DZIENNIK USTAW
RZECZYPOSPOLITEJ POLSKIEJ

Warszawa, dnia 22 stycznia 2015 r.

Poz. 117

UMOWA

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

podpisana w Budapeszcie dnia 29 stycznia 2014 r.

W imieniu Rzeczypospolitej Polskiej

PREZYDENT RZECZYPOSPOLITEJ POLSKIEJ

podaje do powszechnej wiadomości:

Dnia 29 stycznia 2014 r. w Budapeszcie została podpisana Umowa między Rządem Rzeczypospolitej Polskiej i Rządem Węgier o wymianie i wzajemnej ochronie informacji niejawnych, w następującym brzmieniu:

UMOWA

między Rządem Rzeczypospolitej Polskiej i Rządem Węgier o wymianie i wzajemnej ochronie informacji niejawnych

Rząd Rzeczypospolitej Polskiej i Rząd Węgier,

zwane dalej „Stronami",

mając na uwadze doniosłą rolę wzajemnej współpracy,

mając świadomość, iż bliska współpraca może pociągać za sobą konieczność wymiany informacji niejawnych,

pragnąc zapewnić właściwą ochronę wymienianym informacjom niejawnym,

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

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

uzgodniły, co następuje:

ARTYKUŁ 1
PRZEDMIOT UMOWY

1. Przedmiotem niniejszej Umowy jest zapewnienie ochrony informacjom niejawnym wytwarzanym w wyniku współpracy lub wymienianym między Stronami, osobami fizycznymi, osobami prawnymi lub innymi jednostkami organizacyjnymi pozostającymi pod ich jurysdykcją.
2. Umowa niniejsza ma zastosowanie do wszelkich działań, kontraktów lub umów dotyczących informacji niejawnych zawieranych między Stronami, osobami fizycznymi, osobami prawnymi lub innymi jednostkami organizacyjnymi pozostającymi pod ich jurysdykcją.

ARTYKUŁ 2
DEFINICJE

W rozumieniu niniejszej Umowy następujące definicje oznaczają:

1) informacje niejawne – wszelkie informacje niezależnie od ich formy, nośnika i sposobu ich utrwalenia oraz przedmioty lub dowolne ich części, także w trakcie ich opracowywania, które wymagają ochrony przed nieuprawnionym ujawnieniem lub innym nieuprawnionym wykorzystaniem i zostały oznaczone klauzulą tajności zgodnie z prawem krajowym jednej ze Stron;
2) właściwe organy bezpieczeństwa – organy, o których mowa w artykule 3;
3) kontrakt niejawny – umowę, której realizacja wiąże się z dostępem do informacji niejawnych bądź z wytworzeniem takich informacji;
4) strona wytwarzająca – Stronę, jak również osoby fizyczne, osoby prawne lub inne jednostki organizacyjne właściwe do wytwarzania informacji niejawnych zgodnie z prawem krajowym swojej Strony;
5) strona otrzymująca – Stronę, jak również osoby fizyczne, osoby prawne lub inne jednostki organizacyjne właściwe do otrzymywania informacji niejawnych zgodnie z prawem krajowym swojej Strony;

6) strona trzecia – państwo, jak również osoby fizyczne, osoby prawne lub inne jednostki organizacyjne podlegające jego jurysdykcji, a także organizację międzynarodową, niebędące Stroną niniejszej Umowy.

ARTYKUŁ 3
WŁAŚCIWE ORGANY BEZPIECZEŃSTWA

1. Właściwymi organami bezpieczeństwa Stron odpowiedzialnymi za ochronę informacji niejawnych oraz stosowanie niniejszej Umowy są:
   1) w Rzeczypospolitej Polskiej: Szef Agencji Bezpieczeństwa Wewnętrznego;
   2) na Węgrzech: Urząd Bezpieczeństwa Narodowego (Nemzeti Biztonsági Felügyelet).
2. Właściwe organy bezpieczeństwa przekazują sobie służbowe dane kontaktowe.
3. Strony informują się drogą dyplomatyczną o zmianach właściwych organów, o których mowa w ustępie 1, lub zmianach ich właściwości.

ARTYKUŁ 4
KLAZULE TAJNOŚCI

Strony uzgadniają, że niżej wymienione klauzule tajności są równorzędne:

RZECZPOSPOLITA POLSKA	WĘGRY	ODPOWIEDNIK W JĘZYKU ANGIELSKIM
ŚCIŚLE TAJNE	„Szigorúan titkos!”	TOP SECRET
TAJNE	„Titkos!”	SECRET
POUFNE	„Bizalmas!”	CONFIDENTIAL
ZASTRZEŻONE	„Korlátozott terjesztésű!”	RESTRICTED

ARTYKUŁ 5
DOSTĘP DO INFORMACJI NIEJAWNYCH

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.

ARTYKUŁ 6
ZASADY OCHRONY INFORMACJI NIEJAWNYCH

1. Strona wytwarzająca:
   1) odpowiada za oznaczenie informacji niejawnych właściwą klauzulą tajności, zgodnie ze swoim prawem krajowym;
   2) informuje w razie konieczności stronę otrzymującą o warunkach, na jakich udostępnia swoje informacje niejawne;
   3) niezwłocznie informuje na piśmie stronę otrzymującą o zniesieniu lub zmianach klauzuli tajności.
2. Strona otrzymująca:
   1) odpowiada za oznaczenie informacji niejawnych równoważną klauzulą tajności, zgodnie z artykułem 4 niniejszej Umowy;
   2) przyznaje informacjom niejawnym taki sam stopień ochrony, jaki przysługuje krajowym informacjom niejawnym o równoważnej klauzuli tajności;
   3) nie znosi ani nie zmienia klauzuli tajności, jaką oznaczono informacje niejawne;
   4) odpowiada za to, aby informacje niejawne nie były udostępniane stronie trzeciej bez uprzedniej zgody strony wytwarzającej;
   5) wykorzystuje informacje niejawne wyłącznie w celu, dla którego zostały jej udostępnione, oraz na warunkach określonych przez stronę wytwarzającą.

