No. 55796*

Croatia
and
Austria

Agreement between the Government of the Republic of Croatia and the Austrian Federal Government on the exchange and mutual protection of classified information. Zagreb, 24 July 2018

Entry into force: *1 April 2019, in accordance with article 16*

Authentic texts: *Croatian, English and German*

Registration with the Secretariat of the United Nations: *Croatia, 9 April 2019*

**No UNTS volume number has yet been determined for this record. The Text(s) reproduced below, if attached, are the authentic texts of the agreement /action attachment as submitted for registration and publication to the Secretariat. For ease of reference they were sequentially paginated. Translations, if attached, are not final and are provided for information only.*

Croatie
et
Autriche

Accord entre le Gouvernement de la République de Croatie et le Gouvernement fédéral autrichien sur l'échange et la protection mutuelle des informations classifiées. Zagreb, 24 juillet 2018

Entrée en vigueur : *1er avril 2019, conformément à l'article 16*

Textes authentiques : *croate, anglais et allemand*

Enregistrement auprès du Secrétariat de l'Organisation des Nations Unies : *Croatie, 9 avril 2019*

**Aucun numéro de volume n'a encore été attribué à ce dossier. Les textes disponibles qui sont reproduits ci-dessous sont les textes originaux de l'accord ou de l'action tels que soumis pour enregistrement. Par souci de clarté, leurs pages ont été numérotées. Les traductions qui accompagnent ces textes ne sont pas définitives et sont fournies uniquement à titre d'information.*

[CROATIAN TEXT – TEXTE CROATE]

UGOVOR
IZMEĐU
VLADE REPUBLIKE HRVATSKE
I
SAVEZNE VLADE REPUBLIKE AUSTRIJE
O RAZMJENI I UZAJAMNOJ ZAŠTITI KLASIFICIRANIH PODATAKA

Vlada Republike Hrvatske i Savezna vlada Republike Austrije (u daljnjem tekstu „stranke"),

u namjeri osiguravanja sigurnosti svih klasificiranih podataka koji su kao takvi određeni i označeni u skladu s nacionalnim zakonima i propisima bilo koje stranke i prenose se drugoj stranci,

želeći odrediti pravila uzajamne zaštite klasificiranih podataka koji se prenose ili nastaju u tijeku suradnje između stranaka,

sporazumjele su se kako slijedi:

ČLANAK 1.
DEFINICIJE

Za potrebe ovog Ugovora:

a) „klasificirani podaci" označava sve podatke, neovisno o njihovom obliku, koji su kao takvi određeni i označeni u skladu s nacionalnim zakonima i propisima bilo koje stranke, kako bi se osigurala zaštita od neovlaštenog otkrivanja, zlouporabe ili gubitka;

b) „stupanj tajnosti" označava kategoriju koja, u skladu s nacionalnim zakonima i propisima, predstavlja stupanj ograničenja pristupa klasificiranim podacima i minimalni stupanj njihove zaštite od strane stranaka;

c) „nadležno tijelo" označava nacionalno sigurnosno tijelo i svako drugo nadležno tijelo i službu notificiranu u skladu s člankom 13. ovog Ugovora;

d) „uvjerenje o sigurnosnoj provjeri osobe" označava potvrdu nadležnog tijela da fizička osoba ispunjava uvjete za pristup klasificiranim podacima u skladu s nacionalnim zakonima i propisima;

e) „uvjerenje o sigurnosnoj provjeri pravne osobe" označava potvrdu nadležnog tijela da pravna osoba ima fizičku i organizacijsku sposobnost ispuniti uvjete za pristup i rukovanje klasificiranim podacima u skladu s nacionalnim zakonima i propisima;

f) „klasificirani ugovor" označava ugovor ili podugovor između pravne ili fizičke osobe iz države jedne stranke i pravne ili fizičke osobe iz države druge stranke, čija provedba zahtijeva pristup klasificiranim podacima ili njihov nastanak;

