ACORD

ÎNTRE

GUVERNUL ROMÂNIEI

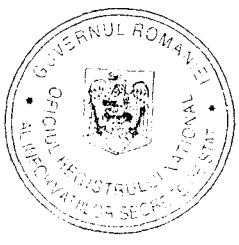
ŞI

GUVERNUL REPUBLICII SERBIA

PRIVIND

PROTECŢIA RECIPROCĂ

A INFORMAŢIILOR CLASIFICATE SCHIMBATE



PREAMBUL

Guvernul României şi Guvernul Republicii Serbia (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 din statele Părţilor,

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

Au convenit următoarele:

ARTICOLUL 1
SCOP ŞI DOMENIU DE APLICARE

(1) Scopul prezentului Acord este de a asigura protecţia informaţiilor clasificate schimbate sau produse 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 încheiate cu terţi 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:

a) **Informaţie Clasificată:** 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 necesită protecţie împotriva dezvăluirii neautorizate sau a oricărei forme de compromitere;

b) **Nivel de Clasificare:** un marcaj care, în conformitate cu legislația statului Părții, determină anumite restricții privind accesul la Informații Clasificate și măsurile de protecție;

c) **Parte Emitentă:** Partea, inclusiv orice altă persoană juridică din statul Părții respective, care generează și transmite Informații Clasificate către cealaltă Parte;

d) **Parte Primitoare:** Partea, inclusiv orice altă persoană juridică din statul Părții respective, care primește Informații Clasificate de la cealaltă Parte;

e) **Contract Clasificat:** orice contract care conține sau implică Informații Clasificate;

f) **Certificat de Securitate a Personalului:** un document emis în conformitate cu legislația statului Părții în baza verificării de securitate efectuate, finalizată printr-o decizie pozitivă prin care unei persoane i se acordă accesul la Informații Clasificate și permisiunea de a le gestiona;

g) **Certificat de Securitate Industrială:** un document emis în conformitate cu legislația statului Părții în baza verificării de securitate efectuate, finalizată printr-o decizie pozitivă prin care se abilitează o persoană juridică să desfășoare activități legate de un Contract Clasificat;

h) **Autoritate Competentă de Securitate:** instituția menționată la art. 3 al prezentului Acord, învestită cu autoritate la nivel național care, în conformitate cu legislațiile statelor Părților, asigură implementarea unitară a măsurilor de protecție a Informațiilor Clasificate;

i) **Principiul 'necesitatea de a cunoaște':** principiul conform căruia accesul la Informații Clasificate poate fi acordat unei persoane numai dacă acesta este necesar în vederea îndeplinirii îndatoririlor oficiale și sarcinilor de serviciu;

j) **Compromitere:** orice întrebuințare necorespunzătoare, contrară legislației naționale, care are drept rezultat deteriorarea sau accesul neautorizat, modificarea, dezvăluirea ori distrugerea Informațiilor Clasificate, precum și orice acțiune sau inacțiune care duce la pierderea confidențialității, integrității sau disponibilității acestora.

ARTICOLUL 3
AUTORITĂȚI COMPETENTE DE SECURITATE

(1) Autoritățile Competente de Securitate responsabile pentru implementarea prezentului Acord sunt:

În România:
Oficiul Registrului Național al Informațiilor Secrete de Stat

În Republica Serbia:
Kancelarija Saveta za nacionalnu bezbednost i zaštitu tajnih podataka

(2) Părțile se vor informa reciproc, pe canale diplomatice, despre orice modificare cu privire la Autoritățile Competente de Securitate.

ARTICOLUL 4
NIVELURI DE CLASIFICARE

(1) Echivalența nivelurilor de clasificare naționale este următoarea:

Pentru România	Pentru Republica Serbia
STRICT SECRET DE IMPORTANȚĂ DEOSEBITĂ	ДРЖАВНА ТАЈНА
STRICT SECRET	СТРОГО ПОВЕРЉИВО
SECRET	ПОВЕРЉИВО
SECRET DE SERVICIU	ИНТЕРНО

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

(3) Partea Emitentă va informa Partea Primitoare asupra condițiilor suplimentare de transmitere sau de limitare a utilizării Informațiilor Clasificate transmise.

(4) Partea Primitoare se va asigura că Informațiile Clasificate sunt marcate cu Nivelul de Clasificare național echivalent, în conformitate cu alin. (1) al prezentului Acord.

(5) 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. al prezentului Acord.

(2) Nimic din conţinutul prezentului Acord nu va prejudicia legislaţiile şi reglementările naţionale ale 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 sunt 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, după caz, 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;

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

(2) Dacă oricare alt acord încheiat între Părți cuprinde reglementări mai stricte referitoare la schimbul sau protecția Informațiilor Clasificate, se vor aplica reglementările respective.

ARTICOLUL 7
ACCESUL LA INFORMAȚII CLASIFICATE

(1) Accesul la informațiile clasificate SECRET/ПОВЕРЉИВО și de nivel superior precum și în încăperile și obiectivele unde se desfășoară activități ce implică astfel de informații este permis, cu respectarea principiului Necesitatea de a cunoaște, numai persoanelor autorizate și care dețin Certificat de Securitate a Personalului valabil pentru Nivelul de Clasificare al informațiilor pentru care se solicită accesul.