ARTYKUŁ 7
WSPÓŁPRACA W ZAKRESIE BEZPIECZEŃSTWA

1. W celu zachowania porównywalnych standardów bezpieczeństwa, właściwe organy bezpieczeństwa udzielają sobie, na wniosek, informacji dotyczących przepisów krajowych związanych z ochroną informacji niejawnych oraz praktyk wynikających z ich stosowania.
2. Na wniosek i zgodnie ze swoim prawem krajowym, właściwe organy bezpieczeństwa współpracują podczas przeprowadzania postępowań bezpieczeństwa osobowego i postępowań bezpieczeństwa przemysłowego.
3. Każda ze Stron, na wniosek i zgodnie z prawem krajowym, uznaje poświadczenia bezpieczeństwa osobowego i świadectwa bezpieczeństwa przemysłowego wydane przez drugą Stronę.
4. Właściwe organy bezpieczeństwa informują się niezwłocznie o zmianach w uznanych poświadczeniach bezpieczeństwa osobowego i świadectwach bezpieczeństwa przemysłowego, w szczególności o przypadkach ich cofnięcia.
5. Współpraca na podstawie niniejszej Umowy będzie prowadzona w języku angielskim.

ARTYKUŁ 8
KONTRAKTY NIEJAWNE

1. Kontrakty niejawne są zawierane i realizowane zgodnie z prawem krajowym każdej ze Stron. W przypadku kontraktów związanych z dostępem do informacji niejawnych o klauzuli POUFNE/„Bizalmas!"/CONFIDENTIAL lub wyższej, właściwe organy bezpieczeństwa, na wniosek, potwierdzają, iż proponowani kontrahenci, jak również osoby fizyczne uczestniczące w trwających przed zawarciem kontraktu negocjacjach lub w realizacji kontraktu niejawnego, posiadają

stosowne poświadczenia bezpieczeństwa osobowego lub świadectwa bezpieczeństwa przemysłowego.

2. Właściwy organ bezpieczeństwa Strony może wystąpić z wnioskiem o przeprowadzenie inspekcji bezpieczeństwa w obiekcie znajdującym się na terytorium drugiej Strony w celu zapewnienia trwałej ochrony informacji niejawnych.
3. Integralną częścią kontraktu niejawnego jest instrukcja bezpieczeństwa przemysłowego zawierająca postanowienia dotyczące wymogów bezpieczeństwa oraz klauzule tajności informacji niejawnych związanych z danym kontraktem niejawnym. Kopia instrukcji bezpieczeństwa przemysłowego będzie przekazana właściwemu organowi bezpieczeństwa Strony, pod jurysdykcją której realizowany jest dany kontrakt niejawny.

ARTYKUŁ 9
PRZEKAZYWANIE INFORMACJI NIEJAWNYCH

1. Informacje niejawne są przekazywane zgodnie z prawem krajowy strony wytwarzającej, drogą dyplomatyczną lub w inny sposób uzgodniony między właściwymi organami bezpieczeństwa w uzgodnieniach technicznych.
2. Strony mogą przekazywać informacje niejawne środkami elektronicznymi zgodnie z procedurami bezpieczeństwa zatwierdzonymi przez właściwe organy bezpieczeństwa.

ARTYKUŁ 10
POWIELANIE, TŁUMACZENIE I NISZCZENIE INFORMACJI NIEJAWNYCH

1. Kopie i tłumaczenia informacji niejawnych przekazanych na podstawie niniejszej Umowy opatrzone są właściwą klauzulą tajności i podlegają takiej samej ochronie jak oryginały. Liczba kopii lub tłumaczeń będzie ograniczona do liczby wymaganej dla celów służbowych.
2. Tłumaczenia informacji niejawnych przekazanych na podstawie niniejszej Umowy opatrzone są adnotacją w języku, na który zostały przetłumaczone, iż zawierają informacje niejawne strony wytwarzającej.
3. Informacje niejawne o klauzuli ŚCIŚLE TAJNE/„Szigorúan titkos!"/TOP SECRET przekazane na podstawie niniejszej Umowy są powielane lub tłumaczone tylko po uprzednim uzyskaniu pisemnego zezwolenia wydanego przez stronę wytwarzającą.
4. Informacje niejawne o klauzuli ŚCIŚLE TAJNE/„Szigorúan titkos!"/TOP SECRET przekazane na podstawie niniejszej Umowy nie są niszczone; są one zwracane stronie wytwarzającej.
5. W przypadku sytuacji kryzysowej, w której nie jest możliwe zapewnienie informacjom niejawnym wytworzonym lub udostępnionym na podstawie niniejszej Umowy odpowiedniej do ich klauzuli tajności ochrony, lub jeżeli nie jest możliwe ich zwrócenie, informacje niejawne zostaną niezwłocznie zniszczone. Właściwy organ bezpieczeństwa strony otrzymującej poinformuje bez zbędnej zwłoki właściwy organ bezpieczeństwa strony wytwarzającej o ich zniszczeniu.

