Anexă la HN - 805 din 20.09.2017

ACORD

ÎNTRE

GUVERNUL ROMÂNIEI

ŞI

GUVERNUL REPUBLICII CROAŢIA

PRIVIND PROTECŢIA RECIPROCĂ

A INFORMAŢIILOR CLASIFICATE

Guvernul României şi Guvernul Republicii Croaţia (denumite în continuare: Părţi),

Cunoscând faptul că buna cooperare poate face necesar un schimb de informaţii clasificate între Părţi, direct sau prin intermediul altor persoane juridice,

Dorind să stabilească un set de reguli care să reglementeze protecţia reciprocă a informaţiilor clasificate ce se vor aplica tuturor acordurilor de cooperare şi contractelor viitoare ce vor fi stabilite între Părţi, sau între persoanele juridice din statele acestora, şi care conţin sau implică accesul la informaţii clasificate,

Au convenit următoarele:

ARTICOLUL 1
SCOPUL ŞI DOMENIUL DE APLICARE

1. Scopul prezentului Acord este de a asigura protecţia Informaţiilor Clasificate schimbate sau generate în procesul de cooperare dintre Părţi sau dintre persoanele juridice din statele Părţilor.

2. Prezentul Acord se aplică oricărei activităţi ce implică schimbul de Informaţii Clasificate şi care se derulează sau urmează a se derula între Părţi sau între persoanele juridice din statele Părţilor.

3. Prezentul Acord nu va afecta obligaţiile celor două Părţi ce derivă din alte acorduri internaţionale la care sunt parte şi nu va fi folosit împotriva intereselor, securităţii şi integrităţii teritoriale ale altor state.

ARTICOLUL 2
DEFINIŢII

În prezentul Acord se vor utiliza următoarele definiţii:

(1) **Informaţie Clasificată:** înseamnă orice informaţie, document sau material, indiferent de forma fizică a acesteia, căreia i s-a atribuit un anumit nivel de clasificare în conformitate cu legislaţiile statelor Părţilor şi care va fi protejată corespunzător;

(2) **Nivel de Clasificare:** înseamnă o categorie care, în conformitate cu legislaţia statului Părţii, determină anumite restricţii privind accesul la Informaţii Clasificate, măsuri de protecţie şi marcaje;

(3) **Partea Emitentă:** înseamnă Partea, inclusiv orice altă persoană juridică din statul Părţii respective, care generează şi transmite Informaţii Clasificate către cealaltă Parte;

(4) **Partea Primitoare:** înseamnă Partea, inclusiv orice altă persoană juridică din statul Părţii respective, care primeşte Informaţii Clasificate de la cealaltă Parte;

(5) **Contract Clasificat:** înseamnă orice contract sau sub-contract care conţine sau implică accesul la Informaţii Clasificate;

(6) **Certificat de Securitate a Personalului:** înseamnă un document emis în conformitate cu legislaţia statului Părţii în baza unei proceduri de investigare finalizată printr-o decizie pozitivă şi prin care se acordă accesul la Informaţii Clasificate şi permisiunea de a gestiona Informaţiile Clasificate de un anumit Nivel de Clasificare;

(7) **Certificat de Securitate Industrială:** înseamnă un document emis în conformitate cu legislaţia statului Părţii, în baza unei proceduri de investigare finalizată printr-o decizie pozitivă, prin care se atestă că o persoană juridică este abilitată să desfăşoare activităţi legate de un Contract Clasificat;

(8) **Autoritate Competentă de Securitate:** înseamnă instituţia menţionată la art. 3, învestită cu autoritate la nivel naţional care, în conformitate cu legislaţiile statelor Părţilor, asigură implementarea unitară a măsurilor de protecţie a Informaţiilor Clasificate;

(9) **Necesitatea de a cunoaşte:** înseamnă principiul conform căruia accesul la Informaţii Clasificate poate fi acordat unei persoane în vederea îndeplinirii îndatoririlor oficiale şi sarcinilor de serviciu;

(10) **Compromiterea:** înseamnă orice întrebuinţare necorespunzătoare, contrară legislaţiei naţionale, care are drept rezultat deteriorarea sau accesul neautorizat, modificarea, dezvăluirea ori distrugerea Informaţiilor Clasificate precum şi orice altă acţiune sau inacţiune care duce la pierderea confidenţialităţii, integrităţii sau disponibilităţii acestora.

ARTICOLUL 3
AUTORITĂŢILE COMPETENTE DE SECURITATE

1. Autorităţile Competente de Securitate responsabile pentru implementarea prezentului Acord sunt:

În România:
Guvernul României
Oficiul Registrului Naţional al Informaţiilor Secrete de Stat

În Republica Croaţia:
Oficiul Consiliului Naţional de Securitate

2. Părţile se vor informa reciproc, pe canale diplomatice, despre orice modificare relevantă cu privire la Autorităţile Competente de Securitate.

ARTICOLUL 4
NIVELURI DE CLASIFICARE

1. Echivalenţa nivelurilor de clasificare naţionale este următoarea:

În România	**În Republica Croaţia**
STRICT SECRET DE IMPORTANŢĂ DEOSEBITĂ	VRLO TAJNO
STRICT SECRET	TAJNO
SECRET	POVJERLJIVO
SECRET DE SERVICIU	OGRANIČENO

2. Partea Emitentă va informa cu promptitudine Partea Primitoare asupra oricăror modificări survenite în Nivelurile de Clasificare ale Informaţiilor Clasificate transmise.

3. Partea Emitentă va informa Partea Primitoare asupra condiţiilor suplimentare de transmitere sau de limitare a utilizării Informaţiilor Clasificate transmise.

4. Partea Primitoare se va asigura că Informaţiile Clasificate primite sunt marcate cu Nivelul de Clasificare naţional echivalent, în conformitate cu alin. (1) al acestui articol.

5. Atribuirea unui Nivel de Clasificare Informaţiilor Clasificate generate în comun, modificarea acestuia precum şi declasificarea acestor informaţii se vor efectua cu acordul reciproc al Părţilor.

6. Părţile se vor informa reciproc asupra oricăror modificări survenite în Nivelurile de Clasificare naţionale.

ARTICOLUL 5
PROTECŢIA INFORMAŢIILOR CLASIFICATE

1. Partea Primitoare va asigura pentru toate Informaţiile Clasificate primite acelaşi nivel de protecţie ca şi pentru Informaţiile Clasificate naţionale având Nivel de Clasificare echivalent, în conformitate cu art. 4 alin.(1).

2. Nimic din conţinutul prezentului Acord nu va prejudicia legislaţia din statele Părţilor referitoare la accesul persoanelor la documente sau accesul la informaţiile de interes public, protecţia datelor personale sau protecţia Informaţiilor Clasificate.

3. Fiecare Parte se va asigura că au fost aplicate măsurile corespunzătoare pentru protecţia Informaţiilor Clasificate prelucrate, stocate sau transmise prin sistemele informatice şi de comunicaţii. Aceste măsuri vor asigura confidenţialitatea, integritatea, disponibilitatea şi, dacă este cazul, ne-repudierea şi autenticitatea Informaţiilor Clasificate, precum şi un grad corespunzător de evidenţă şi urmărire a acţiunilor legate de informaţiile respective.

ARTICOLUL 6
DEZVĂLUIREA ŞI UTILIZAREA INFORMAŢIILOR CLASIFICATE

1. Fiecare Parte se va asigura că Informaţiile Clasificate furnizate sau schimbate în baza prezentului Acord nu vor fi:

   a) declasificate şi nici nu li se va scădea Nivelul de Clasificare fără acordul prealabil scris al Părţii Emitente sau la cererea acesteia;

   b) folosite în alte scopuri decât cele pentru care au fost furnizate şi în afara limitelor stabilite de Partea Emitentă;

c) divulgate unui stat terţ, organism internaţional, persoană fizică sau juridică fără acordul prealabil scris al Părţii Emitente.

2. Dacă oricare alt acord încheiat între Părţi cuprinde reglementări mai stricte referitoare la schimbul sau protecţia Informaţiilor Clasificate, se vor aplica reglementările respective.

ARTICOLUL 7
ACCESUL LA INFORMAŢII CLASIFICATE

1. Accesul la informaţiile clasificate SECRET/POVJERLJIVO şi de nivel superior şi /sau în zonele şi incintele unde se desfăşoară activităţi ce implică astfel de informaţii este permis, cu respectarea principiului Necesităţii de a cunoaşte, numai persoanelor autorizate şi care deţin Certificat de Securitate a Personalului valabil pentru Nivelul de Clasificare al informaţiilor pentru care se solicită accesul.

2. Accesul la informaţiile clasificate SECRET DE SERVICIU/ OGRANIČENO se va limita numai la persoanele care respectă principiul Necesităţii de a cunoaşte şi sub condiţia ca acestea să îndeplinească cerinţele pentru acces la această categorie de Informaţii Clasificate în conformitate cu legislaţia din statele Părţilor.

3. Fiecare Parte se va asigura că toate persoanele cărora li s-a acordat accesul la Informaţii Clasificate sunt informate cu privire la responsabilităţile de a proteja aceste informaţii în conformitate cu reglementările de securitate corespunzătoare.

