ACORD

ÎNTRE

GUVERNUL ROMÂNIEI

ŞI

CABINETUL DE MINIŞTRI AL UCRAINEI

PRIVIND PROTECŢIA RECIPROCĂ

A INFORMAŢIILOR CLASIFICATE

Guvernul României şi Cabinetul de Miniştri al Ucrainei, denumite în continuare "Părţile",

În scopul asigurării protecţiei Informaţiilor Clasificate, generate în comun sau schimbate între Părţi direct sau prin intermediul autorităţilor publice şi/sau al altor persoane juridice, cât şi în cadrul activităţilor care sunt în responsabilitatea Autorităţilor Competente de Securitate ale Părţilor,

Au convenit următoarele:

ARTICOLUL 1
DOMENIUL DE APLICARE

1. Prezentul Acord va sta la baza schimbului de Informaţii Clasificate între Părţi, direct sau prin intermediul autorităţilor publice sau al altor persoane juridice, cât şi la baza generării în comun a unor astfel de informaţii.

2. Prezentul Acord nu va afecta obligaţiile asumate de fiecare Parte prin alte acorduri internaţionale şi nu va fi folosit împotriva intereselor, securităţii şi integrităţii teritoriale ale altor State.

ARTICOLUL 2
DEFINIŢII

În sensul prezentului Acord:

a. Informaţii Clasificate înseamnă:
orice informaţie, indiferent de forma sa fizică, modalitatea de transmitere şi modul de înregistrare, căreia i s-a atribuit un anumit nivel de clasificare de securitate în conformitate cu legislaţia naţională şi care va fi protejată corespunzător;

b. Marcaj al Clasificării de Securitate înseamnă:
marcaj ce indică nivelul clasificării de securitate atribuit unei Informaţii Clasificate în conformitate cu legislaţia naţională a Părţilor;

c. Contract Clasificat înseamnă:
acord sub orice formă încheiat între autorităţile publice şi/sau alte persoane juridice din Statele Părţilor şi care conţine Informaţii Clasificate;

d. Parte Emitentă înseamnă:
autoritate publică sau altă persoană juridică din Statul Părții care emite și transmite Informații Clasificate;

e. Parte Primitoare înseamnă:
autoritate publică sau altă persoană juridică a Statului Părții care primește informații clasificate ale Părții Emitente;

f. Incident de Securitate înseamnă:
acțiune sau omisiune contrară reglementărilor naționale de securitate care are ca rezultat Compromiterea efectivă sau posibilă a Informațiilor Clasificate;

g. Compromiterea Informației Clasificate înseamnă:
situație în care - datorită unui Incident de Securitate sau unei activități ostile (precum spionaj, act de terorism sau furt) - Informațiile Clasificate și-au pierdut confidențialitatea, integritatea sau disponibilitatea ori atunci când serviciile și resursele conexe și-au pierdut integritatea sau disponibilitatea. Aceasta include pierderea, dezvăluirea parțială sau totală, modificarea și distrugerea neautorizate sau repudierea serviciului;

h. Certificat de Securitate a Personalului înseamnă:
document emis în conformitate cu legislația națională a Părților și care atestă faptul că, în îndeplinirea sarcinilor de serviciu, deținătorul este autorizat să aibă acces la Informații Clasificate de un anumit nivel de clasificare de securitate, în conformitate cu principiul „Necesitatea de a Cunoaște";

i. Necesitatea de a Cunoaște înseamnă:
principiu conform căruia accesul la Informații Clasificate poate fi acordat în mod individual numai persoanelor care, pentru îndeplinirea îndatoririlor de serviciu, trebuie să aibă acces la astfel de informații;

j. Autoritate Competentă de Securitate înseamnă:
instituția învestită cu autoritate la nivel național și care, conform legislațiilor naționale ale Părților, asigură implementarea măsurilor de protecție a Informațiilor Clasificate. Aceste autorități sunt menționate la art. 3.

ARTICOLUL 3
AUTORITĂȚILE COMPETENTE DE SECURITATE

1. Autoritățile Competente de Securitate ale Părților sunt:

În România	În Ucraina
Guvernul României Oficiul Registrului Național al Informațiilor Secrete de Stat Str. Mureş nr.4 Bucureşti 1 ROMÂNIA	Serviciul de Securitate al Ucrainei Str. Volodymyrska nr.33 Kiev UCRAINA

2. Autoritățile Competente de Securitate își vor furniza reciproc, la cerere, informații privind organizarea şi procedurile lor de securitate. În acest sens, Autoritățile Competente de Securitate vor conveni asupra unor vizite reciproce.

3. Autoritățile Competente de Securitate se vor informa reciproc cu privire la orice modificări survenite în denumirile lor sau în legătură cu orice transfer al competenței acestora către alte autorități.

ARTICOLUL 4
ECHIVALENȚA MARCAJELOR CLASIFICĂRII DE SECURITATE

1. Părțile au stabilit următoarea echivalență a Marcajelor naționale ale Clasificării de Securitate:

Pentru România	Pentru Ucraina	Echivalentul în limba engleză
STRICT SECRET DE IMPORTANȚĂ DEOSEBITĂ	Особливої важливості	TOP SECRET
STRICT SECRET	Цілком таємно	SECRET
SECRET	Таємно	CONFIDENTIAL
SECRET DE SERVICIU	Для службового користування	RESTRICTED

2. Fiecare Parte va marca toate Informațiile Clasificate primite de la cealaltă Parte cu Marcajul național al Clasificării de Securitate corespunzător, în conformitate cu echivalența stabilită în alin.(1) al prezentului articol.

ARTICOLUL 5
PROTECȚIA INFORMAȚIILOR CLASIFICATE

1. În conformitate cu legislația națională proprie, Părțile vor lua măsurile adecvate pentru protecția Informațiilor Clasificate transmise, primite, produse sau elaborate ca rezultat al oricărui acord, sub orice formă, încheiat între autoritățile publice şi/sau alte persoane juridice din Statele Părţilor. Părțile vor acorda tuturor Informațiilor Clasificate primite sau produse în comun acelaşi nivel de protecție ca cel prevăzut pentru Informațiile Clasificate naționale ce poartă Marcajul corespunzător al Clasificării de Securitate, în conformitate cu alin. (1), articolul 4 al prezentului Acord.