(2) Accesul la informațiile clasificate SECRET DE SERVICIU/ ИНТЕРНО se va limita numai la persoanele care respectă principiul Necesitatea de a cunoaște și condiționat de îndeplinirea de către acestea a cerințelor pentru acces la această categorie de Informații Clasificate în conformitate cu legislațiile naționale ale Părților.

(3) Fiecare Parte se va asigura că toate persoanele cărora li s-a acordat accesul la Informații Clasificate sunt informate cu privire la responsabilitățile de a proteja aceste informații în conformitate cu reglementările de securitate corespunzătoare.

ARTICOLUL 8
TRADUCEREA ȘI MULTIPLICAREA INFORMAȚIILOR CLASIFICATE

(1) Toate traducerile și multiplicările Informațiilor Clasificate vor fi marcate cu Nivelul de Clasificare național corespunzător și vor fi protejate în același mod ca și Informațiile Clasificate originale.

(2) Toate traducerile și multiplicările Informațiilor Clasificate vor fi efectuate de persoane care dețin Certificate de Securitate a Personalului corespunzătoare.

(3) Toate traducerile Informațiilor Clasificate vor conține o adnotare corespunzătoare în limba în care au fost traduse în care se va indica faptul că acestea conțin Informații Clasificate ale Părții Emitente.

(4) Informațiile Clasificate marcate STRICT SECRET DE IMPORTANȚĂ DEOSEBITĂ/ДРЖАВНА ТАЈНА vor fi traduse sau multiplicate numai în baza permisiunii prealabile scrise a Părții Emitente.

(5) Toate multiplicările și traducerile Informațiilor Clasificate vor fi supuse aceloraşi măsuri de protecție ca şi informațiile originale. Numărul de copii se va limita la cel necesar pentru scopurile oficiale.

ARTICOLUL 9
DISTRUGEREA INFORMAȚIILOR CLASIFICATE

(1) Informațiile Clasificate vor fi distruse în conformitate cu legislația națională a Părții Primitoare astfel încât reconstrucția parțială sau totală a acestora să nu fie posibilă.

(2) Distrugerea Informațiilor Clasificate se realizează numai cu acordul prealabil scris sau la cererea Părții Emitente.

(3) Informațiile STRICT SECRET DE IMPORTANȚĂ DEOSEBITĂ/ ДРЖАВНА ТАЈНА nu vor fi distruse. Acestea vor fi returnate Părții Emitente după ce Partea Primitoare consideră că nu îi mai sunt necesare.

(4) Partea Primitoare va informa în scris Partea Emitentă cu privire la distrugerea Informațiilor Clasificate.

(5) În cazul în care este imposibilă protejarea sau returnarea Informațiilor 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 Părții Emitente cu privire la distrugerea Informațiilor Clasificate.

ARTICOLUL 10
TRANSMITEREA INFORMAȚIILOR CLASIFICATE

1) Informațiile Clasificate vor fi transmise prin canale diplomatice, curieri militari sau alte mijloace convenite de Autoritățile Competente de Securitate în conformitate cu legislația națională ale Părții care inițiază transmiterea. Partea Primitoare va confirma în scris primirea Informațiilor Clasificate.

2) Informațiile Clasificate vor fi transmise electronic în formă criptată, prin utilizarea mijloacelor și dispozitivelor criptografice acceptate reciproc de Autoritățile Competente de Securitate, în conformitate cu legislațiile naționale ale Părților.

3) Dacă există un volum mare de Informații Clasificate ce trebuie transmis, Autoritățile Competente de Securitate vor conveni mijloacele de transport, traseul și măsurile de securitate pentru fiecare caz în parte.

ARTICOLUL 11
VIZITE

1) Vizitele ce implică acces la Informații Clasificate efectuate pe teritoriul statului Părți gazdă sunt supuse autorizării scrise prealabile a Autorității Competente de Securitate a Părții gazdă, în conformitate cu legislația națională a acesteia.

2) Cererea de vizită va fi transmisă Autorității Competente de Securitate a Părții gazdă și va cuprinde următoarele date ce vor fi folosite numai în scopul vizitei:
   a) numele și prenumele vizitatorului, data și locul nașterii, cetățenia, și numărul pașaportului sau al cărții de identitate;

   b) funcția vizitatorului, cu menționarea angajatorului pe care vizitatorul îl reprezintă;

   c) specificarea proiectului la care participă vizitatorul;

   d) confirmarea deținerii Certificatului de Securitate a Personalului de către vizitator, valabilitatea acestuia și Nivelul de Clasificare a informațiilor până la care acesta poate acorda acces;

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

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 între Autorităţile Competente de Securitate;

i) data şi semnătura Autorităţii Competente de Securitate transmiţătoare.

(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.

(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 12 luni şi poate fi extinsă pentru o perioadă suplimentară nu mai mare de 12 luni. Cererea de vizite repetate va fi transmisă în conformitate cu alin. (3) al prezentului articol. După aprobarea listei, vizitele pot fi aranjate direct între instituţiile implicate.

(8) Părţile vor garanta protecţia datelor personale ale vizitatorilor în conformitate cu legislaţiile naţionale ale acestora.

ARTICOLUL 12
CONTRACTE CLASIFICATE

(1) În cazul în care o Parte sau o persoană juridică din statul său intenționează să încheie un Contract Clasificat ce urmează a se derula pe teritoriul statului celeilalte Părți, atunci Partea pe teritoriul căreia se derulează contractul își va asuma responsabilitatea de a proteja Informațiile Clasificate legate de contract, în conformitate cu legislația statului său și cu prevederile prezentului Acord.