4. La cerere, Părţile, prin intermediul Autorităţilor Competente de Securitate, vor confirma faptul că unei persoane i s-a acordat Certificat de Securitate a Personalului anterior accesării Informaţiilor Clasificate emise de Partea Emitentă.

ARTICOLUL 8
TRADUCEREA ŞI MULTIPLICAREA INFORMAŢIILOR CLASIFICATE

1. Toate traducerile şi multiplicările Informaţiilor Clasificate vor fi marcate cu Nivelul de Clasificare naţional corespunzător şi vor fi protejate în acelaşi mod ca şi Informaţiile Clasificate originale.

2. Toate traducerile şi multiplicările Informaţiilor Clasificate vor fi efectuate de persoane care deţin Certificate de Securitate a Personalului corespunzătoare.

3. Toate traducerile Informaţiilor Clasificate vor conţine o adnotare corespunzătoare în limba în care au fost traduse prin care se va indica faptul că acestea conţin Informaţii Clasificate ale Părţii Emitente.

4. Informaţiile Clasificate marcate STRICT SECRET DE IMPORTANŢĂ DEOSEBITĂ/VRLO TAJNO vor fi traduse sau multiplicate numai în baza permisiunii prealabile scrise a Părţii Emitente.

5. Toate multiplicările şi traducerile Informaţiilor Clasificate vor fi supuse aceloraşi măsuri de protecţie ca şi informaţiile originale. Numărul de copii se va limita la cel necesar pentru scopurile oficiale.

ARTICOLUL 9
DISTRUGEREA INFORMAŢIILOR CLASIFICATE

1. Informaţiile Clasificate vor fi distruse în conformitate cu legislaţia naţională a Părţii Primitoare astfel încât reconstrucţia parţială sau totală a acestora să nu fie posibilă.

2. Distrugerea Informaţiilor Clasificate se realizează numai cu acordul prealabil scris sau la cererea Părţii Emitente.

3. Informaţiile STRICT SECRET DE IMPORTANŢĂ DEOSEBITĂ/ VRLO TAJNO nu vor fi distruse. Acestea vor fi returnate Părţii Emitente după ce Partea Primitoare consideră că nu mai sunt necesare sau la cererea Părţii Emitente.

4. Partea Primitoare va informa în scris Partea Emitentă cu privire la distrugerea Informaţiilor Clasificate.

5. În cazul în care este imposibilă protejarea sau returnarea Informaţiilor Clasificate generate sau transmise în baza prezentului Acord, acestea vor fi distruse imediat. Partea Primitoare va notifica în cel mai scurt timp Autoritatea Competentă de Securitate a Părţii Emitente cu privire la distrugerea Informaţiilor Clasificate.

ARTICOLUL 10
TRANSMITEREA INFORMAŢIILOR CLASIFICATE

1. Informaţiile clasificate vor fi transmise prin canale diplomatice, curieri militari sau alte mijloace convenite de Autorităţile Competente de Securitate în conformitate cu legislaţia statului Părţii care iniţiază transmiterea. Partea primitoare va confirma în scris primirea Informaţiilor Clasificate.

2. Informaţiile Clasificate vor fi transmise electronic în formă criptată, prin utilizarea mijloacelor şi dispozitivelor criptografice acceptate reciproc de Autorităţile Competente de Securitate, în conformitate cu legislaţiile statelor Părţilor.

3. Dacă există un volum mare de Informaţii Clasificate ce trebuie transmis, Autorităţile Competente de Securitate vor conveni mijloacele de transport, traseul şi măsurile de securitate pentru fiecare caz în parte.

ARTICOLUL 11
VIZITE

1. Vizitele ce implică acces la Informaţii Clasificate efectuate pe teritoriul statului Părţii gazdă sunt supuse autorizării scrise prealabile a Autorităţii Competente de Securitate a Părţii gazdă, sau unei alte proceduri convenite între Părţi, în conformitate cu legislaţia statului respectiv.

2. Cererea de vizită va fi transmisă Autorităţii Competente de Securitate a Părţii gazdă şi va cuprinde următoarele date ce vor fi folosite numai în scopul vizitei:

   a) numele şi prenumele vizitatorului, data şi locul naşterii, cetăţenia, şi numărul paşaportului sau al cărţii de identitate;

   b) funcţia vizitatorului, cu specificarea numelui angajatorului pe care vizitatorul îl reprezintă;

   c) specificarea proiectului la care participă vizitatorul;

   d) confirmarea deţinerii Certificatului de Securitate a Personalului de către vizitator, valabilitatea acestuia şi Nivelul de Clasificare a informaţiilor până la care acesta poate acorda acces vizitatorului;

e) numele, adresa, numărul de telefon / fax, adresa de e-mail şi persoana de contact din cadrul instituţiei ce urmează a fi vizitată;

f) scopul vizitei, inclusiv cel mai înalt Nivel de Clasificare a Informaţiilor Clasificate implicate;

g) data şi durata vizitei. În cazul vizitelor repetate, se va menţiona întreaga perioadă acoperită de vizite;

h) alte date, dacă s-a convenit astfel cu Autorităţile Competente de Securitate;

i) data, semnătura şi ştampila Autorităţii Competente de Securitate a Părţii solicitante.

3. Cererea de vizită va fi transmisă cu cel puţin douăzeci de zile înainte de vizită, dacă Autorităţile Competente de Securitate nu au convenit altfel, de comun acord.

4. Autoritatea Competentă de Securitate a Părţii care primeşte cererea de vizită va informa, în timp util, Autoritatea Competentă de Securitate a Părţii solicitante cu privire la decizia luată.

5. După aprobarea vizitei, Autoritatea Competentă de Securitate a Părţii gazdă va transmite funcţionarului de securitate din obiectivul ce urmează a fi vizitat un exemplar al cererii de vizită.

6. Vizitatorii vor respecta reglementările şi instrucţiunile de securitate ale Părţii gazdă.

7. Autorităţile Competente de Securitate pot conveni asupra unei liste de vizitatori care au dreptul să efectueze vizite repetate. Această listă este valabilă pentru o perioadă iniţială ce nu depăşeşte douăsprezece (12) luni şi poate fi extinsă pentru o perioadă de timp suplimentară nu mai mare de 12 luni. Cererea de vizite repetate va fi transmisă în conformitate cu alin. (3) al acestui articol. După aprobarea listei, vizitele pot fi aranjate direct între instituţiile implicate.

8. Partea gazdă va garanta protecţia datelor personale ale vizitatorilor în conformitate cu legislaţia statului său.

ARTICOLUL 12
CONTRACTE CLASIFICATE

1. În cazul în care o Parte sau o persoană juridică din statul său intenţionează să încheie un Contract Clasificat ce urmează a se derula pe teritoriul statului celeilalte Părţi, atunci Partea pe teritoriul căreia se derulează contractul îşi va asuma responsabilitatea de a proteja Informaţiile Clasificate legate de contract, în conformitate cu legislaţia statului său şi cu prevederile prezentului Acord.

2. La cerere, Autorităţile Competente de Securitate vor confirma dacă au fost eliberate Certificate de Securitate Industrială şi Certificate de Securitate a Personalului corespunzătoare persoanelor şi contractanţilor propuşi să participe la negocierile pre-contractuale sau la derularea Contractelor Clasificate anterior accesării de către aceştia a Informaţiilor Clasificate ale Părţii Emitente.

3. Fiecare Contract Clasificat încheiat între contractanţi, în conformitate cu prevederile prezentului Acord, va cuprinde o anexă de securitate corespunzătoare în care sunt menţionate cel puţin următoarele aspecte:

   a) lista Informaţiilor Clasificate gestionate în cadrul Contractului Clasificat şi Nivelurile de Clasificare ale acestora;

   b) procedura de comunicare a modificărilor apărute în Nivelurile de Clasificare ale informaţiilor schimbate;

   c) canale de comunicare şi mijloace de transmitere electromagnetică;

   d) procedura de transport a Informaţiilor Clasificate;

   e) obligaţia de a informa despre orice Compromitere survenită efectiv sau suspectată.

4. O copie a anexei de securitate a oricărui Contract Clasificat va fi transmisă Autorităţii Competente de Securitate a Părţii pe teritoriul căreia urmează să se deruleze Contractul Clasificat în vederea asigurării unei monitorizări corespunzătoare de securitate şi control.

5. Contractele Clasificate care implică accesul la informaţii SECRET DE SERVICIU/ OGRANIČENO vor conţine o clauză în care sunt specificate măsurile minime ce urmează a fi implementate pentru protecţia acestei categorii de Informaţii Clasificate.

6. Orice sub-contractant trebuie să îndeplinească aceleaşi obligaţii de securitate ca şi contractantul.

7. Autorităţile Competente de Securitate pot conveni asupra unor vizite reciproce în vederea analizării eficienţei măsurilor adoptate de contractant sau sub-contractant pentru protecţia Informaţiilor Clasificate vehiculate în Contractul Clasificat.