2. Partea Primitoare nu va atribui Informațiilor Clasificate primite un nivel de clasificare de securitate mai scăzut şi nici nu le va declasifica fără acordul prealabil scris al Autorității Competente de Securitate din Statul Părții Emitente. Partea Emitentă va informa Partea Primitoare asupra oricăror modificări survenite în nivelul de clasificare de securitate a Informațiilor Clasificate transmise.

3. Toate multiplicările Informațiilor Clasificate vor fi marcate cu aceleaşi Marcaj al Clasificării de Securitate ca şi Informațiile Clasificate originale şi vor fi protejate corespunzător. Numărul multiplicărilor se va limita la numărul necesar scopurilor oficiale.

4. Informațiile Clasificate primite marcate cu Marcajul Clasificării de Securitate STRICT SECRET DE IMPORTANTĂ DEOSEBITĂ / "Особливої важливості" / TOP SECRET vor fi multiplicate sau traduse numai cu acordul prealabil scris al Părții Emitente.

5. Informațiile Clasificate marcate cu Marcajul Clasificării de Securitate SECRET / ТАЄМНО / CONFIDENTIAL sau STRICT SECRET / "Цілком таємно" / SECRET pot fi distruse numai cu acordul prealabil scris al Părții Emitente sau la cererea acesteia, în conformitate cu legislația națională a Părții Primitoare, astfel încât să fie imposibilă reconstituirea totală sau parțială a acestora. Informațiile STRICT SECRET DE IMPORTANTĂ DEOSEBITĂ / "Особливої важливості" / TOP SECRET nu vor fi distruse ci vor fi returnate Părții Emitente.

6. Partea Primitoare va informa Partea Emitentă cu privire la distrugerea Informațiilor Clasificate.

7. În cazul unui pericol iminent, Informațiile Clasificate vor fi distruse fără o autorizare prealabilă. Autoritatea Competentă de Securitate a Părții Emitente va fi informată imediat despre această situație.

8. Accesul la Informațiile Clasificate primite în baza prezentului Acord este permis, cu respectarea principiului „Necesitatea de a Cunoaşte", numai persoanelor care dețin Certificat de Securitate a Personalului echivalent cu nivelul de clasificare de securitate al informațiilor pentru care se solicită accesul sau persoanelor care au fost autorizate în conformitate cu legislația națională.

9. Niciuna dintre Părți nu va transmite unui terț Informațiile Clasificate primite, fără acordul prealabil scris al Autorității Competente de Securitate din Statul Părții Emitente. Prezentul Acord nu va fi invocat de niciuna dintre Părți în scopul obținerii Informațiilor Clasificate primite de cealaltă Parte de la un terț.

ARTICOLUL 6
CERTIFICATUL DE SECURITATE A PERSONALULUI

1. Certificatul de Securitate a Personalului va fi acordat în urma verificării de securitate efectuate în conformitate cu legislația națională a fiecărei Părți.

2. La cerere, în conformitate cu legislația națională proprie, Autoritățile Competente de Securitate din Statele Părților își vor acorda asistență reciprocă la procedurile de vetting privind emiterea Certificatelor de Securitate a Personalului şi a certificatelor de securitate industrială. În acest sens, se pot conveni aranjamente specifice între Autoritățile Competente de Securitate din Statele Părților.

3. Părțile vor recunoaşte reciproc Certificatele de Securitate a Personalului şi certificatele de securitate industrială emise în conformitate cu legislațiile naționale proprii.

4. În cadrul implementării prezentului Acord, Autoritățile Competente de Securitate se vor informa reciproc asupra oricăror modificări ale Certificatelor de Securitate a Personalului şi certificatelor de securitate industrială, în special asupra cazurilor de retragere a acestora.

ARTICOLUL 7
VIZITE

1. Vizitele ce implică acces la Informații Clasificate sau în incintele unde se elaborează, se gestionează sau se stochează astfel de informații sau unde se desfăşoară activități ce presupun Informații Clasificate vor fi autorizate de către o Parte pentru vizitatorii din Statul celeilalte Părți numai după obținerea aprobării prealabile scrise a Autorității Competente de Securitate din Statul Părții gazdă. Această aprobare va fi acordată numai persoanelor care dețin Certificate de Securitate a Personalului şi respectă principiul „Necesitatea de a Cunoaşte".

2. Vizitele vor fi anunțate cu douăzeci (20) de zile lucrătoare în avans.

3. În situații urgente, cererea de vizită poate fi transmisă ulterior, dar cu minimum cinci (5) zile lucrătoare înainte de vizita propriu-zisă.

4. Cererea de vizită va cuprinde:
   a. Numele şi prenumele vizitatorului, locul şi data naşterii, cetățenia, numărul paşaportului sau a documentului de identitate;
   b. Denumirea instituției, companiei sau organizației pe care o reprezintă sau de care aparține vizitatorul;
   c. Denumirea şi adresa instituției, companiei sau organizației ce urmează să fie vizitată;
   d. Confirmarea Certificatului de Securitate a Personalului sau a autorizației vizitatorului;
   e. Obiectivul şi scopul vizitei sau vizitelor;
   f. Data şi durata estimată a vizitei/vizitelor solicitată/e. În cazul unor vizite periodice se va specifica perioada totală acoperită de vizite;
   g. Denumirea şi numărul de telefon al punctului de contact al instituției/obiectivului ce urmează a fi vizitat, contactele anterioare şi orice alte informații utile pentru stabilirea motivului vizitei sau vizitelor;
   h. Data, semnătura şi ştampila oficială a Autorității Competente de Securitate.

5. Autoritatea Competentă de Securitate din Statul Părții gazdă va informa funcționarii de securitate ai instituției, obiectivului sau organizației care urmează să fie vizitată cu privire la datele persoanelor confirmate pentru vizită.

6. În cazul unor vizite periodice valabilitatea autorizațiilor de vizită nu va depăși douăsprezece (12) luni.

7. Fiecare Parte va garanta protecția datelor personale ale vizitatorilor în conformitate cu legislația națională proprie.

ARTICOLUL 8
CONTRACTE CLASIFICATE

1. În cazul în care una dintre Părți intenționează să încredințeze un Contract Clasificat ce urmează a se derula pe teritoriul Statului celeilalte Părți, Partea Primitoare își va asuma responsabilitatea protejării Informațiilor Clasificate referitoare la contract, în conformitate cu legislația națională proprie.