ARTYKUŁ 11
WIZYTY

1. Wizyty związane z dostępem do informacji niejawnych odbywają się po uprzednim uzyskaniu pisemnego zezwolenia wydanego przez właściwy organ bezpieczeństwa.
2. Wniosek o wyrażenie zgody na wizytę przekazuje się co najmniej dwadzieścia dni przed rozpoczęciem wizyty do właściwego organu bezpieczeństwa strony wysyłającej, który przekazuje go z kolei do właściwego organu bezpieczeństwa strony przyjmującej. W pilnych przypadkach dopuszcza się złożenie wniosku w krótszym terminie.
3. We wniosku o wizytę zamieszcza się:

1) imię i nazwisko, datę i miejsce urodzenia, obywatelstwo i numer paszportu lub innego dokumentu tożsamości osoby przybywającej z wizytą;
2) stanowisko służbowe osoby przybywającej z wizytą wraz z nazwą podmiotu, który reprezentuje;
3) poziom i datę ważności poświadczenia bezpieczeństwa posiadanego przez osobę przybywającą z wizytą;
4) termin wizyty, a w przypadku powtarzających się wizyt – całkowity czas ich trwania;
5) cel wizyty z uwzględnieniem najwyższego poziomu informacji niejawnych związanych z wizytą;
6) nazwę i adres odwiedzanego podmiotu oraz imię i nazwisko, numer telefonu lub faksu, adres e-mail osoby przyjmującej;
7) datę, podpis oraz oficjalną pieczęć właściwego organu bezpieczeństwa strony wysyłającej.

4. Właściwe organy bezpieczeństwa mogą wyrazić zgodę na sporządzenie listy osób upoważnionych do składania wielokrotnych wizyt. Właściwe organy bezpieczeństwa uzgodnią niezbędne szczegóły związane z organizacją wizyt wielokrotnych.

5. Strony odpowiadają, zgodnie ze swoim prawem krajowym, za ochronę danych osobowych osób przybywających z wizytą.
6. Wizyty związane z dostępem do informacji niejawnych o klauzuli ZASTRZEŻONE/„Korlátozott terjesztésű!"/RESTRICTED są uzgadniane bezpośrednio między zainteresowanymi podmiotami.

ARTYKUŁ 12
NARUSZENIE REGULACJI DOTYCZĄCYCH OCHRONY INFORMACJI NIEJAWNYCH

1. Właściwe organy bezpieczeństwa informują się niezwłocznie na piśmie o przypadkach naruszenia bądź podejrzeniu naruszenia regulacji dotyczących ochrony informacji niejawnych, w rezultacie których doszło do nieuprawnionego ujawnienia lub innego nieuprawnionego wykorzystania informacji niejawnych wymienianych na podstawie niniejszej Umowy.
2. Właściwy organ bezpieczeństwa Strony, na terytorium której miało miejsce lub zaistniało podejrzenie naruszenia regulacji dotyczących ochrony informacji niejawnych, przeprowadzi niezwłocznie postępowanie wyjaśniające. Właściwy organ bezpieczeństwa drugiej Strony będzie, w razie potrzeby, współpracował przy czynnościach wyjaśniających.
3. W każdym przypadku naruszenia lub podejrzenia naruszenia regulacji dotyczących ochrony informacji niejawnych, właściwy organ bezpieczeństwa strony otrzymującej pisemnie informuje właściwy organ bezpieczeństwa strony wytwarzającej o jego okolicznościach, rozmiarze wyrządzonych szkód, środkach podjętych w celu ich złagodzenia oraz wyniku postępowania wyjaśniającego.

ARTYKUŁ 13
KOSZTY

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

ARTYKUŁ 14
ROZSTRZYGANIE SPORÓW

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

ARTYKUŁ 15
POSTANOWIENIA KOŃCOWE

1. Umowa niniejsza zawarta jest na czas nieokreślony. Umowa wejdzie w życie w pierwszym dniu drugiego miesiąca, który nastąpi po dniu otrzymania drogą dyplomatyczną ostatniej z not wymienionych przez Strony, informującej o zakończeniu wewnętrznych procedur prawnych, niezbędnych do wejścia niniejszej Umowy w życie.
2. Umowa niniejsza może zostać zmieniona na podstawie wspólnej pisemnej zgody obu Stron. Takie zmiany wejdą w życie zgodnie z postanowieniami ustępu 1.
3. Umowa niniejsza może być wypowiedziana w drodze notyfikacji przez każdą ze Stron. W takim przypadku utraci moc po upływie sześciu miesięcy od dnia otrzymania przez drugą Stronę noty informującej o wypowiedzeniu.

4. Mimo wypowiedzenia niniejszej Umowy, wszystkie informacje niejawne przekazane lub wytworzone na jej podstawie będą nadal chronione zgodnie z jej postanowieniami, aż do momentu, kiedy strona wytwarzająca pisemnie zwolni z tego obowiązku stronę otrzymującą.

Na dowód czego niżej podpisani, odpowiednio upoważnieni, podpisali niniejszą Umowę.

Sporządzono w Budapeszcie dnia 29.01.2014 roku w dwóch jednobrzmiących egzemplarzach, każdy w językach polskim, węgierskim i angielskim, przy czym wszystkie teksty posiadają jednakową moc. W przypadku rozbieżności przy ich interpretacji, tekst w języku angielskim będzie rozstrzygający.