g) „pošiljatelj" označava stranku pošiljateljicu, kao i bilo koju pravnu ili fizičku osobu u njezinoj nadležnosti, koja ustupa klasificirane podatke;

h) „primatelj" označava stranku primateljicu, kao i bilo koju pravnu ili fizičku osobu u njezinoj nadležnosti, koja prima klasificirane podatke;

i) „treća strana" označava pravnu ili fizičku osobu koja nije pošiljatelj ni primatelj klasificiranih podataka koji se prenose u skladu s ovim Ugovorom, vladu koja nije stranka ovog Ugovora ili međunarodnu organizaciju;

j) „povreda sigurnosti" označava svaki oblik otkrivanja, zlouporabe, neovlaštene izmjene, oštećivanja ili uništavanja klasificiranih podataka, kao i bilo koje drugo činjenje ili nečinjenje koje dovodi do gubitka povjerljivosti, cjelovitosti ili dostupnosti klasificiranih podataka.

ČLANAK 2.
STUPNJEVI TAJNOSTI

Stranke su suglasne po pitanju istoznačnosti sljedećih stupnjeva tajnosti:

Republika Hrvatska:	Republika Austrija:	Istoznačnica na engleskom jeziku:
VRLO TAJNO	STRENG GEHEIM	TOP SECRET
TAJNO	GEHEIM	SECRET
POVJERLJIVO	VERTRAULICH	CONFIDENTIAL
OGRANIČENO	EINGESCHRÄNKT	RESTRICTED

ČLANAK 3.
OZNAČAVANJE

(1) Klasificirane podatke koji se trebaju prenijeti označava pošiljatelj, u skladu s odgovarajućim stupnjem tajnosti. Primatelj označava primljene klasificirane podatke stupnjem tajnosti koji je istoznačan oznaci pošiljatelja.

(2) Klasificirani podaci koji nastaju, umnožavaju se ili prevode u tijeku suradnje u skladu s ovim Ugovorom također se označavaju.

(3) Stupanj tajnosti mijenja se ili uklanja samo uz pisanu suglasnost pošiljatelja. Pošiljatelj bez odgode obavješćuje primatelja o svakoj promjeni ili uklanjanju stupnja tajnosti prenesenih klasificiranih podataka.

ČLANAK 4.
NAČELA ZAŠTITE KLASIFICIRANIH PODATAKA

(1) Stranke poduzimaju sve odgovarajuće mjere kako bi osigurale zaštitu prenesenih klasificiranih podataka i omogućile potrebni nadzor te zaštite.

(2) Stranke prenesenim klasificiranim podacima pružaju stupanj zaštite koji je najmanje jednak onome koji pružaju vlastitim klasificiranim podacima istog stupnja tajnosti.

(3) Preneseni klasificirani podaci koriste se samo u svrhu za koju su ustupljeni.

(4) Preneseni klasificirani podaci dostupni su samo osobama koje su, u skladu s nacionalnim zakonima i propisima, ovlaštene za pristup klasificiranim podacima istog stupnja tajnosti i kojima je taj pristup potreban za obavljanje njihovih dužnosti.

(5) Stranka klasificirane podatke ne čini dostupnima trećoj strani bez prethodne pisane suglasnosti nadležnog tijela pošiljatelja.

(6) Klasificirani podaci nastali u tijeku suradnje u skladu s ovim Ugovorom uživaju jednaku zaštitu kao klasificirani podaci preneseni u tijeku suradnje u skladu s ovim Ugovorom.

ČLANAK 5.
UVJERENJE O SIGURNOSNOJ PROVJERI OSOBE

(1) U okviru područja primjene ovog Ugovora, svaka stranka priznaje uvjerenja o sigurnosnoj provjeri osobe koja je izdala druga stranka.

(2) Nadležna tijela, na zahtjev i u skladu s nacionalnim zakonima i propisima, pomažu jedno drugom u obavljanju postupaka provjere potrebnih za primjenu ovog Ugovora.

