarzania informacji niejawnych zgodnie z prawem krajowym państwa odpowiedniej Strony;

d) **kontrakt niejawny** – umowę, której realizacja wiąże się z dostępem do informacji niejawnych lub z wytworzeniem takich informacji;

e) **kontrahent** – osobę prawną albo inną jednostkę organizacyjną podlegającą prawodawstwu państwa jednej ze Stron, która posiada zdolność do zawierania kontraktów niejawnych;

f) **strona trzecia** – organizację międzynarodową lub państwo, niebędące Stroną niniejszej umowy, osobę fizyczną albo inny podmiot.

ARTYKUŁ 2
KLAUZULE TAJNOŚCI

1. Informacjom niejawnym przyznaje się odpowiednią do ich treści klauzulę tajności zgodnie z prawem krajowym państwa upoważnionego podmiotu wytwarzającego. Upoważniony podmiot otrzymujący gwarantuje co najmniej równorzędny poziom ochrony otrzymanych informacji niejawnych, zgodnie z postanowieniami ustępu 3 niniejszego artykułu.

2. Klauzula tajności może być zmieniona lub zniesiona wyłącznie przez upoważniony podmiot, który ją nadał. Upoważniony podmiot otrzymujący informacje niejawne 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	GRUZJA	ODPOWIEDNIK W JĘZYKU ANGIELSKIM
ŚCIŚLE TAJNE	განსაკუთრებული მნიშვნელობის GANSAKUTREBULI MNISHVNELOBIS	TOP SECRET
TAJNE	სრულიად საიდუმლო SRULİAD SAİDUMLO	SECRET
POUFNE	საიდუმლო SAİDUMLO	CONFIDENTIAL
ZASTRZEŻONE	შეზღუდული სარგებლობისთ SHEZGUDULİ SARGEBLOBİSTVİS	RESTRICTED

ARTYKUŁ 3
WŁAŚCIWE ORGANY

1. Dla celów niniejszej Umowy właściwymi organami Stron są:
   a) dla Rzeczypospolitej Polskiej: Szef Agencji Bezpieczeństwa Wewnętrznego;
   b) dla Gruzji: Służba Bezpieczeństwa Państwa Gruzji.

2. Strony informują się drogą dyplomatyczną o zmianach właściwych organów Stron, o których mowa w ustępie 1 niniejszego artykułu, lub zmianach ich właściwości.

ARTYKUŁ 4
ZASADY OCHRONY INFORMACJI NIEJAWNYCH

1. Strony podejmują wszelkie określone w niniejszej Umowie oraz zgodne z prawem krajowym swoich państw działania w celu ochrony informacji niejawnych wymienianych lub wytwarzanych w wyniku wspólnej działalności Stron lub upoważnionych podmiotów, w tym także informacji niejawnych wytworzonych w związku z realizacją kontraktów niejawnych.
2. Upoważniony podmiot otrzymujący wykorzystuje informacje niejawne wyłącznie w celach określonych przy ich przekazaniu.
3. Informacje niejawne mogą być udostępniane tylko tym osobom, których zadania wymagają zapoznania się z nimi i które - zgodnie z prawem krajowym państwa Strony upoważnionego podmiotu otrzymującego - zostały upoważnione do dostępu do nich.
4. Upoważniony podmiot otrzymujący nie udostępnia informacji, o których mowa w ustępie 1 niniejszego artykułu, stronie trzeciej bez uprzedniej pisemnej zgody upoważnionego podmiotu wytwarzającego.

ARTYKUŁ 5
POŚWIADCZENIA BEZPIECZEŃSTWA ORAZ ŚWIADECTWA BEZPIECZEŃSTWA PRZEMYSŁOWEGO

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

ARTYKUŁ 6
KONTRAKTY NIEJAWNE

1. Przed zawarciem kontraktu niejawnego każdy potencjalny kontrahent występuje do właściwego organu swojej Strony, aby ten zwrócił się do właściwego organu drugiej Strony o pisemne zaświadczenie, że potencjalny kontrahent drugiej Strony spełnia wymogi w zakresie ochrony informacji niejawnych o odpowiedniej klauzuli lub posiada odpowiednie świadectwo bezpieczeństwa przemysłowego.
2. Informacje niejawne nie są udostępniane kontrahentowi do czasu uzyskania zaświadczenia, o którym mowa w ustępie 1 niniejszego artykułu.
3. Kontrahent otrzymujący informacje niejawne związane z kontraktem niejawnym otrzymuje od kontrahenta drugiej Strony instrukcję bezpieczeństwa przemysłowego, która stanowi integralną część każdego kontraktu niejawnego. Instrukcja bezpieczeństwa przemysłowego zawiera postanowienia dotyczące wymogów bezpieczeństwa, w szczególności:
   a) wykaz rodzajów informacji niejawnych odnoszących się do danego kontraktu niejawnego, z uwzględnieniem ich klauzul tajności;
   b) zasady przyznawania klauzul tajności informacjom wytworzonym podczas realizacji danego kontraktu niejawnego.

   Instrukcja bezpieczeństwa przemysłowego może także zawierać dodatkowe zasady ochrony informacji niejawnych odnoszące się do danego kontraktu niejawnego.
4. Kontrahent przekazuje kopię instrukcji bezpieczeństwa przemysłowego właściwemu organowi swojej Strony.
5. Realizacja kontraktu niejawnego w części związanej z dostępem do informacji niejawnych jest możliwa, o ile kontrahent spełnia wymogi niezbędne do ochrony informacji niejawnych oznaczonych odpowiednią klauzulą tajności lub posiada odpowiednie świadectwo bezpieczeństwa przemysłowego i postępuje zgodnie z instrukcją bezpieczeństwa przemysłowego.

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

ARTYKUŁ 7
PRZEKAZYWANIE INFORMACJI NIEJAWNYCH

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

ARTYKUŁ 8
POWIELANIE I TŁUMACZENIE INFORMACJI NIEJAWNYCH

1. Powielanie lub tłumaczenie informacji niejawnych odbywa się w sposób zgodny z prawem krajowym państwa każdej ze Stron. Powielone lub przetłumaczone informacje są przetwarzane tak jak oryginały. Liczba kopii lub tłumaczeń jest ograniczona do liczby wymaganej dla celów służbowych.

2. Informacje niejawne o klauzuli ŚCIŚLE TAJNE/ განსაკუთრებული მნიშვნელობის / TOP SECRET nie są powielane. Informacje te mogą być tłumaczone tylko po uprzednim uzyskaniu pisemnego zezwolenia wydanego przez upoważniony podmiot wytwarzający.

ARTYKUŁ 9
NISZCZENIE I ZWROT INFORMACJI NIEJAWNYCH

1. Informacje niejawne są niszczone zgodnie z prawem krajowym państwa upoważnionego podmiotu otrzymującego, w sposób uniemożliwiający ich częściowe lub całkowite odtworzenie.
2. Upoważniony podmiot otrzymujący niezwłocznie informuje pisemnie właściwy organ swojej Strony o zniszczeniu informacji niejawnych, który następnie przekazuje tę informację właściwemu organowi Strony przekazującej.
3. Z zastrzeżeniem ustępu 5 niniejszego artykułu, informacje niejawne o klauzuli ŚCIŚLE TAJNE/განსაკუთრებული მნიშვნელობის /TOP SECRET nie są niszczone, ale są zwracane upoważnionemu podmiotowi wytwarzającemu, o ile nie są dłużej potrzebne do osiągnięcia celu, dla którego zostały przekazane.
4. Na wniosek upoważnionego podmiotu wytwarzającego informacje niejawne są zwracane.
5. W sytuacjach wyjątkowych, kiedy ochrona lub zwrot informacji niejawnych, w tym oznaczonych klauzulą ŚCIŚLE TAJNE/ განსაკუთრებული მნიშვნელობის / TOP SECRET, nie jest możliwy, są one niezwłocznie niszczone. O takim przypadku, zgodnie z ustępem 2 niniejszego artykułu, informowany jest właściwy organ Strony przekazującej.

