AGREEMENT

BETWEEN

THE GOVERNMENT OF ROMANIA

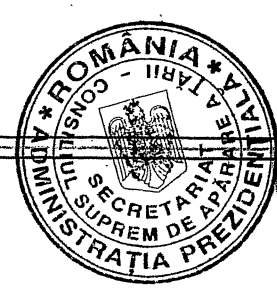
AND

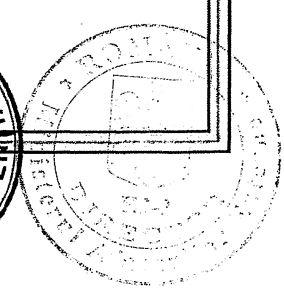
THE COUNCIL OF MINISTERS OF BOSNIA AND HERZEGOVINA

ON

THE MUTUAL PROTECTION

OF CLASSIFIED INFORMATION





PREAMBLE

The Government of Romania and the Council of Ministers of Bosnia and Herzegovina (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 shall 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 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**: 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 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:
National Registry Office for Classified Information

For Bosnia and Herzegovina:
Ministry of Security
Sector for Protection of Classified Information
National Security Authority

(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 Bosnia and Herzegovina
STRICT SECRET DE IMPORTANŢĂ DEOSEBITĂ	VRLO TAJNO
STRICT SECRET	TAJNO
SECRET	POVJERLJIVO
SECRET DE SERVICIU	INTERNO

(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 legislations of the states 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

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.

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/INTERNO 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 legislations of the states of the Parties.

(3)Each Party shall ensure that all individuals who have been 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 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.

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

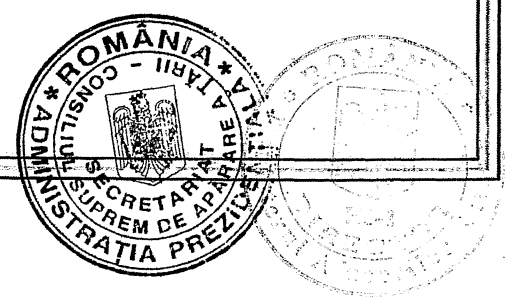
(5) In case of a situation that makes it impossible to protect and return Classified Information created or released according to this Agreement, the Classified Information shall be destroyed immediately. The Recipient Party shall notify in due time the Competent Security Authority of the Originating 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 encrypted form, by using the cryptographic methods and devices mutually accepted by the Competent Security Authorities in accordance with the legislations of the states 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 the legislation of its state.

(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 Competent Security Authority of the requesting Party.

(3)A request for a visit shall be submitted at least 30 days prior to the visit unless otherwise mutually approved by the Competent Security Authorities.

(4)The Competent Security Authority of the host Party 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 the legislations of their states.

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 shall 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) Classified Contract concluded between contractors, under the provisions of this Agreement, entailing access to SECRET/POVJERLJIVO information and above shall include an appropriate security annex including at least the following:

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 Contract entailing access to SECRET DE SERVICIU/INTERNO information shall only 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 analyse 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 purpose, 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 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 the legislations of their states, 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 legislations of their states.

ARTICLE 14
COMPROMISE OF CLASSIFIED INFORMATION

(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. 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 related to the interpretation or the implementation 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 legislations of the states 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 procedures 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 legislations of their states 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.

Done in SARAJEVO ... on 27 JANUARY 2020 in two originals, each in the Romanian language, official languages of Bosnia and Herzegovina (Bosnian, Croatian and Serbian) and English language, 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.

For the Government of Romania	**For the Council of Ministers of Bosnia and Herzegovina**
[redacted]	[redacted]

Copie certificată pentru conformitate cu originalul

Corina Badea, director

[redacted]

Direcția Tratate Internaționale

Ministerul Afacerilor Externe

ROMÂNIA * CONSILIUL SUPREM DE APĂRARE A ȚĂRII * ADMINISTRAȚIA PREZIDENȚIALĂ * SECRETARIAT

SPORAZUM

IZMEĐU

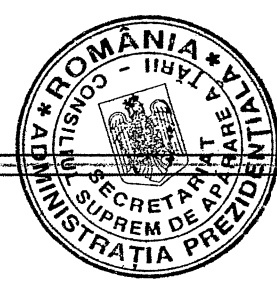
VLADE RUMUNJSKE

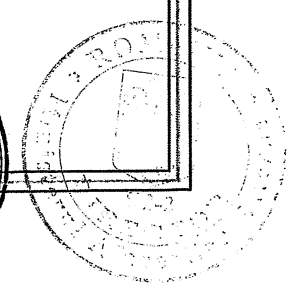
I

VIJEĆA MINISTARA BOSNE I HERCEGOVINE

O UZAJAMNOJ ZAŠTITI

TAJNIH PODATAKA





PREAMBULA

Vlada Rumunjske i Vijeće ministara Bosne i Hercegovine (u daljnjem tekstu: „Stranke"),

uzimajući u obzir da dobra suradnja između Stranaka može podrazumijevati razmjenu tajnih podataka, izravno ili putem drugih pravnih subjekata država Stranaka,

u želji da uspostave zakonski okvir za uzajamnu zaštitu razmijenjenih tajnih podataka koji bi bio primjenjiv na svaki budući sporazum i ugovor o suradnji između Stranaka ili između pravnih subjekata država Stranaka, a koji sadrži ili omogućava pristup tajnim podacima,

usuglasili su se o sljedećem:

ČLANAK 1.
CILJ I OPSEG

(1) Sporazum ima za cilj jamčiti zaštitu tajnih podataka, koji su razmijenjeni ili nastali kroz suradnju između Stranaka ili između pravnih subjekata država Stranaka.

(2) Sporazum se primijenjuje na svaku aktivnost koja uključuje razmjenu tajnih podataka između Stranaka ili između pravnih subjekata iz država Stranaka, bilo da je završena ili se tek treba izvršiti.

(3) Sporazum neće utjecati na obveze bilo koje od Stranaka koje proističu iz međunarodnih sporazuma s trećim stranama i neće se koristiti protiv interesa, sigurnosti i teritorijalnog integriteta drugih država.

ČLANAK 2.
DEFINICIJE

U ovom će se Sporazumu koristiti slijedeće definicije:

a) **Tajni podatak:** Svaka informacija, dokument ili materijal, bez obzira na njegovu formu, označen određenim stupnjem tajnosti sukladno zakonodavstvu država Stranaka i koji zahtijeva zaštitu od neovlaštenog otkrivanja odnosno bilo kojeg drugog oblika zlouporabe;

b) **Označavanje tajnosti:** označavanje kojim se, sukladno zakonodavstvu države Stranke, određuju odgovarajuća ograničenja u pristupu tajnim podacima i mjere zaštite;

c) **Stranka pošiljateljica:** Stranka, uključujući svaki drugi pravni subjekt države Stranke, koja stvara i šalje tajni podatak drugoj Stranci;

d) **Stranka primateljica:** Stranka, uključujući i svaki drugi pravni subjekt države predmetne Stranke, koja prima tajni podatak od druge Stranke;

e) **Ugovor s tajnim podacima:** ugovor koji sadrži odnosno uključuje tajne podatke;

f) **Osobna sigurnosna dozvola:** dokument izdan sukladno zakonodavstvu države Stranke na temelju izvršene sigurnosne provjere koja je okončana pozitivnom odlukom, a koja omogućava osobi pristup i rukovanje tajnim podacima;

g) **Industrijska sigurnosna dozvola:** dokument izdan sukladno zakonodavstvu države Stranke na temelju izvršene sigurnosne provjere koja je okončana pozitivnom odlukom, te kojom se pravnom subjektu omogućava vršenje poslova vezano za ugovor s tajnim podacima;

h) **Nadležno sigurnosno tijelo:** tijela iz članka 3. ovog Sporazuma ovlaštena, sukladno zakonodavstvu država Stranaka, da na državnoj razini osiguraju jednaku primjenu mjera zaštite tajnih podataka;

i) **Načelo „potrebno znati":** načelo po kojem se pristup tajnim podacima omogućava osobama kojima je to potrebno radi obavljanja službene dužnosti i zadataka;

j) **Zlouporaba:** bilo koji oblik zlouporabe, suprotno državnom zakonodavstvu, koji za posljedicu ima nanošenje štete ili neovlašteni pristup, izmjenu, otkrivanje ili uništenje tajnih podataka, kao i bilo koja druga radnja odnosno nepoduzimanje radnje, koja za posljedicu ima gubitak tajnosti, integriteta i dostupnosti.

ČLANAK 3.
Nadležna sigurnosna tijela

(1) Nadležna sigurnosna tijela odgovorna za primjenu ovog Sporazuma su:

Za Rumunjsku:

Nacionalni ured registra za tajne podatke

Za Bosnu i Hercegovinu:

Ministarstvo sigurnosti Bosne i Hercegovine
Sektor za zaštitu tajnih podataka
Državno sigurnosno tijelo

(2) Stranke se uzajamno obavještavaju diplomatskim putem o svakoj izmjeni vezanoj za nadležna sigurnosna tijela.

ČLANAK 4.
STUPNJEVI TAJNOSTI

(1) Oznake stupnjeva tajnosti su ekvivalentne kako slijedi:

Za Rumunjsku	Za Bosnu i Hercegovinu
STRICT SECRET DE IMPORTANȚĂ DEOSEBITĂ	VRLO TAJNO
STRICT SECRET	TAJNO
SECRET	POVJERLJIVO
SECRET DE SERVICIU	INTERNO

(2) Stranka pošiljateljica će bez odlaganja obavijestiti Stranku primateljicu o svim promjenama stupnjeva tajnosti razmijenjenih tajnih podataka.