(2) La cerere, Autoritățile Competente de Securitate vor confirma dacă au fost eliberate Certificate de Securitate a Personalului și Certificate de Securitate Industrială corespunzătoare persoanelor și contractanților propuși să participe la negocierile pre-contractuale sau la derularea Contractelor Clasificate anterior accesării de către aceștia a Informațiilor Clasificate ale Părții Emitente.

(3) Fiecare Contract Clasificat încheiat între contractanți, în conformitate cu prevederile prezentului Acord, va cuprinde o anexă de securitate corespunzătoare în care sunt menționate cel puțin următoarele aspecte:
   a) lista Informațiilor Clasificate gestionate în cadrul Contractului Clasificat și Nivelurile de Clasificare ale acestora;
   b) procedura de comunicare a modificărilor apărute în Nivelurile de Clasificare ale informațiilor schimbate;
   c) canale de comunicare și mijloace de transmitere electromagnetică;
   d) procedura de transport a Informațiilor Clasificate;
   e) obligația de a informa despre orice Compromitere survenită efectiv sau suspectată.

(4) Un exemplar al anexei de securitate a oricărui Contract Clasificat va fi transmis Autorității Competente de Securitate a Părții pe teritoriul căreia urmează să se deruleze Contractul Clasificat în vederea asigurării unei monitorizări de securitate și control corespunzătoare.

(5) Contractele Clasificate care implică accesul la informații SECRET DE SERVICIU/ИНТЕРНО vor conține o clauză în care sunt specificate măsurile minime ce urmează a fi implementate pentru protecția acestei categorii de Informații Clasificate.

(6) Orice sub-contractant trebuie să îndeplinească aceleași obligații de securitate ca și contractantul.

7) Autoritățile Competente de Securitate pot conveni asupra unor vizite reciproce în vederea analizării eficienței măsurilor adoptate de contractant sau sub-contractant pentru protecția Informațiilor Clasificate vehiculate în Contractul Clasificat.

8) Părțile vor asigura protecția drepturilor de autor, a drepturilor de proprietate industrială – inclusiv licențele, secretele comerciale și a oricăror alte drepturi legate de Informațiile Clasificate schimbate între statele lor, în conformitate cu legislațiile naționale.

9) Alte proceduri detaliate referitoare la Contractele Clasificate pot fi convenite între Autoritățile Competente de Securitate ale Părților.

ARTICOLUL 13
COOPERAREA DE SECURITATE

1) În vederea realizării și menținerii unor standarde de securitate similare, Autoritățile Competente de Securitate își vor furniza, la cerere, informații referitoare la standardele, procedurile și practicile naționale de securitate pentru protecția Informațiilor Clasificate. În acest sens, Autoritățile Competente de Securitate pot efectua vizite reciproce.

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

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

4) La cerere, Autoritățile Competente de Securitate ale Părților, respectând legislațiile statelor acestora, își vor acorda asistență reciprocă în procedura de eliberare a Certificatelor de Securitate a Personalului și a Certificatelor de Securitate Industrială pentru proprii cetățeni care locuiesc pe teritoriul statului celeilalte Părți sau pentru obiectivele industriale amplasate pe teritoriul statului celeilalte Părți.

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

(6) Părţile îşi 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 lor naţionale, în ceea ce priveşte accesul la Informaţiile Clasificate schimbate în baza prezentului Acord.

(7) Serviciile de securitate, de informaţii şi de poliţie 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 corespunzătoare, în conformitate cu legislaţiile lor naţionale, 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 prezentului articol.

(4) 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 prezentului articol. Notificarea respectivă trebuie să cuprindă suficiente detalii pentru ca Partea Emitentă să poată evalua pe deplin consecinţele.

ARTICOLUL 15
INTERPRETARE ŞI DIFERENDE

Orice diferend între Părți privind interpretarea sau implementarea prezentului Acord se va soluționa numai prin consultări între Părți.

ARTICOLUL 16
CHELTUIELI

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

ARTICOLUL 17
DISPOZIȚII FINALE

(1) Prezentul Acord se încheie pe o perioadă nedeterminată de timp. Acesta este supus ratificării în conformitate cu procedurile legale naționale ale Părților și intră în vigoare în prima zi a celei de-a doua luni de la data primirii, pe canale diplomatice, a ultimei notificări între Părți, prin care se informează de faptul că au fost îndeplinite cerințele necesare pentru intrarea în vigoare a prezentului Acord.

(2) Prezentul Acord poate fi amendat pe baza consimțământului reciproc, scris, al Părților. Modificările respective vor intra în vigoare în conformitate cu alin.(1) al prezentului articol.

(3) Fiecare Parte are dreptul să denunțe oricând, în scris, prezentul Acord. În acest caz, valabilitatea acestuia expiră după șase (6) luni de la data la care notificarea de denunțare a fost primită de cealaltă Parte.

(4) Chiar și în situația denunțării prezentului Acord, toate Informațiile Clasificate transmise în baza acestuia vor continua să fie protejate în conformitate cu prevederile stipulate până când Partea Emitentă dispensează Partea Primitoare de această obligație.