8. Părţile vor asigura protecţia drepturilor de autor, a drepturilor de proprietate industrială – inclusiv licenţele, secretele comerciale şi a oricăror alte drepturi legate de Informaţiile Clasificate schimbate între statele lor, în conformitate cu legislaţiile statelor Părţilor.

9. Alte proceduri detaliate referitoare la Contractele Clasificate pot fi convenite între Autorităţile Competente de Securitate ale Părţilor.

ARTICOLUL 13
COOPERAREA DE SECURITATE

1. În vederea realizării şi menţinerii unor standarde de securitate similare, Autorităţile Competente de Securitate îşi vor furniza, la cerere, informaţii referitoare la standardele, procedurile şi practicile naţionale de securitate pentru protecţia Informaţiilor Clasificate. În acest sens, Autorităţile Competente de Securitate pot efectua vizite reciproce.

2. Dacă este necesar, Autorităţile Competente de Securitate pot încheia aranjamente de securitate pe aspecte tehnice specifice privind implementarea prezentului Acord.

3. După caz, Autorităţile Competente de Securitate se vor informa reciproc asupra riscurilor specifice de securitate care pot periclita Informaţiile Clasificate transmise.

4. La cerere, Autorităţile Competente de Securitate ale Părţilor, respectând legislaţiile statelor acestora, îşi vor acorda asistenţă reciprocă în procedura de eliberare a Certificatelor de Securitate a Personalului şi a Certificatelor de Securitate Industrială pentru proprii cetăţeni care locuiesc pe teritoriul

statului celeilalte Părţi sau pentru obiectivele industriale amplasate pe teritoriul statului celeilalte Părţi.

5. Autorităţile Competente de Securitate se vor informa reciproc asupra oricăror modificări privind Certificatele de Securitate a Personalului şi Certificatele de Securitate Industrială legate de cooperarea în baza prezentului Acord.

6. Părţile vor recunoaşte reciproc Certificatele de Securitate a Personalului şi Certificatele de Securitate Industrială emise pentru cetăţenii şi persoanele juridice din statele Părţilor, în conformitate cu legislaţiile statelor lor, în ceea ce priveşte accesul la Informaţiile Clasificate schimbate în baza prezentului Acord.

7. Serviciile de securitate şi de informaţii din statele Părţilor pot coopera şi schimba direct informaţii operative şi/sau de securitate în conformitate cu legislaţiile naţionale.

ARTICOLUL 14
COMPROMITEREA INFORMAŢIILOR CLASIFICATE

1. Părţile vor lua toate măsurile adecvate, în conformitate cu legislaţiile statelor lor, pentru a stabili circumstanţele în care există certitudinea compromiterii sau motive temeinice de a suspecta compromiterea Informaţiilor Clasificate.

2. În cazul unei Compromiteri ce implică Informaţii Clasificate emise şi primite de la cealaltă Parte, Autoritatea Competentă de Securitate din statul în care s-a produs Compromiterea va informa imediat Autoritatea Competentă de Securitate a Părţii Emitente şi va asigura implementarea măsurilor corespunzătoare, în conformitate cu legislaţia naţională. Dacă va fi necesar, Părţile vor coopera pe parcursul procedurilor de mai sus.

3. În situaţia în care Compromiterea are loc pe teritoriul unui stat terţ, Autoritatea Competentă de Securitate a Părţii care a transmis informaţiile va acţiona conform alin. (2) al acestui articol.

4. În oricare dintre cazuri, Autoritatea Competentă de Securitate a Părţii Primitoare va informa în scris Autoritatea Competentă de Securitate a Părţii Emitente cu privire la circumstanţele producerii compromiterii, întinderea prejudiciului, măsurile adoptate pentru diminuarea prejudiciului şi rezultatul investigaţiei la care s-a făcut referire în alin.(2) al acestui articol. Notificarea respectivă trebuie să cuprindă suficiente detalii pentru ca Partea Emitentă să poată evalua pe deplin consecinţele.

ARTICOLUL 15
SOLUŢIONAREA DIFERENDELOR

Orice diferend între Părţi privind interpretarea sau implementarea prezentului Acord se va soluţiona numai prin consultări între Părţi.

ARTICOLUL 16
CHELTUIELI

Fiecare Parte va suporta cheltuielile proprii generate de implementarea prezentului Acord.

ARTICOLUL 17
DISPOZIŢII FINALE

1. Prezentul Acord se încheie pe o perioadă nedeterminată de timp. Acesta este supus aprobării în conformitate cu procedurile legale naţionale ale Părţilor şi intră în vigoare în prima zi a celei de-a doua luni de la data primirii, pe canale diplomatice, a ultimei notificări scrise prin care Părţile se informează reciproc că cerinţele legale interne necesare intrării în vigoare a prezentului Acord au fost îndeplinite.

2. Prezentul Acord poate fi amendat în orice moment pe baza consimţământului reciproc, scris, al Părţilor. Modificările respective vor intra în vigoare în conformitate cu prevederile alin.(1) al acestui articol.

3. Fiecare Parte are dreptul să denunţe prezentul Acord în orice moment, prin notificare scrisă transmisă celeilalte Părţi pe canale diplomatice. În acest caz, valabilitatea Acordului expiră după şase (6) luni de la data la care notificarea de denunţare a fost primită de cealaltă Parte.

4. Chiar şi în situaţia încetării valabilităţii prezentului Acord, toate Informaţiile Clasificate transmise în baza acestuia vor continua să fie protejate în conformitate cu prevederile stipulate până când Partea Emitentă dispensează Partea Primitoare de această obligaţie.

5. Părţile se vor informa reciproc, cu promptitudine, cu privire la orice modificări survenite în legislaţiile statelor acestora care ar putea afecta protecţia Informaţiilor Clasificate transmise în baza prezentului Acord. Într-o asemenea situaţie, Părţile se vor consulta în legătură cu oportunitatea unor posibile modificări ale prezentului Acord. Între timp, Informaţiile Clasificate vor continua să fie protejate aşa cum s-a prevăzut în acest Acord dacă Partea Emitentă nu solicită altfel, în scris.

Drept dovadă subsemnaţii, pe deplin autorizaţi în acest sens de guvernele lor proprii, am semnat prezentul Acord.

Încheiat la ZAGREB, la 12 IUNIE 2017, în două exemplare originale, fiecare în limbile română, croată şi engleză, toate textele fiind egal autentice. În caz de divergenţe de interpretare, va prevala textul în limba engleză.

PENTRU GUVERNUL ROMÂNIEI

PENTRU GUVERNUL REPUBLICII CROAŢIA

Copie certificată a exemplarului deţinut de MAE

14

Corina Badea, director

Direcţia Tratate Internaţionale

Ministerul Afacerilor Externe

ROMÂNIA * MINISTERUL AFACERILOR EXTERNE * Director General H2

Anexă la NN-805 din 20.09.2017

AGREEMENT

BETWEEN

THE GOVERNMENT OF ROMANIA

AND

THE GOVERNMENT OF THE REPUBLIC OF CROATIA

ON MUTUAL PROTECTION

OF CLASSIFIED INFORMATION

ROMÂNIA
Ministerul Afacerilor Externe
H2-2
DIRECTOR

The Government of Romania and the Government of the Republic of Croatia (hereinafter: the Parties),

Realizing that good cooperation may require exchange of classified information between the Parties, directly or through other legal entities,

Desiring to create a set of rules regulating the mutual protection of classified information applicable to any future co-operation agreements and contracts, which will be implemented between the Parties, or between legal entities of their states, containing or providing for access to classified information,

Have agreed as follows:

ARTICLE 1
OBJECTIVE AND SCOPE

1. The objective of this Agreement is to ensure the protection of Classified Information that is exchanged or created in the process of cooperation between the Parties or between legal entities of the states of the Parties.

2. This Agreement is applicable to any activity involving the exchange of Classified Information, conducted or to be conducted between the Parties or between legal entities of the states of the Parties.

3. This Agreement shall not affect the commitments of both Parties which stem from other international agreements by which they are bound and shall not be used against the interests, security and territorial integrity of other states.

ARTICLE 2
DEFINITIONS

In this Agreement, the following definitions shall be used:

(1) **Classified Information:** Any information, document or material, regardless of its physical form, to which a particular classification level has been assigned in accordance with the legislations of the states of the Parties and which shall be protected appropriately;

(2) **Classification Level:** A category which, in accordance with the legislation of the state of the Party, determines certain restrictions of access to Classified Information, measures of protection and markings;

(3) **Originating Party:** The Party, including any other legal entity of its state, which creates and releases Classified Information to the other Party;

(4) **Recipient Party:** The Party, including any other legal entity of its state, which receives Classified Information from the other Party;

(5) **Classified Contract:** A contract or sub-contract that contains or involves access to Classified Information;

(6) **Personnel Security Certificate:** A document issued in accordance with the legislation of the state of the Party and stemming from a vetting procedure finalized with a positive decision, which enables a person to be granted access and permission to handle Classified Information of a certain classification level;

(7) **Facility Security Certificate:** A document issued in accordance with the legislation of the state of the Party and stemming from a vetting procedure finalized with a positive decision, which is to enable a legal entity to carry out activities related to a Classified Contract;

(8) **Competent Security Authority:** The institution listed in Article 3, empowered with authority at national level which, in accordance with the legislation of the state of the Party, ensures the unitary implementation of the protective measures for Classified Information;

(9) **Need-to-know principle:** A principle by which access to Classified Information may be granted to an individual in order to be able to perform official duties and tasks;

(10) **Compromise:** Any form of misuse, contrary to the legislation of the state of the Party, which results in damage or unauthorized access, alteration, disclosure or destruction of Classified Information, as well as any other action or inaction, resulting in loss of its confidentiality, integrity or availability.