(3) Stranka pošiljateljica će obavijestiti Stranku primateljicu o svim dodatnim uvjetima slanja ili ograničenjima u uporabi razmijenjenih tajnih podataka.

(4) Stranka primateljica će osigurati da je tajni podatak označen s ekvivalentnom oznakom tajnosti sukladno stavku (1) ovog članka.

(5) Stranke se uzajamno obavještavaju o svakoj promjeni vezanoj za državne oznake tajnosti.

ROMÂNIA CONSILIUL SUPREM DE APĂRARE A ȚĂRII SECRETARIAT ADMINISTRAȚIA PREZIDENȚIALĂ

ČLANAK 5.
ZAŠTITA TAJNIH PODATAKA

(1) Stranka primateljica osigurava isti stupanj zaštite svih zaprimljenih tajnih podataka kao što osigurava državnim tajnim podacima istog stupnja tajnosti sukladno članku 4. ovog Sporazuma.

(2) Odredbe ovog Sporazuma se neće tumačiti na način koji bi uvjetovao štetne posljedice prema zakonodavstvu država Stranaka koje se odnose na pristup dokumentima od javnog interesa odnosno pristup infomacijama javnog karaktera, zaštitu osobnih podataka ili zaštitu tajnih podataka.

(3) Svaka Stranka osigurava primjenu odgovarajućih mjera zaštite tajnih podataka prilikom njihove obrade, pohrane ili prijenosa u informacijsko – komunikacijskim sustavima. Te mjere osiguravaju povjerljivost, integritet, dostupnost, te prema potrebi neosporavanje i autentičnost tajnih podataka, kao i odgovarajuću razinu odgovornosti i slijedivosti radnji preduzetih u vezi sa zaštitom tajnih podataka.

ČLANAK 6.
OTKRIVANJE I UPORABA TAJNIH PODATAKA

Svaka Stranka jamči da tajnim podacima poslanim ili razmijenjenim prema ovom Sporazumu

a) nije snižena ili ukinuta oznaka tajnosti bez prethodne pisane suglasnosti ili bez zahtjeva Stranke pošiljateljice;

b) da nisu korišteni u svrhu koja se razlikuje od one za koju su dostavljeni;

c) da nisu ustupljeni trećoj stranci, međunarodnoj organizaciji, fizičkoj ili pravnoj osobi bez prethodne pisane suglasnosti Stranke pošiljateljice.

ČLANAK 7.
PRISTUP TAJNIM PODACIMA

(1) Pristup podacima oznake tajnosti SECRET/POVJERLJIVO i više i/ili lokacijama gdje se obavljaju aktivnosti koje uključuju takve podatke dozvoljava se, uz poštivanje načela „potrebno znati", isključivo ovlaštenim osobama koje posjeduju važeće osobne sigurnosne dozvole stupnja tajnosti podataka kojima se pristupa.

(2) Pristup podacima oznake SECRET DE SERVICIU/INTERNO ograničava se na osobe koje ispunjavaju princip „potrebno znati", a pod uvjetom da ispunjavaju uvjete za pristup takvim tajnim podacima sukladno zakonodavstvu država Stranaka.

(3) Svaka Stranka osigurava da sve osobe kojima je dodijeljen pristup tajnim podacima budu upoznate o svojim odgovornostima vezano za zaštitu takvih podataka sukladno odgovarajućim sigurnosnim propisima.

ČLANAK 8.
PREVOĐENJE I UMNOŽAVANJE TAJNIH PODATAKA

(1) Svaki prijevod i preslika tajnih podataka označava se odgovarajućim stupnjem tajnosti i štiti se jednako kao izvornik tajnog podatka.

(2) Sve prijevode i preslike tajnih podataka vrše osobe koje posjeduju odgovarajuću osobnu sigurnosnu dozvolu.

(3) Svi prijevodi tajnih podataka sadrže odgovarajuću napomenu na jeziku prijevoda ukazujući da sadrže tajne podatke Stranke pošiljateljice.

(4) Tajni podaci oznake tajnosti STRICT SECRET DE IMPORTANŢĂ DEOSEBITĂ/VRLO TAJNO prevode se odnosno umnožavaju isključivo uz prethodnu pisanu suglasnost Stranke pošiljateljice.

(5) Svi preslici i prijevodi tajnih podataka se čuvaju na isti način kao i izvorni podatak. Broj preslika se ograničava na broj potreban za službenu uporabu.

ČLANAK 9.
UNIŠTAVANJE TAJNIH PODATAKA

(1) Tajni podaci se uništavaju sukladno zakonodavstvu države Stranke primateljice i to na način da se onemogući njihovo djelimično ili potpuno obnavljanje.

(2) Tajni podaci se uništavaju isključivo uz prethodnu pisanu suglasnost ili po zahtjevu Stranke pošiljateljice.

(3) Tajni podaci oznake STRICT SECRET DE IMPORTANŢĂ DEOSEBITĂ /VRLO TAJNO se ne uništavaju. Oni se vraćaju Stranci pošiljateljici nakon što ih Stranka primateljica ne smatra potrebnim za uporabu.

(4) Stranka primateljica pisanim putem obavještava Stranku pošiljateljicu o uništenju tajnih podataka.

(5) U slučaju kada je nemoguće zaštititi ili vratiti tajne podatke koji su nastali ili razmijenjeni sukladno ovom Sporazumu, takvi tajni podaci se odmah uništavaju. Stranka primateljica pravovremeno obavještava nadležno sigurnosno tijelo Stranke pošiljateljice o uništenju tih tajnih podataka.

ČLANAK 10.
PRIJENOS TAJNIH PODATAKA

(1) Tajni podaci se prenose između Stranaka diplomatskim putem, vojnim kurirom ili drugim sredstvima o kojima se nadležna sigurnosna tijela dogovore i to sukladno zakonodavstvu države one Stranke koja je tražila prijenos. Stranka primateljica pisanim putem potvrđuje primitak tajnih podataka.

(2) Elektronski prijenos tajnih podataka vrši se u kriptovanom obliku, korištenjem kripto metoda i uređaja koji su zajednički odobreni od strane nadležnih sigurnosnih tijela sukladno zakonodavstvu država Stranaka.

(3) Ako je potreban prijenos velike pošiljke koja sadrži tajne podatke, nadležna sigurnosna tijela se kod svakog takvog slučaja pojedinačno dogovaraju o sredstvu transporta, ruti puta i sigurnosnim mjerama.

ČLANAK 11.
POSJETI

(1) Posjeti koji uključuju pristup tajnim podacima na teritoriju države Stranke domaćina predmetom su prethodnog pisanog odobrenja koje izdaje nadležno sigurnosno tijelo Stranke domaćina sukladno državnom zakonodavstvu.

(2) Zahtjev za posjet se dostavlja Nadležnom sigurnosnom tijelu Stranke domaćina i uključuje slijedeće podatke koji se isključivo koriste u svrhu predmetnog posjeta:

a) ime i prezime posjetitelja, datum i mjesto rođenja, državljanstvo, broj osobne karte/putovnice;

b) pozicija posjetitelja uz naznaku poslodavca kojeg posjetitelj predstavlja;

c) specifikacija projekta u kojem posjetitelj sudjeluje;

d) potvrda da posjetitelj posjeduje osobnu sigurnosnu dozvolu, razdoblje važenja, te stupanj tajnosti podataka do kojih mu/joj se može dozvoliti pristup;

e) naziv, adresa, broj telefona/faksa, email i kontakt točka u objektu koji se posjećuje;

f) cilj posjeta, uključujući i najviši stupanj tajnosti podataka;

g) datum i trajanje posjeta. U slučaju višestrukih posjeta navodi se ukupno vremensko razdoblje koje obuhvaćaju posjeti;

h) ostali podaci, ako se o tome usuglase nadležna sigurnosna tijela;

i) datum i potpis nadležnog sigurnosnog tijela Stranke pošiljateljice.

(3) Zahtjev za posjet se dostavlja najmanje 30 dana prije predmetnog posjeta, osim ako se drugačije uzajamno ne dogovore nadležna sigurnosna tijela.

(4) Nadležna sigurnosna tijela Stranke domaćina pravovremeno obavještava Nadležno sigurnosno tijelo Stranke podnositeljice zahtjeva o svojoj odluci.

(5) Po odobrenju posjeta, Nadležno sigurnosno tijelo Stranke domaćina dostavlja preslik zahtjeva za posjet sigurnosnom službeniku objekta koji se treba posjetiti.

(6) Posjetitelji poštivaju sigurnosna pravila i naputke Stranke domaćina.

(7) Nadležna sigurnosna tijela se mogu usuglasiti o popisu posjetitelja ovlaštenih za višestruke posjete. Ovaj popis vrijedi najdulje 12 mjeseci, ali se može dodatno produljiti za vremensko razdoblje koje ne prelazi 12 mjeseci. Zahtjev za višestruke posjete podnosi se sukladno stavku (3) ovog članka. Po dobijanju suglasnosti za popis, posjeti se mogu izravno dogovarati između pravnih osoba.

(8) Zaštitu osobnih podataka posjetitelja Stranke jamče sukladno zakonodavstvu svojih država.

ČLANAK 12.
UGOVOR SA TAJNIM PODACIMA

(1) U slučaju da jedna Stranka ili pravni subjekt iz te države namjerava zaključiti ugovor s tajnim podacima koji će se realizirati na teritoriju države druge Stranke, onda odgovornost za zaštitu tajnih podataka vezanih za predmetni ugovor preuzima ona Stranka na čijem će se teritoriju provoditi

ugovor sukladno zakonodavstvu svoje države i odredbama ovog Sporazuma.