5) Părțile se vor informa reciproc, cu promptitudine, cu privire la orice modificări survenite în legislațiile naționale care ar putea afecta protecția Informațiilor Clasificate transmise în baza prezentului Acord. Într-o asemenea situație, Părțile se vor consulta în legătură cu oportunitatea unor posibile modificări ale prezentului Acord. Între timp, Informațiile Clasificate vor continua să fie protejate așa cum s-a prevăzut în acest Acord dacă Partea Emitentă nu solicită altfel, în scris.

6) La data intrării în vigoare a prezentului Acord, Acordul între Ministerul Apărării Naționale din România și Ministerul Apărării din Republica Serbia privind protecția informațiilor clasificate militare schimbate, semnat la București la 6 iunie 2013 și la Belgrad la 27 iulie 2013 își va înceta valabilitatea.

Semnat la București, la 8 februarie 2017, în două exemplare originale, fiecare în limbile română, sârbă și engleză, toate textele fiind egal autentice. În caz de divergențe de interpretare, textul în limba engleză prevalează.

Drept dovadă, subsemnații, pe deplin autorizați de guvernele lor proprii, am semnat prezentul Acord.

PENTRU GUVERNUL ROMÂNIEI	**PENTRU GUVERNUL REPUBLICII SERBIA**
Prof.univ.dr. MARIUS PETRESCU	**dr. GORAN MATIĆ**
Secretar de Stat	**Directorul Oficiului Consiliului**
Directorul General	**pentru Securitate Națională și**
al Oficiului Registrului Național al	**Protecția Informațiilor Clasificate**
Informațiilor Secrete de Stat	

Conform cu originalul

AGREEMENT

BETWEEN

THE GOVERNMENT OF ROMANIA

AND

THE GOVERNMENT OF THE REPUBLIC OF SERBIA

ON THE MUTUAL PROTECTION OF EXCHANGED

CLASSIFIED INFORMATION

PREAMBLE

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

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

Desiring to establish a legal framework for the mutual protection of exchanged classified information applicable to any future co-operation agreements and contracts, which will be implemented between the Parties, or between legal entities of the states of the Parties, 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 cooperation between the Parties or between legal entities of the states of the Parties.

(2) This Agreement shall apply 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 with third parties 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:

a) **Classified Information:** Any information, document or material, regardless of its form, to which a particular classification level has been assigned in compliance with the legislations of the states of the Parties and which demands protection from the unauthorized disclosure or any another form of compromise;

b) **Classification Level:** A marking which, according to the legislation of the state of the Party, determines certain restrictions of access to Classified Information and measures of protection;

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

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

e) **Classified Contract:** A contract that contains or involves Classified Information;

f) **Personnel Security Certificate**: A document issued in accordance with the legislation of the state of the Party based on the conducted security vetting that is finalized with a positive decision, which enables a person to be granted access and permission to handle Classified Information;

g) **Facility Security Certificate**: A document issued in accordance with the legislation of the state of the Party based on the conducted security vetting that is finalized with a positive decision, which is to enable a legal entity to carry out activities related to a Classified Contract;

h) **Competent Security Authority:** The institution listed in Article 3 of this Agreement, empowered with authority at national level which, in compliance with the legislations of the states of the Parties, ensures the unitary implementation of the protective measures for Classified Information;

i) **Need-to-know principle**: A principle by which access to Classified Information may be granted to an individual only if it is necessary for the performance of his/her official duties and tasks;

j) **Compromise**: Any form of misuse, contrary to the national legislation, 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:
Oficiul Registrului Național al Informațiilor Secrete de Stat

For the Republic of Serbia:
Kancelarija Saveta za nacionalnu bezbednost i zaštitu tajnih podataka

(2) The Parties shall inform each other through diplomatic channels of any 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 Serbia
STRICT SECRET DE IMPORTANȚĂ DEOSEBITĂ	ДРЖАВНА ТАЈНА
STRICT SECRET	СТРОГО ПОВЕРЉИВО
SECRET	ПОВЕРЉИВО
SECRET DE SERVICIU	ИНТЕРНО

(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 Classified Information is marked with an equivalent national Classification Level in accordance with Paragraph 1 of this Article.

(5) 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, according to Article 4 of this Agreement.

(2) The provisions in this Agreement shall not be construed in such a way as to cause prejudice to the national legislations of the Parties regarding access to documents of public interest 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;
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 rules regarding the exchange or protection of Classified Information, these regulations shall apply.

ARTICLE 7
ACCESS TO CLASSIFIED INFORMATION

(1) Access to information classified SECRET/ПОВЕРЉИВО 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/ИНТЕРНО shall be limited to those persons who have Need-to-know and provided they meet the requirements for access to such Classified Information according to the national legislations of the Parties.

(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.

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 IMPORTANȚĂ DEOSEBITĂ/ДРЖАВНА ТАЈНА 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 national legislation 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 IMPORTANȚĂ DEOSEBITĂ/ДРЖАВНА ТАЈНА information shall not be destroyed. It shall be returned to the Originating Party after it is no longer considered necessary by the Recipient 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 national legislation 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 encrypted form, by using the cryptographic methods and devices mutually accepted by the Competent Security Authorities in accordance with the national legislations of the Parties.

(3) If a large consignment containing Classified Information is to be transmitted 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, according to its national legislation.