ARTYKUŁ 10
WIZYTY

1. Z zastrzeżeniem ustępów 5 i 6 niniejszego artykułu, osobom przybywającym z wizytą na terytorium państwa drugiej Strony zezwala się na dostęp do informacji niejawnych tylko po uprzednim uzyskaniu pisemnego zezwolenia wydanego przez właściwy organ drugiej Strony.
2. Co najmniej trzydzieści dni przed planowanym terminem wizyty, a w nagłych przypadkach - w krótszym czasie, właściwy organ Strony wysyłającej zwraca się do właściwego organu Strony przyjmującej z wnioskiem o wyrażenie zgody na wizytę.
3. Wniosek, o którym mowa w ustępie 2 niniejszego artykułu, powinien zawierać:
   a) cel, termin i program wizyty;
   b) przewidywaną klauzulę informacji niejawnych niezbędną dla osiągnięcia celów wizyty;
   c) imię i nazwisko, datę i miejsce urodzenia, obywatelstwo i numer paszportu lub innego dokumentu tożsamości osoby przybywającej z wizytą;
   d) stanowisko służbowe osoby przybywającej z wizytą wraz z nazwą podmiotu, który reprezentuje;
   e) poziom i datę ważności poświadczenia bezpieczeństwa posiadanego przez osobę przybywającą z wizytą;
   f) nazwę i adres odwiedzanego podmiotu;
   g) imię i nazwisko oraz stanowisko służbowe osoby przyjmującej;
   h) datę, podpis oraz oficjalną pieczęć właściwego organu.
4. Do ochrony danych osobowych, o których mowa w ustępie 3 niniejszego artykułu, przekazywanych w związku z postanowieniami ustępów 1, 5 oraz 6 niniejszego artykułu, stosuje się, z uwzględnieniem prawa krajowego państwa każdej ze Stron, następujące postanowienia:

a) otrzymane przez Stronę przyjmującą wizytę dane osobowe będą wykorzystane wyłącznie w celu i na warunkach określonych przez Stronę przekazującą;

b) Strona przyjmująca wizytę nie przechowuje danych osobowych dłużej, aniżeli jest to niezbędne dla celu ich przetwarzania;

c) w przypadku przekazania danych, których nie wolno było przekazać, Strona przekazująca zawiadamia o tym Stronę przyjmującą wizytę, która jest zobowiązana do usunięcia tych danych w sposób uniemożliwiający ich częściowe lub całkowite odtworzenie;

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

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

f) 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 niniejszego artykułu i są ważne przez okres dwunastu miesięcy. Po zatwierdzeniu takich list przez właściwe organy Stron, terminy wizyt uzgadniane są bezpośrednio między jednostką wysyłającą a jednostką przyjmującą wizytę, zgodnie z ustalonymi przez nie warunkami.

6. Z zastrzeżeniem ustępu 2 artykułu 6, wizyty związane z dostępem do informacji niejawnych o klauzuli ZASTRZEŻONE/ შეზღუდული სარგებლობისთვის /RESTRICTED są uzgadniane bezpośrednio między upoważnionym podmiotem wysyłającym a upoważnionym podmiotem przyjmującym wizytę.

ARTYKUŁ 11
NARUSZENIE REGULACJI DOTYCZĄCYCH OCHRONY INFORMACJI NIEJAWNYCH

1. Naruszeniem regulacji dotyczących ochrony informacji niejawnych jest działanie lub zaniechanie sprzeczne z niniejszą Umową lub prawem krajowym państw Stron dotyczącym ochrony informacji niejawnych.
2. Informacja o każdym przypadku naruszenia lub o podejrzeniu naruszenia regulacji dotyczących ochrony informacji niejawnych przekazanych przez upoważniony podmiot wytwarzający lub informacji niejawnych wytworzonych w wyniku wspólnego działania upoważnionych podmiotów będzie niezwłocznie przekazywana właściwemu organowi Strony, na terytorium państwa którego miało miejsce lub zaistniało podejrzenie takiego naruszenia.
3. Każdy przypadek naruszenia lub podejrzenia naruszenia regulacji dotyczących ochrony informacji niejawnych będzie wyjaśniany zgodnie z prawem krajowym państwa Strony, na terytorium którego zdarzenie miało miejsce.
4. W przypadku naruszenia regulacji dotyczących ochrony informacji niejawnych, o którym mowa w ustępie 1 niniejszego artykułu, właściwy organ Strony, na terytorium państwa którego naruszenie miało miejsce, niezwłocznie pisemnie informuje właściwy organ drugiej Strony o tym naruszeniu, jego okolicznościach oraz wyniku czynności, o których mowa w ustępie 3 niniejszego artykułu.

5. Właściwe organy Stron współpracują przy czynnościach, o których mowa w ustępie 3 niniejszego artykułu, na wniosek jednego z nich.

ARTYKUŁ 12
JĘZYKI

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

ARTYKUŁ 13
KOSZTY

Każda ze Stron pokrywa koszty własne, poniesione w związku z realizacją postanowień niniejszej Umowy, o ile właściwe organy Stron lub upoważnione podmioty nie uzgodnią inaczej.

ARTYKUŁ 14
KONSULTACJE

1. Właściwe organy Stron informują się wzajemnie o wszelkich zmianach w prawie krajowym swoich państw dotyczącym ochrony informacji niejawnych, w zakresie niezbędnym do wykonywania postanowień niniejszej Umowy.
2. W celu zapewnienia ścisłej współpracy przy realizacji postanowień niniejszej Umowy właściwe organy Stron konsultują się na wniosek jednego z nich.
3. Każda ze Stron zezwoli przedstawicielom właściwego organu drugiej Strony na składanie wizyt na terytorium swojego państwa w celu omówienia procedur służących ochronie informacji niejawnych, które zostały jej przekazane przez drugą Stronę.

4. W celu zapewnienia skutecznej współpracy będącej przedmiotem niniejszej Umowy i w zakresie kompetencji przyznanych właściwym organom prawem krajowym państw ich Stron, organy te mogą, w razie potrzeby, zawierać pisemne szczegółowe uzgodnienia techniczne lub organizacyjne.

ARTYKUŁ 15
ROZSTRZYGANIE SPORÓW

1. Wszelkie sporne kwestie dotyczące interpretowania lub stosowania niniejszej Umowy będą rozstrzygane w drodze bezpośrednich konsultacji między właściwymi organami Stron.
2. Jeśli nie jest możliwe rozwiązanie sporu w sposób, o którym mowa w ustępie 1 niniejszego artykułu, będzie on rozstrzygany drogą dyplomatyczną.

ARTYKUŁ 16
STOSUNEK DO INNYCH UMÓW

Z dniem wejścia w życie niniejszej Umowy przestaje być stosowany artykuł 3 Umowy między Rządem Rzeczypospolitej Polskiej a Rządem Gruzji o współpracy w zwalczaniu przestępczości zorganizowanej oraz innych form przestępczości, podpisanej w Tbilisi dnia 31 maja 2007 roku. Informacje niejawne, które zostały przekazane albo mają być przekazywane na podstawie wyżej wymienionej Umowy, będą chronione zgodnie z postanowieniami niniejszej Umowy.