2. Înainte ca Partea Emitentă să transmită Informații Clasificate unei autorități publice și/sau unei alte persoane juridice a Statului celeilalte Părți, Autoritatea Competentă de Securitate a Părții Primitoare:
   a. Va confirma faptul că respectiva autoritate publică și/sau altă persoană juridică are dreptul de a gestiona Informații Clasificate sau va acorda un certificat de securitate industrială în conformitate cu legislația națională;
   b. Va confirma faptul că întregul personal care, prin atribuțiile sale, necesită acces la Informații Clasificate, a primit, în conformitate cu legislația națională, Certificate de Securitate a Personalului corespunzătoare nivelului Clasificării de Securitate al Informațiilor.

3. Părțile se vor asigura că fiecare Contract Clasificat conține o anexă de securitate corespunzătoare ce cuprinde:
   a. O listă a Informațiilor Clasificate ce urmează a fi transmise sau generate în baza Contractului Clasificat împreună cu marcajele lor de securitate;
   b. Cerințe speciale privind stocarea Informațiilor Clasificate;
   c. Procedura pentru comunicarea modificărilor survenite în nivelul clasificării de securitate al Informațiilor Clasificate;
   d. Canale de comunicare și mijloace de transmitere electromagnetică;
   e. Procedura de transmitere;
   f. Obligația de a informa asupra oricărei Compromiteri efective sau posibile a Informațiilor Clasificate;
   g. Proceduri de soluționare a diferendelor.

4. Proceduri detaliate privind Contractele Clasificate pot fi elaborate şi convenite între Autorităţile Competente de Securitate din Statele Părţilor.

ARTICOLUL 9
TRANSMITEREA INFORMAŢIILOR CLASIFICATE

1. Informaţiile Clasificate vor fi transmise prin curier diplomatic/militar sau prin alte mijloace convenite de Autorităţile Competente de Securitate. Partea Primitoare va confirma în scris Părţii Emitente primirea Informaţiilor Clasificate.

2. Dacă există un volum mare de Informaţii Clasificate ce trebuie transmis, Autorităţile Competente de Securitate pot conveni şi aproba reciproc modalităţile de transmitere şi măsurile de securitate pentru fiecare caz în parte.

3. Schimbul de Informaţii Clasificate prin intermediul mijloacelor electromagnetice se va realiza potrivit procedurilor de securitate stabilite prin aranjamente reciproce de către Autorităţile Competente de Securitate, în conformitate cu legislaţia naţională.

ARTICOLUL 10
INCIDENTE DE SECURITATE ŞI COMPROMITEREA INFORMAŢIILOR CLASIFICATE

1. În situaţia producerii unui Incident de Securitate, Autoritatea Competentă de Securitate din Statul Părţii Primitoare va informa Autoritatea Competentă de Securitate din Statul Părţii Emitente, va asigura investigaţia de securitate adecvată a acestui caz şi va lua măsurile necesare în vederea limitării consecinţelor, în conformitate cu legislaţia naţională. Dacă este necesar, Autorităţile Competente de Securitate vor coopera la investigaţie.

2. În cazul în care Compromiterea Informaţiilor Clasificate s-a produs pe teritoriul unui Stat terţ, Autoritatea Competentă de Securitate din Statul Părţii care transmite informaţiile va informa Autoritatea Competentă de Securitate din Statul Părţii Emitente, va sprijini investigaţia de securitate a acestui caz şi va lua măsurile necesare pentru limitarea consecinţelor, în conformitate cu legislaţia naţională.

3. După finalizarea investigației, Autoritatea Competentă de Securitate din Statul în care s-a produs Compromiterea sau o posibilă Compromitere a Informațiilor Clasificate va informa imediat, în scris, Autoritatea Competentă de Securitate din Statul celeilalte Părți asupra constatărilor și concluziilor investigației.

ARTICOLUL 11
SOLUȚIONAREA DIFERENDELOR

Orice diferend privind interpretarea sau aplicarea prezentului Acord va fi soluționat prin negocieri între Părți și nu va fi deferit unui terț pentru soluționare.

ARTICOLUL 12
CHELTUIELI

Fiecare Parte va suporta în mod individual posibilele costuri legate de aplicarea prezentului Acord, în conformitate cu legislația națională proprie.

ARTICOLUL 13
ASISTENȚĂ RECIPROCĂ

1. Fiecare Parte va acorda asistență personalului din Statul celeilalte Părți în aplicarea și interpretarea dispozițiilor prezentului Acord.

2. Dacă este necesar, Autoritățile Competente de Securitate din Statele Părților se vor consulta reciproc în baza unei cereri scrise.

3. Autoritățile Competente de Securitate din Statele Părților se vor informa reciproc asupra oricăror modificări ale legislației naționale în domeniul protecției Informațiilor Clasificate care ar putea afecta aplicarea dispozițiilor prezentului Acord.

ARTICOLUL 14
DISPOZIȚII FINALE

1. Prezentul Acord este încheiat pe o perioadă nedeterminată și este supus aprobării în conformitate cu legislațiile naționale ale Părților.

2. Prezentul Acord va intra în vigoare în prima zi din a doua lună după primirea ultimei notificări între Părți prin care se menționează că au fost îndeplinite procedurile interne legale necesare intrării în vigoare a prezentului Acord.

3. Fiecare Parte are dreptul să denunțe prezentul Acord în orice moment. În astfel de cazuri valabilitatea Acordului va înceta după 6 (șase) luni de la data la care notificarea de denunțare a fost trimisă celeilalte Părți.

4. Fără a ține cont de denunțarea prezentului Acord, toate Informațiile Clasificate furnizate în baza acestuia vor continua să fie protejate în conformitate cu prevederile stabilite în acest Acord.

5. Prezentul Acord poate fi amendat pe baza acordului reciproc al Părților. Amendamentele vor intra în vigoare în conformitate cu prevederile alin. (2).

6. Fiecare Parte va notifica prompt cealaltă Parte asupra oricăror modificări intervenite în legislația și reglementările naționale care ar putea afecta protecția Informațiilor Clasificate în baza prezentului Acord. În acest caz, Părțile se vor consulta reciproc pentru a analiza posibilele modificări ale acestui Acord. În tot acest timp, Informațiile Clasificate vor continua să fie protejate așa cum s-a stabilit în prezentul Acord, dacă nu se solicită altfel, în scris, de către Partea Emitentă.

Semnat la București la 22 octombrie 2013, în două exemplare originale, fiecare în limbile română, ucraineană și engleză, toate textele fiind egal autentice. În caz de diferențe în interpretare, textul în limba engleză va prevala.