(2) Na zahtjev, nadležna sigurnosna tijela potvrđuju da li predloženi ugovarači posla, kao i osobe koje sudjeluju u predugovornim pregovorima odnosno u provođenju ugovora s tajnim podacima posjeduju odgovarajuću industrijsku sigurnosnu dozvolu i osobne sigurnosne dozvole i to prije pristupa tajnim podacima Stranke pošiljateljice.

(3) Svaki ugovor s tajnim podacima zaključen između ugovaratelja poslova prema odredbama ovog Sporazuma, koji podrazumijeva pristup tajnim podacima stepena tajnosti SECRET/POVJERLJIVO i više, će sadržavati odgovarajući sigurnosni prilog kojim se obvezatno određuju:

a) popis tajnih podataka vezanih za ugovor s tajnim podacima i stupnjeve tajnosti;
b) postupci obavještavanja o izmjenama stupnja tajnosti razmijenjenih podataka;
c) komunikacijski kanali i sredstva elektronskog prijenosa;
d) postupci za slanje tajnih podataka;
e) obvezu obavještenja o svakoj zlouporabi ili sumnji na zlouporabu.

(4) Primjerak sigurnosnog priloga za svaki ugovor s tajnim podacima se dostavlja nadležnom sigurnosnom tijelu Stranke na čijem teritoriju se provodi ugovor, u cilju odgovarajućeg sigurnosnog nadzora i kontrole.

(5) Ugovor s tajnim podacima koji uključuje pristup tajnim podacima stupnja tajnosti SECRET DE SERVICIU/INTERNO sadrži samo odgovarajuću klauzulu s kojom se određuje minimum mjera za zaštitu tih tajnih podataka.

(6) Svaki pod-ugovoratelj ispunjava iste sigurnosne zahtjeve kao i ugovaratelj.

(7) Nadležna sigurnosna tijela mogu dogovoriti zajedničke posjete kako bi analizirali efikasnost mjera primijenjenih od strane ugovaratelja ili pod-ugovaratelja u cilju zaštite tajnih podataka iz ugovora s tajnim podacima.

(8) Stranke osiguravaju zaštitu autorskih prava, industrijskog vlasništva – uključujući i patente, poslovne tajne, te druga prava vezana za tajne podatake razmijenjene između država Stranaka sukladno domaćim zakonodavstvima.

(9) Nadležna sigurnosna tijela Stranaka mogu dogovoriti dodatne detalje procedura vezanih za ugovore s tajnim podacima.

ČLANAK 13.
SIGURNOSNA SURADNJA

(1) U cilju uspostavljanja i održavanja usporednih sigurnosnih standarda, nadležna sigurnosna tijela, po zahtjevu, uzajamno dostavljaju informacije o sigurnosnim standardima i procedurama zaštite tajnih podataka. S tim ciljem, nadležna sigurnosna tijela mogu organizirati uzajamne posjete.

(2) U slučaju potrebe, nadležna sigurnosna tijela mogu zaključiti sigurnosne aranžmane vezane za specifične tehničke aspekte implementacije ovog Sporazuma.

(3) Nadležna sigurnosna tijela se, po potrebi, uzajamno obavještavaju o specifičnim sigurnosnim rizicima, koji mogu ugroziti razmijenjene tajne podatke.

(4) Na zahtjev, nadležna sigurnosna tijela Stranaka se uzajamno pomažu u postupku izdavanja osobnih sigurnosnih dozvola i industrijskih sigurnosnih dozvola za svoje državljane koji borave odnosno pravne osobe koja se nalaze na teritoriju države druge Stranke, sukladno zakonodavstvima svojih država.

(5) Nadležna sigurnosna tijela se uzajamno obavještavaju o svakoj izmjeni osobnih sigurnosnih dozvola i industrijskih sigurnosnih dozvola vezanih za suradnju po ovom Sporazumu.

(6) Stranke uzajamno priznaju osobne sigurnosne dozvole i industrijske sigurnosne dozvole, koja se osobama i pravnim subjektima iz njihovih država izdaju sukladno njihovom zakonodavstvu, a u vezi pristupa tajnim podacima koji se razmijenjuju prema ovom Sporazumu.

(7) Sigurnosne, obavještajne i policijske službe država Stranaka mogu surađivati i direktno razmijenjivati operativne i/ili obavještajne podatke sukladno zakonodavstvu svojih država.

ČLANAK 14.
ZLOUPORABA TAJNIH PODATAKA

(1) U slučaju zlouporabe ili postojanja osnovane sumnje zlouporabe, Stranke poduzimaju sve odgovarajuće mjere s ciljem utvrđivanja okolnosti sukladno domaćem zakonodavstvu.

(2) U slučaju da zlouporaba uključuje i tajne podatke koji su nastali i zaprimljeni od druge Stranke, Nadležno sigurnosno tijelo u čijoj se državi

dogodila zlouporaba obavještava bez odlaganja Nadležno sigurnosno tijelo Stranke pošiljateljice, te osigurava primjenu odgovarajućih mjera sukladno domaćem zakonodavstvu. Ukoliko je potrebno, Stranke surađuju tijekom gore navedenog postupka.

(3) U slučaju zlouporabe na teritoriju treće države, aktivnosti iz stavka (2) ovog članka poduzima Nadležno sigurnosno tijelo Stranke koja ih je poslala.

(4) Nadležno sigurnosno tijelo Stranke primateljice pisanim putem obavještava Nadležno sigurnosno tijelo Stranke pošiljateljice o okolnostima pod kojima se dogodila zlouporaba, stupanj štete, mjere poduzete kako bi se ista umanjila, te rezultat postupka navedenog u stavku (2) ovog članka. Takva obavijest sadrži dovoljno informacija kako bi Stranka pošiljalateljica u potpunosti mogla sagledati posljedice zlouporabe.

ČLANAK 15.
TUMAČENJE I SPOROVI

Bilo koji spor vezan za tumačenje ili primjenu ovog Sporazuma se riješava isključivo kroz konzultacije između Stranaka.

ČLANAK 16.
TROŠKOVI

Svaka Stranka snosi vlastite troškove nastale tijekom provedbe ovog Sporazuma.

ČLANAK 17.
ZAVRŠNE ODREDBE

(1) Ovaj se Sporazum zaključuje na neodređeno vremensko razdoblje. Predmetom je ratifikacije sukladno zakonodavstvima država Stranaka i stupa na snagu prvog dana drugog mjeseca od dana posljednjeg pisanog obavještenja diplomatskim putem između Stranaka da su ispunjeni uvjeti potrebni za stupanje na snagu ovog Sporazuma.

(2) Ovaj se Sporazum može mijenjati uz obostranu pisanu suglasnost obje Stranke. Takve izmjene i dopune stupaju na snagu sukladno stavku (1) ovog članka.

(3) Svaka Stranka može u bilo kojem trenutku pisanim putem raskinuti ovaj Sporazum. U tom slučaju, Sporazum prestaje važiti po isteku šest (6) mjeseci od dana kada je druga Stranka zaprimila obavijest o raskidu.

(4) Bez obzira na raskidanje ovog Sporazuma, svi tajni podaci razmijenjeni sukladno ovom Sporazumu se i nadalje štite sukladno ovdje navedenim odredbama sve dok Stranka pošiljateljica ne razriješi Stranku primateljicu od takvih obveza.

(5) Stranke se bez odlaganja uzajamno obavještavaju o svim promjenama u zakonodavstvu svojih država koje utječu na zaštitu tajnih podataka razmijenjenih prema ovom Sporazumu. U slučaju takvih izmjena, Stranke se konzultiraju u cilju razmatranja potencijalnih izmjena ovog Sporazuma. U međuvremenu, tajni podaci se i nadalje čuvaju na način kako je Sporazumom određeno, osim ako Stranka pošiljateljica drugačije ne zatraži pisanim putem.

Sačinjeno u Sarajevu dana 27. januara 2020. u dva izvornika, svaki na rumunjskom, na službenim jezicima Bosne i Hercegovine (bosanski, hrvatski, srpski) i engleskom jeziku, pri čemu su svaki od tekstova podjednako vjerodostojni. U slučaju razlika u tumačenju prevladava tekst na engleskom jeziku.

U potvrdu svega, dolje navedeni, kao osobe ovlaštene za potpis, potpisali su ovaj Sporazum.

Za
Vladu Rumunjske

[redacted]

Za
Vijeće ministara
Bosne i Hercegovine

[redacted]

Copie certificată pentru conformitate cu originalul

Corina Badea, director [redacted]

Direcția Tratate Internaționale
Ministerul Afacerilor Externe

SPORAZUM

IZMEĐU

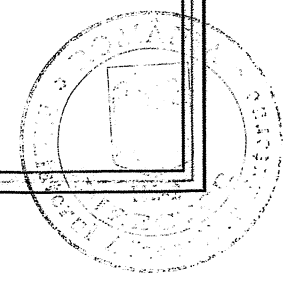
VLADE RUMUNIJE

I

VIJEĆA MINISTARA BOSNE I HERCEGOVINE

O MEĐUSOBNOJ ZAŠTITI

TAJNIH PODATAKA



PREAMBULA

Vlada Rumunije i Vijeće ministara Bosne i Hercegovine (u daljem tekstu: „Strane"),

uzimajući u obzir da dobra saradnja između Strana može podrazumijevati razmjenu tajnih podataka, direktno ili putem drugih pravnih subjekata država Strana,

u želji da uspostave zakonski okvir za obostranu zaštitu razmijenjenih tajnih podataka koji bi bio primjenjiv na svaki naredni sporazum i ugovor o saradnji između Strana ili između pravnih subjekata država Strana, a koji sadrži ili omogućava pristup tajnim podacima,

usaglasili su se o sljedećem:

ČLAN 1.
CILJ I OPSEG

(1) Sporazum ima za cilj da osigura zaštitu tajnih podataka, koji su razmijenjeni ili nastali kroz saradnju između Strana ili između pravnih subjekata država Strana.