ARTYKUŁ 17
POSTANOWIENIA KOŃCOWE

1. Niniejsza Umowa wejdzie w życie w pierwszym dniu drugiego miesiąca, który nastąpi po dniu otrzymania późniejszej z not, którymi Strony poinformują się o zakończeniu swoich procedur wewnętrznych niezbędnych do wejścia w życie niniejszej Umowy.

2. Niniejsza Umowa może zostać zmieniona za wspólną pisemną zgodą obu Stron. Takie zmiany zostaną ujęte w odrębnym dokumencie, który będzie stanowił integralną część niniejszej Umowy, i wejdą w życie zgodnie z postanowieniami ustępu 1 niniejszego artykułu.
3. Niniejsza Umowa zawarta jest na czas nieokreślony. Może być ona wypowiedziana w dowolnym czasie przez każdą ze Stron w drodze pisemnej notyfikacji przekazanej kanałem dyplomatycznym drugiej Stronie. W takim przypadku utraci moc po upływie sześciu miesięcy od dnia otrzymania noty informującej o wypowiedzeniu.
4. W przypadku wypowiedzenia niniejszej Umowy wszystkie wymienione na jej podstawie informacje niejawne zostaną zniszczone lub zwrócone zgodnie z artykułem 9, nie później niż niniejsza Umowa utraci moc na podstawie ustępu 3 niniejszego artykułu.

Sporządzono w Tbilisi dnia 8 października 2015 roku w dwóch jednobrzmiących egzemplarzach, każdy w językach polskim, gruzińskim i angielskim, przy czym wszystkie teksty są jednakowo autentyczne. W przypadku rozbieżności przy ich interpretacji tekst w języku angielskim uważany będzie za rozstrzygający.

Z UPOWAŻNIENIA RZĄDU RZECZYPOSPOLITEJ POLSKIEJ	Z UPOWAŻNIENIA RZĄDU GRUZJI
T. Szymański	

შეთანხმება
პოლონეთის რესპუბლიკის მთავრობასა და საქართველოს მთავრობას შორის საიდუმლო ინფორმაციის გაცვლისა და ორმხრივად დაცვის შესახებ

პოლონეთის რესპუბლიკის მთავრობა და საქართველოს მთავრობა,
შემდგომში წოდებულნი როგორც „მხარეები“,

სათანადოდ ითვალისწინებენ რა მხარეებს შორის გაცვლილი ან თანამშრომლობის პროცესის დროს წარმოშობილი საიდუმლო ინფორმაციის ეფექტური დაცვის გარანტირების აუცილებლობას,

ხელმძღვანელობენ რა საიდუმლო ინფორმაციის დაცვის კუთხით ორივე მხარისთვის ერთნაირი რეგულაციების მიღების განზრახვით,

საერთაშორისო სამართლის სავალდებულო წესებისა და მხარეების სახელმწიფოთა შიდასახელმწიფოებრივი კანონმდებლობის პატივისცემის საფუძველზე,

შეთანხმდნენ შემდეგზე:

მუხლი 1

განსაზღვრებები

წინამდებარე შეთანხმების მიზნით, შემდეგი განსაზღვრებები ნიშნავს:

a) **საიდუმლო ინფორმაცია** - ნებისმიერი ინფორმაცია, მისი ფორმის, მატარებლის და ჩაწერის ხერხის მიუხედავად, აგრეთვე ობიექტები ან მათი ნებისმიერი ნაწილები, მათ შორის შექმნის პროცესში არსებული, რომელიც მოითხოვს დაცვას უნებართვო გამჟღავნებისგან მხარის სახელმწიფოს შიდასახელმწიფოებრივი კანონმდებლობისა და წინამდებარე შეთანხმების შესაბამისად;

b) **კომპეტენტური ორგანო** - წინამდებარე შეთანხმების მე-3 მუხლში მითითებული ორგანო;

c) **უფლებამოსილი ორგანო** - ფიზიკური პირი, იურიდიული პირი ან სხვა ორგანიზაციული სტრუქტურა, რომელიც კომპეტენტურია, წარმოშოს, გადასცეს, მიიღოს, შეინახოს, დაიცვას და გამოიყენოს საიდუმლო ინფორმაცია შესაბამისი მხარის სახელმწიფოს შიდასახელმწიფოებრივი კანონმდებლობის შესაბამისად;

d) **საიდუმლო კონტრაქტი** - კონტრაქტი, რომლის განხორციელებაც მოიცავს საიდუმლო ინფორმაციის გაცნობას ან რომელიც წარმოშობს ასეთ ინფორმაციას;

e) **კონტრაქტორი** - ერთ-ერთი მხარის სახელმწიფოს შიდასახელმწიფოებრივი კანონმდებლობით განსაზღვრული იურიდიული პირი ან სხვა ორგანიზაციული სტრუქტურა, რომელსაც გააჩნია სამართლებრივი უფლებაუნარიანობა, დადოს საიდუმლო კონტრაქტები;

f) **მესამე მხარე** - საერთაშორისო ორგანიზაცია ან სახელმწიფო, რომელიც არ არის წინამდებარე შეთანხმების მხარე, მათი ფიზიკური პირი ან სხვა ორგანო.

მუხლი 2

საიდუმლოობის ხარისხები

1. საიდუმლო ინფორმაციას ენიჭება საიდუმლოობის ხარისხი მისი შინაარსის გათვალისწინებით წარმომშობი უფლებამოსილი ორგანოს სახელმწიფოს შიდასახელმწიფოებრივი კანონმდებლობის შესაბამისად. მიმღებმა უფლებამოსილმა ორგანომ უნდა უზრუნველყოს მიღებული საიდუმლო ინფორმაციის დაცვის სულ მცირე ეკვივალენტური დონე ამ მუხლის მე-3 პუნქტის დებულებათა თანახმად.

2. საიდუმლოობის ხარისხი შეიძლება შეიცვალოს ან მოიხსნას მხოლოდ მისი მიმნიჭებელი უფლებამოსილი ორგანოს მიერ. მიმღებ უფლებამოსილ ორგანოს წერილობით უნდა ეცნობოს ადრე მიღებული საიდუმლო ინფორმაციის საიდუმლო ხარისხის ყოველი ცვლილების ან მოხსნის შესახებ.

3. მხარეები თანხმდებიან, რომ შემდეგი საიდუმლოობის ხარისხები არის ეკვივალენტური:

პოლონეთის რესპუბლიკა	საქართველო	ეკვივალენტი ინგლისურ ენაზე
ŚCIŚLE TAJNE	განსაკუთრებული მნიშვნელობის	TOP SECRET
TAJNE	სრულიად საიდუმლო	SECRET

POUFNE	საიდუმლო	CONFIDENTIAL
ZASTRZEŻONE	შეზღუდული სარგებლობისთვის	RESTRICTED

მუხლი 3

კომპეტენტური ორგანოები

1. წინამდებარე შეთანხმების მიზნისთვის, მხარეების კომპეტენტური ორგანოები არიან:

a) პოლონეთის რესპუბლიკისთვის: შიდა უსაფრთხოების სააგენტოს უფროსი;

b) საქართველოსთვის: საქართველოს სახელმწიფო უსაფრთხოების სამსახური.

2. მხარეებმა დიპლომატიური არხებით უნდა აცნობონ ერთმანეთს ამ მუხლის პირველ პუნქტში მითითებული მხარეების კომპეტენტური ორგანოების ცვლილების ან მათი კომპეტენციების ცვლილების შესახებ.

