NN 1/2021 (5.3.2021.), Odluka o objavi Sporazuma između Vlade Republike Hrvatske i Vlade Sjedinjenih Američkih Država o sigurnosnim mjerama za zaštitu klasificiranih podataka

VLADA REPUBLIKE HRVATSKE

Na temelju članka 32. Zakona o sklapanju i izvršavanju međunarodnih ugovora (»Narodne novine«, broj 28/96.), Vlada Republike Hrvatske je na sjednici održanoj 11. veljače 2021. donijela

ODLUKU

O OBJAVI SPORAZUMA IZMEĐU VLADE REPUBLIKE HRVATSKE I VLADE SJEDINJENIH AMERIČKIH DRŽAVA O SIGURNOSNIM MJERAMA ZA ZAŠTITU KLASIFICIRANIH PODATAKA

I.

Objavljuje se Sporazum između Vlade Republike Hrvatske i Vlade Sjedinjenih Američkih Država o sigurnosnim mjerama za zaštitu klasificiranih podataka potpisan u Zagrebu, 5. siječnja 2021., u izvorniku na engleskom jeziku.

II.

Tekst Sporazuma iz točke I. ove Odluke, u izvorniku na engleskom jeziku i u prijevodu na hrvatski jezik, glasi:

AGREEMENT
BETWEEN THE GOVERNMENT OF THE REPUBLIC OF CROATIA AND THE GOVERNMENT OF THE UNITED STATES OF AMERICA CONCERNING SECURITY MEASURES FOR THE PROTECTION OF CLASSIFIED INFORMATION

The Government of the Republic of Croatia («Croatia») and the Government of the United States of America (the «United States»), each a «Party,» and collectively the «Parties»;

Considering that the Parties cooperate in matters including, but not limited to, foreign affairs, defense, security, law enforcement, science, industry, and technology; and

Having a mutual interest in the protection of Classified Information exchanged in confidence between the Parties;

Have agreed as follows:

Article 1
DEFINITIONS

For the purpose of this Agreement:

1. *Classified Information:* Information provided by one Party to the other Party that is designated as classified by the releasing Party for national security purposes and therefore requires protection against unauthorized disclosure. The information may be in oral, visual, electronic, or documentary form, or in the form of material, including equipment or technology.

2. *Classified Contract:* A contract that requires, or will require, access to, or production of, Classified Information by a Contractor or by its employees in the performance of the contract.

3. *Contractor:* An individual or a legal entity, possessing the legal capacity to conclude contracts, who is a party to a Classified Contract.

4. *Facility Security Clearance:* A certification provided by the National Security Authority of a Party, as designated in Article 4, for a Contractor facility under the Party's jurisdiction that indicates the facility is cleared to a specified level and also has suitable security safeguards in place at a specified level to safeguard Classified Information. Such a certification shall signify that Classified Information at the POVJERLJIVO / CONFIDENTIAL level or above shall be protected by the Contractor for which the Facility Security Clearance (FSC) is provided in accordance with the provisions of this Agreement and that compliance shall be monitored and enforced by the relevant National Security Authority. An FSC is not required for a Contractor to undertake Contracts that only require the receipt or production of Classified Information at the OGRANIČENO (RESTRICTED) level.

5. *Personnel Security Clearance (PSC):*

a. A determination by the National Security Authority of a Party, as designated in Article 4, that an individual who is employed by a government agency of that Party or a Contractor under the jurisdiction of that Party is authorized to access Classified Information up to a specified level.

b. A determination by the National Security Authority of a Party, as designated in Article 4, that an individual who is a citizen of one Party but is to be employed by the other Party or by one of the other Party's Contractors is authorized access to Classified Information up to a specified level.

6. Need *to Know:* A determination made by an authorized holder of Classified Information that a prospective recipient of Classified Information requires access to specific Classified Information in order to perform or assist in a lawful and authorized governmental function.

Article 2

LIMITATIONS ON THE SCOPE OF THE AGREEMENT

This Agreement shall not apply to Classified Information within the scope of the terms of another agreement or arrangement between the Parties or agencies thereof providing for the protection of a particular item or category of Classified Information exchanged between the Parties or agencies thereof, except to the extent that such other agreement or arrangement expressly makes this Agreement's terms applicable. This Agreement also shall not apply to the exchange of Restricted Data, as defined in the U.S. Atomic Energy Act of 1954, as amended (the «AEA»), or to Formerly Restricted Data, which is data removed from the Restricted Data category in accordance with the AEA but still considered to be defense information by the United States.

Article 3

COMMITMENT TO THE PROTECTION OF CLASSIFIED INFORMATION

1. Each Party shall protect Classified Information of the other Party according to the terms set forth herein.

2. Classified Information shall be protected by the recipient Party in a manner that is at least equivalent to the protection afforded to Classified Information by the releasing Party.

3. Each Party shall promptly notify the other of any changes to its laws and regulations that would affect the protection of Classified Information under this Agreement. The obligations in this Agreement shall not be affected by such changes in domestic law. In such cases, the Parties shall consult regarding possible amendments to this Agreement or other measures that may be appropriate to maintain protection of Classified Information exchanged under this Agreement.

Article 4

NATIONAL SECURITY AUTHORITIES

1. The Parties shall inform each other of the National Security Authorities responsible for implementation of this Agreement and any subsequent changes to these Authorities.

2. For the purpose of this Agreement, the National Security Authorities shall be:

a. for Croatia: Director, Office of the National Security Council (UVNS)

b. for the United States: Assistant Director, International Engagement Directorate, Defense Technology Security Administration, Office of the Under Secretary of Defense for Policy, U.S. Department of Defense.

3. The Parties may conclude supplemental implementing arrangements to this Agreement where additional technical security measures may be required to protect Classified Information transferred to the recipient Party through foreign military sales or cooperative programs for co-production or co-development of defense articles or services. Such implementing arrangements may include Special Security Agreements or Industrial Security Agreements.

Article 5

DESIGNATION OF CLASSIFIED INFORMATION

1. Classified Information shall be designated, and stamped or marked where possible, by the releasing Party as classified at one of the following national security classification levels. For purposes of ensuring equivalent treatment, the Parties agree that the following security classification levels are equivalent:

CROATIA	UNITED STATES
VRLO TAJNO	TOP SECRET
TAJNO	SECRET
POVJERLJIVO	CONFIDENTIAL
OGRANIČENO (RESTRICTED)	No equivalent (see paragraph 2)

2. During the implementation of this Agreement, if Croatia provides Classified Information designated as OGRANIČENO (RESTRICTED), the United States shall handle it in accordance with the Appendix to this Agreement.

