Warszawa, dnia 12 kwietnia 2023 r.

Poz. 677

UMOWA

między Rządem Rzeczypospolitej Polskiej a Rządem Mongolii o wzajemnej ochronie informacji niejawnych w dziedzinie obronności,

podpisana w Warszawie dnia 8 stycznia 2019 r.

W imieniu Rzeczypospolitej Polskiej

PREZYDENT RZECZYPOSPOLITEJ POLSKIEJ

podaje do powszechnej wiadomości:

Dnia 8 stycznia 2019 roku w Warszawie została podpisana Umowa między Rządem Rzeczypospolitej Polskiej a Rządem Mongolii o wzajemnej ochronie informacji niejawnych w dziedzinie obronności, w następującym brzmieniu:

UMOWA

między Rządem Rzeczypospolitej Polskiej a Rządem Mongolii o wzajemnej ochronie informacji niejawnych w dziedzinie obronności

Rząd Rzeczypospolitej Polskiej i Rząd Mongolii,

zwane dalej „Stronami",

mając na uwadze konieczność zagwarantowania ochrony wszystkich informacji, które zostały zakwalifikowane jako informacje niejawne zgodnie z prawem krajowym jednej ze Stron i przekazane drugiej Stronie lub powstały w wyniku współpracy,

kierując się w tym celu zamiarem przyjęcia regulacji w zakresie ochrony informacji niejawnych w dziedzinie obronności, które znajdą zastosowanie w odniesieniu do wszelkiej wspólnej działalności związanej z wymianą informacji niejawnych,

z zastrzeżeniem poszanowania norm prawa międzynarodowego i prawa krajowego Stron, kierując się zasadami równości, wzajemności i obustronnych korzyści,

uzgodniły, co następuje:

ARTYKUŁ 1
PRZEDMIOT UMOWY

1. Przedmiotem niniejszej Umowy jest zapewnienie ochrony informacjom niejawnym wytwarzanym w wyniku współpracy lub wymienianym między Stronami.
2. Niniejsza Umowa ma zastosowanie do wszelkich kontraktów lub umów dotyczących informacji niejawnych, realizowanych bądź zawieranych między Stronami oraz do wszelkich działań realizowanych między nimi.

ARTYKUŁ 2
DEFINICJE

W rozumieniu niniejszej Umowy następujące definicje oznaczają:

1) **informacje niejawne** – informacje wyrażone w dowolnej formie, niezależnie od nośnika i sposobu ich utrwalenia, w tym przedmioty lub dowolne ich części, będące także w trakcie ich opracowywania, które zostały zakwalifikowane, zgodnie z prawem krajowym każdej ze Stron, jako wymagające ochrony przed nieuprawnionym ujawnieniem;
2) **właściwe organy** – organy wskazane w artykule 4 niniejszej Umowy, które są odpowiedzialne za ochronę informacji niejawnych i wykonywanie postanowień niniejszej Umowy dla każdej ze Stron;
3) **upoważnione podmioty** – określone w prawie krajowym każdej ze Stron osoby fizyczne, osoby prawne oraz inne jednostki organizacyjne, właściwe do wytwarzania, przekazywania, otrzymywania, przechowywania, ochrony i wykorzystywania informacji niejawnych;
4) **kontrakt niejawny** – umowę, która zawiera informacje niejawne lub której realizacja wiąże się z dostępem do takich informacji, bądź ich wytworzeniem;
5) **kontrahent** – osobę fizyczną, osobę prawną albo inną jednostkę organizacyjną, podlegającą prawu krajowemu jednej ze Stron, uprawnioną do zawierania kontraktów niejawnych;

6) **zlecający** – osobę fizyczną, osobę prawną albo inną jednostkę organizacyjną, podlegającą prawu krajowemu jednej ze Stron, uprawnioną do zlecania kontraktów niejawnych;

7) **Strona wytwarzająca** – Stronę, która wytwarza i przekazuje informacje niejawne drugiej Stronie, w tym osobę fizyczną oraz każdy podmiot publiczny lub prywatny znajdujący się pod jej jurysdykcją, upoważniony do wymiany informacji niejawnych;

8) **Strona otrzymująca** – Stronę, która otrzymuje informacje niejawne od drugiej Strony, w tym osobę fizyczną oraz każdy podmiot publiczny lub prywatny znajdujący się pod jej jurysdykcją, upoważniony do wymiany informacji niejawnych;

9) **Strona trzecia** – państwo, w tym wszelkie podmioty publiczne lub prywatne znajdujące się pod jego jurysdykcją, lub organizację międzynarodową, niebędące Stroną niniejszej Umowy;

10) **poświadczenie bezpieczeństwa** – dokument wydany zgodnie z prawem krajowym przez właściwy organ lub inny uprawniony podmiot jednej ze Stron, który potwierdza, że osoba fizyczna została poddana postępowaniu sprawdzającemu i jest uprawniona do dostępu do informacji niejawnych;

11) **świadectwo bezpieczeństwa przemysłowego** – dokument wydany zgodnie z prawem krajowym przez właściwy organ lub inny uprawniony podmiot jednej ze Stron, który potwierdza, że kontrahent posiada zdolność do ochrony informacji niejawnych.

ARTYKUŁ 3
KLAUZULE TAJNOŚCI

1. Informacjom niejawnym przyznaje się odpowiednią do ich treści klauzulę tajności, zgodnie z prawem krajowym Strony wytwarzającej. Strona otrzymująca gwarantuje co najmniej równorzędny poziom ochrony otrzymanych informacji niejawnych, zgodnie z postanowieniami ustępu 3.

2. Klauzula tajności jest zmieniana lub znoszona wyłącznie przez upoważniony podmiot, który ją nadał. Strona otrzymująca jest pisemnie informowana o każdym przypadku zmiany lub zniesienia klauzuli tajności wcześniej otrzymanych informacji niejawnych.
3. Strony uzgadniają, że niżej wymienione klauzule tajności są równorzędne:

RZECZPOSPOLITA POLSKA	**MONGOLIA**	**ODPOWIEDNIK W JĘZYKU ANGIELSKIM**
ŚCIŚLE TAJNE	МАШ НУУЦ	TOP SECRET
TAJNE	НУУЦ	SECRET
POUFNE	АЛБАН ХЭРЭГЦЭЭНД	CONFIDENTIAL
ZASTRZEŻONE	ХЯЗГААРЛАГДМАЛ	RESTRICTED

ARTYKUŁ 4
WŁAŚCIWE ORGANY

1. W rozumieniu niniejszej Umowy właściwymi organami są:
   1) w Rzeczypospolitej Polskiej: Szef Agencji Bezpieczeństwa Wewnętrznego;
   2) w Mongolii: Ministerstwo Obrony.
2. Strony poinformują się drogą dyplomatyczną o zmianach właściwych organów, o których mowa w ustępie 1, lub zmianach ich właściwości.