(2) Sporazum se primijenjuje na svaku aktivnost koja uključuje razmjenu tajnih podataka između Strana ili između pravnih subjekata iz država Strana, bilo da je završena ili se tek treba izvršiti.

(3) Sporazum neće uticati na obaveze bilo koje od Strana koje proističu iz međunarodnih sporazuma sa trećim stranama i neće se koristiti protiv interesa, sigurnosti i teritorijalnog integriteta drugih država.

ČLAN 2.
DEFINICIJE

U ovom će se Sporazumu koristiti slijedeće definicije:

a) **Tajni podatak:** Svaka informacija, dokument ili materijal, bez obzira na njegovu formu, označen određenim stepenom tajnosti u skladu sa zakonodavstvom država Strana i koji zahtijeva zaštitu od neovlaštenog otkrivanja odnosno bilo kojeg drugog oblika zloupotrebe;

b) **Označavanje tajnosti:** označavanje kojim se, u skladu sa zakonodavstvom države Strane, određuju odgovarajuća ograničenja u pristupu tajnim podacima i mjere zaštite;

c) **Strana pošiljalac:** Strana, uključujući svaki drugi pravni subjekt države Strane, koja stvara i šalje tajni podatak drugoj Strani;

d) **Strana primalac:** Strana, uključujući i svaki drugi pravni subjekt države predmetne Strane, koja prima tajni podatak od druge Strane;

e) **Ugovor sa tajnim podacima:** ugovor koji sadrži odnosno uključuje tajne podatke;

f) **Lična sigurnosna dozvola:** dokument izdan u skladu sa zakonodavstvom države Strane na osnovu izvršene sigurnosne provjere koja je okončana pozitivnom odlukom, a koja omogućava licu pristup i rukovanje tajnim podacima;

g) **Industrijska sigurnosna dozvola:** dokument izdan u skladu sa zakonodavstvom države Strane na osnovu izvršene sigurnosne provjere koja je okončana pozitivnom odlukom, te kojom se pravnom subjektu omogućava vršenje poslova vezano za ugovor sa tajnim podacima;

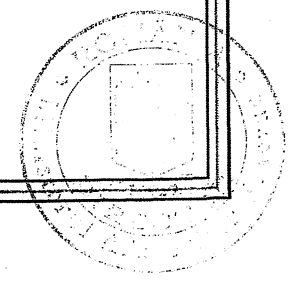
h) **Nadležni sigurnosni organ:** organi iz člana 3. ovog Sporazuma ovlašteni, u skladu sa zakonodavstvom država Strana, da na državnom nivou osiguravaju jednaku primjenu mjera zaštite tajnih podataka;

i) **Princip „potrebno znati":** princip po kojem se pristup tajnim podacima omogućava licima kojima je to potrebno radi obavljanja službene dužnosti i zadataka;

j) **Zloupotreba:** bilo koji oblik zloupotrebe, suprotno državnom zakonodavstvu, koji za posljedicu ima nanošenje štete ili neovlašteni pristup, izmjenu, otkrivanje ili uništavanje tajnih podataka, kao i bilo koja druga radnja odnosno nepreduzimanje radnje, koja za posljedicu ima gubitak tajnosti, integriteta i dostupnosti.

ČLAN 3.
Nadležni sigurnosni organi

(1) Nadležni sigurnosni organi odgovorni za primjenu ovog Sporazuma su:



Za Rumuniju:

Nacionalni ured registra za tajne podatke

Za Bosnu i Hercegovinu:

Ministarstvo sigurnosti Bosne i Hercegovine
Sektor za zaštitu tajnih podataka
Državni sigurnosni organ

(2) Strane se međusobno obavještavaju diplomatskim putem o svakoj izmjeni vezanoj za nadležne sigurnosne organe.

ČLAN 4.
STEPENI TAJNOSTI

(1) Oznake stepena tajnosti su ekvivalentne kako slijedi:

Za Rumuniju	Za Bosnu i Hercegovinu
STRICT SECRET DE IMPORTANŢĂ DEOSEBITĂ	VRLO TAJNO
STRICT SECRET	TAJNO
SECRET	POVJERLJIVO
SECRET DE SERVICIU	INTERNO

(2) Strana pošiljalac će bez odlaganja obavijestiti Stranu primaoca o svim promjenama stepena tajnosti razmijenjenih tajnih podataka.

(3) Strana pošiljalac će obavijestiti Stranu primaoca o svim dodatnim uslovima slanja ili ograničenjima u upotrebi razmijenjenih tajnih podataka.

(4) Strana primalac će osigurati da je tajni podatak označen sa ekvivalentnom oznakom tajnosti u skladu sa stavom (1) ovog člana.

(5) Strane se međusobno obavještavaju o svakoj promjeni vezanoj za državne oznake tajnosti.

ČLAN 5.
ZAŠTITA TAJNIH PODATAKA

(1) Strana primalac osigurava isti stepen zaštite svih zaprimljenih tajnih podataka kao što osigurava državnim tajnim podacima istog stepena tajnosti u skladu sa članom 4. ovog Sporazuma.

(2) Odredbe ovog Sporazuma se neće tumačiti na način koji bi uzrokovao štetne posljedice prema zakonodavstvu država Strana koje se odnose na pristup dokumentima od javnog interesa odnosno pristup infomacijama javnog karaktera, zaštitu ličnih podataka ili zaštitu tajnih podataka.

(3) Svaka Strana osigurava primjenu odgovarajućih mjera zaštite tajnih podataka prilikom njihove obrade, pohrane ili prijenosa u informaciono – komunikacionim sistemima. Te mjere osiguravaju povjerljivost, integritet, dostupnost, te prema potrebi neosporavanje i autentičnost tajnih podataka, kao i odgovarajući nivo odgovornosti i slijedivosti radnji preduzetih u vezi zaštite tajnih podataka.

ČLAN 6.
OTKRIVANJE I UPOTREBA TAJNIH PODATAKA

Svaka Strana osigurava da tajnim podacima poslanim ili razmijenjenim prema ovom Sporazumu

a) nije snižena ili ukinuta oznaka tajnosti bez prethodne pismene saglasnosti ili bez zahtjeva Strane pošiljaoca;

b) da nisu korišteni u svrhu koja se razlikuje od one za koju su dostavljeni;

c) da nisu ustupljeni trećoj strani, međunarodnoj organizaciji, fizičkom ili pravnom licu bez prethodne pismene saglasnosti Strane pošiljaoca.

ČLAN 7.
PRISTUP TAJNIM PODACIMA

(1) Pristup podacima oznake tajnosti SECRET/POVJERLJIVO i više i/ili lokacijama gdje se obavljaju aktivnosti koje uključuju takve podatke dozvoljava se, uz poštovanje principa „potrebno znati", isključivo ovlaštenim licima koja posjeduju važeće lične sigurnosne dozvole stepena tajnosti podataka kojima se pristupa.

(2) Pristup podacima oznake SECRET DE SERVICIU/INTERNO ograničava se na lica koja ispunjavaju princip „potrebno znati", a pod uslovom da ispunjavaju uslove za pristup takvim tajnim podacima u skladu sa zakonodavstvom država Strana.

(3) Svaka Strana osigurava da sva lica kojima je dodijeljen pristup tajnim podacima budu upoznate o svojim odgovornostima vezano za zaštitu takvih podataka u skladu sa odgovarajućim sigurnosnim propisima.

ČLAN 8.
PREVOĐENJE I UMNOŽAVANJE TAJNIH PODATAKA

(1) Svaki prijevod i kopija tajnih podataka označava se odgovarajućim stepenom tajnosti i štiti se jednako kao original tajnog podatka.

(2) Sve prijevode i kopije tajnih podataka vrše lica koja posjeduju odgovarajuću ličnu sigurnosnu dozvolu.

(3) Svi prijevodi tajnih podataka sadrže odgovarajuću napomenu na jeziku prijevoda ukazujući da sadrže tajne podatke Strane pošiljaoca.

(4) Tajni podaci oznake tajnosti STRICT SECRET DE IMPORTANŢĂ DEOSEBITĂ/VRLO TAJNO prevode se odnosno umnožavaju isključivo uz prethodnu pismenu saglasnost Strane pošiljaoca.

(5) Sve kopije i prijevodi tajnih podataka se čuvaju na isti način kao i originalni podatak. Broj kopija se ograničava na broj potreban za službenu upotrebu.

ČLAN 9.
UNIŠTAVANJE TAJNIH PODATAKA

(1) Tajni podaci se uništavaju u skladu sa zakonodavstvom države Strane primaoca i to na način da se onemogući njihovo djelimično ili potpuno obnavljanje.

(2) Tajni podaci se uništavaju isključivo uz prethodnu pismenu saglasnost ili po zahtjevu Strane pošiljaoca.

(3) Tajni podaci oznake STRICT SECRET DE IMPORTANŢĂ DEOSEBITĂ /VRLO TAJNO se ne uništavaju. Oni se vraćaju Strani pošiljaocu nakon što ih Strana primalac ne smatra potrebnim za upotrebu.

(4) Strana primalac pismeno obavještava Stranu pošiljaoca o uništavanju tajnih podataka.

(5) U slučaju kada je nemoguće zaštititi ili vratiti tajne podatke koji su nastali ili razmijenjeni u skladu sa ovim Sporazumom, takvi tajni podaci se odmah uništavaju. Strana primalac pravovremeno obavještava nadležni sigurnosni organ Strane pošiljaoca o uništavanju tih tajnih podataka.