PENTRU
GUVERNUL ROMÂNIEI

Prof.univ.dr. MARIUS PETRESCU
Secretar de Stat
Directorul General
al Oficiului Registrului Național al
Informațiilor Secrete de Stat

PENTRU
CABINETUL DE MINIȘTRI AL
UCRAINEI

VOLODYMYR PORODKO
Vicepreședintele
Serviciului de Securitate al Ucrainei

AGREEMENT

BETWEEN

THE GOVERNMENT OF ROMANIA

AND

THE CABINET OF MINISTERS OF UKRAINE

ON MUTUAL PROTECTION OF CLASSIFIED INFORMATION

The Government of Romania and the Cabinet of Ministers of Ukraine, hereinafter referred to as "the Parties",

In order to ensure the protection of all Classified Information jointly produced or exchanged between the Parties directly or through public authorities and/or other legal entities, and within the framework of activities which fall under the responsibility of the Competent Security Authorities of the Parties,

Have agreed on the following:

ARTICLE 1
APPLICABILITY

1. This Agreement shall form the basis for any exchange of Classified Information between the Parties directly or through the public authorities or other legal entities or the joint production of such information.

2. This Agreement shall not affect the commitments taken by each Party under other international agreements and shall not be used against the interests, the security and the territorial integrity of other States.

ARTICLE 2
DEFINITIONS

For the purpose of this Agreement:

a. Classified Information means:
any information, regardless of its physical form, carrier and record mode, to which a particular security classification level has been assigned in compliance with national legislation and which shall be protected accordingly;

b. Security Classification Marking means:
marking indicating the security classification level assigned to Classified Information in accordance with national legislation of the Parties;

c. Classified Contract means:
an agreement in any form between public authorities and/or other legal entities of the States of the Parties involving Classified Information;

d. Originating Party means:
public authority or other legal entity of the State of the Party which originates and transfers Classified Information;

e. Receiving Party means:
public authority or other legal entity of the State of the Party which receives Classified Information of the Originating Party;

f. Breach of Security means:
an act or an omission contrary to national security regulations, that results in an actual or possible Compromise of Classified Information;

g. Compromise of Classified Information means:
a situation when – due to a Breach of Security or adverse activity (such as espionage, act of terrorism or theft) – Classified Information has lost its confidentiality, integrity or availability, or when supporting services and resources have lost their integrity or availability. This includes loss, partial or total disclosure, unauthorized modification and unauthorized destruction or denial of service;

h. Personnel Security Clearance Certificate means:
a document issued in accordance with the national legislation of the Parties certifying that, in performing his/her duties, the holder is authorized to have access to Classified Information of a certain security classification level, in compliance with the Need-to-Know principle;

i. Need-to-Know means:
a principle by which access to Classified Information may be granted individually only to those persons who, in performing their official duties, need to have access to such information;

j. Competent Security Authority means:
the institution empowered with authority at national level which, in compliance with the national legislations of the Parties, ensures the implementation of the protective measures for Classified Information. Such authorities are listed in Article 3.

ARTICLE 3
COMPETENT SECURITY AUTHORITIES

1. The Competent Security Authorities of the Parties are:

In Romania	In Ukraine
Government of Romania National Registry Office for Classified Information 4 Mures Street Bucharest 1 ROMANIA	Security Service of Ukraine Volodymyrska St., 33 Kyiv Ukraine

2. The Competent Security Authorities shall provide each other, upon request, with information about their security organization and procedures. To this end, the Competent Security Authorities shall agree on mutual visits.

3. The Competent Security Authorities shall notify each other any changes of their names or any transfer of their competence to other authorities.

ARTICLE 4
EQUIVALENCE OF SECURITY CLASSIFICATION MARKINGS

1. The Parties have determined that the equivalence of the national Security Classification Markings is as follows:

For Romania	For Ukraine	English language Equivalent
STRICT SECRET DE IMPORTANTĂ DEOSEBITĂ	Особливої важливості	TOP SECRET
STRICT SECRET	Цілком таємно	SECRET
SECRET	Таємно	CONFIDENTIAL
SECRET DE SERVICIU	Для службового користування	RESTRICTED

2. Each of the Parties shall mark all the Classified Information received from the other Party with the corresponding national Security Classification Marking according the equivalence stated in paragraph (1) of this Article.

ARTICLE 5
PROTECTION OF CLASSIFIED INFORMATION

1. In accordance with their national legislation, the Parties shall take appropriate measures to protect Classified Information which is transmitted, received, produced or developed as a result of any agreement in any form between the public authorities and/or other legal entities of the States of the Parties. The Parties shall ensure to all the received or jointly produced Classified Information the same protection, as it is provided for the national Classified Information marked with the corresponding Security Classification Marking, according to paragraph (1) of Article 4 of this Agreement.

2. The Receiving Party shall neither assign a lower security classification level for the received Classified Information nor declassify it without the prior written consent of the Competent Security Authority of the State of the Originating Party. The Originating Party shall inform the Receiving Party of any changes in the security classification level of the transferred Classified Information.

3. All reproductions of Classified Information shall be marked with the same Security Classification Marking as the original Classified Information and shall be protected accordingly. The number of reproductions shall be limited to that necessary for official purposes.

4. The received Classified Information marked with a Security Classification Marking STRICT SECRET DE IMPORTANTĂ DEOSEBITĂ / "Особливої важливості" / TOP SECRET shall be reproduced or translated only with the prior written consent of the Originating Party.

5. Classified Information marked with the Security Classification Marking SECRET / "Таємно" / CONFIDENTIAL or STRICT SECRET / "Цілком таємно" / SECRET may be destroyed only with the prior written consent of or at the request of the Originating Party in accordance with the national legislation of the Receiving Party, in such a manner that its reconstruction in whole or in part be impossible. The STRICT SECRET DE IMPORTANTĂ DEOSEBITĂ / "Особливої важливості" / TOP SECRET information shall not be destroyed but returned to the Originating Party.

6. The Receiving Party shall inform the Originating Party of the destruction of Classified Information.

7. In case of an imminent danger, Classified Information shall be destroyed without prior authorization. The Competent Security Authority of the Originating Party shall immediately be notified about this.

8. Access to Classified Information received under this Agreement is allowed, with the observance of the Need-to-know principle, only to those individuals who have been granted a Personnel Security Clearance Certificate equivalent to security classification level of the information for which the access is required, or who have been authorized in accordance with the national legislation.

9. None of the Parties shall release received Classified Information to a third party without prior written consent of the Competent Security Authority of the State of the Originating Party. This Agreement shall not be invoked by either Party to obtain Classified Information that the other Party has received from a third party.