ARTYKUŁ 5
ZASADY OCHRONY INFORMACJI NIEJAWNYCH

1. Strony podejmują wszelkie działania określone w niniejszej Umowie, zgodnie z prawem krajowym każdej ze Stron, w celu ochrony informacji niejawnych

wytwarzanych lub przekazywanych w wyniku wspólnej działalności Stron lub upoważnionych podmiotów, w tym także wytworzonych w związku z realizacją kontraktów niejawnych.

2. Strona otrzymująca wykorzystuje informacje niejawne wyłącznie w celach, dla których zostały one przekazane.
3. Informacje niejawne są udostępniane tylko tym osobom, których zadania wymagają zapoznania się z nimi i które zgodnie z prawem krajowym Strony otrzymującej zostały upoważnione do dostępu do nich.
4. Strona otrzymująca nie udostępnia informacji, o których mowa w ustępie 1, Stronie trzeciej bez uprzedniej pisemnej zgody Strony wytwarzającej.

ARTYKUŁ 6
POŚWIADCZENIA BEZPIECZEŃSTWA ORAZ ŚWIADECTWA BEZPIECZEŃSTWA PRZEMYSŁOWEGO

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 / АЛБАН ХЭРЭГЦЭЭНД / CONFIDENTIAL lub wyższej zlecający składa wniosek do właściwego organu swojej Strony w celu wystąpienia do właściwego organu drugiej Strony, z prośbą o wydanie pisemnego zaświadczenia, że kontrahent posiada ważne świadectwo bezpieczeństwa przemysłowego odpowiednie do klauzuli informacji niejawnych, do których będzie miał dostęp.

2. Wydanie zaświadczenia, o którym mowa w ustępie 1, jest równoznaczne z gwarancją, że zostały przeprowadzone czynności niezbędne do stwierdzenia, że kontrahent spełnia warunki w zakresie ochrony informacji niejawnych określone w prawie krajowym Strony, na terytorium państwa której posiada siedzibę.
3. Informacje niejawne nie są udostępniane kontrahentowi do czasu uzyskania zaświadczenia, o którym mowa w ustępie 1.
4. 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 kieruje ją do właściwego organu Strony kontrahenta.
6. Realizacja kontraktu niejawnego w części związanej z dostępem do informacji niejawnych jest możliwa po spełnieniu przez kontrahenta warunków niezbędnych do ochrony informacji niejawnych, zgodnie z instrukcją bezpieczeństwa przemysłowego.
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 / ХЯЗГААРЛАГДМАЛ / RESTRICTED oraz POUFNE / АЛБАН ХЭРЭГЦЭЭНД / 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 informacji niejawnych, jeżeli spełnione są wymogi bezpieczeństwa określone prawem krajowym Strony przekazującej, dopuszcza się przewóz osobisty informacji niejawnych o klauzuli ZASTRZEŻONE / ХЯЗГААРЛАГДМАЛ / RESTRICTED oraz POUFNE / АЛБАН ХЭРЭГЦЭЭНД / CONFIDENTIAL.
4. Właściwe organy Stron mogą ustalić inne sposoby przekazywania informacji niejawnych zapewniające ochronę przed ich nieuprawnionym ujawnieniem.
5. Strona otrzymująca 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 jest ograniczana do liczby wymaganej dla celów służbowych. Przetłumaczone informacje będą opatrzone adnotacją w języku tłumaczenia, wskazującą, iż zawierają one informacje niejawne otrzymane od Strony wytwarzającej.
2. Informacje niejawne o klauzuli ŚCIŚLE TAJNE / МАШ НУУЦ / TOP SECRET są powielane i tłumaczone tylko po uprzednim uzyskaniu pisemnego zezwolenia wydanego przez Stronę wytwarzającą.

ARTYKUŁ 10
NISZCZENIE INFORMACJI NIEJAWNYCH

1. Z zastrzeżeniem ustępu 2, informacje niejawne są niszczone zgodnie z prawem krajowym Strony otrzymującej w taki sposób, aby uniemożliwić ich częściowe lub całkowite odtworzenie.
2. Informacje niejawne o klauzuli ŚCIŚLE TAJNE / МАШ НУУЦ / TOP SECRET nie są niszczone. Takie informacje są zwracane Stronie wytwarzającej.

ARTYKUŁ 11
WIZYTY

1. Obywatelom państwa jednej Strony przybywającym z wizytą na terytorium państwa drugiej Strony, z zastrzeżeniem ustępów 5 i 6, 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 otrzymuje wniosek w sprawie wizyty od właściwego organu drugiej Strony.
3. We wniosku, o którym mowa w ustępie 2, zamieszcza się informacje o:
   1) celu, terminie i programie wizyty;
   2) imieniu i nazwisku, dacie i miejscu urodzenia, obywatelstwie i numerze paszportu lub innego dokumentu tożsamości osoby przybywającej z wizytą;
   3) stanowisku służbowym osoby przybywającej z wizytą wraz z nazwą podmiotu, który reprezentuje;
   4) poziomie i dacie ważności poświadczenia bezpieczeństwa posiadanego przez osobę przybywającą z wizytą;

5) nazwie i adresie odwiedzanego podmiotu;

6) imieniu i nazwisku oraz stanowisku służbowym osoby przyjmującej.

Ponadto przedmiotowy wniosek zawiera datę, podpis oraz oficjalną pieczęć właściwego organu.

4. Do ochrony danych osobowych, o których mowa w ustępie 3, przekazywanych w związku z postanowieniami ustępów 1, 5 oraz 6, stosuje się, z uwzględnieniem prawa krajowego każdej ze Stron, następujące postanowienia:

1) otrzymane przez Stronę przyjmującą wizytę dane osobowe są wykorzystywane wyłącznie w celu określonym przez Stronę je przekazującą i na warunkach określonych przez tę Stronę;

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

3) w przypadku przekazania danych, których nie wolno było przekazać zgodnie z prawem krajowym Strony przekazującej dane osobowe, Strona ta zawiadamia o tym Stronę przyjmującą wizytę; Strona przyjmująca wizytę jest zobowiązana do usunięcia tych danych w sposób uniemożliwiający ich częściowe lub całkowite odtworzenie;

4) Strona przekazująca dane osobowe odpowiada za ich merytoryczną poprawność, a w razie przekazania danych nieprawdziwych lub niekompletnych, 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 przekazywania, otrzymywania i usuwania tych danych;

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 informacje określone w ustępie 3 i są ważne przez okres dwunastu miesięcy. Po zatwierdzeniu takich list przez właściwe organy terminy wizyt uzgadniane są bezpośrednio między podmiotem wysyłającym a podmiotem przyjmującym wizytę, zgodnie z ustalonymi warunkami.
6. Wizyty związane z dostępem do informacji niejawnych o klauzuli ZASTRZEŻONE / ХЯЗГААРЛИАГДМАЛ / RESTRICTED są uzgadniane bezpośrednio między podmiotem wysyłającym a podmiotem przyjmującym wizytę.