3. Classified Information shall be designated, and stamped or marked where possible, with the name of the releasing Party.

Article 6

RESPONSIBILITY FOR CLASSIFIED INFORMATION

The recipient Party shall be responsible for the protection of all Classified Information of the releasing Party in a manner that is at least equivalent to the protection afforded to Classified Information by the releasing Party while the Classified Information is under its control. While in transit, the releasing Party shall be responsible for all Classified Information until custody of the Classified Information is formally transferred to the recipient Party.

Article 7

PROTECTION OF CLASSIFIED INFORMATION

1. No individual shall be entitled to have access to Classified Information solely by virtue of rank, position, appointment, or PSC. Access to such information shall be granted only to individuals who have a Need to Know and who have been granted the requisite PSC in accordance with the prescribed standards of the recipient Party.

2. Except as otherwise provided in this Agreement, the recipient Party shall not release Classified Information of the releasing Party to any third party, including any third-party government, individual, firm, institution, organization, or other entity, without the prior written consent of the releasing Party.

3. The recipient Party shall not use or permit the use of Classified Information of the releasing Party for any other purpose than that for which it was provided without the prior written consent of the releasing Party.

4. The recipient Party shall respect any private rights that are associated with Classified Information of the releasing Party, including those rights with respect to patents, copyrights, or trade secrets, and shall not release, use, exchange, or disclose such Classified Information in a manner inconsistent with those rights without the prior written authorization of the owner of those rights.

5. The recipient Party shall ensure that each facility or establishment that handles Classified Information covered by this Agreement maintains a list of individuals at the facility or establishment who are authorized to have access to such information.

6. Each Party shall develop accountability and control procedures to manage the dissemination of, and access to, Classified Information.

7. Each Party shall comply with any and all limitations on use, disclosure, release, and access to Classified Information as may be specified by the releasing Party when it discloses such Classified Information. If a Party is unable to comply with the specified limitations, that Party shall immediately consult with the other Party and shall undertake all lawful measures to prevent or minimize any such use, disclosure, release, or access.

Article 8

PERSONNEL SECURITY CLEARANCES

1. The Parties shall ensure that all individuals who in the conduct of their official duties require access or whose duties or functions may afford access to Classified Information pursuant to this Agreement receive an appropriate PSC before they are granted access to such information.

2. The Party granting the PSC shall conduct an appropriate investigation in sufficient detail to determine an individual's suitability for access to Classified Information. The determination to grant a PSC will be made in accordance with the national laws and regulations of the granting Party.

3. Before an official or representative of one Party releases Classified Information to an official or representative of the other Party, the recipient Party shall provide to the releasing Party an assurance that the official or representative has the necessary PSC level and a Need to Know and that the Classified Information will be protected by the recipient Party in accordance with this Agreement.

Article 9

RELEASE OF CLASSIFIED INFORMATION TO CONTRACTORS

1. Classified Information received by a recipient Party may be provided by the recipient Party to a Contractor or prospective Contractor whose duties require access to such information with the prior written consent of the releasing Party. Prior to releasing any Classified Information to a Contractor or prospective Contractor, the recipient Party shall:

a. Confirm that such Contractor or prospective Contractor and the Contractor's facility have the capability to safeguard the information in accordance with the terms of this Agreement;

b. Confirm that such Contractor or prospective Contractor and the Contractor's facility have been granted appropriate PSCs and FSCs, as applicable;

c. Confirm that the Contractor or prospective Contractor has procedures in place to ensure that all individuals having access to the information are informed of their responsibilities to protect the information in accordance with applicable laws and regulations;

d. Carry out periodic security inspections of cleared facilities to ensure that the information is protected as required by this Agreement; and

e. Confirm that the Contractor or prospective Contractor has procedures in place to ensure that access to the information is limited to those individuals who have a Need to Know.

Article 10
CLASSIFIED CONTRACTS

1. When a Party proposes to place, or authorizes a Contractor in its country to place, a Classified Contract that is classified at the POVJERLJIVO / CONFIDENTIAL level or above, with a Contractor in the country of the other Party, the Party that is to place or authorize the Contractor to place such Classified Contract shall request an assurance that an FSC has been issued from the National Security Authority of the other Party. The National Security Authority of the requested Party shall monitor and take all appropriate steps to ensure the security conduct by the Contractor will be in accordance with applicable laws and regulations.

2. The National Security Authority of a Party negotiating a Classified Contract to be performed in the country of the other Party shall incorporate in the Classified Contract, request for proposal, or subcontract document appropriate security clauses and other relevant provisions, including costs for security. This includes provisions requiring any Contractors to include appropriate security clauses in their subcontract documents.

Article 11
RESPONSIBILITY FOR FACILITIES

Each Party shall be responsible for the security of all government and private facilities and establishments where it stores Classified Information of the other Party and shall ensure that such facilities or establishments have qualified and appropriately cleared individuals appointed with the responsibility and authority for the control and protection of such information.

Article 12
STORAGE OF CLASSIFIED INFORMATION

Classified Information exchanged between the Parties shall be stored in a manner that ensures access only by those individuals who have been authorized access.

Article 13
TRANSMISSION

1. Classified Information shall be transmitted between the Parties through government-to-government channels or other channels mutually approved in advance in writing.

2. The minimum requirements for the security of Classified Information during transmission shall be as follows:

a. Documents or other media:

(1) Documents or other media containing Classified Information shall be transmitted in double, sealed envelopes. The inner envelope shall indicate only the classification of the documents or other media and the organizational address of the intended recipient. The outer envelope shall indicate the organizational address of the intended recipient, the organizational address of the sender, and the document control number, if applicable.

(2) No indication of the classification of the enclosed documents or other media shall be made on the outer envelope. The double sealed envelope shall be transmitted according to the prescribed procedures of the Parties.

(3) Receipts shall be prepared by the recipient for packages containing documents or other media containing Classified Information that are transmitted between the Parties, and such receipts shall be signed by the final recipient and returned to the sender.

b. Material:

(1) Material, including equipment, that contains Classified Information shall be transported in sealed, covered vehicles, or shall otherwise be securely packaged or protected in order to prevent identification of its shape, size, or contents, and kept under continuous control to prevent access by unauthorized persons.

(2) Material, including equipment, that contains Classified Information that must be stored temporarily awaiting shipment shall be placed in protected storage areas. Such areas shall be protected by intrusion detection equipment or guards with requisite PSCs who shall maintain continuous surveillance of those areas. Only authorized personnel with the requisite PSC shall have access to the protected storage areas.