(3) U okviru područja primjene ovog Ugovora, nadležna tijela, bez odgode, obavješćuju jedno drugo o svakoj promjeni u pogledu uvjerenja o sigurnosnoj provjeri osobe, a osobito o uklanjanju ili promjeni stupnja tajnosti.

(4) Na zahtjev nadležnog tijela pošiljatelja, nadležno tijelo primatelja izdaje pisanu potvrdu o tome da je fizička osoba ovlaštena za pristup klasificiranim podacima.

ČLANAK 6.
KLASIFICIRANI UGOVORI

(1) Klasificirani ugovor sadrži odredbe o sigurnosnim uvjetima i o stupnju tajnosti podataka koji se ustupaju. Primjerak odredbi šalje se nadležnom tijelu.

(2) U kontekstu klasificiranih ugovora, svaka stranka priznaje uvjerenja o sigurnosnoj provjeri pravne osobe koja je izdala druga stranka.

(3) U kontekstu pripreme ili sklapanja klasificiranih ugovora, nadležna tijela na zahtjev obavješćuju jedno drugo o tome je li izdano valjano uvjerenje o sigurnosnoj provjeri pravne osobe ili su pokrenuti potrebni postupci, kao i o sigurnosnim uvjetima vezanim za uključene klasificirane podatke.

(4) Nadležna tijela obavješćuju jedno drugo o svim klasificiranim ugovorima koji potpadaju pod ovaj Ugovor.

(5) Nadležna tijela bez odgode obavješćuju jedno drugo o svakoj promjeni u pogledu uvjerenja o sigurnosnoj provjeri pravne osobe koja potpadaju pod ovaj članak, a osobito o uklanjanju ili promjeni stupnja tajnosti.

(6) Pošiljatelj dostavlja primatelju i nadležnom tijelu primatelja popis klasificiranih podataka koji se prenose u skladu s klasificiranim ugovorom.

(7) Ugovaratelj može za izvršenje dijela klasificiranog ugovora uposliti podugovaratelja. Podugovaratelji podliježu istim sigurnosnim uvjetima kakvi vrijede za ugovaratelja.

ČLANAK 7.
PRIJENOS

Klasificirani podaci prenose se diplomatskim putem ili bilo kojim drugim putem koji stranke međusobno dogovore. Primitak klasificiranih podataka označenih stupnjem tajnosti POVJERLJIVO / VERTRAULICH / CONFIDENTIAL i višim potvrđuje se pisano. Na zahtjev pošiljatelja, primitak klasificiranih podataka označenih stupnjem tajnosti OGRANIČENO / EINGESCHRÄNKT / RESTRICTED također se potvrđuje pisano.

ČLANAK 8.
UMNOŽAVANJE I PREVOĐENJE

(1) Umnožavanje i prevođenje klasificiranih podataka može ograničiti ili isključiti pošiljatelj. Broj umnoženih primjeraka ograničen je na broj potreban u službene svrhe.

(2) Klasificirani podaci označeni stupnjem tajnosti VRLO TAJNO / STRENG GEHEIM / TOP SECRET ne umnožavaju se i ne prevode bez prethodne pisane suglasnosti pošiljatelja.

(3) Klasificirane podatke prevode samo osobe ovlaštene za pristup klasificiranim podacima odgovarajućeg stupnja tajnosti.

(4) Umnožene primjerke i prijevode štiti se na isti način kao i izvornike. Prijevod nosi odgovarajuću napomenu, na jeziku na koji je preveden, da prijevod sadrži klasificirane podatke pošiljatelja.

ČLANAK 9.
UNIŠTAVANJE

(1) Klasificirani podaci uništavaju se na način koji onemogućuje potpuno ili djelomično obnavljanje. Uništavanje klasificiranih podataka registriranih u skladu s nacionalnim zakonima i propisima se evidentira.