ARTYKUŁ 12
NARUSZENIE REGULACJI DOTYCZĄCYCH WZAJEMNEJ OCHRONY INFORMACJI NIEJAWNYCH

1. Naruszeniem regulacji dotyczących ochrony informacji niejawnych jest działanie lub zaniechanie sprzeczne z niniejszą Umową lub prawem krajowym Stron w zakresie dotyczącym ochrony informacji niejawnych, w tym również nieuprawnione ujawnienie informacji niejawnych.
2. Informacja o każdym przypadku naruszenia lub o podejrzeniu naruszenia regulacji dotyczących ochrony informacji niejawnych Strony wytwarzającej lub informacji niejawnych wytworzonych w wyniku wspólnego działania Stron jest niezwłocznie przekazywana właściwemu organowi Strony, na terytorium państwa której miało miejsce takie naruszenie lub zaistniało jego podejrzenie.
3. Każdy przypadek naruszenia lub podejrzenia naruszenia regulacji dotyczących ochrony informacji niejawnych jest wyjaśniany zgodnie z prawem krajowym Strony, na terytorium państwa której zdarzenie miało miejsce.

4. W przypadku naruszenia regulacji dotyczących ochrony informacji niejawnych, właściwy organ Strony, na terytorium państwa której naruszenie miało miejsce, niezwłocznie pisemnie informuje właściwy organ drugiej Strony o tym fakcie, o okolicznościach naruszenia oraz o 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 będą posługiwać się swoimi językami urzędowymi lub językiem angielskim. W przypadku stosowania języków urzędowych, Strony zobowiązują się przekazać także 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 poinformują się wzajemnie o wszelkich zmianach w prawie krajowym Stron 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 omawiania 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 w prawie krajowym każdej ze Stron, 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 Stron.
2. W przypadku nieosiągnięcia porozumienia w drodze konsultacji określonych w ustępie 1, spory będą rozstrzygane drogą dyplomatyczną i nie będą przedkładane Stronie trzeciej.

ARTYKUŁ 17
POSTANOWIENIA KOŃCOWE

1. Niniejsza Umowa podlega przyjęciu zgodnie z prawem krajowym każdej ze Stron, co zostanie stwierdzone w drodze wymiany not. Umowa wejdzie w życie w pierwszym dniu drugiego miesiąca, który nastąpi po dniu otrzymania noty późniejszej.
2. Niniejsza Umowa może zostać zmieniona na podstawie wspólnej pisemnej zgody obu Stron. Takie zmiany wejdą w życie zgodnie z postanowieniami ustępu 1.

3. Niniejsza Umowa zawarta jest na czas nieokreślony. Może być ona wypowiedziana w drodze notyfikacji przez każdą ze Stron. W takim przypadku utraci moc po upływie sześciu miesięcy od dnia otrzymania noty informującej o wypowiedzeniu.
4. W przypadku wypowiedzenia niniejszej Umowy, informacje niejawne przekazane lub wytworzone na jej podstawie będą nadal chronione zgodnie z jej postanowieniami.

Podpisano w WARSZAWIE dnia 08 STYCZNIA 2019 roku w dwóch jednobrzmiących egzemplarzach, każdy w językach polskim, mongolskim i angielskim, przy czym wszystkie teksty posiadają jednakową moc. W przypadku rozbieżności przy ich interpretacji, tekst w języku angielskim będzie uważany za rozstrzygający.

Z UPOWAŻNIENIA RZĄDU RZECZYPOSPOLITEJ POLSKIEJ

Z UPOWAŻNIENIA RZĄDU MONGOLII

“БАТЛАН ХАМГААЛАХ САЛБАРЫН НУУЦ МЭДЭЭ МЭДЭЭЛЛИЙГ ХАРИЛЦАН СОЛИЛЦОХ, ХАМГААЛАХ ТУХАЙ БҮГД НАЙРАМДАХ ПОЛЬШ УЛСЫН ЗАСГИЙН ГАЗАР, МОНГОЛ УЛСЫН ЗАСГИЙН ГАЗАР ХООРОНДЫН ХЭЛЭЛЦЭЭР”

Бүгд Найрамдах Польш Улсын Засгийн газар, Монгол Улсын Засгийн газар (цаашид “Талууд” гэх)

Аль нэг Талуудын дотоодын хууль тогтоомжид нийцүүлэн нууцалсан болон нөгөө талд дамжуулсан эсхүл хамтын ажиллагааны үед бий болсон бүх төрлийн нууцын зэрэглэлтэй мэдээллийг хамгаалах шаардлагатай баталгааг хүндэтгэн үзэж,

Батлан хамгаалах салбарын нууцын зэрэглэлтэй мэдээллийг хоёр тал харилцан солилцохтой холбогдох тус нууцын зэрэглэлтэй мэдээллийн үйлчлэх хүрээний дүрэм журмыг чиглэл болгон,

Олон улсын эрх зүй болон Талуудын дотоодын хууль тогтоомжийг дээдлэн, тэгш эрх, хамтран ажиллах болон харилцан ашигтай байх зарчмыг удирдлага болгон дараахь зүйлийг хэлэлцэн тохиров. Үүнд:

1 ДҮГЭЭР ЗҮЙЛ
ХЭЛЭЛЦЭЭРИЙН ЗОРИЛГО

1. Энэхүү хэлэлцээрийн зорилго нь Талууд харилцан боловсруулсан эсхүл солилцсон нууцын зэрэглэлтэй мэдээллийг хамгаалах явдал юм.

2. Энэхүү хэлэлцээр нь Талуудын хооронд үүрэг болгосон аливаа үйл ажиллагааг зохион байгуулсан эсхүл дүгнэсэн талаар нууцын зэрэглэлтэй мэдээлэл агуулсан бүх гэрээ, хэлэлцээрт үйлчилнэ.

2 ДУГААР ЗҮЙЛ
НЭР ТОМЪЁО

Энэхүү хэлэлцээрийг хэрэгжүүлэхийн тулд:

1) “Нууцын зэрэглэлтэй мэдээлэл” гэдэг нь Талуудын дотоодын хууль тогтоомжийн дагуу зөвшөөрөлгүй задруулахаас хамгаалагдсан ямарч хэлбэрээр илэрхийлсэн тээвэрлэгч Талуудын дотоодын хууль тогтоомжийн дагуу;

2) “Эрх бүхий байгууллага” гэдэг нь энэхүү хэлэлцээрийн 4 дүгээр зүйлд заасан Талуудын эрх бүхий байгууллага тус хэлэлцээрийг хэрэгжүүлэх болон нууцын зэрэглэлтэй мэдээллийн аюулгүй байдлыг хангах үүрэгтэй;

3) “Бүрэн эрхт нэгж” гэдэг нь нууцын зэрэглэлтэй мэдээллийг боловсруулах, шилжүүлэх, хүлээн авах, хадгалах, хамгаалах болон ашиглах эрх бүхий Талуудын дотоодын хуулиар тодорхойлогдсон хувь хүн, хуулийн этгээд эсхүл бусад байгууллагыг хэлнэ;