ARTICLE 6
PERSONNEL SECURITY CLEARANCE CERTIFICATE

1. The Personnel Security Clearance Certificate shall be granted following the security vetting procedure conducted in accordance with the national legislation of each Party.

2. On request, the Competent Security Authorities of the States of the Parties, taking into account the respective national legislation, shall assist each other in the vetting procedures related to the issuance of the Personnel Security Clearance Certificates and of the facility security clearance certificates. To this end specific arrangements may be agreed upon between the Competent Security Authorities of the States of the Parties.

3. The Parties shall mutually recognize the Personnel Security Clearance Certificates and the facility security clearance certificates issued in accordance with their national legislations.

4. Within the framework of the implementation of this Agreement, the Competent Security Authorities shall inform each other of any changes to

the Personnel Security Clearance Certificates and to the facility security clearance certificates, in particular of their revoke.

ARTICLE 7
VISITS

1. Visits involving access to Classified Information or to premises where such information is created, handled or stored, or where activities involving Classified Information are carried out, shall only be granted by one Party to visitors from the State of the other Party if a prior written permission from the Competent Security Authority of the host Party has been obtained. Such permission shall only be granted to persons who hold appropriate Personnel Security Clearance Certificates and have a Need-to-Know.

2. Visits shall be notified twenty (20) working days in advance.

3. In urgent cases, the request for visit could be transmitted later, but not less than five (5) working days before.

4. A request for visit shall include:
   a. Visitor's first and last name, place and date of birth, nationality, passport or identity card number;
   b. Name of the establishment, company or organization he/she represents or to which he/she belongs;
   c. Name and address of the establishment, company or organization to be visited;
   d. Confirmation of the visitor's Personnel Security Clearance Certificate or authorization;
   e. Object and purpose of the visit or visits;
   f. Expected date and duration of the requested visit or visits. In case of recurring visits the total period covered by the visits should be stated;
   g. Name and phone number of the point of contact at the establishment/facility to be visited, previous contacts and any other information useful to determine the justification of the visit or visits;
   h. The date, signature and stamping of the official seal of the Competent Security Authority.

5. The Competent Security Authority of the State of the host Party shall inform the security officers of the establishment, facility or organization to be visited of data of those persons confirmed for a visit.

6. In case of repeated visits the validity of visit authorizations shall not exceed twelve (12) months.

7. Each Party shall guarantee the protection of personal data of the visitors according to its national legislation.

ARTICLE 8
CLASSIFIED CONTRACTS

1. In the event that either Party intends to grant a Classified Contract to be performed within the territory of the State of the other Party, the Receiving Party will assume responsibility for the protection of Classified Information related to the contract in accordance with its national legislation.

2. Before the Originating Party releases Classified Information to a public authority and/or to other legal entity of the State of the other Party, the Competent Security Authority of the State of the Receiving Party shall:

   a. Confirm that the respective public authority and/or other legal entity has the right to handle Classified Information or grant a facility security clearance certificate in accordance with the national legislation;
   b. Confirm that all personnel whose duties require access to Classified Information have been granted in accordance with the national legislation Personnel Security Clearance Certificates corresponding to the security classification level of the information.

3. The Parties shall ensure that every Classified Contract includes an appropriate security annex containing:
   a. A List of Classified Information to be transmitted or produced under the Classified Contract and its Security Classification Markings;
   b. Special demands on storage of Classified Information;
   c. Procedure for the communication of changes in the security classification level of Classified Information;
   d. Communication channels and means for electromagnetic transmission;
   e. Transmission procedure;
   f. An obligation to notify any actual or suspected Compromise of Classified Information;
   g. Procedures for settlement of disputes.

4. Detailed procedures related to Classified Contracts may be developed and agreed between the Competent Security Authorities of the States of the Parties.

ARTICLE 9
TRANSMISSION OF CLASSIFIED INFORMATION

1. Classified Information shall be transmitted by diplomatic / military courier or by other means agreed upon by the Competent Security Authorities. The Receiving Party shall confirm in written to the Originating Party the receipt of Classified Information.

2. If a large consignment of Classified Information is to be transmitted, the Competent Security Authorities may mutually agree on and approve the means of transmission and security measures for each such case.

3. The exchange of Classified Information via electromagnetic means shall take place in accordance with the security procedures established through mutual arrangements by the Competent Security Authorities in accordance with national legislation.

ARTICLE 10
BREACHES OF SECURITY
AND COMPROMISE OF CLASSIFIED INFORMATION

1. In case of a Breach of Security the Competent Security Authority of the State of the Receiving Party shall inform the Competent Security Authority of the State of the Originating Party, ensure proper security investigation of such event and take the necessary measures to limit the consequences, in accordance with national legislation. If required, the Competent Security Authorities shall cooperate in the investigation.

2. In case the Compromise of Classified Information occurs on the territory of a third State the Competent Security Authority of the State of the transmitting Party shall inform the Competent Security Authority of the State of the Originating Party, ensure assistance in the security investigation of such event and take the necessary measures to limit the consequences in accordance with national legislation.

3. After completing the investigation, the Competent Security Authority of the State where the Compromise or possible Compromise of Classified Information occurred shall immediately inform in writing the Competent Security Authority of the State of the other Party on the findings and conclusions of the investigation.

ARTICLE 11
SETTLEMENT OF DISPUTES

Any dispute regarding the interpretation or implementation of this Agreement shall be settled by negotiation between the Parties and shall not be referred to any third party for settlement.

ARTICLE 12
COSTS

Each Party shall independently bear the eventual costs related to the implementation of this Agreement in accordance with its national legislation.

ARTICLE 13
MUTUAL ASSISTANCE

1. Each Party shall assist personnel from the State of the other Party in the implementation and interpretation of the provisions of this Agreement.

2. Should the need arise the Competent Security Authorities of the States of the Parties upon written request will have mutual consultations.

3. The Competent Security Authorities of the States of the Parties shall inform each other of any changes to the national legislation in the sphere of protection of Classified Information that would affect the implementation of this Agreement provisions.

ARTICLE 14
FINAL PROVISIONS

1. This Agreement is concluded for an indefinite period of time and is subject to approval in accordance with national legislations of the Parties.

2. This Agreement shall enter into force on the first day of the second month following the receipt of the last of the notifications between the Parties that the internal legal procedures necessary for this Agreement to enter into force have been completed.