მუხლი 4

საიდუმლო ინფორმაციის დაცვის პრინციპები

1. წინამდებარე შეთანხმებისა და მათი სახელმწიფოების შიდასახელმწიფოებრივი კანონმდებლობის შესაბამისად, მხარეებმა უნდა მიიღონ ყველა ზომა, რომელიც მიზნად ისახავს მხარეებს ან უფლებამოსილ ორგანოებს შორის გაცვლილი ან თანამშრომლობის შედეგად წარმოშობილი, მათ შორის საიდუმლო კონტრაქტების

განხორციელებასთან დაკავშირებით წარმოშობილი, საიდუმლო ინფორმაციის დაცვას.

2. მიმღებმა უფლებამოსილმა ორგანომ უნდა გამოიყენოს საიდუმლო ინფორმაცია მხოლოდ იმ მიზნებით, რომლებიც განისაზღვრა მისი გადაცემის დროს.

3. საიდუმლო ინფორმაციის გაცნობის უფლება შეიძლება მიენიჭოს მხოლოდ იმ ფიზიკურ პირებს, რომლებსაც გააჩნიათ ინფორმაციის გაცნობის საჭიროება და რომლებიც უფლებამოსილნი არიან, გაეცნონ ასეთ ინფორმაციას მიმღები უფლებამოსილი ორგანოს სახელმწიფოს შიდასახელმწიფოებრივი კანონმდებლობის შესაბამისად.

4. მიმღებმა უფლებამოსილმა ორგანომ ამ მუხლის პირველ პუნქტში მითითებული საიდუმლო ინფორმაცია არ უნდა გადასცეს არცერთ მესამე მხარეს წარმომშობი უფლებამოსილი ორგანოს წინასწარი წერილობითი თანხმობის გარეშე.

მუხლი 5

საიდუმლო ინფორმაციასთან ინდივიდუალური დაშვებები და საიდუმლო ინფორმაციასთან იურიდიული პირის დაშვებები

წინამდებარე შეთანხმების ფარგლებში მხარეებმა უნდა ცნონ მეორე მხარის სახელმწიფოს შიდასახელმწიფოებრივი კანონმდებლობის შესაბამისად გაცემული საიდუმლო ინფორმაციასთან ინდივიდუალური დაშვებები და საიდუმლო ინფორმაციასთან იურიდიული პირის დაშვებები.

მუხლი 6

საიდუმლო კონტრაქტები

1. საიდუმლო კონტრაქტის დადებამდე, თითოეულმა პოტენციურმა კონტრაქტორმა უნდა მიმართოს თავისი მხარის კომპეტენტურ ორგანოს, რათა მან მეორე მხარის კომპეტენტური ორგანოსგან მოითხოვოს წერილობითი დადასტურება იმის თაობაზე, რომ მეორე მხარის პოტენციური კონტრაქტორი აკმაყოფილებს შესაბამისი ხარისხის საიდუმლო ინფორმაციის დაცვის მოთხოვნებს ან რომ მას გააჩნია საიდუმლო ინფორმაციასთან იურიდიული პირის სათანადო დაშვება.

2. საიდუმლო ინფორმაცია არ შეიძლება გადაეცეს კონტრაქტორს მანამდე, სანამ არ იქნება მიღებული ამ მუხლის პირველ პუნქტში მითითებული დადასტურება.

3. კონტრაქტორმა, რომელიც იღებს საიდუმლო კონტრაქტთან დაკავშირებულ საიდუმლო ინფორმაციას, მეორე სახელმწიფოს კონტრაქტორისგან უნდა მოიპოვოს იურიდიული პირის უსაფრთხოების ინსტრუქცია, რომელიც საიდუმლო კონტრაქტის განუყოფელ ნაწილს წარმოადგენს. იურიდიული პირის უსაფრთხოების ინსტრუქცია შეიცავს დებულებებს უსაფრთხოების მოთხოვნებზე, კერძოდ:

a) მოცემულ საიდუმლო კონტრაქტთან დაკავშირებული საიდუმლო ინფორმაციის სახეობების ნუსხას, მათ შორის მათ საიდუმლოობის ხარისხებს;

b) მოცემული საიდუმლო კონტრაქტის განხორციელების პროცესში წარმოშობილი ინფორმაციისთვის საიდუმლოობის ხარისხების მინიჭების წესებს.

იურიდიული პირის უსაფრთხოების ინსტრუქცია შეიძლება ასევე შეიცავდეს მოცემულ საიდუმლო კონტრაქტთან დაკავშირებული საიდუმლო ინფორმაციის დაცვის დამატებით წესებს.

4. კონტრაქტორმა იურიდიული პირის უსაფრთხოების ინსტრუქციის ასლი უნდა წარუდგინოს თავისი მხარის კომპეტენტურ ორგანოს.

5. საიდუმლო კონტრაქტის განხორციელება იმ ნაწილში, რომელიც დაკავშირებულია საიდუმლო ინფორმაციის გაცნობასთან, შესაძლებელია მხოლოდ იმ შემთხვევაში, თუ კონტრაქტორი აკმაყოფილებს შესაბამისი ხარისხის საიდუმლო ინფორმაციის დაცვის მოთხოვნებს ან თუ მას გააჩნია საიდუმლო ინფორმაციასთან იურიდიული პირის სათანადო დაშვება, და თუ იგი მოქმედებს იურიდიული პირის უსაფრთხოების ინსტრუქციის შესაბამისად.

6. ყველა ქვეკონტრაქტორი უნდა დაემორჩილოს საიდუმლო ინფორმაციის დაცვის იმავე პირობებს, რომლებიც გათვალისწინებულია კონტრაქტორისთვის.

მუხლი 7

საიდუმლო ინფორმაციის გადაცემა

1. საიდუმლო ინფორმაცია უნდა გადაიცეს დიპლომატიური არხებით.

2. ZASTRZEŻONE / შეზღუდული სარგებლობისთვის / RESTRICTED ან POUFNE / საიდუმლო / CONFIDENTIAL გრიფით დასაიდუმლოებული ინფორმაცია შეიძლება აგრეთვე გადაიცეს უფლებამოსილი კურიერების მიერ, გადამცემი მხარის სახელმწიფოს შიდასახელმწიფოებრივი კანონმდებლობის შესაბამისად.

3. გადაუდებელ შემთხვევებში, თუ შეუძლებელია გადაცემის სხვა ფორმის გამოყენება და თუ გადამცემი მხარის სახელმწიფოს შიდასახელმწიფოებრივი კანონმდებლობით განსაზღვრული უსაფრთხოების მოთხოვნები არის დაცული, დასაშვებია ZASTRZEŻONE / შეზღუდული სარგებლობისთვის / RESTRICTED ან POUFNE / საიდუმლო / CONFIDENTIAL გრიფით დასაიდუმლოებული ინფორმაციის პირადად ხელით გადატანა.

4. მხარეების კომპეტენტური ორგანოები შეიძლება შეთანხმდნენ საიდუმლო ინფორმაციის გადაცემის სხვა ისეთ ფორმებზე, რომლებიც უზრუნველყოფს უნებართვო გამჟღავნებისგან მის დაცვას.

5. მხარეებს შორის გადაცემული საიდუმლო ინფორმაცია საჭიროებს მიღება-ჩაბარების აქტს.