(3) Receipts shall be obtained whenever material that contains Classified Information, including equipment, changes hands during transit, and a receipt for such material shall be signed by the final recipient and returned to the sender.

c. Electronic transmissions:

(1) Classified Information that is classified at the POVJERLJIVO / CONFIDENTIAL level or above that is to be transferred electronically shall be transmitted using secure means that have been approved by each Party's National Security Authority.

Article 14

VISITS TO FACILITIES AND ESTABLISHMENTS OF THE PARTIES

1. Visits by representatives of one Party to facilities and establishments of the other Party that require access to Classified Information, or visits for which a PSC is required to permit access, shall be limited to those necessary for official purposes. Authorization shall only be granted to representatives who possess a valid PSC.

2. Authorization to visit such facilities and establishments shall be granted only by the Party in whose territory the facility or establishment to be visited is located. The visited Party, or its designated officials, shall be responsible for advising the facility or establishment of the proposed visit, and the scope and highest level of Classified Information that may be furnished to the visitor.

3. Requests for visits by representatives of the Parties shall be submitted by the Embassy of the Republic of Croatia in Washington, D.C., in the case of Croatian visitors, and by the Embassy of the United States in Zagreb in the case of U.S. visitors.

Article 15

SECURITY VISITS

Implementation of security requirements set out in this Agreement may be verified through reciprocal visits by security personnel of the Parties. The security representatives of each Party, after prior consultation, shall be permitted to visit the other Party to discuss and observe the implementing procedures of the other Party in the interest of achieving reasonable comparability of security systems. The host Party shall assist the visiting security representatives in determining whether Classified Information received from the other Party is being adequately protected.

Article 16

SECURITY STANDARDS

On request, each Party shall provide the other Party with information about its security standards, practices, and procedures for safeguarding of Classified Information.

Article 17

REPRODUCTION OF CLASSIFIED INFORMATION

When Classified Information is reproduced, all of the original security markings thereon shall also be reproduced, stamped, or marked on each reproduction of such information. Such reproductions shall be subject to the same controls as the original information. The number of reproductions shall be limited to the minimum number required for official purposes.

Article 18

DESTRUCTION OF CLASSIFIED INFORMATION

1. Documents and other media containing Classified Information shall be destroyed by burning, shredding, pulping, or other means that prevent reconstruction of the Classified Information contained therein.

2. Material, including equipment, containing Classified Information shall be destroyed through means that render it no longer recognizable so as to preclude reconstruction of the Classified Information in whole or in part.

Article 19

DOWNGRADING AND DECLASSIFICATION

1. The Parties agree that Classified Information should be downgraded in classification as soon as the information ceases to require that higher degree of protection or should be declassified as soon as the information no longer requires protection against unauthorized disclosure.

2. The releasing Party has complete discretion concerning downgrading or declassification of its Classified Information. The recipient Party shall not downgrade the security classification or declassify Classified Information received from the releasing Party, notwithstanding any apparent declassification instructions on the document, without the prior written consent of the releasing Party.

Article 20
LOSS OR COMPROMISE

The recipient Party shall inform the releasing Party immediately upon discovery of all losses or compromises, as well as possible losses or compromises, of Classified Information of the releasing Party. In the event of an actual or possible loss or compromise of such information, the recipient Party shall initiate an investigation immediately to determine the circumstances of the actual or possible loss or compromise. The results of the investigation and information regarding measures taken to prevent recurrence shall be provided to the releasing Party.

Article 21
DISPUTES

Disagreements between the Parties arising under or relating to this Agreement shall be settled solely through consultations between the Parties and shall not be referred to a national court, an international tribunal, or any other person or entity for settlement.

Article 22
COSTS

Each Party shall be responsible for bearing its own costs incurred in implementing this Agreement. All obligations of the Parties under this Agreement shall be subject to the availability of funds.

Article 23
FINAL PROVISIONS

1. This Agreement shall enter into force on the date of the last signature by the Parties.

2. Either Party may terminate this Agreement by notifying the other Party in writing through diplomatic channels ninety days in advance of its intention to terminate the Agreement.

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

IN WITNESS WHEREOF, the undersigned, being duly authorized thereto by their respective Governments, have signed this Agreement.

Done in duplicate at Zagreb this 5th day of January 2021, in the English language.

FOR THE GOVERNMENT
OF THE REPUBLIC OF
CROATIA
Maja Čavlović
Director of the Office
of the National Security Council

FOR THE GOVERNMENT OF THE UNITED STATES OF AMERICA
William Robert Kohorst
Ambassador Extraordinary and Plenipotentiary of the United States
of America to the Republic of Croatia

APPENDIX

PROCEDURES FOR PROTECTING REPUBLIC OF CROATIA OGRANIČENO (RESTRICTED) CLASSIFIED INFORMATION PROVIDED TO THE UNITED STATES

1. Upon receipt, Croatian Classified Information provided to the United States and designated as «OGRANIČENO (RESTRICTED)» shall be protected by the United States in accordance with the following procedures.

2. Information designated as «OGRANIČENO (RESTRICTED)» shall be stored in locked containers or closed areas that prevent access by unauthorized personnel.

3. «OGRANIČENO (RESTRICTED)» Classified Information shall not be disclosed to unauthorized persons or entities without the prior written approval of the originator or the National Security Authority of the Republic of Croatia, except as required by U.S. law, including the Freedom of Information Act.

4. «OGRANIČENO (RESTRICTED)» Classified Information shall, as applicable, be stored, processed, or transmitted electronically using government- or Contractor-accredited systems. In particular, before any system is used to store, process, or transmit «OGRANIČENO (RESTRICTED)» Classified Information, it must receive security approval, known as Accreditation. An Accreditation is a formal statement by the appropriate accrediting authority confirming that the use of a system meets the appropriate security requirements and does not present an unacceptable risk. Security Standard Operating Procedures are technical procedures to implement security policies and requirements unique to a specific facility to protect automated information systems processing Classified Information. For stand-alone automated information systems such as desktop and laptop computers utilized in U.S. Government establishments, the system registration document together with the Security Standard Operating Procedures shall fulfill the role of the required Accreditation. For Contractors, guidance on the use of communications and information systems shall be incorporated into the Restricted Conditions Requirements Clause in the Contract.

5. «OGRANIČENO (RESTRICTED)» Classified Information shall be transmitted by first class mail within the United States in one sealed envelope. Transmission outside the United States shall be in double, sealed envelopes, with the inner envelope marked «Republic of Croatia OGRANIČENO (RESTRICTED).» Transmission outside the United States shall be by traceable means such as commercial courier or other means agreed upon by the Parties in writing.

6. U.S. documents that contain Croatian «OGRANIČENO (RESTRICTED)» Classified Information shall bear on the cover and the first page the marking «Republic of Croatia OGRANIČENO (RESTRICTED).» The portion of the documents containing Croatian «OGRANIČENO» Classified Information also shall be identified with the marking «Republic of Croatia OGRANIČENO (RESTRICTED).»