(2) A request for a 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 and signature of the sending Competent Security Authority.

(3) A request for a 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 Parties shall guarantee the protection of personal data of the visitors according to their national legislations.

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/ИНТЕРНО 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 fulfill 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 national legislations.

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

ARTICLE 13
SECURITY COOPERATION

(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 arises, 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 national 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 and Facility Security Certificates, issued for the citizens and legal entities of their states, in accordance with their national legislations, as regards the access to Classified Information exchanged under this Agreement.

(7) The security, intelligence and police services of the states of the Parties may cooperate and directly exchange operative and/or intelligence information in accordance with the national legislations.

ARTICLE 14
COMPROMISE OF CLASSIFIED INFORMATION

(1) The Parties shall take all appropriate measures, in accordance with their national legislations, 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 national legislation. If required the Parties shall 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 as of paragraph 2 of this Article.

(4) 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
INTERPRETATION AND DISPUTES

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

ARTICLE 16
EXPENSES

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

ARTICLE 17
FINAL PROVISIONS

(1) This Agreement is concluded for an indefinite period of time. It is subject to ratification in accordance with the national legal procedures of the Parties and shall enter into force on the first day of the second month following the date of the last notification between the Parties, through diplomatic channels, that the necessary requirements for this Agreement to enter into force have been met.

(2) This Agreement may be amended with the mutual written consent of both Parties. Such amendments shall enter into force in accordance with Paragraph 1 of this Article.

(3) Each Party may terminate this Agreement in writing at any time. In this case, the Agreement will expire after six (6) months from the day on which the termination notice was received 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 changes to the national legislations that affect the protection of Classified Information released under this Agreement. In the event of such changes, the Parties shall consult to consider possible changes to this Agreement. In the meantime, the Classified Information shall continue to be protected as provided herein, unless otherwise requested by the Originating Party in writing.

(6) Upon the entry into force of this Agreement, the Agreement between the Ministry of National Defence of Romania and the Ministry of Defence of the Republic of Serbia on the Protection of Exchanged Classified Defence Information signed in Bucharest on 6 June 2013 and in Belgrade on 27 July 2013 shall terminate.

Done in Bucharest on 8th of February 2017, in two originals, each in the Romanian, Serbian and English languages, all texts being equally authentic. In case of divergences of interpretation, the English text shall prevail.

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

ON BEHALF OF THE GOVERNMENT OF ROMANIA

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

ON BEHALF OF THE GOVERNMENT OF THE REPUBLIC OF SERBIA

GORAN MATIĆ, PhD
Director
Office of the National Security Council and Classified Information Protection

Conform cu originalul

Anexă la DJ 11-478 din 06.06.2018

СПОРАЗУМ

ИЗМЕЂУ

ВЛАДЕ РУМУНИЈЕ

И

ВЛАДЕ РЕПУБЛИКЕ СРБИЈЕ

О УЗАЈАМНОЈ ЗАШТИТИ

РАЗМЕЊЕНИХ ТАЈНИХ ПОДАТАКА

Преамбула

Влада Румуније и Влада Републике Србије (у даљем тексту: Стране), увиђајући да добра сарадња може захтевати размену тајних података између Страна, непосредно или преко правних лица држава Страна,

у жељи да утврде правни оквир за узајамну заштиту тајних података који ће важити за све будуће споразуме и уговоре о сарадњи који садрже или предвиђају приступ тајним подацима и који ће бити примењен између Страна или између правних лица држава Страна.

споразумеле су се следеће:

Члан 1.
Циљ и предмет

(1) Циљ овог споразума је да обезбеди заштиту тајних података који се размене или створе у сарадњи између Страна или између правних лица држава Страна.

(2) Овај споразум се примењује на сваку активност која укључује размену тајних података која се обавља или ће бити обављена између Страна или између правних лица држава Страна.

(3) Овај споразум не утиче на обавезе Страна које произлазе из других међународних споразума са трећим странама и не користи се против интереса, безбедности и територијалног интегритета других држава.

Члан 2.
Дефиниције

У овом споразуму, користе се следеће дефиниције:

а) тајни подаци јесу сви подаци, документи или материјал, без обзира на њихов облик, којима је додељен одређени степен тајности у складу са законодавством држава Страна и који захтевају заштиту од неовлашћеног откривања или неког другог облика угрожавања;

b) степен тајности јесте ознака која, према законодавству државе Стране, одређује нека ограничења у погледу приступа тајним подацима и мера заштите;

c) страна давалац јесте страна, укључујући било које друго правно лице државе Стране која ствара тајне податке и уступа их другој Страни;

d) страна прималац јесте страна, укључујући било које друго правно лице државе Стране која прима тајне податке од друге Стране;

e) уговор с тајним подацима јесте уговор који садржи или укључује тајне податке;

f) безбедносни сертификат за физичка лица јесте документ издат у складу са законодавством државе Стране на основу спроведене безбедносне провере окончане позитивном одлуком која омогућава лицу да му се одобри приступ и руковање тајним подацима;

g) безбедносни сертификат за правна лица јесте документ издат у складу са законодавством државе Стране на основу спроведене безбедносне провере окончане позитивном одлуком која треба да омогући правном лицу да изврши активности у вези са уговором с тајним подацима;

h) надлежни безбедносни органи су органи наведени у члану 3. овог споразума, овлашћени на националном нивоу да у складу са законодавством држава Страна, обезбеђује јединствену примену мера за заштиту тајних података;

i) принцип „потребно је да зна“ јесте принцип по коме одређеном лицу може бити одобрен приступ тајним подацима, само ако је то потребно за обављање његових службених дужности или задатака;

j) компромитовање јесте сваки облик злоупотребе, супротан националном законодавству, који за последицу има штету или неовлашћени приступ, измену, откривање или уништавање тајних података, као и свако друго поступање или непоступање које за последицу има губитак поверљивости, интегритета или расположивости;

Члан 3.
Надлежни безбедносни органи

(1) Надлежни безбедносни органи одговорни за примену овог споразума су:

За Румунију:
Oficiul Registrului Național al Informațiilor Secrete de Stat.