(2) Pošiljatelj može, dodatnim označavanjem ili slanjem naknadne pisane obavijesti primatelju, izričito zabraniti uništavanje klasificiranih podataka. Ako je uništavanje klasificiranih podataka zabranjeno, oni se vraćaju pošiljatelju.

(3) U slučaju krizne situacije u kojoj je nemoguće zaštititi ili vratiti klasificirane podatke prenesene ili nastale u skladu s ovim Ugovorom, klasificirani podaci odmah se uništavaju. Primatelj o tom uništavanju obavješćuje nadležno tijelo pošiljatelja što je prije moguće.

ČLANAK 10.
POSJETI

(1) Posjeti koji zahtijevaju pristup klasificiranim podacima podliježu prethodnom odobrenju nadležnog tijela stranke domaćina. Odobrenje se daje samo osobama koje su, u skladu s nacionalnim zakonima i propisima, ovlaštene za pristup klasificiranim podacima odgovarajućeg stupnja tajnosti.

(2) Zahtjevi za posjete podnose se nadležnom tijelu stranke domaćina najmanje deset radnih dana prije posjeta, a u slučaju žurnosti u kraćem razdoblju. Nadležna tijela obavješćuju jedno drugo o pojedinostima posjeta i osiguravaju zaštitu osobnih podataka.

(3) Zahtjevi za posjete sastavljaju se na engleskom jeziku i u njima se posebno navodi sljedeće:

a) svrha i predloženi datum posjeta;

b) ime i prezime, datum i mjesto rođenja, državljanstvo i broj putovnice ili osobne iskaznice posjetitelja;

c) radno mjesto posjetitelja i naziv tijela, službe ili poduzeća koje predstavlja;

d) valjanost i stupanj uvjerenja o sigurnosnoj provjeri posjetitelja;

e) naziv, adresa, broj telefona i telefaksa, adresa elektroničke pošte i kontakt osoba u tijelima, službama ili pravnim osobama koje se posjećuje;

f) datum zahtjeva i potpis nadležnog tijela.

(4) Nadležna tijela stranaka mogu sastaviti popise osoba ovlaštenih za ponovljene posjete. Popisi su valjani tijekom početnog razdoblja od dvanaest mjeseci. Uvjeti pojedinih posjeta dogovaraju se izravno s odgovarajućim kontakt osobama u pravnoj osobi koju dotične osobe posjećuju, u skladu s dogovorenim odredbama i uvjetima.

ČLANAK 11.
POVREDA SIGURNOSTI

(1) U slučaju povrede sigurnosti, nadležno tijelo primatelja odmah, pisano, obavješćuje nadležno tijelo pošiljatelja.

(2) Slučajevi kršenja odredbi o zaštiti klasificiranih podataka koji potpadaju pod ovaj Ugovor istražuju se i procesuiraju u skladu s nacionalnim zakonima i propisima. Stranke na zahtjev pomažu jedna drugoj.

(3) Stranke obavješćuju jedna drugu o rezultatima istraga i poduzetim mjerama.

ČLANAK 12.
TROŠKOVI

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

ČLANAK 13.
NADLEŽNA TIJELA

Stranke obavješćuju jedna drugu diplomatskim putem o nadležnim tijelima odgovornim za provedbu ovog Ugovora.

ČLANAK 14.
KONZULTACIJE

(1) Nadležna tijela obavješćuju jedno drugo o svojim nacionalnim zakonima i propisima o zaštiti klasificiranih podataka i svim značajnim izmjenama i dopunama istih.

(2) Kako bi se osigurala bliska suradnja u provedbi ovog Ugovora, nadležna tijela međusobno se konzultiraju i pomažu pri organizaciji potrebnih uzajamnih posjeta.

ČLANAK 15.
RJEŠAVANJE SPOROVA

Svaki spor u vezi s primjenom ili tumačenjem ovog Ugovora rješava se izravnim konzultacijama i pregovorima između stranaka.