7. «OGRANIČENO (RESTRICTED)» Classified Information may be transmitted or accessed electronically via a public network like the Internet using government or commercial encryption devices mutually accepted by the Parties. Telephone conversations, video conferencing, or facsimile transmissions containing «OGRANIČENO (RESTRICTED)» Classified Information may be conducted if an encryption system is not available and subject to the approval of the releasing Party's National Security Authority.

8. An FSC and PSC are not required for a Contractor to undertake contracts that require only the receipt or production of Classified Information at the «OGRANIČENO (RESTRICTED)» level.

9. Access to such «OGRANIČENO (RESTRICTED)» Classified Information shall be granted only to those individuals who have a Need to Know. A U.S. PSC is not required to access «OGRANIČENO (RESTRICTED)» information. However, for individuals requiring access to «OGRANIČENO (RESTRICTED)» information who do not have a preexisting PSC, a security briefing concerning the handling of «OGRANIČENO (RESTRICTED)» information shall be provided by the individual releasing the information.

SPORAZUM
IZMEĐU VLADE REPUBLIKE HRVATSKE I VLADE SJEDINJENIH AMERIČKIH DRŽAVA O SIGURNOSNIM MJERAMA ZA ZAŠTITU KLASIFICIRANIH PODATAKA

Vlada Republike Hrvatske (»Hrvatska«) i Vlada Sjedinjenih Američkih Država (»Sjedinjene Države«), pojedinačno »stranka«, a zajedno »stranke«;

s obzirom na to da stranke surađuju po pitanjima koja uključuju, ali nisu ograničena na vanjske poslove, obranu, sigurnost, provedbu zakona, znanost, industriju i tehnologiju; te

imajući zajednički interes za zaštitu klasificiranih podataka koji se razmjenjuju u povjerenju između stranaka;

sporazumjele su se kako slijedi:

Članak 1.
DEFINICIJE

Za potrebe ovog Sporazuma:

1. *Klasificirani podaci:* podaci koje jedna stranka ustupa drugoj stranci, a koje je stranka pošiljateljica odredila kao klasificirane za potrebe nacionalne sigurnosti i zato zahtijevaju zaštitu od neovlaštenog otkrivanja. Podaci mogu biti u usmenom, vizualnom, elektroničkom ili dokumentarnom obliku, ili u obliku materijala, uključujući opremu ili tehnologiju.

2. *Klasificirani ugovor:* ugovor koji zahtijeva, ili će zahtijevati, pristup klasificiranim podacima ili stvaranje klasificiranih podataka od strane ugovaratelja ili od strane njegovih zaposlenika u provedbi ugovora.

3. *Ugovaratelj:* fizička ili pravna osoba koja ima pravnu sposobnost sklapanja ugovora, koja je stranka klasificiranog ugovora.

4. Uvjerenje *o sigurnosnoj provjeri pravne osobe:* uvjerenje koje izdaje nacionalno sigurnosno tijelo stranke, kako je određeno u članku 4., za državno tijelo ili pravnu osobu ugovaratelja pod nadležnošću stranke, u kojem se navodi da je državnom tijelu ili pravnoj osobi izdano uvjerenje o sigurnosnoj provjeri naznačenog stupnja te da primjenjuje i odgovarajuću zaštitu naznačenog stupnja za zaštitu klasificiranih podataka. Takvo uvjerenje znači da klasificirane podatke stupnja tajnosti POVJERLJIVO / CONFIDENTIAL ili višeg štiti ugovaratelj za kojeg se uvjerenje o sigurnosnoj provjeri pravne osobe daje u skladu s odredbama ovog Sporazuma za čije pridržavanje i nadzor je nadležno mjerodavno nacionalno sigurnosno tijelo. Uvjerenje o sigurnosnoj provjeri pravne osobe ugovaratelju nije potrebno za provedbu ugovora koji zahtijevaju samo primanje ili stvaranje klasificiranih podataka stupnja OGRANIČENO (RESTRICTED).

5. *Uvjerenje o sigurnosnoj provjeri osobe:*

a. Potvrda nacionalnog sigurnosnog tijela stranke, kako je određeno u članku 4., da osoba koja je zaposlena u vladinoj službi te stranke, ili ugovaratelj pod nadležnošću te stranke, ima ovlaštenje za pristup klasificiranim podacima naznačenog stupnja tajnosti.

b. Potvrda nacionalnog sigurnosnog tijela stranke, kako je određeno u članku 4., da osoba koja je državljanin jedne stranke, ali bi ga trebala zaposliti druga stranka ili jedan od ugovaratelja druge stranke, ima ovlaštenje za pristup klasificiranim podacima naznačenog stupnja tajnosti.

6. *Nužnost pristupa podacima za obavljanje poslova iz djelokruga:* potvrda od strane ovlaštenog imatelja klasificiranih podataka da potencijalni primatelj klasificiranih podataka ima potrebu pristupa određenim klasificiranim podacima kako bi obavljao zakoniti i ovlašten posao državne uprave ili u njemu pomagao.

Članak 2.

OGRANIČENJA U POGLEDU PODRUČJA PRIMJENE SPORAZUMA

Ovaj Sporazum ne primjenjuje se na klasificirane podatke unutar područja primjene odredaba nekog drugog ugovora ili dogovora između stranaka ili njihovih službi koji se odnose na zaštitu određenog elementa ili kategorije klasificiranih podataka koji se razmjenjuju između stranaka ili njihovih službi, osim kada taj drugi ugovor ili dogovor izričito navodi odredbe ovog Sporazuma primjenjivima. Ovaj Sporazum također se ne primjenjuje na razmjenu ograničenih podataka, kako je definirano u Zakonu o atomskoj energiji Sjedinjenih Država iz 1954., s izmjenama i dopunama, ni na nekada ograničene podatke, što su podaci koji su uklonjeni iz kategorije ograničenih podataka u skladu sa Zakonom o atomskoj energiji, ali ih Sjedinjene Države još uvijek smatraju obrambenim podacima.

Članak 3.

OBVEZA ZAŠTITE KLASIFICIRANIH PODATAKA

1. Svaka stranka štiti klasificirane podatke druge stranke u skladu s ovdje utvrđenim uvjetima.

2. Stranka primateljica štiti klasificirane podatke na način koji je najmanje jednak zaštiti koju klasificiranim podacima pruža stranka pošiljateljica.