ARTICLE 3
COMPETENT SECURITY AUTHORITIES

1. The Competent Security Authorities responsible for the implementation of this Agreement are:

For Romania:
Government of Romania
National Registry Office for Classified Information.

For the Republic of Croatia:
Office of the National Security Council

2. The Parties shall inform each other through diplomatic channels of any relevant change regarding the Competent Security Authorities.

ARTICLE 4
CLASSIFICATION LEVELS

1. The equivalence of national classification levels is as follows:

For Romania	For the Republic of Croatia
STRICT SECRET DE IMPORTANŢĂ DEOSEBITĂ	VRLO TAJNO
STRICT SECRET	TAJNO
SECRET	POVJERLJIVO
SECRET DE SERVICIU	OGRANIČENO

2. The Originating Party shall without delay notify the Recipient Party of any changes to the classification level of released Classified Information.

3. The Originating Party shall inform the Recipient Party of additional conditions of release or limitations on the use of released Classified Information.

4. The Recipient Party shall ensure that received Classified Information is marked with an equivalent national Classification Level in accordance with paragraph 1 of this Article.

5. The assignment of a Classification Level to jointly created Classified Information, its change and the declassification of this information shall be made upon common consent of the Parties.

6. The Parties shall notify each other of any changes to national classification levels.

ARTICLE 5
PROTECTION OF CLASSIFIED INFORMATION

1. The Recipient Party shall provide to all received Classified Information the same protection as it is provided for the national Classified Information with the equivalent Classification Level, in accordance with Article 4 paragraph 1.

2. Nothing in this Agreement shall cause prejudice to the legislation of the state of the Party regarding public access to documents or access to information of public character, the protection of personal data or the protection of Classified Information.

3. Each Party shall ensure that appropriate measures are implemented for the protection of Classified Information processed, stored or transmitted in communication and information systems. Such measures shall ensure the confidentiality, integrity, availability and, where applicable, non-repudiation and authenticity of Classified Information, as well as an appropriate level of accountability and traceability of actions in relation to that information.

ARTICLE 6
DISCLOSURE AND USE OF CLASSIFIED INFORMATION

1. Each Party shall ensure that Classified Information provided or exchanged under this Agreement is not:

   a) downgraded or declassified without the prior written consent or at the request of the Originating Party;

   b) used for purposes other than it was provided for and out of the limitations stated by the Originating Party;

c) disclosed to any third state, international organisation, individual or legal entity without the prior written consent of the Originating Party.

2. If any other agreement concluded between the Parties contains stricter regulations regarding the exchange or protection of Classified Information, these regulations shall apply.

ARTICLE 7
ACCESS TO CLASSIFIED INFORMATION

1. Access to information classified SECRET/POVJERLJIVO and above and/or to locations and facilities where activities involving such information are performed is allowed, with the observance of the Need-to-know principle, only to individuals authorised and having a Personnel Security Certificate valid for the Classification Level of the information for which the access is required.

2. Access to information classified SECRET DE SERVICIU/OGRANIČENO shall be limited to those persons who have Need-to-know and provided they meet the requirements for access to such Classified Information in accordance with the legislation of the state of the Party.

3. Each Party shall ensure that all individuals granted access to Classified Information are informed of their responsibilities to protect such information in accordance with the appropriate security regulations.

4. On request, the Parties, through their Competent Security Authorities, shall confirm that a Personnel Security Certificate is granted to an individual before accessing Classified Information of the Originating Party.

ARTICLE 8
TRANSLATION AND REPRODUCTION OF CLASSIFIED INFORMATION

1. All translations and reproductions of Classified Information shall be marked with the appropriate national classification level and shall be protected as the original Classified Information.

2. All translations and reproductions of Classified Information shall be made by persons having appropriate Personnel Security Certificates.

3. All translations of Classified Information shall contain a suitable annotation in the language of translation, indicating that they contain Classified Information of the Originating Party.

4. Classified Information marked STRICT SECRET DE IMPORTANŢĂ DEOSEBITĂ/VRLO TAJNO shall be translated or reproduced only upon the prior written permission of the Originating Party.

5. All reproductions and translations of Classified Information shall be placed under the same protective measures as the original information. The number of copies shall be limited to that required for official purposes.

ARTICLE 9
DESTRUCTION OF CLASSIFIED INFORMATION

1. Classified Information shall be destroyed in accordance with the legislation of the state of the Recipient Party, in such a manner as to eliminate its reconstruction in part or in whole.

2. Classified Information shall be destroyed only with the prior written consent of or at the request of the Originating Party.

3. STRICT SECRET DE IMPORTANŢĂ DEOSEBITĂ/VRLO TAJNO information shall not be destroyed. It shall be returned to the Originating Party after it is no longer considered necessary by the Recipient Party or upon request of the Originating Party.

4. The Recipient Party shall inform in writing the Originating Party of the destruction of Classified Information.

5. In case of a situation that makes it impossible to protect and return Classified Information created or released according to this Agreement, the Classified Information shall be destroyed immediately. The Recipient Party shall notify in due time the Competent Security Authority of the Originating Party about the destruction of the Classified Information.

ARTICLE 10
TRANSFER OF CLASSIFIED INFORMATION

1. Classified Information shall be transferred by diplomatic channels, military courier or other means agreed on by the Competent Security Authorities in accordance with the legislation of the state of the Party initiating the transfer. The Recipient Party shall acknowledge in writing the receipt of the Classified Information.

2. Classified Information shall be transferred electronically in cryptic form, by using the cryptographic methods and devices mutually accepted by the Competent Security Authorities in accordance with the legislation of the state of the Party.

3. If a large consignment containing Classified Information is to be transferred the Competent Security Authorities shall agree upon the means of transportation, the route and security measures for each such case.

ARTICLE 11
VISITS

1. Visits entailing access to Classified Information on the territory of the state of the host Party are subject to prior written authorisation given by the Competent Security Authority of the host Party, or otherwise agreed upon between them, in accordance with the legislation of its state.

2. A request for visit shall be submitted to the Competent Security Authority of the host Party and shall include the following data that shall be used for the purpose of the visit only:

a) the visitor's name, date and place of birth, citizenship and identification card/passport number;

b) the visitor's position, with specification of the employer that the visitor represents;

c) specification of the project in which the visitor is participating;

d) confirmation of the visitor's Personnel Security Certificate, its validity and the Classification Level of the information up to which it may grant access;

e) the name, address, phone/fax number, e-mail and point of contact of the facility to be visited;

f) the purpose of the visit, including the highest Classification Level of Classified Information involved;

g) the date and duration of the visit. For recurring visits, the total period covered by the visits shall be stated;

h) other data, if agreed upon by the Competent Security Authorities;

i) date, signature and stamp of the Competent Security Authority of the requesting Party.

3. A request for visit shall be submitted at least 20 days prior to the visit, unless otherwise mutually approved by the Competent Security Authorities.

4. The Competent Security Authority of the Party receiving the request for visit shall inform, in due time, the Competent Security Authority of the requesting Party about the decision.

5. Once the visit has been approved, the Competent Security Authority of the host Party shall provide a copy of the request for visit to the security officer of the facility to be visited.

6. Visitors shall comply with the security regulations and instructions of the host Party.

7. The Competent Security Authorities may agree on a list of visitors entitled to recurring visits. The list shall be valid for an initial period not exceeding 12 months and may be extended for a further period of time not exceeding 12 months. A request for recurring visits shall be submitted in accordance with paragraph 3 of this Article. Once the list has been approved, visits may be arranged directly between the facilities involved.

8. The host Party shall guarantee the protection of personal data of the visitors in accordance to the legislation of its state.

ARTICLE 12
CLASSIFIED CONTRACTS

1. In the event that a Party or a legal entity of its state intends to conclude a Classified Contract to be performed within the territory of the state of the other Party, then the Party on whose territory the performance is taking place will assume responsibility for the protection of Classified Information related to the contract in accordance with the legislation of its state and the provisions of this Agreement.

2. On request, the Competent Security Authorities shall confirm whether the proposed contractors as well as the individuals participating in pre-contractual negotiations or in the performance of Classified Contracts have been issued appropriate Facility Security Certificates and Personnel Security Certificates, before accessing Classified Information of the Originating Party.

3. Every Classified Contract concluded between contractors, under the provisions of this Agreement, shall include an appropriate security annex identifying at least the following aspects:

a) a listing of Classified Information related to the Classified Contract and its Classification Levels;

b) procedure for the communication of changes in the Classification Levels of the exchanged information;

c) communication channels and means for electromagnetic transmission;

d) procedure for the transportation of Classified Information;

e) an obligation to notify any actual or suspected Compromise.