ČLAN 10.
PRIJENOS TAJNIH PODATAKA

(1) Tajni podaci se prenose između Strana diplomatskim putem, vojnim kurirom ili drugim sredstvima o kojima se nadležni sigurnosni organi dogovore i to u skladu sa zakonodavstvom države one Strane koja je tražila prijenos. Strana primalac pismeno potvrđuje prijem tajnih podataka.

(2) Elektronski prijenos tajnih podataka vrši se u kriptovanom obliku, korištenjem kripto metoda i uređaja koji su zajednički odobreni od strane nadležnih sigurnosnih organa u skladu sa zakonodavstvom država Strana.

(3) Ako je potreban prijenos velike pošiljke koja sadrži tajne podatke, nadležni sigurnosni organi se kod svakog takvog slučaja pojedinačno dogovaraju o sredstvu transporta, ruti puta i sigurnosnim mjerama.

ČLAN 11.
POSJETE

(1) Posjete koje uključuju pristup tajnim podacima na teritoriji države Strane domaćina predmetom su prethodnog pismenog odobrenja koje izdaje nadležni sigurnosni organ Strane domaćina u skladu sa državnim zakonodavstvom.

(2) Zahtjev za posjetu se dostavlja Nadležnom sigurnosnom organu Strane domaćina i uključuje slijedeće podatke koji se isključivo koriste u svrhu predmetne posjete:

a) ime i prezime posjetioca, datum i mjesto rođenja, državljanstvo, broj lične karte/pasoša;

b) pozicija posjetioca uz naznaku poslodavca kojeg posjetilac predstavlja;

c) specifikacija projekta u kojem posjetilac učestvuje;

d) potvrda da posjetilac posjeduje ličnu sigurnosnu dozvolu, period važenja, te stepen tajnosti podataka do kojih mu/joj se može dozvoliti pristup;

e) naziv, adresa, broj telefona/faksa, email i kontakt tačka u objektu koji se posjećuje;

f) cilj posjete, uključujući i najviši stepen tajnosti podataka;

g) datum i trajanje posjete. U slučaju višestrukih posjeta navodi se ukupni vremenski period koji obuhvataju posjete;

h) ostali podaci, ako se o tome usaglase nadležni sigurnosni organi;

i) datum i potpis nadležnog sigurnosnog organa Strane pošiljaoca.

(3) Zahtjev za posjetu se dostavlja najmanje 30 dana prije predmetne posjete, osim ako se drugačije zajednički ne dogovore nadležni sigurnosni organi.

(4) Nadležni sigurnosni organ Strane domaćina blagovremeno obavještava Nadležni sigurnosni organ Strane podnosioca zahtjeva o svojoj odluci.

(5) Po odobrenju posjete, Nadležni sigurnosni organ Strane domaćina dostavlja kopiju zahtjeva za posjetu sigurnosnom službeniku objekta koji se treba posjetiti.

(6) Posjetioci poštuju sigurnosna pravila i instrukcije Strane domaćina.

(7) Nadležni sigurnosni organi se mogu usaglasiti o spisku posjetilaca ovlaštenih za višestruke posjete. Ovaj spisak važi najduže 12 mjeseci, ali se može dodatno produžiti za vremenski period koji ne prelazi 12 mjeseci. Zahtjev za višestruke posjete podnosi se u skladu sa stavom (3) ovog člana. Po dobijanju saglasnosti za spisak, posjete se mogu direktno dogovarati između pravnih lica.

(8) Zaštitu ličnih podataka posjetilaca Strane garantuju u skladu sa zakonodavstvom svojih država.

ČLAN 12.
UGOVOR SA TAJNIM PODACIMA

(1) U slučaju da jedna Strana ili pravni subjekt iz te države namjerava zaključiti ugovor sa tajnim podacima koji će se realizovati na teritoriji države druge Strane, onda odgovornost za zaštitu tajnih podataka vezanih za predmetni

ugovor preuzima ona Strana na čijoj će se teritoriji provoditi ugovor u skladu sa zakonodavstvom svoje države i odredbama ovog Sporazuma.

(2) Na zahtjev, nadležni sigurnosni organi potvrđuju da li predloženi ugovarači poslova, kao i lica koja učestvuju u predugovornim pregovorima odnosno u provođenju ugovora sa tajnim podacima posjeduju odgovarajuću industrijsku sigurnosnu dozvolu i lične sigurnosne dozvole i to prije pristupa tajnim podacima Strane pošiljaoca.

(3) Svaki ugovor sa tajnim podacima zaključen između ugovarača poslova prema odredbama ovog Sporazuma, koji podrazumijeva pristup tajnim podacima stepena tajnosti SECRET/POVJERLJIVO i više, će sadržavati odgovarajući sigurnosni prilog kojim se obavezno određuju:

a) lista tajnih podataka vezanih za ugovor sa tajnim podacima i stepene tajnosti;
b) postupci obavještavanja o izmjenama stepena tajnosti razmijenjenih podataka;
c) komunikacioni kanali i sredstva elektronskog prijenosa;
d) procedure za slanje tajnih podataka;
e) obavezu obavještenja o svakoj zloupotrebi ili sumnji na zloupotrebu.

(4) Primjerak sigurnosnog priloga za svaki ugovor sa tajnim podacima se dostavlja nadležnom sigurnosnom organu Strane na čijoj teritoriji se provodi ugovor, u cilju odgovarajućeg sigurnosnog nadzora i kontrole.

(5) Ugovor sa tajnim podacima koji uključuje pristup tajnim podacima stepena tajnosti SECRET DE SERVICIU/INTERNO sadrži samo odgovarajuću klauzulu sa kojom se određuje minimum mjera za zaštitu tih tajnih podataka.

(6) Svaki pod-ugovorač ispunjava iste sigurnosne zahtjeve kao i ugovarač.

(7) Nadležni sigurnosni organi mogu dogovoriti zajedničke posjete kako bi analizirali efikasnost mjera primijenjenih od strane ugovarača ili pod-ugovarača u cilju zaštite tajnih podataka iz ugovora sa tajnim podacima.

(8) Strane osiguravaju zaštitu autorskih prava, industrijskog vlasništva – uključujući i patente, poslovne tajne, te druga prava vezana za tajne podatake razmijenjene između država Strana u skladu sa domaćim zakonodavstvima.

(9) Nadležni sigurnosni organi Strana mogu dogovoriti dodatne detalje procedura vezanih za ugovore sa tajnim podacima.

ČLAN 13.
SIGURNOSNA SARADNJA

(1) U cilju uspostavljanja i održavanja uporednih sigurnosnih standarda, nadležni sigurnosni organi, po zahtjevu, međusobno dostavljaju informacije o sigurnosnim standardima i procedurama zaštite tajnih podataka. S tim ciljem, nadležni sigurnosni organi mogu organizovati međusobne posjete.

(2) U slučaju potrebe, nadležni sigurnosni organi mogu zaključiti sigurnosne aranžmane vezane za specifične tehničke aspekte implementacije ovog Sporazuma.

(3) Nadležni sigurnosni organi se, po potrebi, međusobno obavještavaju o specifičnim sigurnosnim rizicima, koji mogu ugroziti razmijenjene tajne podatke.

(4) Na zahtjev, nadležni sigurnosni organi Strana se međusobno pomažu u postupku izdavanja ličnih sigurnosnih dozvola i industrijskih sigurnosnih dozvola za svoje državljane koji borave odnosno pravna lica koja se nalaze na teritoriji države druge Strane, u skladu sa zakonodavstvima svojih država.

(5) Nadležni sigurnosni organi se međusobno obavještavaju o svakoj izmjeni ličnih sigurnosnih dozvola i industrijskih sigurnosnih dozvola vezanih za saradnju prema ovom Sporazumu.

(6) Strane međusobno priznaju lične sigurnosne dozvole i industrijske sigurnosne dozvole, koja se licima i pravnim subjektima iz njihovih država izdaju u skladu sa njihovim zakonodavstvom, a u vezi pristupa tajnim podacima koji se razmijenjuju prema ovom Sporazumu.

(7) Sigurnosne, obavještajne i policijske službe država Strana mogu sarađivati i direktno razmijenjivati operativne i/ili obavještajne podatke u skladu sa zakonodavstvom svojih država.

ČLAN 14.
ZLOUPOTREBA TAJNIH PODATAKA

(1) U slučaju zloupotrebe ili postojanja osnovane sumnje zloupotrebe, Strane poduzimaju sve odgovarajuće mjere s ciljem utvrđivanja okolnosti u skladu sa domaćim zakonodavstvom.

(2) U slučaju da zloupotreba uključuje i tajne podatke koji su nastali i zaprimljeni od druge Strane, Nadležni sigurnosni organ u čijoj se državi dogodila zloupotreba obavještava bez odlaganja Nadležni sigurnosni organ Strane pošiljaoca, te osigurava primjenu odgovarajućih mjera u skladu sa domaćim zakonodavstvom. Ukoliko je potrebno, Strane sarađuju tokom gore navedenog postupka.

(3) U slučaju zloupotrebe na teritoriji treće države, aktivnosti iz stava (2) ovog člana poduzima Nadležni sigurnosni organ Strane koja ih je poslala.

(4) Nadležni sigurnosni organ Strane primaoca pismeno obavještava Nadležni sigurnosni organ Strane pošiljaoca o okolnostima pod kojima se dogodila zloupotreba, stepen štete, mjere poduzete kako bi se ista umanjila, te ishod postupka navedenog u stavu (2) ovog člana. Takva obavijest sadrži dovoljno informacija da bi Strana pošiljalac u potpunosti mogla sagledati posljedice zloupotrebe.