3. Svaka stranka žurno obavješćuje drugu stranku o bilo kojim promjenama svojih zakona i propisa koji bi utjecali na zaštitu klasificiranih podataka prema ovom Sporazumu. Takve promjene u domaćim zakonima ne utječu na obveze iz ovog Sporazuma. U takvim slučajevima stranke se konzultiraju u pogledu mogućih izmjena i dopuna ovog Sporazuma ili drugih mjera koje bi mogle biti odgovarajuće za održavanje zaštite klasificiranih podataka koji se razmjenjuju prema ovom Sporazumu.

Članak 4.

NACIONALNA SIGURNOSNA TIJELA

1. Stranke obavješćuju jedna drugu o nacionalnim sigurnosnim tijelima odgovornim za provedbu ovog Sporazuma i bilo kojim naknadnim promjenama tih tijela.

2. Za potrebe ovog Sporazuma, nacionalna sigurnosna tijela su:

a. za Hrvatsku: predstojnik/predstojnica, Ured Vijeća za nacionalnu sigurnost (UVNS)

b. za Sjedinjene Države: pomoćnik/pomoćnica ravnatelja/ravnateljice, Ravnateljstvo za međunarodne odnose, Uprava za sigurnost obrambene tehnologije, Ured državnog podtajnika Ministarstva obrane za politiku, Ministarstvo obrane Sjedinjenih Država.

3. Stranke mogu sklapati dopunske provedbene dogovore ovog Sporazuma u kojima se mogu tražiti dodatne tehničke sigurnosne mjere za zaštitu klasificiranih podataka koji se prenose stranci primateljici kroz inozemnu vojnu prodaju ili programe suradnje za zajedničku proizvodnju ili zajedničko razvijanje obrambenih proizvoda ili usluga. Takvi provedbeni dogovori mogu uključivati posebne sigurnosne sporazume ili sporazume poslovne sigurnosti.

Članak 5.

ODREĐIVANJE KLASIFICIRANIH PODATAKA

1. Stranka pošiljateljica određuje i, kada je to moguće, označava pečatom ili oznakom klasificirane podatke jednim od sljedećih nacionalnih stupnjeva tajnosti. U svrhu osiguravanja jednakog postupanja, stranke su suglasne da su sljedeći stupnjevi tajnosti istoznačni:

HRVATSKA	SJEDINJENE DRŽAVE
VRLO TAJNO	TOP SECRET
TAJNO	SECRET
POVJERLJIVO	CONFIDENTIAL
OGRANIČENO (RESTRICTED)	Nema istoznačnice (vidi stavak 2.)

2. U tijeku provedbe ovog Sporazuma, ukoliko Hrvatska ustupa klasificirane podatke određene kao OGRANIČENO (RESTRICTED), Sjedinjene Države s njima postupaju u skladu s Dodatkom ovog Sporazuma.

3. Klasificirani podaci se određuju i, kada je to moguće, označavaju pečatom ili oznakom, s imenom stranke pošiljateljice.

Članak 6.

ODGOVORNOST ZA KLASIFICIRANE PODATKE

Stranka primateljica odgovorna je za zaštitu svih klasificiranih podataka stranke pošiljateljice na način koji je najmanje jednak zaštiti koju klasificiranim podacima pruža stranka pošiljateljica dok su klasificirani podaci pod njezinim nadzorom. Tijekom tranzita, stranka pošiljateljica odgovorna je za sve klasificirane podatke dok se nadzor nad klasificiranim podacima formalno ne prenese na stranku primateljicu.

Članak 7.

ZAŠTITA KLASIFICIRANIH PODATAKA

1. Nijedna osoba nema pravo pristupa klasificiranim podacima samo na temelju položaja, funkcije, imenovanja ili uvjerenja o sigurnosnoj provjeri osobe. Pristup takvim podacima odobrava se samo osobama kod kojih postoji nužnost pristupa podacima za obavljanje poslova iz djelokruga i kojima je izdano potrebno uvjerenje o sigurnosnoj provjeri osobe u skladu s propisanim standardima stranke primateljice.

2. Osim na način drugačije određen u ovom Sporazumu, stranka primateljica ne ustupa klasificirane podatke stranke pošiljateljice bilo kojoj trećoj strani, uključujući vladu, osobu, tvrtku, instituciju, organizaciju ili drugi subjekt bilo koje treće strane, bez prethodnog pisanog pristanka stranke pošiljateljice.

3. Stranka primateljica ne koristi ni ne dopušta korištenje klasificiranih podataka stranke pošiljateljice u bilo koju drugu svrhu osim one za koju su ustupljeni bez prethodnog pisanog pristanka stranke pošiljateljice.

4. Stranka primateljica poštuje bilo koja privatna prava koja su povezana s klasificiranim podacima stranke pošiljateljice, uključujući prava u pogledu patenata, autorskih prava ili poslovnih tajni te ne ustupa, ne koristi, ne razmjenjuje i ne otkriva takve klasificirane podatke na način koji nije usklađen s tim pravima bez prethodnog pisanog ovlaštenja vlasnika tih prava.

5. Stranka primateljica osigurava da svako državno tijelo ili pravna osoba ili ustanova koja postupa s klasificiranim podacima obuhvaćenim ovim Sporazumom vodi popis osoba u državnom tijelu ili pravnoj osobi ili ustanovi koje su ovlaštene za pristup takvim podacima.

6. Svaka stranka razrađuje postupke vođenja evidencije i nadzora za upravljanje distribucijom klasificiranih podataka i pristupom klasificiranim podacima.

7. Svaka stranka pridržava se svih ograničenja u pogledu korištenja, otkrivanja, ustupanja i pristupa klasificiranim podacima koje može naznačiti stranka pošiljateljica kada ustupa takve klasificirane podatke. Ako se stranka ne može pridržavati naznačenih ograničenja, ta se stranka odmah konzultira s drugom strankom i poduzima sve zakonite mjere kako bi spriječila ili minimalizirala bilo koje takvo korištenje, otkrivanje, ustupanje ili pristup.

Članak 8.

UVJERENJA O SIGURNOSNOJ PROVJERI OSOBE

1. Stranke osiguravaju da sve osobe koje u obavljanju svojih službenih obveza imaju potrebu pristupa, ili čije dužnosti ili funkcije mogu pružiti pristup klasificiranim podacima na temelju ovog Sporazuma, dobiju odgovarajuće uvjerenje o sigurnosnoj provjeri osobe prije nego što im se odobri pristup takvim podacima.

2. Stranka koja izdaje uvjerenje o sigurnosnoj provjeri osobe provodi odgovarajuću provjeru, dovoljno detaljnu da bi se utvrdilo je li osoba pogodna za pristup klasificiranim podacima. Odluka o izdavanju uvjerenja o sigurnosnoj provjeri osobe donijet će se u skladu s nacionalnim zakonima i propisima stranke koja ga izdaje.