4. A copy of the security annex of any Classified Contract shall be forwarded to the Competent Security Authority of the Party on whose territory the Classified Contract is to be performed, in order to allow adequate security supervision and control.

5. Classified Contracts entailing access to SECRET DE SERVICIU/ OGRANIČENO information shall contain an appropriate clause identifying the minimum measures to be implemented for the protection of such Classified Information.

6. Any sub-contractor must fulfil the same security obligations as the contractor.

7. The Competent Security Authorities may agree on mutual visits in order to analyze the efficiency of the measures adopted by a contractor or a sub-contractor for the protection of Classified Information involved in a Classified Contract.

8. The Parties shall ensure protection of copyrights, industrial property rights – including patents, trade secrets and any other rights connected with the Classified Information exchanged between their states, according to the legislations of their states.

9. Further detailed procedures related to Classified Contracts may be agreed upon between the Competent Security Authorities of the Parties.

ARTICLE 13
SECURITY CO-OPERATION

1. In order to achieve and maintain comparable standards of security, the Competent Security Authorities shall, on request, provide each other with information about their national security standards, procedures and practices for the protection of Classified Information. To this end, the Competent Security Authorities may conduct mutual visits.

2. If the need arise, the Competent Security Authorities may conclude security arrangements on specific technical aspects concerning the implementation of this Agreement.

3. The Competent Security Authorities shall inform each other of specific security risks that may endanger released Classified Information, as applicable.

4. On request, the Competent Security Authorities of the Parties, taking into account the legislations of their states, shall assist each other in the procedure of granting the Personnel Security Certificates and the Facility

Security Certificates of their nationals living or facilities located on the territory of the state of the other Party.

5. The Competent Security Authorities shall inform each other about any modifications regarding the Personnel Security Certificates and Facility Security Certificates, which are connected to the cooperation under this Agreement.

6. The Parties shall mutually recognise their respective Personnel Security Certificates and Facility Security Certificates, issued for the citizens and legal entities of their states, in accordance with the legislations of their states, as regards the access to Classified Information exchanged under this Agreement.

7. The security and intelligence services of the states of the Parties may cooperate and directly exchange operative and/or intelligence information in accordance with the legislations of their states.

ARTICLE 14
COMPROMISE

1. The Parties shall take all appropriate measures, in accordance with the legislations of their states, to determine the circumstances where it is known or where there are reasonable grounds for suspecting that Classified Information has been compromised.

2. In case of a Compromise involving Classified Information originated by and received from the other Party, the Competent Security Authority in whose state the Compromise occurred shall inform the Competent Security Authority of the Originating Party as soon as possible and ensure the implementation of appropriate measures in accordance with the legislation of its state. The Parties shall, if required, cooperate during the above referred proceedings.

3. In case the Compromise occurs on the territory of a third state, the Competent Security Authority of the dispatching Party shall take the actions referred to in paragraph 2 of this Article.

4. In any case, the Competent Security Authority of the Recipient Party shall inform the Competent Security Authority of the Originating Party in writing about the circumstances of the Compromise, the extent of the

damage, the measures taken for its mitigation and the outcome of the proceedings referred to in paragraph 2 of this Article. Such notification shall contain enough details so that the Originating Party may fully assess the consequences.

ARTICLE 15
SETTLEMENT OF DISPUTES

Any dispute between the Parties relating to the interpretation or application of this Agreement shall be settled through consultations between the Parties only.

ARTICLE 16
EXPENSES

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

ARTICLE 17
FINAL PROVISIONS

1. This Agreement is concluded for an indefinite period of time. It is subject to approval in accordance with the legal procedures of the state of each Party and shall enter into force on the first day of the second month following the date of receipt of the last written notification by which the Parties have informed each other, through diplomatic channels, that their internal legal requirements for the entry into force of this Agreement have been met.

2. This Agreement may be amended at any time by mutual written consent of the Parties. Such amendments shall enter into force in accordance with the provisions of paragraph 1 of this Article.

3. Each Party may terminate this Agreement at any time by written notification to the other Party through diplomatic channels. In this case, the Agreement shall terminate after six (6) months from the date of receipt of the termination notification by the other Party.

4. Notwithstanding the termination of this Agreement, all Classified Information released under this Agreement shall continue to be protected in

accordance with the provisions set out herein until the Originating Party dispenses the Recipient Party from this obligation.

5. The Parties shall promptly notify each other of any amendments to legislation of their states that affect the protection of Classified Information released under this Agreement. In the event of such amendments, the Parties shall consult to consider possible amendments to this Agreement. In the meantime, Classified Information shall continue to be protected as described herein, unless otherwise requested by the Originating Party in writing.

In witness whereof, the undersigned, duly authorised to this effect by their respective Governments, have signed this Agreement.

Done at ZAGREB on 12. ŽUNIĚ 2017 in two originals, each in the Romanian, Croatian and English languages, all texts being equally authentic. In case of divergences of interpretation, the English text shall prevail.

FOR THE GOVERNMENT OF ROMANIA

FOR THE GOVERNMENT OF THE REPUBLIC OF CROATIA

Copie certificată a exemplarului deținut de MAE

Corina Badea, director

Direcția Tratate Internaționale

Ministerul Afacerilor Externe

MINISTERUL AFACERILOR EXTERNE * ROMÂNIA * Director General H2

Anexă la UN-805 din 20.09.2017

UGOVOR

IZMEĐU

VLADE RUMUNJSKE

I

VLADE REPUBLIKE HRVATSKE

O

UZAJAMNOJ ZAŠTITI

KLASIFICIRANIH PODATAKA

Vlada Rumunjske i Vlada Republike Hrvatske (u daljnjem tekstu: stranke),

shvaćajući da dobra suradnja može zahtijevati razmjenu klasificiranih podataka između stranaka, izravno ili putem drugih pravnih osoba,

želeći uspostaviti skup pravila koja uređuju uzajamnu zaštitu klasificiranih podataka primjenjiv na sve buduće sporazume o suradnji i ugovore, koji će se provoditi između stranaka ili između pravnih osoba njihovih država, koji sadrže ili omogućavaju pristup klasificiranim podacima,

sporazumjele su se kako slijedi:

ČLANAK 1.
PREDMET I PODRUČJE PRIMJENE

1. Predmet ovog Ugovora je osiguravanje zaštite klasificiranih podataka koji se razmjenjuju ili nastaju u procesu suradnje između stranaka ili između pravnih osoba država stranaka.

2. Ovaj Ugovor primjenjuje se na bilo koju aktivnost koja uključuje razmjenu klasificiranih podataka, koja se provodi ili koja će se provoditi između stranaka ili između pravnih osoba država stranaka.

3. Ovaj Ugovor ne utječe na obveze obiju stranaka koje proizlaze iz drugih međunarodnih ugovora koji ih obvezuju i neće se koristiti protivno interesima, sigurnosti i teritorijalnoj cjelovitosti drugih država.

ČLANAK 2.
DEFINICIJE

U ovom Ugovoru koriste se sljedeće definicije:

(1) **klasificirani podaci:** bilo koji podatak, dokument ili materijal, neovisno o njegovom fizičkom obliku, kojem je dodijeljen određeni stupanj tajnosti u skladu sa zakonodavstvima država stranaka i koji se odgovarajuće štiti;

(2) **stupanj tajnosti:** kategorija koja, u skladu sa zakonodavstvom države stranke, utvrđuje određena ograničenja pristupa klasificiranim podacima, mjere zaštite i oznake;

(3) **stranka pošiljateljica:** stranka, uključujući bilo koju drugu pravnu osobu njezine države, koja stvara i ustupa klasificirane podatke drugoj stranci;

(4) **stranka primateljica:** stranka, uključujući bilo koju drugu pravnu osobu njezine države, koja prima klasificirane podatke od druge stranke;

(5) **klasificirani ugovor:** ugovor ili podugovor koji sadrži ili uključuje pristup klasificiranim podacima;

(6) **uvjerenje o sigurnosnoj provjeri osobe:** dokument izdan u skladu sa zakonodavstvom države stranke i koji proizlazi iz postupka provjere koji je okončan pozitivnom odlukom, koji omogućava da se osobi odobri pristup i dopusti postupanje s klasificiranim podacima određenog stupnja tajnosti;

(7) **uvjerenje o sigurnosnoj provjeri pravne osobe:** dokument izdan u skladu sa zakonodavstvom države stranke i koji proizlazi iz postupka provjere koji je okončan pozitivnom odlukom, koji omogućava pravnoj osobi izvršavanje aktivnosti u vezi s klasificiranim ugovorom;

(8) **nadležno sigurnosno tijelo:** tijelo navedeno u članku 3., ovlašteno na nacionalnoj razini, koje, u skladu sa zakonodavstvom države stranke, osigurava jedinstvenu provedbu zaštitnih mjera za klasificirane podatke;

(9) **načelo nužnosti pristupa podacima za obavljanje poslova iz djelokruga:** načelo prema kojem se pristup klasificiranim podacima može odobriti osobi kako bi mogla obavljati službene dužnosti i zadaće;

(10) **povreda sigurnosti klasificiranih podataka:** svaki oblik zlouporabe, suprotan zakonodavstvu države stranke, koji rezultira štetom ili neovlaštenim pristupom, izmjenom, otkrivanjem ili uništavanjem klasificiranih podataka, kao i svaka druga radnja ili nedostatak iste, koja dovodi do gubitka njihove povjerljivosti, cjelovitosti ili dostupnosti.