მუხლი 8

საიდუმლო ინფორმაციის გამრავლება და თარგმნა

1. საიდუმლო ინფორმაციის გამრავლება ან თარგმნა უნდა განხორციელდეს თითოეული მხარის სახელმწიფოს შიდასახელმწიფოებრივი კანონმდებლობის თანახმად. გამრავლებულ ან თარგმნილ საიდუმლო ინფორმაციასთან მოპყრობა ხორციელდება ისევე, როგორც ინფორმაციის დედანთან. ასლების ან თარგმანების რაოდენობა უნდა შეიზღუდოს ოფიციალური მიზნებისთვის საჭირო რაოდენობამდე.

2. ŚCIŚLE TAJNE / განსაკუთრებული მნიშვნელობის / TOP SECRET გრიფით დასაიდუმლოებული ინფორმაცია არ უნდა გამრავლდეს. იგი შეიძლება ითარგმნოს მხოლოდ წარმომშობი

უფლებამოსილი ორგანოს მიერ გაცემული წინასწარი წერილობითი თანხმობის მოპოვების შემდეგ.

მუხლი 9

საიდუმლო ინფორმაციის განადგურება და დაბრუნება

1. საიდუმლო ინფორმაცია უნდა განადგურდეს მიმღები უფლებამოსილი ორგანოს სახელმწიფოს შიდასახელმწიფოებრივი კანონმდებლობის შესაბამისად ისეთი წესით, რომ გამოირიცხოს მისი ნაწილობრივი ან სრული აღდგენა.

2. მიმღებმა უფლებამოსილმა ორგანომ შეუსაბამო დაყოვნების გარეშე უნდა აცნობოს მისი მხარის კომპეტენტურ ორგანოს საიდუმლო ინფორმაციის განადგურების შესახებ, რომელიც თავის მხრივ ამ ინფორმაციას გადაუგზავნის გადამცემი მხარის კომპეტენტურ ორგანოს.

3. ამ მუხლის მე-5 პუნქტისთვის ზიანის მიუყენებლად, ŚCIŚLE TAJNE / განსაკუთრებული მნიშვნელობის / TOP SECRET გრიფით დასაიდუმლოებული ინფორმაცია არ უნდა განადგურდეს, არამედ ის უნდა დაუბრუნდეს წარმომშობ უფლებამოსილ ორგანოს მას შემდეგ, როდესაც იგი აღარ არის საჭირო იმ მიზნისთვის, რისთვისაც ის იქნა მიწოდებული.

4. წარმომშობი უფლებამოსილი ორგანოს მოთხოვნის შემთხვევაში საიდუმლო ინფორმაცია უბრუნდება მას.

5. გამონაკლის შემთხვევებში, როდესაც შეუძლებელია საიდუმლო ინფორმაციის, მათ შორის ŚCIŚLE TAJNE / განსაკუთრებული მნიშვნელობის / TOP SECRET გრიფით დასაიდუმლოებული ინფორმაციის დაცვა ან დაბრუნება, ის

დაუყოვნებლივ უნდა განადგურდეს. ასეთ შემთხვევაში, გადამცემი მხარის კომპეტენტურ ორგანოს უნდა ეცნობოს აღნიშნულის თაობაზე ამ მუხლის მე-2 პუნქტის შესაბამისად.

მუხლი 10

ვიზიტები

1. ამ მუხლის მე-5 და მე-6 პუნქტების გათვალისწინებით, ფიზიკურ პირებს, რომლებიც ვიზიტად ჩადიან მეორე მხარის სახელმწიფოს ტერიტორიაზე, უნდა მიეცეთ ნებართვა, გაეცნონ საიდუმლო ინფორმაციას მხოლოდ მეორე მხარის კომპეტენტური ორგანოს მიერ გაცემული წინასწარი წერილობითი თანხმობის მიღების შემდეგ.

2. ვიზიტის დაგეგმილ თარიღამდე სულ მცირე 30 დღით ადრე და გადაუდებელ შემთხვევებში უფრო მოკლე ვადაში, ვიზიტის განმახორციელებელი მხარის კომპეტენტურმა ორგანომ ვიზიტზე მოთხოვნით უნდა მიმართოს მასპინძელი მხარის კომპეტენტურ ორგანოს.

3. ამ მუხლის მე-2 პუნქტში მითითებული მოთხოვნა უნდა შეიცავდეს:

a) ვიზიტის მიზანს, თარიღსა და პროგრამას;

b) ვიზიტის მიზნისთვის საჭირო საიდუმლო ინფორმაციის წინასწარ განსაზღვრულ ხარისხს;

c) ვიზიტორის სახელს და გვარს, დაბადების თარიღსა და ადგილს, მოქალაქეობას და პასპორტის ან სხვა საიდენტიფიკაციო დოკუმენტის ნომერს;

d) ვიზიტორის თანამდებობას, აგრეთვე იმ უწყების დასახელებას, რომელსაც ის წარმოადგენს;

e) საიდუმლო ინფორმაციასთან იმ ინდივიდუალური დაშვების დონეს და მოქმედების ვადას, რომელსაც ფლობს ვიზიტორი;

f) იმ უწყების დასახელებას და მისამართს, სადაც უნდა განხორციელდეს ვიზიტი;

g) იმ პირის სახელს, გვარს და თანამდებობას, ვისთანაც უნდა განხორციელდეს ვიზიტი;

h) თარიღს, ხელმოწერას და კომპეტენტური ორგანოს ოფიციალურ ბეჭედს.

4. ამ მუხლის მე-3 პუნქტში მითითებული პერსონალური მონაცემების დაცვის მიზნით, რომლებიც გადაიცემა ამ მუხლის პირველი, მე-5 და მე-6 პუნქტების დებულებათა თანახმად, თითოეული მხარის სახელმწიფოს შიდასახელმწიფოებრივი კანონმდებლობის გათვალისწინებით გამოიყენება შემდეგი დებულებები:

a) მასპინძელი მხარის მიერ მიღებული პერსონალური მონაცემი გამოყენებული უნდა იქნეს მხოლოდ გადამცემი მხარის მიერ განსაზღვრული მიზნითა და პირობებით;

b) პერსონალური მონაცემი მასპინძელი მხარის მიერ შენახული უნდა იქნეს არაუმეტეს იმ ვადით, რომელიც აუცილებელია მისი დამუშავების მიზნისთვის;

c) ისეთი პერსონალური მონაცემის გადაცემის შემთხვევაში, რომლის მიწოდება არ იყო ნებადართული, გადამცემმა მხარემ უნდა შეატყობინოს ამის შესახებ მასპინძელ მხარეს, რომელიც ვალდებულია წაშალოს ეს მონაცემი ისეთი წესით, რაც გამორიცხავს მის ნაწილობრივ ან სრულ აღდგენას;

d) გადამცემმა მხარემ უნდა იკისროს პასუხისმგებლობა პერსონალური მონაცემის სისწორესთან დაკავშირებით და იმ

შემთხვევაში, თუ ეს მონაცემი აღმოჩნდება ყალბი ან არასრული, ამის შესახებ უნდა შეატყობინოს მასპინძელ მხარეს, რომელიც ვალდებულია გაასწოროს ან წაშალოს ეს მონაცემი;

e) მასპინძელი მხარე და გადამცემი მხარე ვალდებულნი არიან, აღრიცხონ პერსონალური მონაცემის გადაცემა, მიღება და წაშლა;

f) გადამცემი მხარე და მასპინძელი მხარე ვალდებულნი არიან, ეფექტიანად დაიცვან დამუშავებული პერსონალური მონაცემი არაუფლებამოსილი პირებისთვის მისი გამჟღავნებისგან, მონაცემის არაუფლებამოსილი ცვლილებებისგან, მისი დაკარგვისგან, დაზიანებისგან ან განადგურებისგან.