ČLAN 15.
TUMAČENJE I SPOROVI

Bilo koji spor vezan za tumačenje ili primjenu ovog Sporazuma se rješava isključivo kroz konsultacije između Strana.

ČLAN 16.
TROŠKOVI

Svaka Strana snosi vlastite troškove nastale tokom provedbe ovog Sporazuma.

ČLAN 17.
ZAVRŠNE ODREDBE

(1) Ovaj se Sporazum zaključuje na neodređen vremenski period. Predmetom je ratifikacije u skladu sa zakonodavstvima država Strana i stupa na snagu prvog dana drugog mjeseca od dana posljednjeg pismenog obavještenja diplomatskim putem između Strana da su ispunjeni uslovi potrebni za stupanje na snagu ovog Sporazuma.

(2) Ovaj se Sporazum može mijenjati uz obostranu pismenu saglasnost obje Strane. Takve izmjene i dopune stupaju na snagu u skladu sa stavom (1) ovog člana.

(3) Svaka Strana može u bilo kojem trenutku pismeno raskinuti ovaj Sporazum. U tom slučaju, Sporazum prestaje važiti po isteku šest (6) mjeseci od dana kada je druga Strana zaprimila obavještenje o raskidu.

(4) Bez obzira na raskidanje ovog Sporazuma, svi tajni podaci razmijenjeni u skladu sa ovim Sporazumom se i nadalje štite u skladu sa ovdje prethodno navedenim odredbama sve dok Strana pošiljalac ne razriješi Stranu primaoca od takvih obaveza.

(5) Strane se bez odlaganja međusobno obavještavaju o svim promjenama u zakonodavstvu svojih država koje utiču na zaštitu tajnih podataka razmijenjenih prema ovom Sporazumu. U slučaju takvih izmjena, Strane se konsultuju u cilju razmatranja potencijalnih izmjena ovog Sporazuma. U međuvremenu, tajni podaci se i nadalje čuvaju na način kako je Sporazumom određeno, osim ako Strana pošiljalac drugačije ne zatraži pismenim putem.

Sačinjeno u Sarajevu dana 27 januara 2010. u dva originala, svaki na rumunskom, na službenim jezicima Bosne i Hercegovine (bosanski, hrvatski, srpski) i engleskom jeziku, pri čemu su svaki od tekstova podjednako autentičan. U slučaju razlika u tumačenju prevladava tekst na engleskom jeziku.

U potvrdu svega, dole navedeni, kao lica ovlaštena za potpis, potpisali su ovaj Sporazum.

Za
Vladu Rumunije

[redacted]

Za
Vijeće ministara
Bosne i Hercegovine

[redacted]

Copie certificată pentru conformitate cu originalul

Corina Badea, director [redacted]

Direcția Tratate Internaționale
Ministerul Afacerilor Externe

ROMÂNIA DIRECȚIA TRATATE INTERNAȚIONALE H2-2

ROMÂNIA * CONSILIUL SUPREM DE APĂRARE A ȚĂRII * SECRETARIAT ADMINISTRAȚIA PREZIDENȚIALĂ

СПОРАЗУМ

ИЗМЕЂУ

ВЛАДЕ РУМУНИЈЕ

И

САВЈЕТА МИНИСТАРА БОСНЕ И ХЕРЦЕГОВИНЕ

О МЕЂУСОБНОЈ ЗАШТИТИ

ТАЈНИХ ПОДАТАКА

ПРЕАМБУЛА

Влада Румуније и Савјет министара Босне и Херцеговине (у даљем тексту: „Стране"),

узимајући у обзир да добра сарадња између Страна може подразумијевати размјену тајних података, директно или путем других правних субјеката држава Страна,

у жељи да успоставе законски оквир за обострану заштиту размијењених тајних података који би био примјењив на сваки наредни споразум и уговор о сарадњи између Страна или између правних субјеката држава Страна, а који садржи или омогућава приступ тајним подацима,

усагласили су се о сљедећем:

ЧЛАН 1.
ЦИЉ И ОПСЕГ

(1) Споразум има за циљ да обезбједи заштиту тајних података, који су размијењени или настали кроз сарадњу између Страна или између правних субјеката држава Страна.

(2) Споразум се примијењује на сваку активност која укључује размјену тајних података између Страна или између правних субјеката из држава Страна, било да је завршена или се тек треба извршити.

(3) Споразум неће утицати на обавезе било које од Страна које проистичу из међународних споразума са трећим странама и неће се користити против интереса, безбједности и територијалног интегритета других држава.

ЧЛАН 2.
ДЕФИНИЦИЈЕ

У овом ће се Споразуму користити слиједеће дефиниције:

а) **Тајни податак:** Свака информација, документ или материјал, без обзира на његову форму, означен одређеним степеном тајности у складу са законодавством држава Страна и који захтијева заштиту од неовлаштеног откривања односно било којег другог облика злоупотребе;

b) **Означавање тајности:** означавање којим се, у складу са законодавством државе Стране, одређују одговарајућа ограничења у приступу тајним подацима и мјере заштите;

c) **Страна пошиљалац:** Страна, укључујући сваки други правни субјект државе Стране, која ствара и шаље тајни податак другој Страни;

d) **Страна прималац:** Страна, укључујући и сваки други правни субјект државе предметне Стране, која прима тајни податак од друге Стране;

e) **Уговор са тајним подацима:** уговор који садржи односно укључује тајне податке;

f) **Лична безбједносна дозвола:** документ издан у складу са законодавством државе Стране на основу извршене безбједносне провјере која је окончана позитивном одлуком, а која омогућава лицу приступ и руковање тајним подацима;

g) **Индустријска безбједносна дозвола:** документ издан у складу са законодавством државе Стране на основу извршене безбједносне провјере која је окончана позитивном одлуком, те којом се правном субјекту омогућава вршење послова везано за уговор са тајним подацима;

h) **Надлежни безбједносни орган:** органи из члана 3. овог Споразума овлаштени, у складу са законодавством држава Страна, да на државном нивоу обезбјеђују једнаку примјену мјера заштите тајних података;

i) **Принцип „потребно знати“:** принцип по којем се приступ тајним подацима омогућава лицима којима је то потребно ради обављања службене дужности и задатака;

j) **Злоупотреба:** било који облик злоупотребе, супротно државном законодавству, који за посљедицу има наношење штете или неовлаштени приступ, измјену, откривање или уништавање тајних података, као и било која друга радња односно непредузимање радње, која за посљедицу има губитак тајности, интегритета и доступности.

ЧЛАН 3.
Надлежни безбједносни органи

(1) Надлежни безбједносни органи одговорни за примјену овог Споразума су:

За Румунију:

Национална канцеларија регистра за тајне податке

За Босну и Херцеговину:

Министарство безбједности Босне и Херцеговине
Сектор за заштиту тајних података
Државни безбједносни орган

(2) Стране се међусобно обавјештавају дипломатским путем о свакој измјени везаној за надлежне безбједносне органе.

ЧЛАН 4.
СТЕПЕНИ ТАЈНОСТИ

(1) Ознаке степена тајности су еквивалентне како слиједи:

За Румунију	За Босну и Херцеговину
STRICT SECRET DE IMPORTANŢĂ DEOSEBITĂ	ВРЛО ТАЈНО
STRICT SECRET	ТАЈНО
SECRET	ПОВЈЕРЉИВО
SECRET DE SERVICIU	ИНТЕРНО

(2) Страна пошиљалац ће без одлагања обавијестити Страну примаоца о свим промјенама степена тајности размијењених тајних података.

(3) Страна пошиљалац ће обавијестити Страну примаоца о свим додатним условима слања или ограничењима у употреби размијењених тајних података.

(4) Страна прималац ће обезбједити да је тајни податак означен са еквивалентном ознаком тајности у складу са ставом (1) овог члана.

ROMÂNIA * ADMINISTRAŢIA PREZIDENŢIALĂ - CONSILIUL SUPREM DE APĂRARE A ȚĂRII - SECRETARIAT

(5) Стране се међусобно обавјештавају о свакој промјени везаној за државне ознаке тајности.

ЧЛАН 5.
ЗАШТИТА ТАЈНИХ ПОДАТАКА

(1) Страна прималац обезбјеђује исти степен заштите свих запримљених тајних података као што обезбјеђује државним тајним подацима истог степена тајности у складу са чланом 4. овог Споразума.

(2) Одредбе овог Споразума се неће тумачити на начин који би узроковао штетне посљедице према законодавству држава Страна које се односе на приступ документима од јавног интереса односно приступ инфомацијама јавног карактера, заштиту личних података или заштиту тајних података.

(3) Свака Страна обезбјеђује примјену одговарајућих мјера заштите тајних података приликом њихове обраде, похране или преноса у информационо – комуникационим системима. Те мјере обезбјеђују повјерљивост, интегритет, доступност, те према потреби неоспоравање и аутентичност тајних података, као и одговарајући ниво одговорности и слиједивости радњи предузетих у вези заштите тајних података.

ЧЛАН 6.
ОТКРИВАЊЕ И УПОТРЕБА ТАЈНИХ ПОДАТАКА

Свака Страна обезбјеђује да тајним подацима посланим или размијењеним према овом Споразуму

a) није снижена или укинута ознака тајности без претходне писмене сагласности или без захтјева Стране пошиљаоца;

b) да нису кориштени у сврху која се разликује од оне за коју су достављени;

c) да нису уступљени трећој страни, међународној организацији, физичком или правном лицу без претходне писмене сагласности Стране пошиљаоца.

ЧЛАН 7.
ПРИСТУП ТАЈНИМ ПОДАЦИМА

(1) Приступ подацима ознаке тајности SECRET/ПОВЈЕРЉИВО и више и/или локацијама гдје се обављају активности које укључују такве податке дозвољава се, уз поштовање принципа „потребно знати“, искључиво овлаштеним лицима која посједују важеће личне безбједносне дозволе степена тајности података којима се приступа.