ČLANAK 3.
NADLEŽNA SIGURNOSNA TIJELA

1. Nadležna sigurnosna tijela odgovorna za provedbu ovog Ugovora su:

   Za Rumunjsku:
   Vlada Rumunjske
   Nacionalni ured registra za klasificirane podatke

   Za Republiku Hrvatsku:
   Ured Vijeća za nacionalnu sigurnost.

2. Stranke obavješćuju jedna drugu diplomatskim putem o svakoj mjerodavnoj izmjeni u vezi s nadležnim sigurnosnim tijelima.

ČLANAK 4.
STUPNJEVI TAJNOSTI

1. Istoznačnosti nacionalnih stupnjeva tajnosti su sljedeće:

Za Rumunjsku	Za Republiku Hrvatsku
STRICT SECRET DE IMPORTANȚĂ DEOSEBITĂ	VRLO TAJNO
STRICT SECRET	TAJNO
SECRET	POVJERLJIVO
SECRET DE SERVICIU	OGRANIČENO

2. Stranka pošiljateljica bez odgode obavješćuje stranku primateljicu o bilo kojim izmjenama stupnja tajnosti ustupljenih klasificiranih podataka.

3. Stranka pošiljateljica obavješćuje stranku primateljicu o dodatnim uvjetima ustupanja ili ograničenjima korištenja ustupljenih klasificiranih podataka.

4. Stranka primateljica osigurava da se primljeni klasificirani podaci označavaju istoznačnim nacionalnim stupnjem tajnosti u skladu sa stavkom 1. ovog članka.

5. Dodjeljivanje stupnja tajnosti zajednički stvorenim klasificiranim podacima, njegova promjena i deklasifikacija tih podataka provodi se na temelju zajedničkog pristanka stranaka.

6. Stranke obavješćuju jedna drugu o bilo kojim izmjenama nacionalnih stupnjeva tajnosti.

ČLANAK 5.
ZAŠTITA KLASIFICIRANIH PODATAKA

1. Stranka primateljica dodjeljuje svim primljenim klasificiranim podacima jednaku zaštitu kakva se dodjeljuje nacionalnim klasificiranim podacima istoznačnog stupnja tajnosti, u skladu s člankom 4. stavkom 1.

2. Ništa u ovom Ugovoru ne dovodi u pitanje zakonodavstvo države stranke koje se odnosi na javni pristup dokumentima ili pristup podacima od javnog značaja, zaštitu osobnih podataka ili zaštitu klasificiranih podataka.

3. Svaka stranka osigurava provedbu odgovarajućih mjera za zaštitu klasificiranih podataka koji se obrađuju, pohranjuju ili prenose u komunikacijskim i informacijskim sustavima. Takvim mjerama osigurava se povjerljivost, cjelovitost, dostupnost i, kada je to moguće, neporecivost i autentičnost klasificiranih podataka, kao i odgovarajući stupanj odgovornosti za aktivnosti te sljedivosti aktivnosti u vezi s tim podacima.

ČLANAK 6.
USTUPANJE I KORIŠTENJE KLASIFICIRANIH PODATAKA

1. U vezi s klasificiranim podacima dostavljenim ili razmijenjenim u skladu s ovim Ugovorom, svaka stranka osigurava:

   a) da im se ne smanjuje stupanj tajnosti ili da se ne deklasificiraju bez prethodnog pisanog pristanka ili na zahtjev stranke pošiljateljice;

   b) da se ne koriste za druge svrhe osim onih za koje su dostavljeni i izvan ograničenja koje je postavila stranka pošiljateljica;

   c) da se ne ustupaju bilo kojoj trećoj državi, međunarodnoj organizaciji, fizičkoj ili pravnoj osobi bez prethodnog pisanog pristanka stranke pošiljateljice.

2. Ako bilo koji drugi ugovor koji su stranke sklopile sadrži strože odredbe u vezi s razmjenom ili zaštitom klasificiranih podataka, primjenjuju se te odredbe.

ČLANAK 7.
PRISTUP KLASIFICIRANIM PODACIMA

1. Pristup podacima označenim SECRET/POVJERLJIVO i više i/ili lokacijama i državnim tijelima ili pravnim osobama gdje se obavljaju aktivnosti koje uključuju takve podatke dopušten je, uz poštivanje načela nužnosti pristupa podacima za obavljanje poslova iz djelokruga, samo osobama koje su ovlaštene i posjeduju uvjerenje o sigurnosnoj provjeri osobe važeće za stupanj tajnosti podataka za koje se traži pristup.

2. Pristup podacima označenim SECRET DE SERVICIU/OGRANIČENO ograničen je na one osobe kojima je to nužno za obavljanje poslova iz djelokruga i ako zadovoljavaju uvjete za pristup takvim klasificiranim podacima u skladu sa zakonodavstvom države stranke.

3. Svaka stranka osigurava da su sve osobe kojima je odobren pristup klasificiranim podacima informirane o svojim odgovornostima za zaštitu takvih podataka u skladu s odgovarajućim sigurnosnim propisima.

4. Stranke, na zahtjev, putem svojih nadležnih sigurnosnih tijela, potvrđuju da je nekoj osobi izdano uvjerenje o sigurnosnoj provjeri osobe prije pristupanja klasificiranim podacima stranke pošiljateljice.

ČLANAK 8.
PREVOĐENJE I UMNOŽAVANJE KLASIFICIRANIH PODATAKA

1. Svi prijevodi i umnoženi primjerci klasificiranih podataka označavaju se odgovarajućim nacionalnim stupnjem tajnosti i štite se kao i izvorni klasificirani podaci.

2. Sve prijevode i umnožene primjerke klasificiranih podataka izrađuju osobe koje posjeduju odgovarajuća uvjerenja o sigurnosnoj provjeri osobe.

3. Svi prijevodi klasificiranih podataka sadrže odgovarajuću napomenu na jeziku prijevoda kojom se ukazuje da oni sadrže klasificirane podatke stranke pošiljateljice.

4. Klasificirani podaci označeni STRICT SECRET DE IMPORTANŢĂ DEOSEBITĂ/VRLO TAJNO prevode se ili umnožavaju samo na temelju prethodnog pisanog dopuštenja stranke pošiljateljice.

5. Svi umnoženi primjerci i prijevodi klasificiranih podataka štite se jednakim zaštitnim mjerama kao i izvorni podaci. Broj primjeraka ograničen je na broj potreban za službene svrhe.

ČLANAK 9.
UNIŠTAVANJE KLASIFICIRANIH PODATAKA

1. Klasificirani podaci uništavaju se u skladu sa zakonodavstvom države stranke primateljice, na način koji onemogućava njihovo djelomično ili potpuno obnavljanje.

2. Klasificirani podaci uništavaju se samo uz prethodni pisani pristanak ili na zahtjev stranke pošiljateljice.

3. Podaci STRICT SECRET DE IMPORTANŢĂ DEOSEBITĂ/VRLO TAJNO ne uništavaju se. Oni se vraćaju stranci pošiljateljici nakon što ih stranka primateljica više ne smatra potrebnima ili na zahtjev stranke pošiljateljice.

4. Stranka primateljica pisano obavješćuje stranku pošiljateljicu o uništavanju klasificiranih podataka.

5. U slučaju situacije u kojoj je nemoguće zaštititi i vratiti klasificirane podatke nastale ili ustupljene u skladu s ovim Ugovorom, klasificirani podaci odmah se uništavaju. Stranka primateljica u propisanom roku obavješćuje nadležno sigurnosno tijelo stranke pošiljateljice o uništavanju klasificiranih podataka.

ČLANAK 10.
PRIJENOS KLASIFICIRANIH PODATAKA

1. Klasificirani podaci prenose se diplomatskim putem, vojnim teklićima ili na druge načine koje su dogovorila nadležna sigurnosna tijela u skladu sa zakonodavstvom države stranke koja inicira prijenos. Stranka primateljica pisano potvrđuje primitak klasificiranih podataka.

2. Klasificirani podaci prenose se elektroničkim putem u kriptiranom obliku pomoću kriptografskih metoda i uređaja koje su uzajamno prihvatila nadležna sigurnosna tijela u skladu sa zakonodavstvom države stranke.

3. Ako je potrebno prenijeti veliku pošiljku koja sadrži klasificirane podatke, nadležna sigurnosna tijela dogovaraju način prijevoza, put i sigurnosne mjere za svaki takav slučaj.

ČLANAK 11.
POSJETI

1. Posjeti koji zahtijevaju pristup klasificiranim podacima na državnom području države stranke domaćina podliježu prethodnom pisanom odobrenju izdanom od nadležnog sigurnosnog tijela stranke domaćina, ili na drugi međusobno dogovoreni način, u skladu sa zakonodavstvom njezine države.