5. მხარეების კომპეტენტური ორგანოები შეიძლება შეთანხმდნენ იმ პირთა სიების შედგენაზე, რომლებიც უფლებამოსილნი არიან, განახორციელონ პერიოდული ვიზიტები კონკრეტული პროექტის, პროგრამის ან საიდუმლო კონტრაქტის განხორციელებასთან დაკავშირებით. სიები უნდა შეიცავდეს ამ მუხლის მე-3 პუნქტში მითითებულ მონაცემებს და ძალაში უნდა იყოს 12 თვის ვადით. მას შემდეგ, რაც მხარეების კომპეტენტური ორგანოები დაამტკიცებენ აღნიშნულ სიებს, ვიზიტების თარიღები შეთანხმდება უშუალოდ ვიზიტის განმახორციელებელ და მასპინძელ უფლებამოსილ ორგანოებს შორის, მათ მიერ შეთანხმებული პირობების შესაბამისად.

6. მე-6 მუხლის მე-2 პუნქტის გათვალისწინებით, ვიზიტები, რომლებიც მოიცავენ ZASTRZEŻONE / შეზღუდული სარგებლობისთვის / RESTRICTED გრიფით დასაიდუმლოებული ინფორმაციის გაცნობას, იგეგმება უშუალოდ ვიზიტის განმახორციელებელ და მასპინძელ უფლებამოსილ ორგანოებს შორის.

მუხლი 11

უსაფრთხოების დარღვევა

1. უსაფრთხოების დარღვევა არის მოქმედება ან უმოქმედობა, რომელიც ეწინააღმდეგება წინამდებარე შეთანხმებას ან საიდუმლო ინფორმაციის დაცვასთან დაკავშირებულ მხარეების სახელმწიფოთა შიდასახელმწიფოებრივ კანონმდებლობას.

2. წარმომშობი უფლებამოსილი ორგანოს მიერ გადაცემულ საიდუმლო ინფორმაციასთან, ან უფლებამოსილ ორგანოებს შორის თანამშრომლობის შედეგად წარმოშობილ საიდუმლო ინფორმაციასთან დაკავშირებული უსაფრთხოების ნებისმიერი დარღვევის ან დარღვევის ეჭვის შესახებ ინფორმაცია დაუყოვნებლივ უნდა ეცნობოს იმ მხარის კომპეტენტურ ორგანოს, რომლის სახელმწიფოს ტერიტორიაზეც მოხდა უსაფრთხოების დარღვევა ან არსებობს დარღვევის ეჭვი.

3. უსაფრთხოების ნებისმიერი დარღვევა ან დარღვევის შესახებ ეჭვი გამოძიებულ უნდა იქნეს იმ მხარის სახელმწიფოს შიდასახელმწიფოებრივი კანონმდებლობის მიხედვით, რომლის სახელმწიფოს ტერიტორიაზეც მას ჰქონდა ადგილი.

4. ამ მუხლის პირველ პუნქტში მითითებული უსაფრთხოების დარღვევის შემთხვევაში, იმ მხარის კომპეტენტურმა ორგანომ, რომლის სახელმწიფოს ტერიტორიაზეც მოხდა უსაფრთხოების დარღვევა, მეორე მხარის კომპეტენტურ ორგანოს წერილობით უნდა აცნობოს დარღვევის ფაქტი, გარემოებები და ამ მუხლის მე-3 პუნქტში მითითებული ქმედებების შედეგი.

5. მხარეების კომპეტენტურმა ორგანოებმა, ერთ-ერთი მათგანის მოთხოვნის საფუძველზე, უნდა ითანამშრომლონ ამ მუხლის მე-3 პუნქტში მითითებულ ქმედებებთან დაკავშირებით.

მუხლი 12

ენები

წინამდებარე შეთანხმების დებულებათა განხორციელების ფარგლებში მხარეებმა უნდა გამოიყენონ ინგლისური ენა ან თავიანთი ოფიციალური ენები, რომელთა გამოყენების შემთხვევაში წარდგენილი უნდა იქნეს მეორე მხარის ოფიციალურ ენაზე ან ინგლისურ ენაზე შესრულებული თარგმანი.

მუხლი 13

ხარჯები

თითოეულმა მხარემ უნდა დაფაროს წინამდებარე შეთანხმების დებულებათა განხორციელების შედეგად წარმოშობილი თავისი ხარჯები, თუ მხარეების კომპეტენტური ორგანოები ან უფლებამოსილი ორგანოები სხვაგვარად არ შეთანხმდებიან.

მუხლი 14

კონსულტაციები

1. მხარეების კომპეტენტურმა ორგანოებმა უნდა შეატყობინონ ერთმანეთს საიდუმლო ინფორმაციის დაცვის შესახებ თავიანთი სახელმწიფოების შიდასახელმწიფოებრივ კანონმდებლობაში შეტანილი ნებისმიერი ცვლილების თაობაზე, რომელიც წინამდებარე შეთანხმების განხორციელებას ეხება.

2. მხარეების კომპეტენტურმა ორგანოებმა, ერთ-ერთი მათგანის მოთხოვნის საფუძველზე, უნდა გაიარონ ერთმანეთთან კონსულტაცია წინამდებარე შეთანხმების დებულებათა განხორციელებასთან დაკავშირებით მჭიდრო თანამშრომლობის უზრუნველყოფის მიზნით.

3. თითოეულმა მხარემ უნდა დართოს ნება მეორე მხარის კომპეტენტური ორგანოს წარმომადგენლებს, ვიზიტად ეწვიონ მისი სახელმწიფოს ტერიტორიაზე მეორე მხარის მიერ გადაცემული საიდუმლო ინფორმაციის დაცვის პროცედურების განხილვის მიზნით.

4. ეფექტური თანამშრომლობის უზრუნველყოფის მიზნით, რომელიც წარმოადგენს წინამდებარე შეთანხმების მიზანს, და მათი მხარეების სახელმწიფოთა შიდასახელმწიფოებრივი კანონმდებლობით აღიარებული უფლებამოსილების ფარგლებში, მხარეების კომპეტენტურმა ორგანოებმა, აუცილებლობის შემთხვევაში, შეიძლება წერილობით გააფორმონ დეტალური ტექნიკური ან ორგანიზაციული წესები.

მუხლი 15

დავების გადაწყვეტა

1. წინამდებარე შეთანხმების განმარტებასთან ან განხორციელებასთან დაკავშირებული ნებისმიერი დავა უნდა გადაწყდეს მხარეების კომპეტენტურ ორგანოებს შორის პირდაპირი კონსულტაციების გზით.

2. თუ დავის გადაწყვეტა შეუძლებელია ამ მუხლის პირველ პუნქტში მითითებული წესით, ასეთი დავა უნდა გადაწყდეს დიპლომატიური არხების მეშვეობით.

მუხლი 16

ურთიერთობა სხვა შეთანხმებებთან

წინამდებარე შეთანხმების ძალაში შესვლის თარიღიდან უნდა შეწყდეს 2007 წლის 31 მაისს ქ. თბილისში შესრულებული „პოლონეთის

რესპუბლიკის მთავრობასა და საქართველოს მთავრობას შორის ორგანიზებული და სხვა სახის დანაშაულის წინააღმდეგ ბრძოლაში თანამშრომლობის შესახებ“ შეთანხმების მე-3 მუხლის გამოყენება. ზემოხსენებული შეთანხმების საფუძველზე გაცვლილი ან გასაცვლელი საიდუმლო ინფორმაცია უნდა იქნეს დაცული წინამდებარე შეთანხმების დებულებების შესაბამისად.