За Републику Србију:
Канцеларија Савета за Националну безбедност и заштиту тајних података.

(2) Стране се узајамно обавештавају дипломатским путем о свакој промени у вези са надлежним безбедносним органима.

Члан 4.
Степени тајности

(1) Еквивалентност националних степена тајности је следећа:

За Румунију	За Републику Србију
STRICT SECRET DE IMPORTANȚĂ DEOSEBITĂ	ДРЖАВНА ТАЈНА
STRICT SECRET	СТРОГО ПОВЕРЉИВО
SECRET	ПОВЕРЉИВО
SECRET DE SERVICIU	ИНТЕРНО

(2) Страна давалац обавештава, без одлагања, Страну примаоца о свим променама степена тајности уступљених тајних података.

(3) Страна давалац обавештава Страну примаоца о свим додатним условима уступања или ограничењима употребе уступљених тајних података.

(4) Страна прималац обезбеђује да тајни подаци буду означени еквивалентним националним степеном тајности у складу са ставом 1. овог члана.

(5) Стране се узајамно обавештавају о свим променама у вези са националним степенима тајности.

Члан 5.
Заштита тајних података

(1) Страна прималац пружа свим примљеним подацима исту заштиту као националним тајним подацима еквивалентног степена тајности, у складу са чланом 4. овог споразума.

(2) Одредбе овог споразума, неће се тумачити тако да доводе у питање национално законодавство Страна у вези са приступом документима од јавног значаја или приступом подацима јавног карактера, заштитом личних података или заштитом тајних података.

(3) Свака Страна обезбеђује примену одговарајућих мера за заштиту тајних података који се обрађују, чувају или преносе у комуникационо-информационим системима. Те мере обезбеђују поверљивост, интегритет и расположивост и, по потреби, непорецивост и аутентичност тајних података, као и одговарајући степен одговорности и доказивости радњи у вези с тим подацима.

Члан 6.
Откривање и коришћење тајних података

(1) Свака Страна обезбеђује да тајни подаци који се доставе или размене према овом споразуму буду заштићени од:

a) снижења или скидања степена тајности без претходног писменог одобрења или на захтев Стране даваоца;

b) коришћења у друге сврхе, осим у оне за које су достављени;

c) откривања било којој трећој држави, међународној организацији, лицу или правном лицу без претходног писменог одобрења Стране даваоца;

(2) Уколико било који други споразум који се закључи између Страна садржи строжа правила у вези са разменом или заштитом тајних података, примењују се та правила.

Члан 7.
Приступ тајним подацима

(1) Приступ подацима степена SECRET / ПОВЕРЉИВО и вишем и/или локацијама и објектима у којима се изводе активности које укључују те податке, дозвољен је, уз поштовање принципа „потребно је да зна", само лицима која су овлашћена и имају сертификат о безбедносној провери лица који важи за степен тајности података за које се захтева приступ.

(2) Приступ подацима степена SECRET DE SERVICIU / ИНТЕРНО ограничен је на она лица која поступају према принципу „потребно је да зна", под условом да испуњавају захтеве за приступ тим тајним подацима у складу са националним законодавством Страна.

(3) Свака Страна обезбеђује да сва лица којима се одобри приступ тајним подацима буду обавештена о својој одговорности да заштите те податке у складу са одговарајућим безбедносним прописима.

Члан 8.
Превод и умножавање тајних података

(1) Сви преводи и умножени примерци тајних података означавају се одговарајућим националним степеном тајности и заштићују као оригинални тајни подаци.

(2) Све преводе и умножене примерке тајних података израђују лица која имају одговарајуће сертификате о безбедносној провери физичких лица.

(3) Сви преводи тајних података имају прикладну напомену на језику превода којом се указује да садрже тајне податке Стране даваоца.

(4) Тајни подаци означени STRICT SECRET DE IMPORTANȚĂ DEOSEBITĂ / ДРЖАВНА ТАЈНА преводе се или умножавају само на основу претходног писменог одобрења Стране даваоца.

(5) Сви умножени примерци и преводи стављају се под исте заштитне мере као оригинални подаци. Умножени примерци се ограничавају на број који се захтева у службене сврхе.

Члан 9.
Уништавање тајних података

(1) Тајни подаци се уништавају у складу са националним законодавством Стране примаоца на начин који онемогућава њихову делимичну или потпуну реконструкцију.

(2) Тајни подаци се уништавају само уз претходно писмено одобрење Стране даваоца или на њен захтев.