2. Zahtjev za posjet podnosi se nadležnom sigurnosnom tijelu stranke domaćina i sadrži sljedeće podatke koji se koriste samo u svrhu posjeta:

   a) ime posjetitelja, datum i mjesto rođenja, državljanstvo i broj identifikacijske iskaznice/putovnice;

   b) radno mjesto posjetitelja, s naznakom poslodavca kojeg posjetitelj predstavlja;

   c) specifikaciju projekta u kojem posjetitelj sudjeluje;

   d) potvrdu o uvjerenju o sigurnosnoj provjeri posjetitelja, njegovoj valjanosti i stupnju tajnosti podataka do kojeg se može omogućiti pristup;

   e) ime, adresu, broj telefona/telefaksa, e-mail i kontakt osobu državnog tijela ili pravne osobe koja se posjećuje;

   f) svrhu posjeta, uključujući najviši stupanj tajnosti uključenih klasificiranih podataka;

   g) datum i trajanje posjeta. Za ponovljene posjete navodi se ukupno razdoblje pokriveno posjetima;

   h) druge podatke, ako su to dogovorila nadležna sigurnosna tijela;

   i) datum, potpis i pečat nadležnog sigurnosnog tijela stranke koja podnosi zahtjev.

3. Zahtjev za posjet podnosi se najmanje 20 dana prije posjeta, osim ako nadležna sigurnosna tijela nisu uzajamno odobrila drugačije.

4. Nadležno sigurnosno tijelo stranke koja prima zahtjev za posjet u propisanom roku o odluci obavješćuje nadležno sigurnosno tijelo stranke koja podnosi zahtjev.

5. Nakon što je posjet odobren, nadležno sigurnosno tijelo stranke domaćina dostavlja primjerak zahtjeva za posjet savjetniku za informacijsku sigurnost državnog tijela ili pravne osobe koja se posjećuje.

6. Posjetitelji se pridržavaju sigurnosnih propisa i uputa stranke domaćina.

7. Nadležna sigurnosna tijela mogu dogovoriti popis posjetitelja koji imaju pravo na ponovljene posjete. Popis vrijedi tijekom početnog razdoblja koje nije dulje od 12 mjeseci i može se produljiti za daljnje razdoblje koje nije dulje od 12 mjeseci. Zahtjev za ponovljene posjete podnosi se u skladu sa stavkom 3. ovog članka. Jednom kada je popis odobren, posjeti se mogu dogovarati izravno između državnih tijela ili pravnih osoba koje su uključene u njih.

8. Stranka domaćin jamči zaštitu osobnih podataka posjetitelja u skladu sa zakonodavstvom svoje države.

ČLANAK 12.
KLASIFICIRANI UGOVORI

1. U slučaju da stranka ili pravna osoba njezine države namjerava sklopiti klasificirani ugovor koji se provodi na državnom području države druge stranke, tada stranka na čijem se državnom području odvija provedba preuzima odgovornost za zaštitu klasificiranih podataka u vezi s ugovorom, u skladu sa zakonodavstvom svoje države i odredbama ovog Ugovora.

2. Nadležna sigurnosna tijela, na zahtjev, potvrđuju jesu li predloženim ugovarateljima, kao i osobama koje sudjeluju u predugovornim pregovorima ili u provedbi klasificiranih ugovora, izdana odgovarajuća uvjerenja o sigurnosnoj provjeri pravne osobe i uvjerenja o sigurnosnoj provjeri osobe, prije pristupanja klasificiranim podacima stranke pošiljateljice.

3. Svaki klasificirani ugovor sklopljen između ugovaratelja prema odredbama ovog Ugovora uključuje odgovarajući sigurnosni prilog koji navodi najmanje sljedeće aspekte:
   a) popis klasificiranih podataka u vezi s klasificiranim ugovorom i njihove stupnjeve tajnosti;
   b) postupak obavješćivanja o promjenama stupnjeva tajnosti razmijenjenih podataka;
   c) komunikacijske putove i sredstva za elektromagnetski prijenos;
   d) postupak za prijevoz klasificiranih podataka;
   e) obvezu obavješćivanja o bilo kojoj stvarnoj povredi sigurnosti klasificiranih podataka ili sumnji na povredu sigurnosti klasificiranih podataka.

4. Primjerak sigurnosnog priloga bilo kojeg klasificiranog ugovora prosljeđuje se nadležnom sigurnosnom tijelu stranke na čijem se državnom području klasificirani ugovor provodi, kako bi se omogućio odgovarajući sigurnosni nadzor i kontrola.

5. Klasificirani ugovori koji zahtijevaju pristup podacima SECRET DE SERVICIU/OGRANIČENO sadrže odgovarajuću klauzulu kojom se određuju minimalne mjere koje se provode za zaštitu takvih klasificiranih podataka.

6. Svaki podugovaratelj mora ispunjavati iste sigurnosne obveze kao i ugovaratelj.

7. Nadležna sigurnosna tijela mogu dogovoriti uzajamne posjete kako bi analizirala učinkovitost mjera koje su usvojili ugovaratelj ili podugovaratelj za zaštitu klasificiranih podataka uključenih u klasificirani ugovor.

8. Stranke osiguravaju zaštitu prava intelektualnog vlasništva, prava industrijskog vlasništva - uključujući patente, poslovne tajne i bilo koja druga prava u vezi s klasificiranim podacima razmijenjenim između njihovih država, u skladu sa zakonodavstvima svojih država.

9. Nadležna sigurnosna tijela stranaka mogu dogovoriti daljnje detaljne postupke u vezi s klasificiranim ugovorima.

ČLANAK 13.
SIGURNOSNA SURADNJA

1. Kako bi se postigli i održali usporedivi standardi sigurnosti, nadležna sigurnosna tijela, na zahtjev, dostavljaju jedno drugom podatke o svojim nacionalnim sigurnosnim standardima, postupcima i praksama za zaštitu klasificiranih podataka. S tim ciljem, nadležna sigurnosna tijela mogu se međusobno posjećivati.

2. Bude li potrebno, nadležna sigurnosna tijela mogu sklapati sigurnosne dogovore o posebnim tehničkim aspektima u vezi s provedbom ovog Ugovora.

3. Nadležna sigurnosna tijela obavješćuju jedno drugo o posebnim sigurnosnim rizicima koji mogu ugroziti ustupljene klasificirane podatke, prema potrebi.

4. Nadležna sigurnosna tijela stranaka, na zahtjev, uzimajući u obzir zakonodavstva svojih država, pomažu jedno drugom u postupku izdavanja uvjerenja o sigurnosnoj provjeri osobe i uvjerenja o sigurnosnoj provjeri pravne osobe svojih državljana koji žive ili pravnih osoba koje se nalaze na državnom području države druge stranke.

5. Nadležna sigurnosna tijela obavješćuju jedno drugo o bilo kojim izmjenama u vezi s uvjerenjima o sigurnosnoj provjeri osobe i uvjerenjima o sigurnosnoj provjeri pravne osobe, koje su vezane uz suradnju na temelju ovog Ugovora.

6. Stranke uzajamno priznaju svoja odnosna uvjerenja o sigurnosnoj provjeri osobe i uvjerenja o sigurnosnoj provjeri pravne osobe izdana za državljane i pravne osobe njihovih država, u skladu sa zakonodavstvima njihovih država, u pogledu pristupa klasificiranim podacima razmijenjenim na temelju ovog Ugovora.

7. Sigurnosne i obavještajne službe država stranaka mogu surađivati i izravno razmjenjivati operativne i/ili obavještajne podatke u skladu sa zakonodavstvima svojih država.

ČLANAK 14.
POVREDA SIGURNOSTI KLASIFICIRANIH PODATAKA

1. Stranke poduzimaju sve odgovarajuće mjere, u skladu sa zakonodavstvima svojih država, kako bi utvrdile okolnosti u kojima je poznato ili u kojima postoji osnovani temelj za sumnju da je došlo do povrede sigurnosti klasificiranih podataka.

2. U slučaju povrede sigurnosti klasificiranih podataka koja uključuje klasificirane podatke nastale i primljene od druge stranke, nadležno sigurnosno tijelo u čijoj je državi došlo do povrede sigurnosti klasificiranih podataka obavješćuje nadležno sigurnosno tijelo stranke pošiljateljice što je prije moguće i osigurava provedbu odgovarajućih mjera u skladu sa zakonodavstvom svoje države. Stranke, ako je potrebno, surađuju tijekom gore navedenih postupaka.

3. U slučaju da do povrede sigurnosti klasificiranih podataka dođe na državnom području treće države, nadležno sigurnosno tijelo stranke pošiljatelja poduzima radnje iz stavka 2. ovog članka.

4. U svakom slučaju, nadležno sigurnosno tijelo stranke primateljice pisano obavješćuje nadležno sigurnosno tijelo stranke pošiljateljice o okolnostima povrede sigurnosti klasificiranih podataka, razmjerima štete, mjerama poduzetim za njezino ublažavanje i ishodu postupaka iz stavka 2. ovog članka. Takva obavijest sadrži dovoljno podataka kako bi stranka pošiljateljica mogla u potpunosti procijeniti posljedice.