4) “Нууцын зэрэглэлтэй гэрээ” гэдэг нь нууцын зэрэглэлтэй мэдээлэл эсхүл тус мэдээллийг боловсруулах болон түүнд нэвтрэх үйл явцыг агуулсан гэрээг хэлнэ;

5) “Гэрээлэгч” гэдэг нь аль нэг Талын хууль тогтоомжийн хүрээнд Нууцын зэрэглэлтэй гэрээг эцэслэн байгуулах хувь хүн, хуулийн этгээд эсхүл бусад байгууллага;

6) “Эрх мэдэлтэн” гэдэг нь аль нэг Талын хууль тогтоомжийн хүрээнд Нууцын зэрэглэлтэй гэрээг байгуулахыг зөвшөөрөх эрх бүхий хувь хүн, хуулийн этгээд эсхүл бусад байгууллага;

7) “Мэдээлэгч Тал” гэдэг нь хуулийн дагуу нууцын зэрэглэлтэй мэдээллийг боловсруулах болон нөгөө Талдаа шилжүүлэх Тал болон хувь хүнийг хэлэх бөгөөд нууцын зэрэглэлтэй мэдээлэл солилцох эрх олгогдсон нийтийн эсхүл хувийн байгууллага мөн хамаарна;

8) “Хүлээн авагч Тал” гэдэг нь шилжүүлэгч Талаас ирсэн нууцын зэрэглэлтэй мэдээллийг хүлээн авч буй Тал болон хувь хүнийг хэлэх бөгөөд нууцын зэрэглэлтэй мэдээлэл солилцох эрх олгогдсон нийтийн эсхүл хувийн байгууллага мөн хамаарна;

9) “Гуравдагч этгээд” гэдэг нь энэхүү хэлэлцээрийн оролцогч биш Улс болон Олон улсын байгууллага, мөн нийтийн эсхүл хувийн байгууллага мөн хамаарна;

10) “Хувь хүний нууцын баталгаа” гэдэг нь аль нэг Талын холбогдох дотоодын хууль тогтоомжид заасны дагуу эрх бүхий байгууллага эсхүл албан тушаалтнаас хэн нэг хүнд нууцын зэрэглэлтэй мэдээллийг үзэхийг зөвшөөрөн олгож буй баримт бичиг;

11) “Аюулгүй байгууламж” гэдэг нь аль нэг Талын холбогдох дотоодын хууль тогтоомжид заасны дагуу эрх бүхий байгууллага болон албан тушаалтнаас олгогдсон “гэрээлэгч нууцын зэрэглэлтэй мэдээллийг хамгаалах чадамжтай” эсэхийг баталсан баталгаа юм.

3 ДУГААР ЗҮЙЛ
НУУЦЫН ЗЭРЭГЛЭЛИЙН ТҮВШИН

1. Нууцын зэрэглэлтэй мэдээлэл боловсруулсан Талын дотоодын хууль тогтоомжийг мөрдлөг болгон түүний агууламжаас хамааран аюулгүйн нууцлалын зэргийг олгоно. Хүлээн авагч Тал нь 3 дугаар зүйлд заасны дагуу хүлээн авсан нууцын зэрэглэлтэй мэдээлэлд адил тэнцүү аюулгүйн зэргийг тогтоох ёстой.

2. Нууцлалын зэргийн түвшинг зөвхөн бүрэн эрхт нэгж /нууцын зэрэг олгосон Тал/-ийн зөвшөөрлөөр өөрчилж, хасч болно. Хүлээн авагч Тал өмнө нь хүлээн авсан нууцын зэрэглэлтэй мэдээллийн нууцын зэрэглэлийн өөрчлөлт, хасалтын талаар бичгээр мэдээлүүлсэн байна.

3. Талууд нууцын зэрэглэлтэй мэдээллийн түвшинг дараахь байдлаар адил тэнцүү гэж тодорхойлно:

БҮГД НАЙРАМДАХ ПОЛЬШ УЛС	МОНГОЛ УЛС	АДИЛТГАЛ /АНГЛИ ХЭЛЭЭР/
ŚCIŚLE TAJNE	МАШ НУУЦ	TOP SECRET
TAJNE	НУУЦ	SECRET
POUFNE	АЛБАН ХЭРЭГЦЭЭНД	CONFIDENTIAL
ZASTRZEŻONE	ХЯЗГААРЛАГДМАЛ	RESTRICTED

4 ДҮГЭЭР ЗҮЙЛ
ЭРХ БҮХИЙ БАЙГУУЛЛАГА

1. Аюулгүй байдлыг хангах дараахь эрх бүхий байгууллага хэлэлцээрийн хэрэгжилтийг зохион байгуулна:

(1) БНПУ-ыг төлөөлж:

Дотоодын аюулгүй байдлын агентлаг

(2) Монгол Улсыг төлөөлж:

Монгол Улсын Батлан хамгаалах яам

2. Талууд нь эрх бүхий байгууллага /1 дүгээр заалтад хамааралтай/, эсвэл эрх мэдлийн өөрчлөлтийн талаар дипломат шугамаар мэдэгдэж байна.

5 ДУГААР ЗҮЙЛ
НУУЦЫН ЗЭРЭГЛЭЛТЭЙ МЭДЭЭЛЛИЙГ ХАМГААЛАХ ЗАРЧИМ

1. Талуудын дотоодын хуулийн дагуу Талууд хамтын ажиллагааны үр дүнд боловсруулсан эсхүл солилцсон нууцын зэрэглэлтэй мэдээллийг энэхүү хэлэлцээрийн хүрээнд нууцын зэрэглэлтэй мэдээллийг хамгаалахад чиглэсэн бүхий л арга хэмжээг авч хэрэгжүүлэх ёстой.

2. Хүлээн авагч Тал нууцын зэрэглэлтэй мэдээллийг зөвхөн солилцсон зорилгын хүрээнд ашиглана.

3. Ажлын чиг үүрэг, албан тушаалаар нийцсэн хувь хүн нууцын зэрэглэлтэй материалд нэвтрэх бөгөөд энэ нь хүлээн авч буй Талын дотоодын хууль тогтоомжийн дагуу эрх нь олгогдсон байна.

4. Хүлээн авагч Тал 1 дүгээр зүйлийн дагуу мэдээлэгч Талын бичгээр гаргасан зөвшөөрөлгүйгээр нууцын зэрэглэлтэй мэдээллийг аливаа гуравдагч этгээдэд задлахыг хориглоно.

6 ДУГААР ЗҮЙЛ
“ХУВЬ ХҮНИЙ НУУЦЫН БАТАЛГАА” БА “АЮУЛГҮЙ БАЙГУУЛАМЖ”

Энэхүү хэлэлцээрийн хүрээнд, Талууд хувь хүний нууцын баталгаа болон аюулгүй байгууламжийг өөрийн дотоодын хууль тогтоомжийн дагуу хүлээн зөвшөөрсөн байх ёстой.