Z UPOWAŻNIENIA RZĄDU RZECZYPOSPOLITEJ POLSKIEJ

Z UPOWAŻNIENIA RZĄDU WĘGIER

EGYEZMÉNY

a Lengyel Köztársaság Kormánya és Magyarország Kormánya

között

a minősített adatok cseréjéről és kölcsönös védelméről

a Lengyel Köztársaság Kormánya és Magyarország Kormánya

(a továbbiakban együtt: Felek)

Elismerve a kölcsönös együttműködés fontos szerepét,

Felismerve, hogy a Felek közötti együttműködés során szükség lehet minősített adatok cseréjére,

Kívánatosnak tartva, hogy a közöttük kicserélt minősített adatok megfelelő védelemben részesüljenek,

Attól a szándéktól vezérelve, hogy a Felek a minősített adatok védelme tárgyában egységes szabályokat alkalmazzanak,

Tiszteletben tartva a nemzetközi jog kötelező szabályait,

valamint a Felek nemzeti jogszabályait és rendelkezéseit,

Az alábbiakban állapodtak meg:

1. CIKK
AZ EGYEZMÉNY TÁRGYA

1. Jelen Egyezmény célja, hogy védelmet biztosítson a Felek, valamint joghatóságuk alá tartozó jogi személyek, természetes személyek vagy egyéb szervezetek között keletkezett vagy kicserélt minősített adatok számára.
2. Az Egyezmény alkalmazandó a Felek, valamint joghatóságuk alá tartozó jogi személyek, természetes személyek vagy egyéb szervezetek között a jövőben megvalósuló valamennyi tevékenységre, megállapodásra vagy egyezményre, amely minősített adatot tartalmaz.

2. CIKK
FOGALOMMEGHATÁROZÁSOK

Jelen Egyezmény alkalmazásában:

1. A „Minősített Adat" megjelenési formájától, kézbesítőjétől, rögzítése módjától, tárgyától vagy bármely részétől, valamint létrejöttének folyamatától függetlenül minden olyan adat, amelyet védelemben kell részesíteni a jogosulatlan nyilvánosságra hozatallal, valamint a jogosulatlan vagy nem megfelelő kezeléssel szemben, s amelyet bármelyik Fél nemzeti jogszabályai szerint ennek megfelelően minősítettek.
2. A „Hatáskörrel rendelkező biztonsági hatóságok" a 3. Cikkben megnevezett hatóságok.
3. A „Minősített Szerződés" olyan szerződés, amely minősített adatot tartalmaz, vagy amely alapján minősített adathoz való hozzáférés szükséges.
4. Az „Átadó Fél" az a Fél, vagy annak természetes és jogi személye vagy egyéb szervezete, amely az adott Fél nemzeti jogszabályaival összhangban jogosult minősített adat kibocsátására.

5. Az „Átvevő Fél" az a Fél, vagy annak természetes és jogi személye vagy egyéb szervezete, amely az adott Fél nemzeti jogszabályaival és rendelkezéseivel összhangban jogosult minősített adat átvételére.
6. A „Harmadik Fél" bármely állam, valamint a joghatósága alá tartozó természetes személyek, jogi személyek vagy egyéb szervezet, valamint nemzetközi szervezet, amely nem részese jelen Egyezménynek.

3. CIKK
A HATÁSKÖRREL RENDELKEZŐ BIZTONSÁGI HATÓSÁGOK

1. A Feleknek a minősített adatok védelméért, valamint jelen Egyezmény végrehajtásáért felelős, hatáskörrel rendelkező biztonsági hatóságai a következők:
   1) A Lengyel Köztársaságban: a Belbiztonsági Ügynökség vezetője (Szef Agencji Bezpieczeństwa Wewnętrznego);
   2) Magyarországon: a Nemzeti Biztonsági Felügyelet.
2. A hatáskörrel rendelkező biztonsági hatóságok kötelesek egymást tájékoztatni hivatalos elérhetőségi adataikról.
3. A Felek kötelesek egymást diplomáciai úton tájékoztatni az 1. bekezdésben megnevezett hatáskörrel rendelkező biztonsági hatóságokkal kapcsolatos változásokról vagy hatáskörük módosításáról.

4. CIKK
MINŐSÍTÉSI SZINTEK MEGFELELTETÉSE

Az egyes nemzeti minősítési szintek az alábbiak szerint feleltethetők meg egymásnak:

A LENGYEL KÖZTÁRSASÁGBAN	MAGYARORSZÁGON	ANGOL NYELVŰ MEGFELELŐJÜK
ŚCIŚLE TAJNE	„Szigorúan titkos!"	TOP SECRET

TAJNE	„Titkos!"	SECRET
POUFNE	„Bizalmas!"	CONFIDENTIAL
ZASTRZEŻONE	„Korlátozott terjesztésű!"	RESTRICTED

5. CIKK
MINŐSÍTETT ADATHOZ VALÓ HOZZÁFÉRÉS

Minősített adathoz kizárólag olyan személyek kaphatnak hozzáférést, akik a szükséges ismeret elvének megfelelnek, és akik az Átvevő Fél nemzeti jogszabályaival és rendelkezéseivel összhangban erre megfelelő felhatalmazást kaptak.