(2) Приступ подацима ознаке SECRET DE SERVICIU/ИНТЕРНО ограничава се на лица која испуњавају принцип „потребно знати“, а под условом да испуњавају услове за приступ таквим тајним подацима у складу са законодавством држава Страна.

(3) Свака Страна обезбјеђује да сва лица којима је додијељен приступ тајним подацима буду упознате о својим одговорностима везано за заштиту таквих података у складу са одговарајућим безбједносним прописима.

ЧЛАН 8.
ПРЕВОЂЕЊЕ И УМНОЖАВАЊЕ ТАЈНИХ ПОДАТАКА

(1) Сваки превод и копија тајних података означава се одговарајућим степеном тајности и штити се једнако као оригинал тајног податка.

(2) Све преводе и копије тајних података врше лица које посједују одговарајућу личну безбједносну дозволу.

(3) Сви преводи тајних података садрже одговарајућу напомену на језику превода указујући да садрже тајне податке Стране пошиљаоца.

(4) Тајни подаци ознаке тајности STRICT SECRET DE IMPORTANŢĂ DEOSEBITĂ/ВРЛО ТАЈНО преводе се односно умножавају искључиво уз претходну писмену сагласност Стране пошиљаоца.

(5) Све копије и преводи тајних података се чувају на исти начин као и оригинални податак. Број копија се ограничава на број потребан за службену употребу.

ЧЛАН 9.
УНИШТАВАЊЕ ТАЈНИХ ПОДАТАКА

(1) Тајни подаци се уништавају у складу са законодавством државе Стране примаоца и то на начин да се онемогући њихово дјелимично или потпуно обнављање.

(2) Тајни подаци се уништавају искључиво уз претходну писмену сагласност или по захтјеву Стране пошиљаоца.

(3) Тајни подаци ознаке STRICT SECRET DE IMPORTANŢĂ DEOSEBITĂ /ВРЛО ТАЈНО се не уништавају. Они се враћају Страни пошиљаоцу након што их Страна прималац не сматра потребним за употребу.

(4) Страна прималац писмено обавјештава Страну пошиљаоца о уништавању тајних података.

(5) У случају када је немогуће заштитити или вратити тајне податке који су настали или размијењени у складу са овим Споразумом, такви тајни подаци се одмах уништавају. Страна прималац правовремено обавјештава надлежни безбједносни орган Стране пошиљаоца о уништавању тих тајних података.

ЧЛАН 10.
ПРИЈЕНОС ТАЈНИХ ПОДАТАКА

(1) Тајни подаци се преносе између Страна дипломатским путем, војним куриром или другим средствима о којима се надлежни безбједносни органи договоре и то у складу са законодавством државе оне Стране која је тражила пренос. Страна прималац писмено потврђује пријем тајних података.

(2) Електронски пренос тајних података врши се у криптованом облику, коришћењем крипто метода и уређаја који су заједнички одобрени од стране надлежних безбједносних органа у складу са законодавством држава Страна.

(3) Ако је потребан пренос велике пошиљке која садржи тајне податке, надлежни безбједносни органи се код сваког таквог случаја појединачно договарају о средству транспорта, рути пута и безбједносним мјерама.

ЧЛАН 11.
ПОСЈЕТЕ

(1) Посјете које укључују приступ тајним подацима на територију државе Стране домаћина предметом су претходног писменог одобрења које издаје надлежни безбједносни орган Стране домаћина у складу са државним законодавством.

(2) Захтјев за посјету се доставља Надлежном безбједносном органу Стране домаћина и укључује слиједеће податке који се искључиво користе у сврху предметне посјете:

a) име и презиме посјетиоца, датум и мјесто рођења, држављанство, број личне карте/пасоша;

b) позиција посјетиоца уз назнаку послодавца којег посјетилац представља;

c) спецификација пројекта у којем посјетилац учествује;

d) потврда да посјетилац посједује личну безбједносну дозволу, период важења, те степен тајности података до којих му/јој се може дозволити приступ;

e) назив, адреса, број телефона/факса, e-mail и контакт тачка у објекту који се посјећује;

f) циљ посјете, укључујући и највиши степен тајности података;

g) датум и трајање посјете. У случају вишеструких посјета наводи се укупни временски период који обухватају посјете;

h) остали подаци, ако се о томе усагласе надлежни безбједносни органи;

i) датум и потпис надлежног безбједносног органа Стране пошиљаоца.

(3) Захтјев за посјету се доставља најмање 30 дана прије предметне посјете, осим ако се другачије заједнички не договоре надлежни безбједносни органи.

(4) Надлежни безбједносни орган Стране домаћина благовремено обавјештава Надлежни безбједносни орган Стране подносиоца захтјева о својој одлуци.

(5) По одобрењу посјете, Надлежни безбједносни орган Стране домаћина доставља копију захтјева за посјету безбједносном службенику објекта који се треба посјетити.

(6) Посјетиоци поштују безбједносна правила и инструкције Стране домаћина.

(7) Надлежни безбједносни органи се могу усагласити о списку посјетилаца овлаштених за вишеструке посјете. Овај списак важи најдуже 12 мјесеци, али се може додатно продужити за временски период који не прелази 12 мјесеци. Захтјев за вишеструке посјете подноси се у складу са ставом (3) овог члана. По добијању сагласности за списак, посјете се могу директно договарати између правних лица.

(8) Заштиту личних података посјетилаца Стране гарантују у складу са законодавством својих држава.

ЧЛАН 12.
УГОВОР СА ТАЈНИМ ПОДАЦИМА

(1) У случају да једна Страна или правни субјект из те државе намјерава закључити уговор са тајним подацима који ће се реализовати на територији државе друге Стране, онда одговорност за заштиту тајних података везаних за предметни уговор преузима она Страна на чијој ће се територији проводити уговор у складу са законодавством своје државе и одредбама овог Споразума.

(2) На захтјев, надлежни безбједносни органи потврђују да ли предложени уговарачи послова, као и лица која учествују у предуговорним преговорима односно у провођењу уговора са тајним подацима посједују одговарајућу индустријску безбједносну дозволу и личне безбједносне дозволе и то прије приступа тајним подацима Стране пошиљаоца.

(3) Сваки уговор са тајним подацима закључен између уговарача послова према одредбама овог Споразума, који подразумијева приступ тајним подацима степена тајности SECRET/ПОВЈЕРЉИВО и више, ће садржавати одговарајући безбједносни прилог којим се обавезно одређују:

a) листа тајних података везаних за уговор са тајним подацима и степене тајности;
b) поступци обавјештавања о измјенама степена тајности размијењених података;
c) комуникациони канали и средства електронског преноса;
d) процедуре за слање тајних података;
e) обавезу обавјештења о свакој злоупотреби или сумњи на злоупотребу.

(4) Примјерак безбједносног прилога за сваки уговор са тајним подацима се доставља надлежном безбједносном органу Стране на чијој

територији се спроводи уговор, у циљу одговарајућег безбједносног надзора и контроле.

(5) Уговор са тајним подацима који укључује приступ тајним подацима степена тајности SECRET DE SERVICIU/ИНТЕРНО садржи само одговарајућу клаузулу са којом се одређује минимум мјера за заштиту тих тајних података.

(6) Сваки под-уговорач испуњава исте безбједносне захтјеве као и уговарач.

(7) Надлежни безбједносни органи могу договорити заједничке посјете како би анализирали ефикасност мјера примијењених од стране уговарача или под-уговарача у циљу заштите тајних података из уговора са тајним подацима.

(8) Стране обезбјеђују заштиту ауторских права, индустријског власништва – укључујући и патенте, пословне тајне, те друга права везана за тајне податке размијењене између држава Страна у складу са домаћим законодавствима.

(9) Надлежни безбједносни органи Страна могу договорити додатне детаље процедура везаних за уговоре са тајним подацима.

ЧЛАН 13.
БЕЗБЈЕДНОСНА САРАДЊА

(1) У циљу успостављања и одржавања упоредних безбједносних стандарда, надлежни безбједносни органи, по захтјеву, међусобно достављају информације о безбједносним стандардима и процедурама заштите тајних података. С тим циљем, надлежни безбједносни органи могу организовати међусобне посјете.

(2) У случају потребе, надлежни безбједносни органи могу закључити безбједносне аранжмане везане за специфичне техничке аспекте имплементације овог Споразума.

(3) Надлежни безбједносни органи се, по потреби, међусобно обавјештавају о специфичним безбједносним ризицима, који могу угрозити размијењене тајне податке.

(4) На захтјев, надлежни безбједносни органи Страна се међусобно помажу у поступку издавања личних безбједносних дозвола и индустријских безбједносних дозвола за своје држављане који бораве

ROMÂNIA * ADMINISTRAȚIA PREZIDENȚIALĂ * CONSILIUL SUPREM DE APĂRARE A ȚĂRII - SECRETARIAT

односно правна лица која се налазе на територији државе друге Стране, у складу са законодавствима својих држава.

(5) Надлежни безбједносни органи се међусобно обавјештавају о свакој измјени личних безбједносних дозвола и индустријских безбједносних дозвола везаних за сарадњу према овом Споразуму.

(6) Стране међусобно признају личне безбједносне дозволе и индустријске безбједносне дозволе, која се лицима и правним субјектима из њихових држава издају у складу са њиховим законодавством, а у вези приступа тајним подацима који се размијењују према овом Споразуму.

(7) Безбједносне, обавјештајне и полицијске службе држава Страна могу сарађивати и директно размијењивати оперативне и/или обавјештајне податке у складу са законодавством својих држава.