3. Each Party has the right to terminate this Agreement at any time. In such case the validity of the Agreement will expire after 6 (six) months following the day on which the notification of termination was served to the other Party.

4. Notwithstanding the termination of this Agreement, all Classified Information provided pursuant to this Agreement shall continue to be protected in accordance with the provisions set forth herein.

5. This Agreement may be amended on the basis of the mutual consent of the Parties. Such amendments shall enter info force in accordance with the provisions of paragraph (2).

6. Each Party shall promptly notify the other Party of any changes to its national laws and regulations that would affect the protection of Classified Information under this Agreement. In such case, the Parties shall consult each other to consider possible changes to this Agreement. In the meantime, Classified Information shall continue to be protected as described herein, unless requested otherwise in writing by the Originating Party.

Signed in Bucharest on 22nd of October 2013, in two original copies each one in the Romanian, Ukrainian and English languages, all texts being equally authentic. In case of differences in the interpretation, the English text shall prevail.

FOR THE GOVERNMENT OF ROMANIA

MARIUS PETRESCU, Phd
Secretary of State
Director General
of the National Registry Office
for Classified Information

FOR THE CABINET OF MINISTERS OF UKRAINE

VOLODYMYR PORODKO
Deputy Chairman
of the Security Service of Ukraine

УГОДА

МІЖ

УРЯДОМ РУМУНІЇ

ТА

КАБІНЕТОМ МІНІСТРІВ УКРАЇНИ

ПРО ВЗАЄМНУ ОХОРОНУ ІНФОРМАЦІЇ

З ОБМЕЖЕНИМ ДОСТУПОМ

Уряд Румунії та Кабінет Міністрів України (далі – Сторони),

з метою забезпечення охорони всієї інформації з обмеженим доступом, яка спільно створюється або обмін якою здійснюється між Сторонами безпосередньо або через державні установи та/або юридичні особи, та у рамках діяльності, яка підпадає під відповідальність компетентних органів безпеки Сторін,

домовилися про таке:

СТАТТЯ 1
ЗАСТОСУВАННЯ

1. Ця Угода формує основу для будь-якого обміну інформацією з обмеженим доступом, який здійснюється між Сторонами безпосередньо або через державні органи та інші юридичні особи, або для спільного створення такої інформації.

2. Ця Угода не впливає на зобов'язання Сторін, взяті кожною зі Сторін за іншими міжнародними договорами, і вона не буде використовуватися проти інтересів, безпеки та територіальної цілісності інших держав.

СТАТТЯ 2
ВИЗНАЧЕННЯ ТЕРМІНІВ

Для цілей цієї Угоди терміни вживаються у такому значенні:

a) "інформація з обмеженим доступом" – будь-яка інформація, незалежно від її фізичної форми, носія та способу запису, якій згідно з національним законодавством надано відповідний ступінь обмеження доступу та яка охороняється відповідним чином;

b) "гриф обмеження доступу" – реквізит, що вказує на ступінь обмеження доступу, наданий інформації з обмеженим доступом відповідно до законодавства держав Сторін;

c) "контракт з обмеженим доступом" – договір у будь-якій формі між державними органами та/або іншими юридичними особами держав Сторін, що стосується інформації з обмеженим доступом;

d) "Сторона-джерело" – державний орган або інша юридична особа держави Сторони, що створює та передає інформацію з обмеженим доступом;

e) "Сторона-одержувач" – державний орган або інша юридична особа держави Сторони, яка отримує інформацію з обмеженим доступом Сторони-джерела;

f) "порушення правил безпеки" – дія або бездіяльність, вчинена всупереч національним правилам безпеки, що призводить до дійсної чи можливої компрометації інформації з обмеженим доступом;

g) "компрометація інформації з обмеженим доступом" – ситуація, коли за результатом порушення правил безпеки чи ворожої діяльності (такої як шпигунство, терористичний акт чи викрадення) інформація з обмеженим доступом втратила свою конфіденційність, цілісність чи доступність, або коли підтримуючі служби та ресурси втратили цілісність чи доступність. Це включає втрату, часткове чи повне розголошення, несанкціоноване перетворення та несанкціоноване знищення або відмову від обслуговування;

h) "допуск" – документ, виданий відповідно до законодавства держав Сторін, який засвідчує, що його власника під час виконання своїх обов'язків уповноважено мати доступ до інформації з обмеженим доступом з відповідним ступенем обмеження доступу згідно з принципом "необхідного знання";

i) "необхідне знання" – принцип, за яким доступ до інформації з обмеженим доступом може надаватися в індивідуальному порядку лише тим особам, які під час виконання своїх службових обов'язків мають потребу в доступі до такої інформації;

j) "компетентний орган безпеки" – установа, наділена повноваженнями на державному рівні, яка відповідно до законодавства держав Сторін забезпечує виконання заходів охорони інформації з обмеженим доступом. Такі органи перелічені у статті 3 цієї Угоди.

СТАТТЯ 3
КОМПЕТЕНТНІ ОРГАНИ БЕЗПЕКИ

1. Компетентними органами безпеки Сторін є:

В Румунії	В Україні
Національний офіс реєстрації інформації з обмеженим доступом Уряду Румунії вул. Мурес, 4 Бухарест 1 Румунія	Служба безпеки України вул. Володимирська, 33 Київ Україна

2. Компетентні органи безпеки за запитом інформують один одного про свої організацію та процедури безпеки. Для цього компетентні органи безпеки узгоджують взаємні візити.

3. Компетентні органи безпеки інформують один одного про будь-які зміни у їх найменуваннях або передачу їхньої компетенції іншим органам.

СТАТТЯ 4
ПОРІВНЯННЯ ГРИФІВ ОБМЕЖЕННЯ ДОСТУПУ

1. Сторони визначили, що порівняння національних грифів обмеження доступу є таким:

В Румунії	**В Україні**	**Еквівалент англійською мовою**
STRICT SECRET DE IMPORTANTĂ DEOSEBITĂ	Особливої важливості	TOP SECRET
STRICT SECRET	Цілком таємно	SECRET
SECRET	Таємно	CONFIDENTIAL
SECRET DE SERVICIU	Для службового користування	RESTRICTED

2. Кожна зі Сторін позначає усю інформацію з обмеженим доступом, отриману від іншої Сторони, відповідним національним грифом обмеження доступу згідно з еквівалентністю, визначеною у пункті 1 цієї статті.