მუხლი 17

დასკვნითი დებულებები

1. წინამდებარე შეთანხმება ძალაში შედის იმ უკანასკნელი დიპლომატიური შეტყობინების მიღების თარიღიდან მეორე თვის პირველ დღეს, რომლითაც მხარეები ატყობინებენ ერთმანეთს წინამდებარე შეთანხმების ძალაში შესვლისთვის აუცილებელი მათი შიდასახელმწიფოებრივი პროცედურების დასრულების შესახებ.

2. წინამდებარე შეთანხმებაში შეიძლება შეტანილ იქნეს ცვლილებები ორივე მხარის ერთობლივი წერილობითი თანხმობით. ასეთი ცვლილებები გაფორმდება ცალკე დოკუმენტის სახით და წინამდებარე შეთანხმების განუყოფელი ნაწილი იქნება და ძალაში შევა ამ მუხლის პირველი პუნქტის დებულებათა შესაბამისად.

3. წინამდებარე შეთანხმება იდება განუსაზღვრელი ვადით. მისი მოქმედება შეიძლება შეწყდეს ნებისმიერ დროს ერთ-ერთი მხარის მიერ მეორე მხარისთვის დიპლომატიური არხების მეშვეობით წერილობითი შეტყობინების გაგზავნის გზით. ასეთ შემთხვევაში, წინამდებარე შეთანხმება შეწყვეტს მოქმედებას მოქმედების შეწყვეტის შესახებ შეტყობინების მიღებიდან ექვსი თვის შემდეგ.

4. წინამდებარე შეთანხმების მოქმედების შეწყვეტის შემთხვევაში, წინამდებარე შეთანხმების საფუძველზე გაცვლილი ყველა საიდუმლო ინფორმაცია მე-9 მუხლის შესაბამისად იქნება განადგურებული ან დაბრუნებული მანამდე, სანამ წინამდებარე შეთანხმება შეწყვეტს მოქმედებას ამ მუხლის მე-3 პუნქტის შესაბამისად.

შესრულებულია ქ. თბილისი 2015 წლის 8 ოქტომბერს ორ დედნად, თითოეული პოლონურ, ქართულ და ინგლისურ ენებზე. ამასთან, ყველა ტექსტი თანაბრად აუთენტურია. განსხვავებული განმარტების შემთხვევაში, უპირატესობა ენიჭება ტექსტს ინგლისურ ენაზე.

პოლონეთის რესპუბლიკის მთავრობის სახელით	საქართველოს მთავრობის სახელით
T. Siemoniak	G. Bokeria

AGREEMENT

between the Government of the Republic of Poland

and the Government of Georgia

on the exchange and mutual protection of classified information

The Government of the Republic of Poland and the Government of Georgia,
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 originated during cooperation course,

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 States of the Parties,

have agreed as follows:

ARTICLE 1
DEFINITIONS

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

a) **classified information** – any information, irrespective of the form, carrier and manner of recording thereof, as well as objects or any parts thereof, also in the process of being generated, which require protection against unauthorized disclosure in accordance with the national law of the State of the Party and this Agreement;

b) **competent authority** – the authority referred to in Article 3 of this Agreement;

c) **authorized body** – an individual, a legal entity or other organizational unit, competent to originate, transmit, receive, store, protect and use classified information in accordance with the national law of the State of the respective Party;

d) **classified contract** – a contract, performance of which involves access to classified information or originating of such information;

e) **contractor** – a legal entity or other organizational unit under the national law of the State of one of the Parties, which has legal capacity to conclude classified contracts;

f) **third party** – an international organization or a State not being a party to this Agreement, an individual or other entity thereof.

ARTICLE 2
SECURITY CLASSIFICATION LEVELS

1. Classified information is granted a security classification level in accordance with its content, pursuant to the national law of the State of the originating authorized body. The receiving authorized body shall guarantee at least an equivalent level of protection of the received classified information, pursuant to the provisions of Paragraph 3 of this Article.

2. The security classification level may be changed or removed only by the authorized body which has granted it. The receiving authorized 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:

THE REPUBLIC OF POLAND	GEORGIA	EQUIVALENT IN ENGLISH
ŚCIŚLE TAJNE	განსაკუთრებული მნიშვნელობის GANSAKUTREBULI MNISHVNELOBIS	TOP SECRET
TAJNE	სრულიად საიდუმლო SRULİAD SAİDUMLO	SECRET
POUFNE	საიდუმლო SAİDUMLO	CONFIDENTIAL
ZASTRZEŻONE	შეზღუდული სარგებლობისთვის SHEZGUDULİ SARGEBLOBİSTVİS	RESTRICTED

ARTICLE 3
COMPETENT AUTHORITIES

1. For the purpose of this Agreement, the competent authorities of the Parties shall be:
   a) for the Republic of Poland: the Head of the Internal Security Agency;
   b) for Georgia: State Security Service of Georgia.

2. The Parties shall inform each other via diplomatic channels about changes of the competent authorities of the Parties referred to in Paragraph 1 of this Article or about amendments to their competences.

ARTICLE 4
PRINCIPLES OF CLASSIFIED INFORMATION PROTECTION

1. In accordance with this Agreement and the national law of their States, the Parties shall adopt every measure aimed at the protection of classified information exchanged or originated as a result of cooperation between the Parties or authorized bodies, including classified information originated in connection with performance of classified contracts.
2. The receiving authorized body shall use classified information exclusively for the purposes defined at its transmission.
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 such information in accordance with the national law of the State of receiving authorized body.
4. The receiving authorized body shall not release classified information referred to in Paragraph 1 of this Article to any third party without a prior written consent of the originating authorized body.

ARTICLE 5
PERSONNEL SECURITY CLEARANCES AND FACILITY 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 State of the other Party.

ARTICLE 6

CLASSIFIED CONTRACTS

1. Before concluding a classified contract, each potential contractor shall apply to the competent authority of its Party to request the competent authority of the other Party a written confirmation that the potential contractor of the other Party meets the requirements for the protection of classified information at the relevant level or is a holder of an appropriate facility security clearance.
2. Classified information shall not be released to the contractor until the receipt of the confirmation referred to in Paragraph 1of this Article.
3. The contractor receiving classified information related to the classified contract shall obtain from the contractor of the other State a facility security instruction which is an integral part of classified contract. The facility security instruction contains provisions on the security requirements, in particular:
   a) the list of types of classified information related to a given classified contract, including their security classification levels;
   b) the rules for granting security classification levels to information originated during the performance of a given classified contract;

   The facility security instruction may also contain additional rules for the protection of classified information related to a given classified contract.
4. The contractor shall submit a copy of the facility security instruction to the competent authority of its Party.
5. The performance of a classified contract in the part connected with access to classified information shall be possible as long as the contractor meets the requirements for the protection of classified information at the relevant level or is a holder of an appropriate facility security clearance, and acts in accordance with 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 7
TRANSMISSION OF CLASSIFIED INFORMATION

1. Classified information shall be transmitted via diplomatic channels.
2. Information classified as ZASTRZEŻONE / შეზღუდული სარგებლობისთვის / RESTRICTED or POUFNE / საიდუმლო / CONFIDENTIAL may be also transmitted by authorized couriers, in accordance with the national law of the State of the transmitting Party.
3. In urgent cases, if it is not possible to use other form of transmission and the security requirements defined in the national law of the State of the transmitting Party are complied with, a personal hand carriage of information classified as ZASTRZEŻONE / შეზღუდული სარგებლობისთვის / RESTRICTED or POUFNE / საიდუმლო / CONFIDENTIAL is acceptable.
4. The competent authorities of the Parties may agree on other forms of transmission of classified information which ensure its protection against unauthorized disclosure.
5. Receipts are required for classified information transmitted between the Parties.