ČLANAK 15.
RJEŠAVANJE SPOROVA

Bilo koji spor između stranaka u vezi s tumačenjem ili primjenom ovog Ugovora rješavat će se konzultacijama samo između stranaka.

ČLANAK 16.
TROŠKOVI

Svaka stranka snosi svoje vlastite troškove koji su nastali u tijeku provedbe ovog Ugovora.

ČLANAK 17.
ZAVRŠNE ODREDBE

1. Ovaj Ugovor sklapa se na neodređeno vrijeme. On podliježe odobrenju u skladu s pravnim postupcima države svake stranke i stupa na snagu prvog dana drugog mjeseca koji slijedi nakon datuma primitka posljednje pisane obavijesti kojom stranke obavješćuju jedna drugu, diplomatskim putem, da su ispunjeni njihovi unutarnji pravni uvjeti za stupanje na snagu ovog Ugovora.

2. Ovaj Ugovor može se izmijeniti i dopuniti u svako doba uzajamnim pisanim pristankom stranaka. Takve izmjene i dopune stupaju na snagu u skladu s odredbama stavka 1. ovog članka.

3. Svaka stranka može okončati ovaj Ugovor u svako doba pisanom obaviješću drugoj stranci, diplomatskim putem. U tom slučaju, Ugovor prestaje nakon šest (6) mjeseci od datuma kada je druga stranka primila obavijest o okončanju.

4. Unatoč prestanku ovog Ugovora, svi klasificirani podaci ustupljeni na temelju ovog Ugovora nastavljaju se štititi u skladu s ovdje utvrđenim odredbama dok stranka pošiljateljica ne oslobodi stranku primateljicu te obveze.

5. Stranke odmah obavješćuju jedna drugu o bilo kojim izmjenama i dopunama zakonodavstva njihovih država koje utječu na zaštitu klasificiranih podataka ustupljenih na temelju ovog Ugovora. U slučaju takvih izmjena i dopuna, stranke se konzultiraju kako bi razmotrile moguće izmjene i dopune ovog Ugovora. U međuvremenu, klasificirani podaci nastavljaju se štititi kako je ovdje opisano, osim ako stranka pošiljateljica pisano ne zatraži drugačije.

U potvrdu toga, niže potpisani, za to propisno ovlašteni od svojih odnosnih Vlada, potpisali su ovaj Ugovor.

Sastavljeno u ZAGREB dana 12 JUNIE 2017 u dva izvornika, svaki na rumunjskom, hrvatskom i engleskom jeziku, pri čemu su svi tekstovi jednako vjerodostojni. U slučaju razlika u tumačenju, mjerodavan je engleski tekst.

ZA VLADU RUMUNJSKE

ZA VLADU REPUBLIKE HRVATSKE

Copie certificată a exemplarului deținut de MAE

Corina Badea, director

Direcția Tratate Internaționale

Ministerul Afacerilor Externe

ROMÂNIA * MINISTERUL AFACERILOR EXTERNE * Director General H2

11022
01.08.2014

GUVERNUL ROMÂNIEI
OFICIUL REGISTRULUI NAȚIONAL
AL INFORMAȚIILOR SECRETE DE STAT

Nr. 7255/09.04.2014

DSM/699
22.08.2014

Exemplar unic

APROB,
Președintele Consiliului Suprem de Apărare a Țării

TRAIAN BĂSESCU

De acord,
Prim - ministru

VICTOR VIOREL PONTA

Avizat,
Viceprim – ministru pentru securitate națională, Ministrul Afacerilor Interne

GABRIEL OPREA

MEMORANDUM

Avizat: **ROBERT MARIUS CAZANCIUC**
Ministrul justiției

MIRCEA DUȘA
Ministrul apărării naționale

GEORGE CRISTIAN MAIOR
Directorul Serviciului Român de Informații

TEODOR VIOREL MELEȘCANU
Directorul Serviciului de Informații Externe

TITUS CORLĂȚEAN
Ministrul afacerilor externe

De la: **MARIUS PETRESCU**
Directorul General al Oficiului Registrului Național al Informațiilor Secrete de Stat

Tema: Aprobarea semnării Acordului între Guvernul României și Guvernul Republicii Croația privind protecția reciprocă a informațiilor clasificate

Conform cu originalul

I. În virtutea atribuțiilor conferite prin actul normativ de organizare și funcționare, Oficiul Registrului Național al Informațiilor Secrete de Stat (ORNISS), cu sprijinul instituțiilor cu atribuții în domeniu, a continuat demersurile de consolidare și dezvoltare a cadrului legal care să faciliteze cooperarea cu alte state în toate domeniile de activitate care presupun schimbul de informații clasificate, prin negocierea și încheierea, la dispoziția Prim-ministrului României, a acordurilor internaționale privind protecția reciprocă a acestor informații.

În consecință, ORNISS, prin intermediul canalelor diplomatice, a adresat în anul 2011 autorității competente omologe din Republica Croația invitația de a demara negocierea unui acord bilateral privind protecția reciprocă a informațiilor clasificate.

Ca răspuns, partea croată și-a manifestat disponibilitatea de a demara negocierile, acestea fiind desfășurate în cadrul a două runde, la Zagreb, în perioada 27-30 martie 2012 și la București, în perioada 26-28 iunie 2013.

La negocieri au participat reprezentanții Autorităților Naționale de Securitate, din cele două state, precum și reprezentanți ai instituțiilor cu atribuții în domeniul protecției informațiilor clasificate din România.

În ceea ce privește mandatul părții române la negocieri, menționăm că, pentru statele membre NATO, Consiliul Suprem de Apărare a Țării a aprobat, prin Memorandumul nr. 15461/2004, textul cadru al proiectului de acord român ce constituie mandatul general în acest sens.

II. Negocierile au avut ca scop asigurarea unui cadru comun de reglementare, eficient și sigur, pentru derularea tuturor activităților ce implică schimbul informațiilor clasificate între părți, efectuat direct sau prin intermediul instituțiilor publice ori persoanelor juridice de drept privat.

Așadar, încheierea unui acord de securitate cu Republica Croația va sta la baza activităților ce presupun schimbul de informații clasificate între părți și va asigura standarde comune de protecție a acestor informații, recunoașterea certificatelor de securitate, stabilirea echivalențelor nivelurilor de clasificare, convenirea procedurilor de soluționare a cazurilor de compromitere a informațiilor clasificate.

De menționat este faptul că domeniul de aplicare al Acordului se referă și la activitatea societăților comerciale în ceea ce privește cooperarea și participarea la contracte sau la alte raporturi juridice cu instituții publice ori private din statele părților, la vânzarea de echipamente, produse și know-how, dacă acestea implică schimbul de informații clasificate.

III. Proiectul Acordului rezultat în urma negocierilor stabilește cadrul juridic și organizatoric pentru protecția informațiilor clasificate schimbate și cuprinde dispoziții referitoare la:

- scopul încheierii acordului și domeniul de aplicare;
- definirea termenilor;
- autoritățile competente de securitate ale celor două state;
- echivalența nivelurilor de clasificare;
- protecția informațiilor clasificate;
- accesul la informațiile clasificate;

- traducerea şi reproducerea informaţiilor clasificate;
- distrugerea informaţiilor clasificate;
- transmiterea informaţiilor de securitate;
- procedura efectuării vizitelor reciproce;
- contracte clasificate;
- cooperarea în domeniul securităţii;
- compromiterea informaţiilor clasificate;
- suportare cheltuielilor;
- interpretarea şi soluţionarea diferendelor;
- dispoziţii finale.

Textul rezultat în urma negocierilor este în concordanţă cu mandatul aprobat de Consiliul Suprem de Apărare a Ţării şi în conformitate cu legislaţia naţională în domeniu, reflectând totodată dorinţa Părţilor de a asigura o bază solidă a cooperării viitoare în implementarea proiectelor comune.

IV. Faţă de cele prezentate, **propunem** aprobarea semnării ***Acordului între Guvernul României şi Guvernul Republicii Croaţia privind protecţia reciprocă a informaţiilor clasificate*** de către domnul prof.univ.dr. Marius Petrescu, Directorul general al ORNISS, şi eliberarea, de către Ministerul Afacerilor Externe, a deplinelor puteri.

Vicepreşedintele Consiliului Suprem de Apărare a Ţării

MIHAI TUDOSE _____

Membrii Consiliului Suprem de Apărare a Ţării:

MIHAI-VIOREL FIFOR _____

CARMEN DANIELA DAN _____

TEODOR - VIOREL MELEŞCANU _____

TUDOREL TOADER _____

IONUŢ MIŞA _____

GHEORGHE ŞIMON _____

ION OPRIŞOR _____

EDUARD HELLVIG _____

General NICOLAE-IONEL CIUCĂ _____

Secretarul Consiliului Suprem de Apărare a Ţării

General-maior MIHAI ŞOMORDOLEA _____

Conform cu originalul

GUVERNUL ROMÂNIEI C.I.F.: 15085226 OFICIUL REGISTRULUI NATIONAL AL CIFRELOR SECRETE DE STAT