6. CIKK
BIZTONSÁGI ALAPELVEK

1. Az Átadó Fél:
   1) köteles biztosítani, hogy a minősített adaton a nemzeti jogszabályai szerinti megfelelő minősítési szint feltüntetésre kerüljön;
   2) tájékoztatja az Átvevő Felet a minősített adat felhasználásának esetleges feltételhez kötéséről;
   3) haladéktalanul köteles írásban tájékoztatni az Átvevő Felet az adat minősítésében bekövetkezett változásokról.
2. Az Átvevő Fél:
   1) köteles biztosítani, hogy a minősített adaton feltüntetésre kerüljön a 4. Cikk alapján meghatározott egyenértékű minősítési szint;
   2) ugyanolyan szintű védelemben köteles részesíteni a minősített adatot, mint amelyet a saját, azonos minősítési szintű minősített adata számára biztosít;
   3) köteles biztosítani, hogy az átvett minősített adat minősítését nem szünteti meg, illetve minősítési szintjét nem változtatja meg;

4) köteles biztosítani, hogy az Átadó Fél előzetes írásbeli hozzájárulása nélkül az átvett minősített adatot Harmadik Fél részére nem adja át;
5) a minősített adatot kizárólag az átadás során megjelölt célra használhatja fel, betartva az Átadó Fél által meghatározott kezelési előírásokat.

7. CIKK
BIZTONSÁGI EGYÜTTMŰKÖDÉS

1. A hasonló szintű biztonsági követelmények fenntartása érdekében a hatáskörrel rendelkező biztonsági hatóságok a másik fél megkeresésére kötelesek egymást tájékoztatni a minősített adat védelmével kapcsolatos nemzeti jogszabályokról, valamint mindezek gyakorlati alkalmazásáról.
2. Megkeresés esetén a hatáskörrel rendelkező biztonsági hatóságok, összhangban a nemzeti jogszabályaik rendelkezéseivel, kölcsönösen segítséget nyújtanak egymásnak a személyi biztonsági tanúsítványokkal és a telephely biztonsági tanúsítványokkal kapcsolatos eljárások során.
3. A Felek megkeresés esetén nemzeti jogszabályaik rendelkezéseivel összhangban elismerik a másik Fél által kibocsátott személyi biztonsági tanúsítványokat és telephely biztonsági tanúsítványokat.
4. A hatáskörrel rendelkező biztonsági hatóságok haladéktalanul értesítik egymást az elismert személyi biztonsági tanúsítványokkal és a telephely biztonsági tanúsítványokkal kapcsolatos változásokról, különösen azok visszavonásáról.
5. Jelen Egyezmény végrehajtása során a hatáskörrel rendelkező biztonsági hatóságok az angol nyelvet használják.

8. CIKK
MINŐSÍTETT SZERZŐDÉSEK

1. A minősített szerződéseket a Felek saját nemzeti jogszabályai alapján kell megkötni és teljesíteni. POUFNE/„Bizalmas!"/CONFIDENTIAL vagy magasabb minősítésű szintű minősített adatot érintő szerződések esetén a hatáskörrel rendelkező biztonsági hatóságok megkeresésre kötelesek megerősíteni, hogy az ajánlattevő és az előzetes szerződési tárgyalásokban vagy a minősített szerződések teljesítésében részt vevő természetes személyek rendelkeznek-e megfelelő személyi biztonsági tanúsítvánnyal vagy telephely biztonsági tanúsítvánnyal.
2. A hatáskörrel rendelkező biztonsági hatóságok kérelmezhetik, hogy a másik Fél biztonsági ellenőrzést folytasson le a területén működő létesítményben a minősített adatok folyamatos védelmének biztosítása céljából.
3. A minősített szerződések részét képezi a projekt biztonsági utasítás, amely a biztonsági követelményeket és a minősített szerződés által érintett minősített adat minősítési szintjével kapcsolatos rendelkezéseket határozza meg. A projekt biztonsági utasítás másolatát azon Fél hatáskörrel rendelkező biztonsági hatósága részére kell továbbítani, amelynek joghatósága alatt a minősített szerződés teljesítése történik.

9. CIKK
A MINŐSÍTETT ADAT TOVÁBBÍTÁSA

1. A minősített adat továbbítása az Átadó Fél nemzeti jogszabályaiban meghatározott szabályok szerint, diplomáciai úton, vagy a hatáskörrel rendelkező biztonsági hatóságok által végrehajtási intézkedésekben közösen meghatározott egyéb módon történik.
2. A Felek a hatáskörrel rendelkező biztonsági hatóságok által jóváhagyott eljárási rend szerint, elektronikus úton is továbbíthatnak minősített adatot.

10. CIKK
A MINŐSÍTETT ADAT SOKSZOROSÍTÁSA, FORDÍTÁSA ÉS MEGSEMMISÍTÉSE

1. Jelen Egyezmény alapján átadott minősített adatról készült másolatokon és fordításokon fel kell tüntetni a megfelelő minősítési jelölést és az így készült adatot ugyanolyan védelemben kell részesíteni, mint az eredeti minősített adatot. A sokszorosított példányok számát a hivatalos célból szükséges mértékre kell korlátozni.
2. Jelen Egyezmény alapján átadott minősített adat fordítása során keletkező példányokon a fordítás nyelvén fel kell tüntetni, hogy az az Átadó Fél minősített adatát tartalmazza.
3. Jelen Egyezmény alapján átadott, ŚCIŚLE TAJNE/„Szigorúan titkos!"/TOP SECRET minősítésű adat fordítása vagy sokszorosítása kizárólag az Átadó Fél előzetes írásbeli engedélyével lehetséges.
4. Jelen Egyezmény alapján átadott, ŚCIŚLE TAJNE/„Szigorúan titkos!"/TOP SECRET minősítésű adat nem semmisíthető meg, az ezen minősítési szintű adatokat az Átadó Félnek kell visszaszolgáltatni.
5. A jelen Egyezmény alapján készített vagy átadott minősített adatot olyan válsághelyzet esetén, amely lehetetlenné teszi a minősítési szintjének megfelelő védelmét, vagy ha visszajuttatása nem lehetséges, haladéktalanul meg kell semmisíteni. A megsemmisítésről az Átvevő Fél hatáskörrel rendelkező biztonsági hatósága haladéktalanul értesíti az Átadó Fél hatáskörrel rendelkező biztonsági hatóságát.