7 ДУГААР ЗҮЙЛ
НУУЦ ГЭРЭЭ

1. POUFNE / АЛБАН ХЭРЭГЦЭЭНД / CONFIDENTIAL зэрэглэлтэй эсхүл түүнээс дээш нууцын зэрэглэлтэй нууц гэрээг байгуулахаас өмнө, эрх бүхий албан тушаалтан нь нөгөө Талын эрх бүхий байгууллагаас гэрээлэгч нь нууцын зэрэглэлтэй мэдээлэлд нэвтрэх эрх бүхий этгээд гэсэн батламжийг олгохыг шаардана.

2. Тухай улсын газар нутагт байрлаж буй Талын дотоодын хууль тогтоомжид тодорхойлсон Гэрээлэгч нь нууцын зэрэглэлтэй мэдээллийг хамгаалах хүрээнд шалгуур үзүүлэлтийг хангасан шаардлагатай арга хэмжээг авсан талаарх баталгаа нь 1 дүгээр зүйлийн дагуу гаргасан батламжтай адил тэнцүү хүчинтэй байна.

3. Нууцын зэрэглэлтэй мэдээлэлд гэрээлэгч нь 1 дүгээр зүйлд заасан батламжийг хүлээж авах хүртэл нэвтрэх эрхгүй.

4. Эрх мэдэлтэн нь гэрээлэгчид нууц гэрээний салшгүй бүрдэл болох нууц гэрээг хэрэгжүүлэхэд шаардлагатай аюулгүй ажиллагааны зааварчилгааг шилжүүлэн өгнө. Энэ зааварчилгаанд аюулгүй байдлын шаардлагын заалтууд багтсан байна. Ялангуяа:

(а) нууц гэрээтэй холбоотой нууцын зэрэглэлтэй мэдээллийн жагсаалтыг түүний нууцын зэрэглэлийн түвшингийн хамт;

(б) нууц гэрээний гүйцэтгэлийн үед боловсруулсан мэдээлэлд өгөх нууцын зэрэглэлийн журам.

5. Эрх мэдэлтэн нь аюулгүй ажиллагааны зааварчилгааг өөрийн эрх бүхий байгууллагад санал болгосноор тэр нь гэрээлэгчийн эрх бүхий байгууллагад дамжуулна.

6. Нууцын зэрэглэлтэй мэдээлэлд нэвтрэхтэй холбогдолтой нууц гэрээг хэрэгжүүлэхэд гэрээлэгч аюулгүйн ажиллагааны зааварчилгааны дагуу нууцын зэрэглэлтэй мэдээллийг хамгаалах шаардлага шалгуурыг хангах боломжтой нөхцлийг бүрдүүлэх ёстой.

7. Туслах гэрээлэгч нь үндсэн гэрээлэгчийн адилаар нууцын зэрэглэлтэй мэдээллийг хамгаалах нөхцлүүдийг дагана.

8 ДУГААР ЗҮЙЛ
НУУЦЫН ЗЭРЭГЛЭЛТЭЙ МЭДЭЭЛЛИЙГ ШИЛЖҮҮЛЭХ

1. Нууцын зэрэглэлтэй мэдээлэл нь дипломат шугамаар шилжүүлэгдэнэ.

2. Мэдээлэл нууцын зэргээрээ ZASTRZEŻONE / ХЯЗГААРЛАГДМАЛ / RESTRICTED болон POUFNE / АЛБАН ХЭРЭГЦЭЭНД / CONFIDENTIAL ангилагдсан үед шилжүүлэгч Талын үндэсний хууль тогтоомжийн дагуу эрх олгогдсон шуудангаар шилжүүлэгдэж болно.

3. Бусад шилжүүлгийн төрлийг ашиглах боломжгүй болон шилжүүлэгч Талын дотоодын хууль тогтоомжоор аюулгүйн шаардлагыг хангасан тохиолдолд хувийн шуудангаар ZASTRZEŻONE / ХЯЗГААРЛАГДМАЛ / RESTRICTED болон POUFNE / АЛБАН ХЭРЭГЦЭЭНД / CONFIDENTIAL зэрэглэлийн мэдээллийг шилжүүлэхийг зөвшөөрнө.

4. Талуудын эрх бүхий байгууллагууд нууцын зэрэглэлтэй мэдээллийг шилжүүлэх бусад төрлийг тохиролцож болох бөгөөд зөвшөөрөлгүй задруулахаас хамгаална.

5. Хүлээн авагч Тал нууцын зэрэглэлтэй мэдээллийг хүлээн авснаа бичгээр баталгаажуулна.

9 ДҮГЭЭР ЗҮЙЛ
НУУЦЫН ЗЭРЭГЛЭЛТЭЙ МЭДЭЭЛЛИЙГ ДАХИН БОЛОВСРУУЛАХ, ОРЧУУЛАХ

1. Нууцын зэрэглэлтэй мэдээллийн дахин боловсруулалт болон орчуулалт нь Талуудын дотоодын хууль тогтоомжийн дагуу үйлдэгдсэн байна. Дахин боловсруулсан болон орчуулсан мэдээлэл нь эх мэдээллийн

адил нууцлалтай байна. Албан хэрэгцээнд зориулан шаардлагатай цөөн хэмжээнд олшруулах, хувилсан хуулбар бүрт үндсэн материал дээрхтэй адил хэмжээнд нууцын тэмдэглэлгээ хийх болон хамгаалалтад авна. Орчуулсан мэдээлэлд тухайн хэл дээр нууцын зэрэглэлтэй мэдээлэл гэдгийг илтгэх тохиромжтой тэмдэглэгээг хийсэн байх ёстой.

2. ŚCIŚLE TAJNE / МАШ НУУЦ / TOP SECRET зэрэглэлийн мэдээллийг зөвхөн боловсруулсан Талын бичгээр гаргасан зөвшөөрлийг авсны дараа дахин боловсруулах болон орчуулна.

10 ДУГААР ЗҮЙЛ
НУУЦЫН ЗЭРЭГЛЭЛТЭЙ МЭДЭЭЛЛИЙГ УСТГАХ

1. Хүлээн авагч Талын дотоодын хууль тогтоомжийн дагуу 2 дугаар хэсэгт заасан Нууцын зэрэглэлтэй мэдээллийг хэсэгчилэн болон бүхлээр нь устгаж болно.

2. ŚCIŚLE TAJNE / МАШ НУУЦ / TOP SECRET зэрэглэлд хамааралтай мэдээллийг устгаж болохгүй бөгөөд боловсруулсан Талд нь буцаах ёстой.

11 ДҮГЭЭР ЗҮЙЛ
АЙЛЧЛАЛ, УУЛЗАЛТ

1. Айлчлал хийж буй Талын албан тушаалтан хүлээн авч буй Талын бичгээр өгсөн урьдчилсан зөвшөөрлийн дагуу нууцын зэрэглэлтэй мэдээлэлд нэвтрэнэ.