3. Prije nego što službenik ili predstavnik jedne stranke ustupi klasificirane podatke službeniku ili predstavniku druge stranke, stranka primateljica daje stranci pošiljateljici potvrdu da službenik ili predstavnik ima potrebni stupanj uvjerenja o sigurnosnoj provjeri osobe i nužnost pristupa podacima za obavljanje poslova iz djelokruga te da će stranka primateljica štititi klasificirane podatke u skladu s ovim Sporazumom.

Članak 9.

USTUPANJE KLASIFICIRANIH PODATAKA UGOVARATELJIMA

1. Stranka primateljica može ustupiti klasificirane podatke koje je primila ugovaratelju ili potencijalnom ugovaratelju čije dužnosti zahtijevaju pristup takvim podacima uz prethodni pisani pristanak stranke pošiljateljice. Prije ustupanja bilo kojih klasificiranih podataka ugovaratelju ili potencijalnom ugovaratelju, stranka primateljica:

a. potvrđuje da takav ugovaratelj ili potencijalni ugovaratelj i ugovarateljev objekt imaju sposobnost za zaštitu podataka u skladu s odredbama ovog Sporazuma;

b. potvrđuje da je takvom ugovaratelju ili potencijalnom ugovaratelju i ugovarateljevom objektu izdano odgovarajuće uvjerenje o sigurnosnoj provjeri osobe i uvjerenje o sigurnosnoj provjeri pravne osobe, prema potrebi;

c. potvrđuje da ugovaratelj ili potencijalni ugovaratelj ima uspostavljene postupke kako bi se osiguralo da su sve osobe koje imaju pristup podacima informirane o svojim obvezama u pogledu zaštite podataka u skladu s primjenjivim zakonima i propisima;

d. provodi povremeni sigurnosni nadzor nad državnim tijelima ili pravnim osobama za koja je izdano uvjerenje o sigurnosnoj provjeri kako bi se osiguralo da se podaci štite na način na koji to zahtijeva ovaj Sporazum; te

e. potvrđuje da ugovaratelj ili potencijalni ugovaratelj ima uspostavljene postupke kako bi se osiguralo da je pristup podacima ograničen na one osobe kojima je to nužno za obavljanje poslova iz djelokruga.

Članak 10.

KLASIFICIRANI UGOVORI

1. Kada stranka predloži provedbu, ili ovlasti ugovaratelja u svojoj državi da provodi, klasificirani ugovor stupnja POVJERLJIVO / CONFIDENTIAL ili višeg, ugovaratelju u državi druge stranke, stranka koja treba dodijeliti, ili ovlastiti ugovaratelja da dodijeli takav klasificirani ugovor, traži potvrdu od nacionalnog sigurnosnog tijela druge stranke da je izdano uvjerenje o sigurnosnoj provjeri pravne osobe. Nacionalno sigurnosno tijelo stranke od koje se to traži nadzire i poduzima sve potrebne radnje kako bi se osiguralo da će sigurnosno postupanje ugovaratelja biti u skladu s primjenjivim zakonima i propisima.

2. Nacionalno sigurnosno tijelo stranke koja pregovara o klasificiranom ugovoru koji bi se trebao provoditi u državi druge stranke ugrađuje u klasificirani ugovor, zahtjev za ponudu ili dokument o podugovoru odgovarajuće sigurnosne klauzule i druge mjerodavne odredbe, uključujući troškove za sigurnost. Ovo uključuje odredbe kojima se od svakog ugovaratelja zahtijeva da u svojim dokumentima o podugovoru ugradi odgovarajuće sigurnosne klauzule.

Članak 11.

ODGOVORNOST ZA OBJEKTE

Svaka stranka je odgovorna za sigurnost svih državnih i privatnih objekata i ustanova u kojima pohranjuje klasificirane podatke druge stranke te osigurava da u takvim objektima ili ustanovama postoje kvalificirane osobe kojima je izdano odgovarajuće uvjerenje o sigurnosnoj provjeri, koje su zadužene i ovlaštene za nadzor i zaštitu takvih podataka.

Članak 12.

POHRANA KLASIFICIRANIH PODATAKA

Klasificirani podaci koji se razmjenjuju između stranaka pohranjuju se na način koji osigurava pristup samo onim osobama koje su ovlaštene za pristup.

Članak 13.

PRIJENOS

1. Klasificirani podaci prenose se između stranaka putem ovlaštenih državnih tijela ili na drugi način koji je unaprijed uzajamno pisano odobren.

2. Minimalni zahtjevi za sigurnost klasificiranih podataka tijekom prijenosa su kako slijedi:

a. Dokumenti ili drugi mediji:

(1) Dokumenti ili drugi mediji koji sadrže klasificirane podatke prenose se u dvostrukim, zapečaćenim omotnicama. Na unutarnjoj omotnici naveden je samo stupanj tajnosti dokumenata ili drugih medija i organizacijska adresa primatelja kojem je namijenjena. Na vanjskoj omotnici navedena je organizacijska adresa primatelja kojem je namijenjena, organizacijska adresa pošiljatelja i kontrolni broj dokumenta, ako postoji.

(2) Na vanjskoj omotnici ne navodi se stupanj tajnosti sadržanih dokumenata ili drugih medija. Dvostruka zapečaćena omotnica prenosi se u skladu s propisanim postupcima stranaka.

(3) Primatelj izrađuje potvrde primitka za pakete koji sadrže dokumente ili druge medije koji sadrže klasificirane podatke, koji se prenose između stranaka, a takve potvrde primitka potpisuje krajnji primatelj i one se vraćaju pošiljatelju.

b. Materijal:

(1) Materijal, uključujući opremu, koji sadrži klasificirane podatke, prevozi se u zapečaćenim, prekrivenim vozilima, ili se na drugi način sigurno pakira ili štiti kako bi se spriječilo utvrđivanje njegovog oblika, veličine ili sadržaja te se drži pod neprekidnim nadzorom kako bi se spriječio pristup neovlaštenih osoba.

(2) Materijal, uključujući opremu, koji sadrži klasificirane podatke, a koji se mora privremeno pohraniti dok čeka otpremu, smješta se u zaštićena spremišta. Takvi prostori štite se opremom za otkrivanje neovlaštenog ulaska ili ih štite čuvari koji posjeduju potrebna uvjerenja o sigurnosnoj provjeri osobe, koji te prostore neprekidno nadziru. Pristup zaštićenim spremištima imaju samo ovlašteni zaposlenici koji posjeduju potrebna uvjerenja o sigurnosnoj provjeri osobe.