11. CIKK
LÁTOGATÁSOK

1. Minősített adathoz való hozzáférést igénylő látogatásra az érintett hatáskörrel rendelkező biztonsági hatóság előzetes írásbeli jóváhagyása alapján kerülhet sor.

2. A látogatásra vonatkozó megkeresést legalább 20 nappal a látogatás időpontja előtt a Fél hatáskörrel rendelkező biztonsági hatóságához kell benyújtani, amely azt továbbítja a másik Fél hatáskörrel rendelkező biztonsági hatóságához. Sürgős esetben, a hatáskörrel rendelkező biztonsági hatóságok előzetes egyeztetését követően a látogatásra vonatkozó megkeresés a látogatás kezdetéhez közelebbi időpontban is benyújtható.
3. A látogatásra vonatkozó megkeresésnek az alábbiakat kell tartalmaznia:

1) a látogató neve, születési helye és ideje, állampolgársága, útlevelének vagy más személyazonosító igazolványának száma;
2) a látogató beosztásának és a látogató által képviselt intézmény megjelölése;
3) a látogató személyi biztonsági tanúsítványának szintje és érvényességi ideje;
4) a látogatás időpontja és időtartama, visszatérő látogatások esetén az egyes látogatások összesített időtartama;
5) a látogatás célja, valamint a megismerendő legmagasabb minősítési szintű minősített adat minősítési szintjének megjelölése;
6) a meglátogatandó létesítmény neve és címe, valamint a kapcsolattartójának neve, telefonszáma, faxszáma, e-mail címe;
7) dátum, aláírás és a hatáskörrel rendelkező biztonsági hatóság hivatalos pecsétjének lenyomata.

4. A hatáskörrel rendelkező biztonsági hatóságok közösen meghatározhatják a visszatérő látogatásra jogosult személyek listáját. A visszatérő látogatások szükséges részleteit a hatáskörrel rendelkező biztonsági hatóságok közösen állapítják meg.
5. A Felek nemzeti jogszabályaiknak megfelelően, kötelesek biztosítani a látogatásra érkező személyek személyes adatainak védelmét.
6. ZASTRZEŻONE/„Korlátozott terjesztésű!"/RESTRICTED minősítésű minősített adathoz való hozzáféréssel járó látogatások szervezése az érintettek szervezetek között közvetlenül történik.

12. CIKK
ELJÁRÁS A MINŐSÍTETT ADAT BIZTONSÁGÁNAK MEGSÉRTÉSE ESETÉN

1. A hatáskörrel rendelkező biztonsági hatóságok késedelem nélkül írásban tájékoztatják egymást azon minősített adat biztonságának megsértéséről, amely esetben a jelen Egyezmény hatálya alá tartozó minősített adat jogosulatlan nyilvánosságra hozatalára, a minősített adat jogosulatlan vagy nem megfelelő kezelésére kerül sor, vagy mindezek alapos gyanúja merül fel.
2. Azon Fél hatáskörrel rendelkező biztonsági hatósága, ahol a minősített adat biztonságának megsértésére sor került, késedelem nélkül intézkedik a minősített adat megsértésének kivizsgálása érdekében. A másik Fél hatáskörrel rendelkező biztonsági hatósága szükség esetén részt vesz a vizsgálatban.
3. Az Átvevő Fél hatáskörrel rendelkező biztonsági hatósága minden esetben írásban tájékoztatja az Átadó Felet a minősített adat biztonsága megsértésének körülményeiről, a kár mértékéről, a kár enyhítése érdekében megtett intézkedésekről, valamint a vizsgálat eredményéről.

13. CIKK
KÖLTSÉGEK VISELÉSE

A Felek maguk viselik a jelen Egyezmény végrehajtásával összefüggésben felmerült költségeiket.

14. CIKK
VITÁK RENDEZÉSE

1. Felek a jelen Egyezmény végrehajtásából fakadó vitákat a Felek hatáskörrel rendelkező biztonsági hatóságai közötti közvetlen tárgyalás útján kötelesek rendezni.
2. Amennyiben vita az 1. bekezdésben megnevezett módon nem rendezhető, a vitát a Felek diplomáciai úton kötelesek rendezni.

15. CIKK
ZÁRÓ RENDELKEZÉSEK

1. Jelen Egyezmény határozatlan időre jön létre. Jelen Egyezmény a Felek az Egyezmény hatálybalépéshez szükséges belső feltételek teljesítésére vonatkozó, diplomáciai úton küldött utolsó értesítése kézhezvételének napját követő második hónap első napján lép hatályba.
2. Jelen Egyezmény a Felek kölcsönös egyetértésével írásban módosítható. A módosítások hatályba lépésével kapcsolatban a jelen Cikk 1. pontjában foglaltak az irányadók.
3. Bármelyik Fél jogosult jelen Egyezményt bármikor írásban felmondani. Felmondás esetén az Egyezmény a felmondásról szóló írásbeli értesítés másik Fél általi kézhezvételétől számított 6 hónap elteltével hatályát veszti.
4. Az Egyezmény megszűnésétől függetlenül az annak alapján átadott vagy keletkeztetett minősített adatokat az Egyezményben meghatározott rendelkezések szerint kell védelemben részesíteni, mindaddig, amíg az Átadó Fél írásban felmentést nem ad az Átvevő Fél részére ezen kötelezettség alól.