Талууд харилцан тохиролцсоны үндсэн дээр аль нэг Талын албан тушаалтан нууцын зэрэглэлтэй мэдээлэл хадгалагдаж буй байгууламжийг үзэх тохиолдолд хүлээн авч буй Талын бичгээр өгсөн урьдчилсан зөвшөөрлийн дагуу айлчлалыг зохион байгуулна. Ийнхүү айлчлахдаа мөрдөх ёстой дүрэм, журмыг даган биелүүлнэ.

2. Айлчлал нь дор хаяж 30 хоногийн өмнө төлөвлөгдсөн байх ба яаралтай тохиолдолд хүлээн авагч Тал нь айлчлалын хүсэлтийг нөгөө

Талын бүрэн эрхт байгууллагаас хүлээн авсан байх ёстой.

3. Айлчлалын хүсэлт нь дараах мэдээллүүдийг агуулна:

а. Айлчлалын зорилго, хугацаа ба хөтөлбөр

б. Зочны овог нэр, төрсөн огноо, төрсөн газар, яс үндэс ба паспортын дугаар

в. Зочны төлөөлөх байгууллагын нэр, зочны албан тушаал

г. Зочны нууцын зэрэглэлтэй мэдээ, мэдээлэлтэй танилцах эрх түүний зэрэглэл, хүчинтэй байх

д. Зочны айлчлах байгууллагын нэр, хаяг

е. Зочны албан тушаал, овог нэр, түүнээс гадна эрх бүхий байгууллагын огноо, албан тушаалтны гарын үсэг, тамгатай байх ёстой.

4. Хувийн мэдээллийг хамгаалахын тулд доорх заалтуудыг дагаж мөрдөх ба талуудын үндэсний хуулийг багтаасан байдаг.

а. Хувь хүний мэдээлэл нь явуулсан Талын зорилго зорилтын хүрээнд ашиглагдана.

б. Хувийн мэдээлэл нь хүлээн авагч талд шаардлагатай үйл явцыг гүйцэтгэх хугацаанд хадгалагдана.

в. Илгээгдсэн хувийн мэдээлэл нь илгээж буй Талын үндэсний хуулийн эсрэг байх тохиолдолд хүлээн авагч талд мэдээлэн, түүнийг хэсэгчилэн болон бүрэн устгалд оруулна.

г. Хувийн мэдээлэл илгээж буй Тал нь мэдээллийн үнэн зөв байдалд хариуцлага хүлээх ба мэдээлэл нь худал буюу бүрэн бус байх тохиолдолд хүлээн авагч Талд мэдээлэн, засвар болон устгалыг хийлгэнэ.

д. Хувийн мэдээллийг явуулж буй болон хүлээн авагч Талууд шилжүүлэг, хүлээн авалт, устгалыг бүртгэлд оруулна.

е. Хувийн мэдээллийг явуулж буй болон хүлээн авч байгаа Талууд тус мэдээллийг судлах үйл явцад мэдээллийг алдах, үрэгдүүлэх, устгахаас хамгаалах хариуцлагыг хүлээнэ.

5. Эрх бүхий байгууллага нь тодорхой төсөл, хөтөлбөр, нууц гэрээтэй

холбоотой дахин айлчлалыг зохион байгуулахаар эрх олгогдсон хүмүүсийн нэрийн жагсаалтыг гаргахаар зөвшилцөлд хүрч болно. Энэ жагсаалт нь 12 сарын хугацаанд хүчинтэй байна. Мөн жагсаалт нь эрх бүхий байгууллагаар баталгаажсан тохиолдолд айлчлалын хугацааг хоёр талын зөвшилцсөн нөхцлийн үр дүнд хийгдэнэ.

6. ZASTRZEŻONE / ХЯЗГААРЛАГДМАЛ / RESTRICTED зэрэглэлийн нууц мэдээлэлд нэвтрэх айлчлал нь айлчилж буй болон хүлээн авах байгууллагын хооронд шууд зохион байгуулагдаж болно.

12 ДУГААР ЗҮЙЛ
НУУЦ МЭДЭЭЛЛИЙГ ХАРИЛЦАН ХАМГААЛАХТАЙ ХОЛБООТОЙ АЮУЛГҮЙН ДҮРЭМ ЖУРМЫГ ЗӨРЧИХ

1. Аюулгүй байдлын зөрчил гэдэг нь нууц мэдээллийг зөвшөөрөлгүй задруулах зэрэг нууц мэдээллийг хамгаалахтай холбоотой Талуудын үндэсний хууль эсвэл энэхүү гэрээтэй зөрчилдөх ямар нэгэн үйл ажиллагаа, алдаа дутагдлыг хэлнэ.

2. Талуудын харилцан хамтын ажиллагааны үр дүнд боловсруулсан нууц мэдээлэл эсвэл нууц мэдээллийг боловсруулж буй Талаас аюулгүй байдлыг зөрчсөн тохиолдол эсвэл сэжигтэй тохиолдол бүрийн талаар нэн даруй тухайн зөрчил буюу сэжигтэй тохиолдол гарсан нутаг дэвсгэр дэх Талын эрх бүхий албан тушаалтанд мэдээлэх ёстой.

3. Аюулгүй байдлын зөрчил бий болсон тохиолдолд уг зөрчил аль улсад тохиолдсоноос хамааран тухайн Талын үндэсний хуулийг мөрдлөг болгон асуудлыг шалган шийдвэрлэнэ.

4. Энэхүү зүйлийн 1 дүгээр заалтын дагуу, аюулгүй байдлын зөрчил бий болсон тохиолдолд тухайн Тал нь болсон баримт, үр дагавар, 3 дугаар заалтын дагуу авсан арга хэмжээг нөгөө Талын эрх бүхий байгууллагуудад бичгээр мэдэгдэнэ.

5. Талуудын эрх бүхий албан тушаалтнууд нь Талуудын аль нэгний хүсэлтээр энэхүү зүйлийн 3 дугаар заалтад заасан үйл ажиллагаанд хамтран оролцоно.

13 ДУГААР ЗҮЙЛ
ХЭЛ

Энэхүү хэлэлцээрийн заалтуудын хэрэгжилтийн хүрээнд Талууд англи хэл болон өөрсдийн улсын албан ёсны хэлийг ашиглана. Хэрэв Талууд өөрсдийн албан ёсны хэлийг ашигласан тохиолдолд нөгөө Талын албан ёсны хэлээр орчуулгыг, эсхүл англи хэлээрх орчуулгыг хавсаргах ёстой.

14 ДҮГЭЭР ЗҮЙЛ
ЗАРДАЛ

Талууд энэхүү хэлэлцээрийн хэрэгжилттэй холбогдон гарах зардлаа өөрсдөө хариуцна.

15 ДУГААР ЗҮЙЛ
ЗӨВЛӨЛДӨХ

1. Энэхүү гэрээний зүйлүүдэд нөлөөлж болохуйц нууц мэдээллийг хамгаалахтай холбогдолтой асуудалд Талууд өөрийн үндэсний хууль тогтоомжид нэмэлт өөрчлөлт оруулсан тохиолдолд Талуудын эрх бүхий байгууллагууд бие биедээ мэдэгдэх ёстой.