ARTICLE 8
REPRODUCTION AND TRANSLATION OF CLASSIFIED INFORMATION

1. Reproduction or translation of classified information shall be conducted pursuant to the national law of the State of each of the Parties. Reproduced or translated classified information shall be handled as the original information.

The number of copies or translations shall be limited to that required for official purposes.

2. Information classified as ŚCIŚLE TAJNE / განსაკუთრებული მნიშვნელობის / TOP SECRET shall not be reproduced. It can be translated only after obtaining a prior written consent issued by the originating authorized body.

ARTICLE 9
DESTRUCTION AND RETURN OF CLASSIFIED INFORMATION

1. Classified information shall be destroyed in accordance with the national law of the State of the receiving authorized body in such a manner as to eliminate its partial or total reconstruction.
2. Without undue delay, the receiving authorized body shall inform the competent authority of its Party in writing on the destruction of classified information, which in its turn shall forward this information to the competent authority of the transmitting Party.
3. Without prejudice to Paragraph 5 of this Article, information classified as ŚCIŚLE TAJNE / განსაკუთრებული მნიშვნელობის / TOP SECRET shall not be destroyed but shall be returned to the originating authorized body, when it is no longer necessary for the purpose it was provided.
4. Upon request of the originating authorized body classified information shall be returned.
5. In case of exceptional circumstances, when it is impossible to protect or to return the classified information, including information classified as ŚCIŚLE TAJNE / განსაკუთრებული მნიშვნელობის / TOP SECRET, it shall be destroyed immediately. In such a case the competent authority of the transmitting Party shall be informed in accordance with Paragraph 2 of this Article.

ARTICLE 10
VISITS

1. Subject to Paragraphs 5 and 6 of this Article, individuals arriving on a visit in the territory of the State 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 a planned date of the visit, and in urgent cases in shorter time, the competent authority of the visiting Party shall apply with a request for a visit to the competent authority of the hosting Party.
3. The request referred to in Paragraph 2 of this Article shall include:
   a) purpose, date and program of the visit;
   b) anticipated level of classified information required for the purpose of the visit;
   c) name and surname of the visitor, date and place of birth, citizenship and passport or other identification document's number;
   d) position of the visitor together with the name of the entity which he or she represents;
   e) level and the validity date of personnel security clearance held by the visitor;
   f) name and address of the entity to be visited;
   g) name, surname and position of the person to be visited;
   h) date, signature and official seal of the competent authority.
4. In order to protect personal data referred to in Paragraph 3 of this Article, transmitted in connection with the provisions of Paragraphs 1, 5 and 6 of this Article, the following provisions, subject to the national law of the State of each of the Parties, shall apply:
   a) personal data received by the hosting Party shall be used exclusively for the purpose and on conditions defined by the transmitting Party;

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

c) in case of transmission of personal data that was not allowed to be provided, the transmitting Party shall notify the hosting Party thereof, which is obliged to remove the data in such a manner as to eliminate its partial or total reconstruction;

d) the transmitting Party shall take responsibility for the correctness of personal data and, in case the data appears to be false or incomplete, shall notify the hosting Party thereof, which is obliged to correct or remove the data;

e) the hosting Party and the transmitting Party are obliged to register transmission, receipt and removal of personal data;

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

5. The competent authorities of the Parties may agree to establish lists of persons authorized to make recurring visits connected with implementation of a specific project, program or classified contract. The lists shall contain the data specified in Paragraph 3 of this Article and shall be valid for a period of 12 months. Once such lists have been approved by the competent authorities of the Parties, the dates of the visits shall be arranged directly between the visiting and hosting authorized bodies, in accordance with conditions agreed upon by them.

6. Subject to Paragraph 2 of Article 6, visits involving access to information classified as ZASTRZEŻONE / შეზღუდული სარგებლობისთვის / RESTRICTED are arranged directly between the visiting and hosting authorized bodies.

ARTICLE 11
BREACH OF SECURITY

1. Breach of security is an act or an omission which is contrary to this Agreement or the national law of the States of the Parties concerning classified information protection.
2. Information on every breach of security or a suspicion thereof concerning classified information transmitted by the originating authorized body or classified information originated as a result of cooperation of the authorized bodies shall be immediately reported to the competent authority of the Party in the State territory of which the breach or suspicion thereof has occurred.
3. Every breach of security or a suspicion thereof shall be investigated pursuant to the national law of the State of the Party in the State territory of which it has occurred.
4. In case of a breach of security referred to in Paragraph 1 of this Article, the competent authority of the Party in the State territory of which the breach has occurred shall inform the competent authority of the other Party in writing about the fact, circumstances of the breach and the outcome of the actions referred to in Paragraph 3 of this Article.
5. The competent authorities of the Parties shall cooperate in the actions referred to in Paragraph 3 of this Article, upon the request of one of them.

ARTICLE 12
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 13
EXPENSES

Each Party shall cover its expenses resulting from the implementation of the provisions of this Agreement, unless agreed otherwise between the competent authorities of the Parties or authorized bodies.

ARTICLE 14
CONSULTATIONS

1. The competent authorities of the Parties shall notify each other of any amendments to national law of their States on the protection of classified information concerning implementation of this Agreement.
2. The competent 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. Each Party shall allow the representatives of the competent authority of the other Party to pay visits to its own State territory to discuss the procedures for the protection of classified information transmitted by the other Party.
4. In order to ensure effective cooperation, which is the objective of this Agreement, and in the scope of authority acknowledged by the national law of the States of their Parties, the competent authorities of the Parties may, if necessary, conclude written detailed technical or organizational arrangements.

ARTICLE 15
SETTLEMENT OF DISPUTES

1. Any disputes concerning the interpretation or implementation of this Agreement shall be settled by direct consultations between the competent authorities of the Parties.
2. If settlement of a dispute cannot be reached in the manner referred to in Paragraph 1 of this Article, such a dispute shall be settled through diplomatic channels.

ARTICLE 16
RELATION TO OTHER AGREEMENTS

From the date this Agreement enters into force, Article 3 of the Agreement between the Government of the Republic of Poland and the Government of Georgia on the cooperation in the fight against organized crime and other types of crime, done at Tbilisi on 31 May 2007, shall cease to be applied. Classified information which has been or is to be exchanged on the basis of the Agreement mentioned above, shall be protected according to the provisions of this Agreement.

ARTICLE 17
FINAL PROVISIONS

1. This Agreement shall enter into force on the first day of the second month following the date of the receipt of the last diplomatic note, by which the Parties notify each other on the completion of their internal procedures necessary for the entry into force of this Agreement.
2. This Agreement may be amended by mutual written consent of both Parties. Such amendments shall be formed as a separate document that shall constitute an integral part of this Agreement, and shall enter into force in accordance with the provisions of Paragraph 1 of this Article.

3. This Agreement is concluded for an unlimited period of time. It may be terminated at any time by either Party by giving written notice through diplomatic channels 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 of this Agreement all classified information exchanged under this Agreement shall be either destroyed or returned in accordance with Article 9 no later than this Agreement expires in accordance with Paragraph 3 of this Article.

Done at ..Tbilisi..... on .8...October...2015..... in two original copies, each in the Polish, Georgian 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 GEORGIA
T. Szmoniak	

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 27 czerwca 2016 r.

Prezydent Rzeczypospolitej Polskiej: *A. Duda*

L.S.

Prezes Rady Ministrów: *B. Szydło*