Fentiek tanúbizonyságául, az alulírott és az erre felhatalmazott megbízottak jelen Egyezményt aláírásukkal látták el.

Készült Budapeste -n, 2014.01.29-án, két eredeti példányban, lengyel, magyar és angol nyelven, valamennyi szöveg egyaránt hiteles. Eltérő értelmezés esetén az angol nyelvű szöveg az irányadó.

A LENGYEL KÖZTÁRSASÁG
KORMÁNYA RÉSZÉRŐL

MAGYARORSZÁG
KORMÁNYA RÉSZÉRŐL

AGREEMENT

between the Government of the Republic of Poland

and the Government of Hungary

on the Exchange and Mutual Protection of Classified Information

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

hereinafter referred to as the "Parties",

Recognising the important role of the mutual cooperation,

Realising that good cooperation may require

exchange of Classified Information between the Parties,

Wishing to ensure the protection of Classified Information

exchanged between them,

Being guided by the intention to adopt uniform regulations for both Parties

in the scope of the protection of Classified Information,

In respect of the binding rules of the international law

and the national law of the Parties

Have agreed upon the following:

ARTICLE 1
SCOPE 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, individuals, legal entities or other forms of organisations under their jurisdiction.
2. This Agreement shall be applicable to any activities, contracts or agreements involving Classified Information that will be concluded between the Parties, individuals, legal entities or other forms of organisations under their jurisdiction.

ARTICLE 2
DEFINITIONS

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

1. "Classified Information" – any information, regardless of its form, carrier and manner of recording, as well as objects or any parts thereof, also in the process of being generated, which requires protection against unauthorised disclosure or any other unauthorized or improper handling and has been marked as such under the national law of either Party.
2. "Competent Security Authorities" – the authorities referred to in Article 3.
3. "Classified Contract" – a contract that involves or requires access to Classified Information.
4. "Originating Party" – the Party, as well as individuals, legal entities or other forms of organizations, competent to originate Classified Information in accordance with the national law of the Parties.
5. "Recipient Party" – the Party, as well as individuals, legal entities or other forms of organizations, competent to receive Classified Information in accordance with the national law of the Parties.

6. "Third Party" – any state, including individuals, legal entities or other forms of organizations under its jurisdiction or international organisation not being a party to this Agreement.

ARTICLE 3
COMPETENT SECURITY AUTHORITIES

1. The Competent Security Authorities of the Parties responsible for the protection of Classified Information as well as the implementation of this Agreement are:
   1) in the Republic of Poland: the Head of the Internal Security Agency (Szef Agencji Bezpieczeństwa Wewnętrznego);
   2) in Hungary: the National Security Authority (Nemzeti Biztonsági Felügyelet).
2. The Competent Security Authorities shall provide each other with official contact details.
3. The Parties shall inform each other via diplomatic channels about changes of the Competent Security Authorities referred to in Paragraph 1 or amendments to their competences.

ARTICLE 4
SECURITY CLASSIFICATION LEVELS AND MARKINGS

The equivalence of national security classification levels and markings is as follows:

IN THE REPUBLIC OF POLAND	IN HUNGARY	EQUIVALENT IN THE ENGLISH LANGUAGE
ŚCIŚLE TAJNE	„Szigorúan titkos!"	TOP SECRET
TAJNE	„Titkos!"	SECRET
POUFNE	„Bizalmas!"	CONFIDENTIAL
ZASTRZEŻONE	„Korlátozott terjesztésű!"	RESTRICTED

ARTICLE 5
ACCESS TO CLASSIFIED INFORMATION

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 Recipient Party.

ARTICLE 6
SECURITY PRINCIPLES

1. The Originating Party shall:
   1) ensure that Classified Information is marked with appropriate security classification markings in accordance with its national law;
   2) inform the Recipient Party of any use conditions of Classified Information if necessary;
   3) inform the Recipient Party in writing without undue delay of any subsequent changes in the security classification level.
2. The Recipient Party shall:
   1) ensure that Classified Information is marked with equivalent security classification marking in accordance with Article 4;

2) afford the same degree of protection to Classified Information as afforded to its own Classified Information of equivalent security classification level;
3) ensure that Classified Information is not declassified nor its security classification level changed;
4) ensure that Classified Information is not released to a Third Party without the prior written consent of the Originating Party;
5) use Classified Information only for the purpose it has been released for and in accordance with release conditions of the Originating Party.

ARTICLE 7
SECURITY CO-OPERATION

1. In order to maintain comparable standards of security, the Competent Security Authorities shall, on request, inform each other of their national law concerning protection of Classified Information and the practices stemming from their implementation.
2. On request, the Competent Security Authorities shall, in accordance with their national law, assist each other during the personnel security clearance procedures and facility security clearance procedures.
3. Each Party shall on request and in accordance with their national law, recognise the personnel security clearance certificates and facility security clearance certificates issued by the other Party.
4. The Competent Security Authorities shall promptly notify each other about changes in the recognised personnel security clearance certificates and facility security clearance certificates, in particular in case of their withdrawal.
5. The co-operation under this Agreement shall be effected in the English language.