ЧЛАН 14.
ЗЛОУПОТРЕБА ТАЈНИХ ПОДАТАКА

(1) У случају злоупотребе или постојања основане сумње злоупотребе, Стране предузимају све одговарајуће мјере с циљем утврђивања околности у складу са домаћим законодавством.

(2) У случају да злоупотреба укључује и тајне податке који су настали и запримљени од друге Стране, Надлежни безбједносни орган у чијој се држави догодила злоупотреба обавјештава без одлагања Надлежни безбједносни орган Стране пошиљаоца, те обезбјеђује примјену одговарајућих мјера у складу са домаћим законодавством. Уколико је потребно, Стране сарађују током горе наведеног поступка.

(3) У случају злоупотребе на територији треће државе, активности из става (2) овог члана подузима Надлежни безбједносни орган Стране која их је послала.

(4) Надлежни безбједносни орган Стране примаоца писмено обавјештава Надлежни безбједносни орган Стране пошиљаоца о околностима под којима се догодила злоупотреба, степен штете, мјере подузете како би се иста умањила, те исход поступка наведеног у ставу (2) овог члана. Таква обавијест садржи довољно информација да би Страна пошиљалац у потпуности могла сагледати посљедице злоупотребе.

ЧЛАН 15.
ТУМАЧЕЊЕ И СПОРОВИ

Било који спор везан за тумачење или примјену овог Споразума се рјешава искључиво кроз консултације између Страна.

ЧЛАН 16.
ТРОШКОВИ

Свака Страна сноси властите трошкове настале током спровођења овог Споразума.

ЧЛАН 17.
ЗАВРШНЕ ОДРЕДБЕ

(1) Овај Споразум се закључује на неодређен временски период. Предметом је ратификације у складу са законодавствима држава Страна и ступа на снагу првог дана другог мјесеца од дана посљедњег писменог обавјештења дипломатским путем између Страна да су испуњени услови потребни за ступање на снагу овог Споразума.

(2) Овај Споразум се може мијењати уз обострану писмену сагласност обје Стране. Такве измјене и допуне ступају на снагу у складу са ставом (1) овог члана.

(3) Свака Страна може у било којем тренутку писмено раскинути овај Споразум. У том случају, Споразум престаје важити по истеку шест (6) мјесеци од дана када је друга Страна запримила обавјештење о раскиду.

(4) Без обзира на раскидање овог Споразума, сви тајни подаци размијењени у складу са овим Споразумом се и надаље штите у складу са овдје претходно наведеним одредбама све док Страна пошиљалац не разријеши Страну примаоца од таквих обавеза.

(5) Стране се без одлагања међусобно обавјештавају о свим промјенама у законодавству својих држава које утичу на заштиту тајних података размијењених према овом Споразуму. У случају таквих измјена, Стране се консултују у циљу разматрања потенцијалних измјена овог Споразума. У међувремену, тајни подаци се и надаље чувају на начин како је Споразумом одређено, осим ако Страна пошиљалац другачије не затражи писменим путем.

Сачињено у Сарајеву дана 27. јануара 2020. у два оригинала, сваки на румунском, на службеним језицима Босне и Херцеговине (босански, хрватски, српски) и енглеском језику, при чему су сваки од текстова подједнако аутентичан. У случају разлика у тумачењу превладава текст на енглеском језику.

У потврду свега, доле наведени, као лица овлаштена за потпис, потписали су овај Споразум.

За
Владу Румуније

За
Савјет министара
Босне и Херцеговине

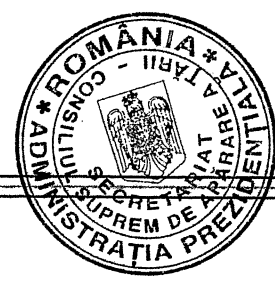
Copie certificată pentru conformitate cu originalul

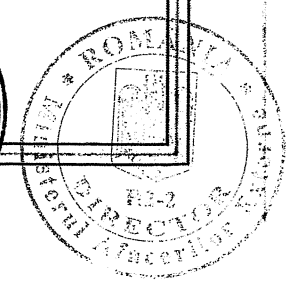
Corina Badea, director

Direcția Tratate Internaționale
Ministerul Afacerilor Externe

ROMÂNIA
CONSILIUL SUPREM DE APĂRARE A ȚĂRII
SECRETARIATUL ADMINISTRAȚIA PREZIDENȚIALĂ

ACORD
ÎNTRE
GUVERNUL ROMÂNIEI
ŞI
CONSILIUL DE MINIŞTRI AL BOSNIEI ŞI HERŢEGOVINEI
PRIVIND
PROTECŢIA RECIPROCĂ
A INFORMAŢIILOR CLASIFICATE





PREAMBUL

Guvernul României şi Consiliul de Miniştri al Bosniei Herţegovinei (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 legislaţia statului Părţii, determină anumite restricţii privind accesul la Informaţii Clasificate şi măsurile de protecţie;

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

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

e) **Contract Clasificat:** orice contract care conţine sau implică Informaţii Clasificate;

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

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

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

i) **'Necesitatea de a cunoaşte':** principiul conform căruia accesul la Informaţii Clasificate poate fi acordat unei persoane numai dacă acesta este necesar în vederea îndeplinirii îndatoririlor oficiale şi sarcinilor de serviciu;

j) **Compromitere:** orice întrebuinţare necorespunzătoare, contrară legislaţiei statului Părţii, care are drept rezultat deteriorarea sau accesul neautorizat, modificarea, dezvăluirea ori distrugerea Informaţiilor Clasificate, precum şi orice acţiune sau inacţiune care duce la pierderea confidenţialităţii, integrităţii sau disponibilităţii acestora.

ARTICOLUL 3
AUTORITĂŢI COMPETENTE DE SECURITATE

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

În România:
Oficiul Registrului Naţional al Informaţiilor Secrete de Stat

În Bosnia şi Herţegovina:
Ministerul Securității
Sectorul pentru Protecția Informațiilor Clasificate
Autoritatea Națională de Securitate

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

ARTICOLUL 4
NIVELURI DE CLASIFICARE

(1) Echivalenţa nivelurilor de clasificare naţionale este următoarea:

Pentru România	Pentru Bosnia şi Herţegovina
STRICT SECRET DE IMPORTANŢĂ DEOSEBITĂ	VRLO TAJNO
STRICT SECRET	TAJNO
SECRET	POVJERLJIVO
SECRET DE SERVICIU	INTERNO

(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 sunt marcate cu Nivelul de Clasificare naţional 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 statelor 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

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.

ARTICOLUL 7
ACCESUL LA INFORMAŢII CLASIFICATE

(1) Accesul la informațiile clasificate SECRET/POVJERLJIVO şi de nivel superior, precum şi în încăperile şi obiectivele unde se desfăşoară activităţii ce implică astfel de informaţii este permis, cu respectarea principiului Necesitatea 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/INTERNO se va limita numai la persoanele care respectă principiul Necesitatea de a cunoaşte şi condiţionat de îndeplinirea de către acestea a cerinţelor pentru acces la această categorie de Informaţii Clasificate în conformitate cu legislaţiile statelor 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.

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 în 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 statului 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 îi mai sunt necesare.

(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, în conformitate cu legislaţia statului acesteia.

(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 menţionarea 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;

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 a Părţii solicitante.

(3) Cererea de vizită va fi transmisă cu cel puţin 30 de zile înainte de vizită, dacă Autorităţile Competente de Securitate nu au convenit altfel.

(4) Autoritatea Competentă de Securitate a Părţii gazdă 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 statelor acestora.

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 a Personalului şi Certificate de Securitate Industrială 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) Contractul Clasificat încheiat între contractanţi, în conformitate cu prevederile prezentului Acord, care implică acces la informaţii de nivel SECRET/POVJERLJIVO şi superior, va cuprinde o anexă de securitate corespunzătoare care va include cel puţin următoarele:
   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) canalele de comunicare şi mijloacele de transmitere electromagnetică;
   d) procedura de transport a Informaţiilor Clasificate;

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

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

(5) Contractul Clasificat care implică accesul la informaţii SECRET DE SERVICIU/INTERNO va conţine doar 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 naţionale.

(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 scop, 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 propriii 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 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 statelor acestora, 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 statelor acestora.

ARTICOLUL 14
COMPROMITEREA INFORMAŢIILOR CLASIFICATE

(1) Părţile vor lua toate măsurile corespunzătoare, 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 statului său. 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 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. Acesta este supus ratificării în conformitate cu legislaţiile statelor Părţilor şi intră în vigoare în prima zi a celei de-a doua luni de la data primirii, pe canale diplomatice, a ultimei notificări între Părţi, prin care se informează de faptul că au fost îndeplinite procedurile necesare pentru intrarea în vigoare a prezentului Acord.

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

(3) Fiecare Parte are dreptul să denunţe oricând, în scris, prezentul Acord. În acest caz, Acordul își încetează valabilitatea după şase (6) luni de la data la care notificarea de denunţare a fost primită de cealaltă Parte.

(4) Chiar şi în situaţia denunţării 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 lor 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.

Semnat la SARAJEVO, la 27 IANUARIE 2020 în două exemplare originale, fiecare în limba română, în limbile oficiale ale Bosniei și Hertegovinei (bosniacă, croată și sârbă) şi în limba engleză, toate textele fiind egal autentice. În caz de divergenţe de interpretare, textul în limba engleză prevalează.

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

PENTRU GUVERNUL ROMÂNIEI

PENTRU CONSILIUL DE MINIȘTRI AL BOSNIEI SI HERTEGOVINEI

Copie certificată pentru conformitate cu originalul

Corina Badea, director

Direcția Tratate Internaționale
Ministerul Afacerilor Externe