(3) Подаци степена STRICT SECRET DE IMPORTANȚĂ DEOSEBITĂ / ДРЖАВНА ТАЈНА степена се не уништавају, већ се враћају Страни даваоцу, пошто Страна прималац процени да јој више нису потребни.

(4) Страна прималац писмено обавештава Страну даваоца о уништавању тајних података.

(5) У случају ситуације која онемогућава заштиту и враћање тајних података који су створени или уступљени према овом споразуму, тајни подаци се одмах уништавају. Страна прималац обавештава благовремено надлежни безбедносни орган о уништавању тајних података.

Члан 10.
Пренос тајних података

(1) Тајни подаци се преносе дипломатским путем, војним куриром или другим средствима која договоре надлежни безбедносни органи у складу с националним законодавством Стране која покреће пренос. Страна прималац писмено потврђује пријем тајних података.

(2) Тајни подаци се преносе електронски у криптованом облику, коришћењем криптографских метода и средстава које су обострано прихватили надлежни безбедносни органи у складу са националним законодавством обе Стране.

(3) Уколико треба пренети већу пошиљку која садржи тајне податке, надлежни безбедносни органи се договарају о превозном средству, путном правцу и мерама безбедности за сваки такав случај појединачно.

Члан 11.
Посете

(1) Посете које захтевају приступ тајним подацима на територији државе Стране домаћина подлежу претходном писменом одобрењу надлежног безбедносног органа Стране домаћина, у складу са њеним националним законодавством.

(2) Захтев за посете се подноси надлежном безбедносном органу Стране домаћина и садржи следеће податке који ће бити коришћени само у сврху те посете:

a) име и презиме посетиоца, датум и место рођења, држављанство и број путне исправе/личне карте;

b) функција посетиоца, уз детаљан опис послодавца кога представља;

c) детаљан опис пројекта у коме посетилац учествује;

d) потврда о сертификату о безбедносној провери посетиоца, његово важење и степен тајности података до кога се одобрава приступ;

e) назив, адреса, број телефона/факса, имејл адреса и лице за контакт код правног лица које ће бити посећено;

f) сврха посете, укључујући, највиши степен тајност података о којима је реч;

g) датум и трајање посете; код чешћих посета, треба навести укупан период обухваћен тим посетама;

h) други подаци, према договору надлежних безбедносних органа;

i) датум и потпис надлежног безбедносног органа пошиљаоца.

(3) Захтев за посету се подноси најмање 20 дана пре обављања посете, осим ако надлежни безбедносни органи не одобре другачије.

(4) Надлежни безбедносни орган Стране који прима захтев за посету благовремено обавештава о својој одлуци надлежни безбедносни орган Стране подносиоца захтева.

(5) Када се посета одобри, надлежни безбедносни орган Стране домаћина доставља примерак захтева за посету руководиоцу правног лица које ће бити посећено.

(6) Посетиоци поступају у складу са безбедносним прописима и упутствима Стране домаћина.

(7) Надлежни безбедносни органи се могу договорити о списку посетилаца који су овлашћени да обављају чешће посете. Списак важи за почетни период од највише дванаест месеци и може бити продужен за додатни период који не прелази дванаест месеци. Захтев за чешће посете се подноси у складу са ставом (3). Када се списак одобри, дотична правна лица могу непосредно организовати међусобне посете.

(8) Стране гарантују заштиту личних података у складу са својим националним законодавством.

Члан 12.
Уговори са тајним подацима

(1) У случају да Страна или правни субјект на територији његове државе намерава да закључи уговор с тајним подацима који ће бити извршен у оквиру територије државе друге Стране, Страна на чијој територији се одвија извршење преузима одговорност за заштиту тајних података у вези са уговором у складу са законодавством своје државе и одредбама овог споразума.
(2) На захтев, надлежни безбедносни органи потврђују да ли су одговарајући сертификати о безбедносној провери правних лица и сертификати о безбедносној провери физичких лица издати предложеним уговарачима и лицима која учествују у преговорима за закључење уговора или у извршењу уговора с тајним подацима, пре него што приступе тајним подацима Стране даваоца.

(3) Сваки уговор с тајним подацима који се закључи између уговарача у складу са одредбама овог споразума укључује одговарајући безбедносни прилог у коме ће бити утврђени најмање следећи аспекти:

a) списак тајних података у вези са уговором с тајним подацима и њихови степени тајности;
b) процедура достављања промена степена тајности размењених података;
c) канали комуникације и средства електромагнетног преноса;
d) процедура транспорта тајних података;
e) обавеза обавештавања о сваком стварном или могућем компромитовању.

(4) Примерак безбедносног прилога уз сваки уговор с тајним подацима прослеђује се надлежном безбедносном органу Стране на чијој територији ће бити извршен уговор с тајним подацима, како би се омогућио адекватан безбедносни надзор и контрола.

(5) Уговори с тајним подацима који захтевају приступ подацима степена SECRET DE SERVICIU/ ИНТЕРНО садрже одговарајућу одредбу у којој се утврђује минимум мера које треба применити у циљу заштите тих тајних података.

(6) Сваки подуговарач мора испунити исте безбедносне услове као уговарач.

(7) Надлежни безбедносни органи могу се договорити о узајамним посетама, како би анализирали делотворност мера које је донео уговарач или подуговарач у циљу заштите тајних података укључених у уговор с тајним подацима.