ARTICLE 8
CLASSIFIED CONTRACTS

1. Classified contracts shall be concluded and implemented in accordance with the national law of each Party. In case of contracts involving information classified POUFNE/„Bizalmas!"/CONFIDENTIAL or above, the Competent Security Authorities shall, on request, confirm that proposed contractors as well as individuals participating in pre-contractual negotiations or in the implementation of Classified Contracts have appropriate personnel security clearance certificate or facility security clearance certificate.
2. The Competent Security Authority of a Party may request that a security inspection is carried out at a facility located in the territory of the other Party to ensure continuing protection of Classified Information.
3. Classified Contracts shall contain project security instructions on the security requirements and on the security classification level of Classified Information involved in the Classified Contract. A copy of the project security instructions shall be forwarded to the Competent Security Authority of the Party under whose jurisdiction the Classified Contract is to be performed.

ARTICLE 9
TRANSMISSION OF CLASSIFIED INFORMATION

1. Classified Information shall be transmitted in accordance with the national law of the Originating Party through diplomatic channels or as otherwise agreed between the Competent Security Authorities in implementing arrangements.

2. The Parties may transmit Classified Information by electronic means in accordance with the security procedures approved by the Competent Security Authorities.

ARTICLE 10
REPRODUCTION, TRANSLATION AND DESTRUCTION OF CLASSIFIED INFORMATION

1. Reproductions and translations of Classified Information released under this Agreement shall bear appropriate security classification markings and shall be protected as the originals. The number of reproductions shall be limited to that required for official purposes.
2. Translations of Classified Information released under this Agreement shall bear a note in the language of translation indicating that they contain Classified Information of the Originating Party.
3. Classified Information released under this Agreement marked ŚCIŚLE TAJNE/„Szigorúan titkos!"/TOP SECRET shall be translated or reproduced only upon the prior written consent of the Originating Party.
4. Classified Information released under this Agreement marked ŚCIŚLE TAJNE/„Szigorúan titkos!"/TOP SECRET shall not be destroyed and shall be returned to the Originating Party.
5. In case of any crisis situation, which makes it impossible to protect the Classified Information generated or released in accordance with this Agreement according to its marking, or if it is impossible to return, the Classified Information shall be destroyed immediately. The Competent Security Authority of the Recipient Party shall notify the Competent Security Authority of the Originating Party about the destruction of the Classified Information as soon as possible.

ARTICLE 11
VISITS

1. Visits requiring access to Classified Information shall be subject to the prior written consent of the respective Competent Security Authority.
2. At least twenty days before the visit takes place, a request for visit shall be submitted to the Competent Security Authority of the respective Party, which shall forward it to the Competent Security Authority of the other Party. In urgent cases, a request for visit may be submitted at a shorter notice, subject to prior co-ordination between the Competent Security Authorities.
3. Requests for visit shall contain:

1) visitor's name, date and place of birth, nationality and passport or ID card number;
2) position of the visitor and specification of the legal entity represented;
3) visitor's personnel security clearance certificate status and its validity;
4) date and duration of the visit and the total period of time covered by the visits in case of recurring visits;
5) purpose of the visit including the highest security classification level of Classified Information involved;
6) name and address of the facility to be visited, as well as the name, phone or fax number, e-mail address of its point of contact;
7) date, signature and stamping of the official seal of the Competent Security Authority.

4. The Competent Security Authorities may agree on a list of visitors entitled to recurring visits. The Competent Security Authorities shall agree on necessary details of the recurring visits.
5. The Parties shall ensure, pursuant to their national law, the protection of the personal data of the persons arriving on a visit.

6. Visits involving access to information classified ZASTRZEŻONE/„Korlátozott terjesztésű!"/RESTRICTED are arranged directly between the entities involved.

ARTICLE 12
BREACH OF SECURITY

1. The Competent Security Authorities shall without undue delay inform each other in writing of a breach of security resulting in unauthorised disclosure or any other unauthorised or improper handling of Classified Information under this Agreement, or suspicion thereof.
2. The Competent Security Authority of the Party where the breach of security has occurred shall investigate the incident without delay. The other Competent Security Authority shall, if required, co-operate in the investigation.
3. In any case, the Competent Security Authority of the Recipient Party shall inform the Originating Party in writing about the circumstances of the breach of security, the extent of the damage, the measures adopted for its mitigation and the outcome of the investigation.

ARTICLE 13
EXPENSES

Each Party shall bear its own expenses incurred in the course of the implementation of this Agreement.

ARTICLE 14
SETTLEMENT OF DISPUTES

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

ARTICLE 15
FINAL PROVISIONS

1. This Agreement is concluded for an indefinite period of time. This Agreement shall enter into force on the first day of the second month following the date of the receipt of the last of notifications exchanged between the Parties through diplomatic channels, stating that the national legal requirements for this Agreement to enter into force have been fulfilled.
2. This Agreement may be amended on the basis of a written mutual agreement of the Parties. Such amendments shall enter into force in accordance with Paragraph 1.
3. Each Party is entitled to terminate this Agreement in writing at any time. In such case, this Agreement shall expire after six months following the day on which the other Party received the written notice of termination.
4. Regardless of the termination of this Agreement, all Classified Information exchanged or generated under this Agreement shall be protected in accordance with the provisions set forth herein until the Originating Party dispenses the Recipient Party from this obligation in writing.

In witness of which, the Undersigned, duly authorised to this effect, have signed this Agreement.

Done in Budapest on 29.01.2014 in two originals, in the Polish, Hungarian and English languages, all texts being equally authentic. In case of divergence in the interpretation the English text shall prevail.

FOR THE GOVERNMENT OF THE REPUBLIC OF POLAND

FOR THE GOVERNMENT OF HUNGARY

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 22 września 2014 r.

Prezydent Rzeczypospolitej Polskiej: *B. Komorowski*

L.S.

Prezes Rady Ministrów: *D. Tusk*