2. Энэ гэрээний зүйлүүдийн хэрэгжилт дээр нягт хамтран ажиллах тал дээр талууд бие биедээ хүсэлт гарган, эрх бүхий байгууллагууд хоорондоо зөвшилцөн шийдвэрлэнэ.

3. Талуудын аль аль нь нөгөө Талын дамжуулсан нууц мэдээллийг хамгаалах үйл явцыг хэлэлцэх зорилгоор ирж буй нөгөө талын эрх бүхий байгууллагуудын төлөөлөгчдийн айлчлалыг хүлээн зөвшөөрнө.

4. Эрх бүхий албан тушаалтнууд энэхүү гэрээнд үндэслэн үр дүнтэй хамтын ажиллагааг явуулахын тулд, мөн Талуудын үндэсний хуульд заасан эрх мэдлийн хүрээнд, шаардлагатай тохиолдолд, дэлгэрэнгүй техникийн болон байгууллагын зохицуулалтыг хийхдээ бичгээр үйлдэнэ.

16 ДУГААР ЗҮЙЛ
МАРГААН ШИЙДВЭРЛЭХ

1. Хэлэлцээрийн тайлбар болон хэрэгжилтэд аливаа маргаан гарвал талууд харилцан зөвшилцөж, эв зүйгээр асуудлыг шийдвэрлэнэ.

2. Энэ зүйлийн 1 дэх хэсэгт заасны дагуу зөвшилцөлд хүрч чадахгүй бол маргааныг гуравдагч тал руу шилжүүлэхгүй бөгөөд дипломат замаар шийдвэрлэнэ.

17 ДУГААР ЗҮЙЛ
ТӨГСГӨЛИЙН ЗҮЙЛ

1. Энэхүү хэлэлцээр нь талууд өөрсдийн дотоодын хууль тогтоомжийн хүрээнд хэлэлцээрийг мөрдөх боломжтойг харилцан ноот бичиг солилцсоноор хүчин төгөлдөр үйлчилнэ. Энэхүү хэлэлцээр нь сүүлчийн ноот бичгийг хүлээн авсны дараа сарын эхний өдрөөс эхлэн хүчин төгөлдөр үйлчилж эхэлнэ.

2. Талуудын харилцан бичгээр гаргасан зөвшөөрлийн үндсэн дээр энэхүү Хэлэлцээрт нэмэлт, өөрчлөлт оруулж болно. Тус нэмэлт, өөрчлөлт нь 1 дүгээр хэсэгт заасны дагуу хүчин төгөлдөр үйлчилнэ.

3. Энэхүү хэлэлцээрийг хугацаагүйгээр байгуулав. Тус хэлэлцээрийг аль ч Тал бичгээр гаргасан мэдэгдэл хүргүүлснээр цуцалж болно. Дээрх

тохиолдолд, цуцлах саналыг хүлээн авсан өдрөөс хойш 6 сарын дараа гэрээний хүчин төгөлдөр хугацаа дуусгавар болно.

4. Хэлэлцээрийг цуцалсан тохиолдолд хэлэлцээрийн хугацаанд боловсруулсан болон солилцсон нууцын зэрэглэлтэй мэдээллийн аюулгүй байдлыг хэлэлцээрт заасны дагуу хамгаална.

Энэхүү хэлэлцээрийг 2019 оны ....01..... дугаар сарын 08, Варшав хот..... өдөр, монгол, польш, англи хэлээр хоёр хувь үйлдэв. Бичвэр тус бүр нь адил хүчинтэй байна. Аливаа маргаан гарсан тохиолдолд, англи хэлээрх эх бичвэрийг баримтална.

БҮГД НАЙРАМДАХ ПОЛЬШ УЛСЫН ЗАСГИЙН ГАЗРЫГ ТӨЛӨӨЛЖ

МОНГОЛ УЛСЫН ЗАСГИЙН ГАЗРЫГ ТӨЛӨӨЛЖ

AGREEMENT

between the Government of the Republic of Poland and the Government of Mongolia on the Mutual Protection of Classified Information in the field of defence

The Government of the Republic of Poland and the Government of Mongolia,

hereinafter referred to as the "Parties",

having due regard for necessity of guaranteeing the protection of all information, which has been classified pursuant to the national law of one of the Parties and transmitted to the other Party or originated during the course of cooperation,

being guided by the intention to adopt regulations in the scope of the protection of Classified Information in the field of defence, which are to be binding in relation to any mutual cooperation involving the exchange of such information,

with due respect for the binding rules of the international law and the national law of the Parties,

being guided by the rules of equality, reciprocity and mutual benefits

have agreed as follows:

ARTICLE 1
OBJECTIVE OF THE AGREEMENT

1. The objective of this Agreement is to ensure the protection of Classified Information that is generated or exchanged between the Parties.
2. This Agreement shall be applicable to any contracts or agreements involving Classified Information that will be conducted or concluded between the Parties as well as to any activities undertaken between them.

ARTICLE 2
DEFINITIONS

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

1) **Classified Information** – information expressed in any form, irrespective of the carrier and manner of recording, as well as objects or any parts thereof, also in the process of being generated, which has been classified in accordance with the national law of either Party as requiring protection against unauthorized disclosure;
2) **Competent Authorities** – the authorities referred to in Article 4 of this Agreement, responsible for the protection of Classified Information as well as implementation of the provisions of this Agreement for each of the Parties;
3) **Authorized Bodies** – individuals, legal entities or other forms of organizations defined in the national law of each of the Parties, competent to originate, transmit, receive, store, protect and use Classified Information;
4) **Classified Contract** – a contract that contains Classified Information or performance of which involves access to Classified Information or originating of such information;

5) **Contractor** – an individual, a legal entity or other form of organization under the law of one of the Parties, authorized to conclude Classified Contracts;

6) **Principal** – an individual, a legal entity or other form of organization under the law of one of the Parties, authorized to let Classified Contracts;

7) **Originating Party** – the Party which originates and transmits Classified Information to the other Party, including an individual, as well as any public or private entity under its jurisdiction, authorized to exchange Classified Information;

8) **Recipient Party** – the Party which receives Classified Information from the other Party, including an individual, as well as any public or private entity under its jurisdiction, authorized to exchange Classified Information;

9) **Third Party** – a State, including any public or private entities under its jurisdiction, or an international organization not being a Party to this Agreement;

10) **Personnel Security Clearance** – a document issued in accordance with the national law by the Competent Authority or other authorized entity of one of the Parties stating that an individual has undergone security vetting and is eligible to have access to Classified Information;

11) **Facility Security Clearance** – a document issued in accordance with the national law by the Competent Authority or other authorized entity of one of the Parties stating that a Contractor has the ability to protect Classified Information.