СТАТТЯ 5
ОХОРОНА ІНФОРМАЦІЇ З ОБМЕЖЕНИМ ДОСТУПОМ

1. Згідно із законодавством своїх держав Сторони здійснюють відповідні заходи з охорони інформації з обмеженим доступом, яка передається, отримується, створюється або розробляється за результатом будь-якої угоди у будь-якій формі між державними органами та/або іншими юридичними особами держав Сторін. Сторони забезпечують стосовно всієї отриманої чи спільно створеної інформації з обмеженим доступом такий самий рівень охорони, який передбачається для національної інформації з обмеженим доступом, позначеної відповідним грифом обмеження доступу, згідно з пунктом 1 статті 4 цієї Угоди.

2. Сторона-одержувач не знижує ступінь обмеження доступу отриманої інформації з обмеженим доступом та не скасовує обмеження доступу до неї без попередньої письмової згоди компетентного органу безпеки держави Сторони-джерела. Сторона-джерело інформує Сторону-одержувача про будь-які зміни ступеня обмеження доступу переданої інформації з обмеженим доступом.

3. Усі відтворення інформації з обмеженим доступом позначаються таким самим грифом обмеження доступу, як і оригінальна інформація з обмеженим доступом, та охороняються відповідним чином. Кількість відтворень обмежується кількістю, необхідною для службових цілей.

4. Отримана інформація з обмеженим доступом, позначена грифом STRICT SECRET DE IMPORTANTĂ DEOSEBITĂ/"Особливої важливості"/TOP SECRET, відтворюється або перекладається лише за попередньою письмовою згодою Сторони-джерела.

5. Інформація з обмеженим доступом, позначена грифом обмеження доступу SECRET/"Таємно"/CONFIDENTIAL чи STRICT SECRET/"Цілком таємно"/SECRET, може знищуватися лише за письмовою згодою або за вимогою Сторони-джерела відповідно до законодавства держави Сторони-одержувача таким чином, що її повне чи часткове відновлення стає неможливим. Інформація з грифом STRICT SECRET DE IMPORTANTĂ DEOSEBITĂ/"Особливої важливості"/TOP SECRET не знищується, а повертається Стороні-джерелу.

6. Сторона-одержувач інформує Сторону-джерело про знищення інформації з обмеженим доступом.

7. У разі невідворотної загрози інформація з обмеженим доступом знищується без попереднього дозволу. Компетентний орган безпеки держави Сторони-джерела негайно інформується про це.

8. Доступ до інформації з обмеженим доступом, одержаної за цією Угодою, дозволяється за умови дотримання принципу "необхідного знання" лише тим особам, яким надано допуск, що відповідає ступеню обмеження доступу інформації, доступ до якої потребується, або яких уповноважено на це відповідно до національного законодавства.

9. Жодна із Сторін не передає отриману інформацію з обмеженим доступом третій стороні без попереднього письмового дозволу компетентного органу безпеки держави Сторони-джерела. Ця Угода не застосовується будь-якою зі Сторін для того, щоб одержати інформацію з обмеженим доступом, яку інша Сторона отримала від третьої сторони.

СТАТТЯ 6
ДОПУСК

1. Допуск надається за результатами перевірки відповідно до законодавства держави кожної Сторони.

2. За запитом компетентні органи безпеки держав Сторін, беручи до уваги відповідне національне законодавство, сприяють один одному у проведенні процедур перевірки стосовно надання допуску та дозволу на провадження діяльності, пов'язаної з інформацією з обмеженим доступом. Для цього між компетентними органами безпеки держав Сторін можуть укладатися відповідні домовленості.

3. Сторони взаємно визнають допуски та дозволи на провадження діяльності, пов'язаної з інформацією з обмеженим доступом, видані згідно із законодавством їхніх держав.

4. У рамках виконання цієї Угоди компетентні органи безпеки інформують один одного про будь-які зміни в допусках та дозволах на провадження діяльності, пов'язаної з інформацією з обмеженим доступом, зокрема про їх скасування.

СТАТТЯ 7
ВІЗИТИ

1. Візити, що включають доступ до інформації з обмеженим доступом або до приміщень, де така інформація створюється, обробляється чи зберігається, або де здійснюється діяльність, пов'язана з інформацією з обмеженим доступом, дозволяються одною Стороною відвідувачам з держави іншої Сторони лише після отримання попереднього письмового дозволу компетентного органу безпеки держави Сторони, що приймає. Такий дозвіл надається лише особам, які мають відповідний допуск, та за принципом "необхідного знання".

2. Про здійснення візитів повідомляється заздалегідь за 20 (двадцять) робочих днів.

3. У термінових випадках запит на візит може передаватися пізніше, але не менш ніж за 5 (п'ять) робочих днів заздалегідь.

4. Запит на візит має містити:

a) ім'я, прізвище відвідувача, місце і дату народження, громадянство, номер паспорта чи посвідчення;

b) найменування установи, компанії або організації, яку він/вона представляє або співробітником якої він/вона є;

c) найменування та адресу установи, компанії або організації, яку планується відвідати;

d) підтвердження щодо допуску чи повноваження відвідувача;

e) мету візиту чи візитів;

f) очікувану дату та тривалість візиту чи візитів, стосовно яких робиться запит. У разі повторних візитів зазначається загальний період їх здійснення;

g) назву та телефонний номер контактного пункту в установі, яку планується відвідати, попередні контакти та будь-яку іншу інформацію, корисну для визначення обґрунтування візиту чи візитів;

h) дату, підпис та офіційну печатку компетентного органу безпеки.

5. Компетентний орган безпеки держави Сторони, що приймає, інформує відповідальних осіб з питань безпеки установ чи організацій, які планується відвідати, про дату та осіб, чий візит підтверджено.

6. У разі повторних візитів термін дії дозволу на візит не може перевищувати 12 (дванадцяти) місяців.

7. Кожна Сторона забезпечує охорону персональних даних відвідувачів відповідно до законодавства своєї держави.

СТАТТЯ 8
КОНТРАКТИ З ОБМЕЖЕНИМ ДОСТУПОМ

1. У разі, коли будь-яка зі Сторін має намір укласти контракт, пов'язаний з інформацією з обмеженим доступом, який буде виконуватися на території держави іншої Сторони, Сторона-одержувач бере на себе відповідальність за охорону інформації з обмеженим доступом, пов'язаної з контрактом, відповідно до законодавства своєї держави.