(3) Svaki puta kada tijekom tranzita netko drugi preuzima materijal koji sadrži klasificirane podatke, uključujući opremu, treba ishoditi potvrde primitka, a potvrdu primitka za takav materijal potpisuje krajnji primatelj i one se vraćaju pošiljatelju.

c. Elektronički prijenos:

(1) Klasificirani podaci stupnja POVJERLJIVO / CONFIDENTIAL ili višeg koje treba prenijeti elektroničkim putem, prenose se putem zaštićenih sredstava koja su odobrila nacionalna sigurnosna tijela svake stranke.

Članak 14.

POSJETI DRŽAVNIM TIJELIMA ILI PRAVNIM OSOBAMA I USTANOVAMA STRANAKA

1. Posjeti predstavnika jedne stranke državnim tijelima ili pravnim osobama i ustanovama druge stranke koji zahtijevaju pristup klasificiranim podacima, ili posjeti kod kojih je za odobrenje pristupa potrebno uvjerenje o sigurnosnoj provjeri osobe, ograničeni su na one koji su potrebni u službene svrhe. Ovlaštenje se daje samo predstavnicima koji posjeduju važeće uvjerenje o sigurnosnoj provjeri osobe.

2. Ovlaštenje za posjet takvim državnim tijelima ili pravnim osobama i ustanovama daje samo stranka na čijem se državnom području nalazi državno tijelo ili pravna osoba ili ustanova koju se posjećuje. Stranka koju se posjećuje, ili njezini određeni službenici, zaduženi su za obavješćivanje državnog tijela ili pravne osobe ili ustanove o predloženom posjetu te opsegu i najvišem stupnju tajnosti klasificiranih podataka koji se mogu dati posjetitelju.

3. Zahtjeve za posjet predstavnika stranaka predaje Veleposlanstvo Republike Hrvatske u Washingtonu, D.C., u slučaju posjetitelja iz Hrvatske te Veleposlanstvo Sjedinjenih Država u Zagrebu u slučaju posjetitelja iz Sjedinjenih Država.

Članak 15.

SIGURNOSNI POSJETI

Provedba sigurnosnih zahtjeva utvrđenih u ovom Sporazumu može se provjeriti uzajamnim posjetima sigurnosnog osoblja stranaka. Sigurnosnim predstavnicima svake stranke, nakon prethodne konzultacije, odobrava se posjet drugoj stranci kako bi se razgovaralo o provedbenim postupcima druge stranke i kako bi se ti postupci pratili u interesu postizanja prihvatljive usporedivosti sigurnosnih sustava. Stranka domaćin sigurnosnim predstavnicima koji su u posjetu pomaže pri utvrđivanju štite li se klasificirani podaci primljeni od druge stranke na odgovarajući način.

Članak 16.

SIGURNOSNI STANDARDI

Na zahtjev, svaka stranka dostavlja drugoj stranci podatke o svojim sigurnosnim standardima, praksama i postupcima za zaštitu klasificiranih podataka.

Članak 17.

UMNOŽAVANJE KLASIFICIRANIH PODATAKA

Kada se klasificirani podaci umnožavaju, sve izvorne sigurnosne oznake koje se na njima nalaze također se umnožavaju, označavaju pečatom ili oznakom na svakom umnoženom primjerku takvih podataka. Takvi umnoženi primjerci podliježu istom nadzoru kao izvorni podaci. Broj umnoženih primjeraka ograničen je na minimalni broj potreban za službene svrhe.

Članak 18.

UNIŠTAVANJE KLASIFICIRANIH PODATAKA

1. Dokumenti i drugi mediji koji sadrže klasificirane podatke uništavaju se spaljivanjem, rezanjem, mljevenjem ili na drugi način koji onemogućava obnavljanje klasificiranih podataka koje sadrže.

2. Materijal, uključujući opremu, koji sadrži klasificirane podatke uništava se tako da ga se učini neprepoznatljivim kako bi se spriječilo potpuno ili djelomično obnavljanje klasificiranih podataka.

Članak 19.

SNIŽAVANJE STUPNJA TAJNOSTI I DEKLASIFIKACIJA

1. Stranke su suglasne da bi klasificiranim podacima trebalo sniziti stupanj tajnosti čim podaci prestanu zahtijevati taj viši stupanj zaštite ili bi ih se trebalo deklasificirati čim podacima više ne bude potrebna zaštita od neovlaštenog otkrivanja.

2. Stranka pošiljateljica ima puno pravo slobodne ocjene u pogledu snižavanja stupnja tajnosti ili deklasifikacije svojih klasificiranih podataka. Stranka primateljica ne snižava stupanj tajnosti i ne deklasificira klasificirane podatke primljene od stranke pošiljateljice, bez obzira na bilo koje očite upute o deklasifikaciji na dokumentu, bez prethodnog pisanog pristanka stranke pošiljateljice.

Članak 20.

GUBITAK ILI POVREDA SIGURNOSTI

Stranka primateljica obavješćuje stranku pošiljateljicu odmah po otkrivanju o svim gubicima ili povredama sigurnosti, kao i o mogućim gubicima ili povredama sigurnosti, klasificiranih podataka stranke pošiljateljice. U slučaju stvarnog ili mogućeg gubitka ili povrede sigurnosti takvih podataka, stranka primateljica odmah pokreće istragu kako bi se utvrdile okolnosti stvarnog ili mogućeg gubitka ili povrede sigurnosti. Stranci pošiljateljici dostavljaju se rezultati istrage i podaci o mjerama poduzetim kako bi se spriječilo ponavljanje.

Članak 21.

SPOROVI

Neslaganja između stranaka do kojih dođe na temelju ovog Sporazuma ili u vezi s ovim Sporazumom rješavaju se isključivo konzultacijama između stranaka i ne podnose se na rješavanje nacionalnom sudu, međunarodnom sudu ni bilo kojoj drugoj osobi ili subjektu.

Članak 22.

TROŠKOVI

Svaka stranka dužna je snositi svoje vlastite troškove koji nastanu u provedbi ovog Sporazuma. Sve obveze stranaka na temelju ovog Sporazuma podliježu raspoloživosti sredstava.

Članak 23.

ZAVRŠNE ODREDBE

1. Ovaj Sporazum stupa na snagu datumom zadnjeg potpisa stranaka.

2. Svaka stranka može okončati ovaj Sporazum obavješćujući drugu stranku pisano, diplomatskim putem, o svojoj namjeri okončanja Sporazuma devedeset dana unaprijed.

3. Bez obzira na prestanak ovog Sporazuma, svi klasificirani podaci koji su razmijenjeni ili na drugi način ustupljeni na temelju ovog Sporazuma nastavljaju se štititi u skladu s ovdje utvrđenim odredbama.