(8) Стране обезбеђују заштиту ауторских права, права индустријске својине, укључујући патенте, пословне тајне и сва друга права у вези са тајним подацима који се размене између њихових држава у складу са њиховим националним законодавством.

(9) Надлежни безбедносни органи Страна могу се договорити о додатним детаљним процедурама у вези са уговором с тајним подацима.

Безбедносна сарадња

(1) Како би остварили и применили сличне стандарде безбедности, надлежни безбедносни органи, на захтев, достављају међусобно податке о својим националним безбедносним стандардима, процедурама и пракси у заштити тајних података. У том циљу, надлежни безбедносни органи могу обавити узајамне посете.

(2) У случају потребе, надлежни безбедносни органи могу закључити безбедносне аранжмане о посебним техничким аспектима у вези са применом овог споразума.

(3) Надлежни безбедносни органи се, према потреби, узајамно обавештавају о свим посебним безбедносним ризицима који могу да угрозе уступљене тајне податке.

(4) На захтев, надлежни безбедносни органи Страна, узимајући у обзир законодавство својих држава, пружају међусобну помоћ у поступку издавања сертификата о безбедносној провери за физичка лица и сертификата о безбедносној провери за правна лица за своје држављане који бораве или за правна лица која се налазе на територији државе друге Стране.

(5) Надлежни безбедносни органи се узајамно обавештавају о свим изменама које се тичу сертификата о безбедносној провери физичких лица и сертификата о безбедносној провери правних лица који су у вези са сарадњом према овом споразуму.

(6) Стране међусобно признају своје сертификате о безбедносној провери физичких и правних лица који су издати држављанима и правним лицима у њиховим државама у складу са њиховим националним законодавством у вези са приступом тајним подацима који су размењени у складу са овим споразумом.

(7) Безбедносно-обавештајне и полицијске службе држава Страна могу сарађивати и непосредно размењивати оперативне и/или обавештајне податке у складу са националним законодавством.

Члан 14.
Компромитовање тајних података

(1) Стране предузимају све одговарајуће мере, у складу са својим националним законодавством, како би утврдиле околности у случају да је познато или се основано сумња да су тајни подаци компромитовани.

(2) У случају компромитовања које укључује тајне податке које је створила или примила друга Страна, надлежни безбедносни орган на територији чије државе се догодило компромитовање обавештава о томе, што је пре могуће, надлежни безбедносни орган Стране даваоца и примењује одговарајуће мере у складу са националним законодавством. Стране, по потреби, сарађују током наведеног поступка.

(3) У случају да се компромитовање догоди на територији треће државе, надлежни безбедносни орган Стране пошиљаоца предузима радње из става 2. овог члана.

(4) Надлежни безбедносни орган Стране примаоца писмено обавештава надлежни безбедносни орган Стране даваоца о околностима компромитовања, обиму штете, предузетим мерама за њено смањење и резултатима поступка који се помињу у ставу 2. овог члана. То обавештење треба да садржи довољно појединости, тако да Страна прималац може потпуно да процени последице.

Члан 15.
Тумачење и спорови

Сваки спор између Страна у вези са тумачењем или применом овог споразума решава се искључиво путем консултација између Страна.

Члан 16.
Трошкови

Свака Страна сноси своје трошкове који настану у примени овог споразума.

Члан 17.
Завршне одредбе

(1) Овај споразум се закључује на неодређено време и подлеже потврђивању у складу са процедурама националног законодавства Страна и ступа на снагу првог дана следећег месеца после датума последњег обавештења достављеног дипломатским путем којим се Стране узајамно обавештавају да су испуњени потребни услови за ступање на снагу овог споразума.

(2) Измене и допуне овог споразума врше се на основу сагласности обе Стране. Те измене и допуне ступају на снагу у складу са ставом (1). овог члана.

(3) Свака Страна може у сваком тренутку писмено отказати овај споразум. У том случају, важење овог споразума истиче после шест (6) месеци од дана када друга Страна прими обавештење о отказу.

(4) Без обзира на отказ овог споразума, сви тајни подаци уступљени према овом споразуму су и даље заштићени у складу са одредбама Споразума, док Страна давалац не ослободи од ове обавезе Страну примаоца.

(5) Стране се одмах узајамно обавештавају о свакој промени националног законодавства која утиче на заштиту тајних података уступљених према овом споразуму. У случају промена, Стране обављају консултације да би размотриле могуће измене овог споразума. У међувремену, тајни подаци су и даље заштићени, као што је предвиђено овим споразумом, осим ако Страна давалац не захтева другачије у писменом облику.

(6) Ступањем на снагу овог споразума престаје да важи Споразум између Министарства националне одбране Румуније и Министарства одбране Републике Србије о заштити размењених тајних војних података потписан у Букурешту 6. јуна и у Београду 27. јула 2013. године.

Сачињено у Букурешту, 8 фебруара 2017. године, у два оригинала на српском, румунском и енглеском језику, при чему су сви текстови подједнако веродостојни. У случају неслагања у тумачењу, меродаван је текст на енглеском језику.

Потврђујући наведено, доле потписани прописно овлашћени представници својих влада потписали су овај споразум.

За Владу Румуније

др Мариус Петреску,
државни секретар националне канцеларије за класификацију поверљивих информација

За Владу Републике Србије

др Горан Матић,
директор Канцеларије Савета за националну безбедност и заштиту тајних података

Conform cu originalul