2. Перед передачею Стороною-джерелом інформації з обмеженим доступом державному органу та/або іншій юридичній особі держави іншої Сторони компетентний орган безпеки держави Сторони-одержувача має:

a) підтвердити, що відповідний державний орган та/або інша юридична особа має право на провадження діяльності, пов'язаної з інформацією з обмеженим доступом, або надати дозвіл на провадження діяльності, пов'язаної з інформацією з обмеженим доступом, відповідно до національного законодавства;

b) підтвердити, що усім особам, чиї обов'язки потребують доступу до інформації з обмеженим доступом, згідно з національним законодавством надано допуск, який відповідає ступеню обмеження доступу інформації.

3. Сторони забезпечують, щоб кожний контракт з обмеженим доступом включав відповідний додаток, який би містив:

a) перелік інформації з обмеженим доступом, що передається чи створюється за контрактом з обмеженим доступом, та її грифи обмеження доступу;

b) особливі вимоги щодо зберігання інформації з обмеженим доступом;

c) процедуру зв'язку для зміни ступеня обмеження доступу інформації з обмеженим доступом;

d) канали зв'язку та засоби електронної передачі;

e) процедуру передачі інформації;

f) зобов'язання повідомляти про будь-яку дійсну компрометацію інформації з обмеженим доступом або таку, що підозрюється;

g) порядок вирішення спорів.

4. Між компетентними органами безпеки держав Сторін можуть розроблятися та узгоджуватися детальні процедури, що стосуються контрактів з обмеженим доступом.

СТАТТЯ 9
ПЕРЕДАЧА ІНФОРМАЦІЇ З ОБМЕЖЕНИМ ДОСТУПОМ

1. Інформація з обмеженим доступом передається дипломатичними/військовими кур'єрами або іншими засобами, узгодженими компетентними органами безпеки. Сторона-одержувач письмово підтверджує Стороні-джерелу щодо отримання інформації з обмеженим доступом.

2. У разі відправлення інформації з обмеженим доступом великого розміру чи обсягу компетентні органи безпеки можуть взаємно узгодити та затвердити засоби передачі, а також заходи безпеки для кожного такого випадку.

3. Обмін інформацією з обмеженим доступом з використанням електронних засобів здійснюється відповідно до безпекових процедур, встановлених за взаємними домовленостями компетентними органами безпеки згідно з національним законодавством.

СТАТТЯ 10
ПОРУШЕННЯ ПРАВИЛ БЕЗПЕКИ ТА КОМПРОМЕТАЦІЯ ІНФОРМАЦІЇ З ОБМЕЖЕНИМ ДОСТУПОМ

1. У разі порушення правил безпеки компетентний орган безпеки держави Сторони-одержувача інформує компетентний орган безпеки держави Сторони-джерела, забезпечує належне розслідування такого випадку та здійснює необхідні заходи з обмеження наслідків відповідно до національного законодавства. За запитом компетентні органи безпеки сприяють один одному в розслідуванні.

2. У разі якщо компрометація інформації з обмеженим доступом сталася на території третьої сторони, компетентний орган безпеки держави Сторони, що здійснює передачу, інформує компетентний орган безпеки держави Сторони-джерела, забезпечує сприяння розслідуванню такого випадку та здійснює необхідні заходи з обмеження наслідків згідно з національним законодавством.

3. Після завершення розслідування компетентний орган безпеки держави, де компрометація чи можлива компрометація інформації з обмеженим доступом сталася, негайно письмово інформує компетентний орган безпеки держави іншої Сторони про результати та висновки розслідування.

СТАТТЯ 11
ВИРІШЕННЯ СПОРІВ

Будь-які спори стосовно тлумачення або виконання цієї Угоди вирішуються шляхом переговорів між Сторонами та не можуть бути передані третій стороні для врегулювання.

СТАТТЯ 12
ВИТРАТИ

Кожна Сторона самостійно несе можливі витрати, пов'язані з виконанням цієї Угоди, відповідно до законодавства своєї держави.

СТАТТЯ 13
ВЗАЄМНЕ СПРИЯННЯ

1. Кожна Сторона надає сприяння представникам держави іншої Сторони при виконанні та тлумаченні положень цієї Угоди.

2. У разі потреби компетентні органи безпеки держав Сторін за письмовим запитом проводять взаємні консультації.

3. Компетентні органи безпеки держав Сторін повідомляють одна одну про будь-які зміни національного законодавства у сфері охорони інформації з обмеженим доступом, які можуть вплинути на виконання положень цієї Угоди.

СТАТТЯ 14
ПРИКІНЦЕВІ ПОЛОЖЕННЯ

1. Ця Угода укладається на невизначений період і підлягає погодженню відповідно до законодавства держав Сторін.

2. Ця Угода набирає чинності на перший день другого місяця після отримання Сторонами останнього письмового повідомлення про виконання усіх внутрішньодержавних процедур, необхідних для набрання нею чинності.

3. Кожна Сторона має право у будь-який час припинити дію цієї Угоди. У такому разі термін дії Угоди завершується на наступний день через 6 (шість) місяців після надсилання іншою Стороною повідомлення про припинення дії.

4. Незважаючи на припинення дії цієї Угоди, вся інформація з обмеженим доступом, передана відповідно до цієї Угоди, охороняється згідно з положеннями, викладеними в ній.

5. На основі взаємної згоди Сторін до цієї Угоди може бути внесено зміни та доповнення. Зміни та доповнення до цієї Угоди набирають чинності відповідно до положень пункту 2 цієї статті.

6. Кожна із Сторін невідкладно інформує одна одну про будь-які зміни законів та правил своїх держав, які впливатимуть на охорону інформації з обмеженим доступом за цією Угодою. У такому разі Сторони консультують одна одну про розгляд можливості внесення змін до цієї Угоди. Одночасно інформація з обмеженим доступом продовжує охоронятися, як це встановлено Угодою, доки Сторона-джерело письмово не повідомить про інше.

Підписано у м. Бухарест 22 жовтня 2013 року в двох примірниках, кожний румунською, українською та англійською мовами, при цьому всі тексти є автентичними. У випадку виникнення розбіжностей щодо тлумачення положень цієї Угоди, текст англійською мовою має переважну силу.

ЗА УРЯД
РУМУНІЇ

МАРИУС ПЕТРЕСКУ
Державний секретар
Генеральний директор
Національного офісу реєстрації
інформації з обмеженим доступом

ЗА КАБІНЕТ МІНІСТРІВ
УКРАЇНИ

ВОЛОДИМИР ПОРОДЬКО
Заступник Голови
Служби безпеки України