ARTICLE 3
SECURITY CLASSIFICATION LEVELS

1. Classified Information is granted a security classification level appropriate to its content, in accordance with the national law of the Originating Party.

The Recipient Party shall guarantee at least an equivalent level of protection of the received Classified Information, pursuant to the provisions of Paragraph 3.

2 The security classification level may be changed or removed only by the Authorized Body which has granted it. The Recipient Party 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	MONGOLIA	EQUIVALENT IN ENGLISH
ŚCIŚLE TAJNE	МАШ НУУЦ	TOP SECRET
TAJNE	НУУЦ	SECRET
POUFNE	АЛБАН ХЭРЭГЦЭЭНД	CONFIDENTIAL
ZASTRZEŻONE	ХЯЗГААРЛАГДМАЛ	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 Mongolia: the Ministry of Defence.
2. The Parties shall inform each other via diplomatic channels about changes of the Competent Authorities referred to in Paragraph 1 or amendments to their competences.

ARTICLE 5
PRINCIPLES OF CLASSIFIED INFORMATION PROTECTION

1. In accordance with their national law, the Parties shall adopt every measure defined in this Agreement in order to protect Classified Information which has been originated or exchanged 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 Party shall use Classified Information exclusively for the purposes for which it has been exchanged.
3. Access to Classified Information shall be granted only to those individuals whose official duties require their access to it and who have been authorized to access such information in accordance with the national law of the Recipient Party.
4. The Recipient Party shall not release the information referred to in Paragraph 1 to any Third Party without a prior written consent of the Originating Party.

ARTICLE 6
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 other Party.

ARTICLE 7
CLASSIFIED CONTRACTS

1. Before concluding a Classified Contract connected with access to information classified as POUFNE / АЛБАН ХЭРЭГЦЭЭНД /

CONFIDENTIAL or above, the Principal shall apply to its Competent Authority to request that the Competent Authority of the other Party issue a certificate that the Contractor is a holder of a valid Facility Security Clearance relevant to the security classification level of the Classified Information the Contractor is to have access to.

2. Issuing the certificate referred to in Paragraph 1 shall be tantamount to a guarantee that necessary actions have been conducted to declare that the Contractor meets the criteria in the scope of the protection of Classified Information, defined in the national law of the Party, in the territory of the state of which it is located.

3. Classified Information shall not be released to the Contractor until the receipt of the certificate referred to in Paragraph 1.

4. The Principal shall transmit to the Contractor a facility security instruction necessary to perform a Classified Contract, which is an integral part of every Classified Contract. The facility security instruction contains provisions on the security requirements, in particular:

   1) the list of types of Classified Information related to a given Classified Contract, including their security classification levels;

   2) the rules for granting security classification levels to information originated during the performance of a given Classified Contract.

5. The Principal shall deliver 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 meets the criteria necessary for the protection of Classified Information, according to the facility security instruction.

7. Every Sub-Contractor shall comply with the same conditions for the protection of Classified Information as those laid down for the Contractor.

ARTICLE 8
TRANSMISSION OF CLASSIFIED INFORMATION

1. Classified Information shall be transmitted via diplomatic channels.
2. Information classified as ZASTRZEŻONE / ХЯЗГААРЛАГДМАЛ / RESTRICTED and POUFNE / АЛБАН ХЭРЭГЦЭЭНД / CONFIDENTIAL may be transmitted also through authorized couriers, in accordance with the national law of the transmitting Party.
3. In urgent cases, unless it is possible to use other forms of transmission and if the security requirements defined by the national law of the transmitting Party are met, the personal carriage of information classified as ZASTRZEŻONE / ХЯЗГААРЛАГДМАЛ / RESTRICTED and POUFNE / АЛБАН ХЭРЭГЦЭЭНД / CONFIDENTIAL is allowed.
4. The Competent Authorities of the Parties may agree on other forms of transmitting Classified Information which ensure its protection against unauthorized disclosure.
5. The Recipient Party 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 conducted in accordance with the national law of each of the Parties. Reproduced and translated information shall be placed under the same protection as the original information. The number of copies and translations shall be reduced to that required for official purposes. Translated information shall bear a note in the language into which it is translated indicating that it contains Classified Information received from the Originating Party.

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

ARTICLE 10

DESTRUCTION OF CLASSIFIED INFORMATION

1. Subject to Paragraph 2, Classified Information shall be destroyed according to the national law of the Recipient Party in such a manner as to eliminate its partial or total reconstruction.
2. Information classified as ŚCIŚLE TAJNE / МАШ НУУЦ / TOP SECRET shall not be destroyed, it shall be returned to the Originating Party.

ARTICLE 11

VISITS

1. Subject to Paragraphs 5 and 6, citizens of the State of one of the Parties 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 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. The request referred to in Paragraph 2 shall include information about:
   1) purpose, date and program of the visit;
   2) name and surname of the visitor, their date and place of birth, citizenship and passport or other identification document's number;
   3) position of the visitor together with the name of the entity which he or she represents;

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

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

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

In addition, the request shall include 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, subject to the national law of the Parties:

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 achieving 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 shall be 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 notify the hosting Party, which shall be obliged to correct or remove the data;

5) the hosting Party and the Party transmitting personal data shall be obliged to register its transmission, receipt and removal;

6) the Party transmitting personal data and the hosting Party shall be 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 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 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 visiting and hosting entities, in accordance with the conditions agreed upon.

6. Visits connected to access to information classified as ZASTRZEŻONE / ХЯЗГААРЛАГДМАЛ / RESTRICTED shall be arranged directly between the visiting and hosting entities.

ARTICLE 12
BREACH OF SECURITY

1. Breach of security is an action or an omission which is contrary to this Agreement or the national law of the Parties in the scope of protection of Classified Information, including an unauthorized disclosure of Classified Information.
2. Information regarding every breach of security or a suspicion of a breach of security concerning Classified Information of the Originating Party or Classified Information originated as a result of cooperation of the Parties shall be immediately reported to the Competent Authority of the Party in the territory of the state of which 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 in accordance with the national law of the Party in the territory of the state of which it has occurred.
4. In case of a breach of security the Competent Authority of the Party in the territory of the state of which the breach has occurred shall immediately 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.

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 English or their official languages. In case of using official languages, the Parties shall attach 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 the national law of the Parties 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 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 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 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 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, such a dispute shall be settled through diplomatic channels and not submitted to any Third Party.

ARTICLE 17
FINAL PROVISIONS

1. This Agreement shall enter into force in accordance with the national law of each of the Parties, which 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 case, this Agreement shall expire after six months following the receipt of the termination notice.
4. In case of termination of this Agreement, Classified Information exchanged or originated on its basis shall be protected in accordance with the provisions hereof.

Done at WARSAW on 08 JANUARY 2019 in two original copies, each in the Polish, Mongolian 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 MONGOLIA

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 20 stycznia 2020 roku.

Prezydent Rzeczypospolitej Polskiej: *A. Duda*

L.S.

Prezes Rady Ministrów: *M. Morawiecki*