U POTVRDU TOGA, niže potpisani, za to propisno ovlašteni od strane svojih odnosnih Vlada, potpisali su ovaj Sporazum.

Sastavljeno u dva primjerka u Zagrebu dana 5. siječnja 2021., na engleskom jeziku.

ZA VLADU REPUBLIKE HRVATSKE	ZA VLADU SJEDINJENIH AMERIČKIH DRŽAVA
Maja Čavlović, v. r.	**William Robert Kohorst,** v. r.
Predstojnica Ureda Vijeća za nacionalnu sigurnost u Republici Hrvatskoj	izvanredni i opunomoćeni veleposlanik Sjedinjenih Američkih Država

DODATAK

POSTUPCI ZA ZAŠTITU KLASIFICIRANIH PODATAKA REPUBLIKE HRVATSKE STUPNJA TAJNOSTI OGRANIČENO (RESTRICTED) KOJI SE USTUPAJU SJEDINJENIM DRŽAVAMA

1. Po primitku, hrvatske klasificirane podatke ustupljene Sjedinjenim Državama i označene stupnjem tajnosti »OGRANIČENO (RESTRICTED)«, Sjedinjene Države štite u skladu sa sljedećim postupcima.

2. Podaci označeni stupnjem tajnosti »OGRANIČENO (RESTRICTED)« pohranjuju se u zaključane spremnike ili zatvorene prostore koji sprječavaju pristup neovlaštenog osoblja.

3. Klasificirani podaci stupnja tajnosti »OGRANIČENO (RESTRICTED)« ne ustupaju se neovlaštenim osobama ni subjektima bez prethodnog pisanog odobrenja stvaratelja ili nacionalnog sigurnosnog tijela Republike Hrvatske, osim kada to zahtijevaju američki zakoni, uključujući Zakon o slobodi informiranja/pristupa informacijama.

4. Klasificirani podaci stupnja tajnosti »OGRANIČENO (RESTRICTED)«, ako je to primjenjivo, pohranjuju se, obrađuju ili prenose elektroničkim putem koristeći sustave akreditirane od strane vlade ili ugovaratelja. Konkretno, prije korištenja bilo kojeg sustava za pohranu, obradu ili prijenos klasificiranih podataka stupnja »OGRANIČENO (RESTRICTED)«, on mora dobiti sigurnosno odobrenje poznato kao akreditacija. Akreditacija je formalna izjava odgovarajućeg akreditacijskog tijela kojom se potvrđuje da korištenje sustava zadovoljava odgovarajuće sigurnosne zahtjeve i ne predstavlja neprihvatljivi rizik. Sigurnosni standardni operativni postupci su tehnički postupci za provedbu sigurnosnih politika i zahtjeva jedinstvenih za pojedino državno tijelo ili pravnu osobu za zaštitu automatiziranih informacijskih sustava u kojima se obrađuju klasificirani podaci. Za samostojeće automatizirane informacijske sustave poput stolnih i prijenosnih računala koja se koriste u ustanovama Vlade Sjedinjenih Država, dokument registracije sustava, zajedno sa Sigurnosnim standardnim postupcima, ima ulogu potrebne akreditacije. Za ugovaratelje, smjernice za korištenje komunikacijskih i informacijskih sustava ugrađuju se u klauzulu ugovora o zahtjevima za ograničene uvjete.

5. Klasificirani podaci stupnja »OGRANIČENO (RESTRICTED)« prenose se poštom prve klase unutar Sjedinjenih Država u jednoj zapečaćenoj omotnici. Prijenos izvan Sjedinjenih Država vrši se u dvostrukim, zapečaćenim omotnicama, pri čemu je unutarnja omotnica označena s »Republika Hrvatska OGRANIČENO (RESTRICTED)«. Prijenos izvan Sjedinjenih Država vrši se na način koji je moguće pratiti, poput komercijalne dostavne službe ili na drugi način koji stranke pisano dogovore.

6. Dokumenti Sjedinjenih Država koji sadrže hrvatske klasificirane podatke stupnja tajnosti »OGRANIČENO (RESTRICTED)« na naslovnoj stranici i prvoj stranici nose oznaku »Republika Hrvatska OGRANIČENO (RESTRICTED)«. Dio dokumenata koji sadrži hrvatske klasificirane podatke stupnja tajnosti »OGRANIČENO« također se označava oznakom »Republika Hrvatska OGRANIČENO (RESTRICTED)«.

7. Klasificirani podaci stupnja tajnosti »OGRANIČENO (RESTRICTED)« mogu se prenositi ili im se može pristupiti elektroničkim putem preko javne mreže poput interneta koristeći vladine ili komercijalne uređaje za kriptiranje koje su stranke uzajamno prihvatile. Telefonski razgovori, videokonferencije ili prijenos faksimila koji sadrže klasificirane podatke stupnja tajnosti »OGRANIČENO (RESTRICTED)« mogu se obavljati ako sustav za kriptiranje nije dostupan i uz uvjet odobrenja od strane nacionalnog sigurnosnog tijela stranke pošiljateljice.

8. Ugovaratelj ne mora posjedovati uvjerenje o sigurnosnoj provjeri pravne osobe i uvjerenje o sigurnosnoj provjeri osobe za provedbu ugovora koji zahtijevaju samo primanje ili stvaranje klasificiranih podataka stupnja tajnosti »OGRANIČENO (RESTRICTED)«.

9. Pristup takvim klasificiranim podacima stupnja tajnosti »OGRANIČENO (RESTRICTED)« odobrava se samo onim osobama kojima je to nužno za obavljanje poslova iz djelokruga. Uvjerenje o sigurnosnoj provjeri osobe Sjedinjenih Država nije potrebno za pristup podacima stupnja tajnosti »OGRANIČENO (RESTRICTED)«. Međutim, za osobe koje imaju potrebu pristupa podacima stupnja tajnosti »OGRANIČENO (RESTRICTED)«, a kojima prethodno nije izdano uvjerenje o sigurnosnoj provjeri osobe, potrebno je provesti sigurnosno informiranje u vezi s postupanjem s podacima stupnja tajnosti »OGRANIČENO (RESTRICTED)« koje provodi osoba koja ustupa podatke.

III.

Provedba Sporazuma iz točke I. ove Odluke u djelokrugu je tijela državne uprave nadležnog za poslove informacijske sigurnosti.

IV.

Ova Odluka stupa na snagu osmoga dana od dana objave u »Narodnim novinama«.

Klasa: 022-03/20-11/57
Urbroj: 50301-29/23-21-10
Zagreb, 11. veljače 2021.

Predsjednik
mr. sc. Andrej Plenković, v. r.