ČLANAK 16.
ZAVRŠNE ODREDBE

(1) Ovaj Ugovor sklapa se na neodređeno vrijeme i stupa na snagu prvog dana drugog mjeseca koji slijedi nakon dana na koji su stranke obavijestile jedna drugu pisano, diplomatskim putem, o okončanju unutarnjih postupaka potrebnih za stupanje ovog Ugovora na snagu.

(2) Ovaj Ugovor može se izmijeniti i dopuniti uzajamnim pisanim pristankom stranaka. Izmjene i dopune stupaju na snagu u skladu sa stavkom 1. ovog članka.

(3) Svaka stranka može okončati ovaj Ugovor u svako doba pisanom obaviješću drugoj stranci diplomatskim putem. U tom slučaju Ugovor prestaje šest mjeseci nakon što druga stranka primi obavijest o okončanju. U slučaju prestanka, svi klasificirani podaci koji su preneseni ili nastali u primjeni ovog Ugovora i dalje se štite u skladu s odredbama sadržanim u ovom Ugovoru.

Sastavljeno u Zagrebu dana 24. srpnja 2018. u dva izvornika na hrvatskom, njemačkom i engleskom jeziku, pri čemu su svi tekstovi jednako vjerodostojni. U slučaju bilo kakvih razlika u tumačenju, mjerodavan je engleski tekst.

Za Vladu Republike Hrvatske

Za Saveznu vladu Republike Austrije

[ENGLISH TEXT – TEXTE ANGLAIS]

AGREEMENT

BETWEEN

THE GOVERNMENT OF THE REPUBLIC OF CROATIA

AND

THE AUSTRIAN FEDERAL GOVERNMENT

ON THE EXCHANGE AND MUTUAL PROTECTION OF CLASSIFIED INFORMATION

The Government of the Republic of Croatia and the Austrian Federal Government (hereinafter referred to as "the Parties"),

Intending to ensure the security of all classified information designated and marked as such in accordance with national laws and regulations of either Party and transmitted to the other Party,

Wishing to provide rules for the mutual protection of classified information transmitted or generated in the course of the cooperation between the Parties,

Have agreed upon the following:

ARTICLE 1
DEFINITIONS

For the purposes of this Agreement:

a) "Classified Information" means any information, regardless of its form, designated and marked as such in accordance with the national laws and regulations of either Party in order to ensure protection against unauthorized disclosure, misappropriation or loss;

b) "Security Classification Level" means a category which, in accordance with national laws and regulations, characterises the level of restriction of access to Classified Information and the minimum level of its protection by the Parties;

c) "Competent Authority" means the National Security Authority and any other competent authority and agency notified in accordance with Article 13 of this Agreement;

d) "Personnel Security Clearance" means the determination by a Competent Authority that an individual is eligible to have access to Classified Information in accordance with national laws and regulations;

e) "Facility Security Clearance" means the determination by a Competent Authority that a legal entity has the physical and organizational capability to meet the conditions for access to and handling of Classified Information in accordance with national laws and regulations;

f) "Classified Contract" means a contract or subcontract between a legal entity or individual from the State of one Party and a legal entity or individual from the State of the other Party, the implementation of which requires access to Classified Information or its generation;

g) "Originator" means the originating Party as well as any legal entity or individual under its jurisdiction which releases Classified Information;

h) "Recipient" means the receiving Party as well as any legal entity or individual under its jurisdiction which receives Classified Information;

i) "Third Party" means a legal entity or an individual which is not an Originator or Recipient of the Classified Information transmitted in accordance with this Agreement, a government not Party to this Agreement or an international organisation;

j) "Breach of Security" means any form of disclosure, misuse, unauthorized alteration, damage or destruction of Classified Information, as well as any other action or inaction, resulting in loss of its confidentiality, integrity or availability.

ARTICLE 2
SECURITY CLASSIFICATION LEVELS

The Parties agree on the equivalence of the following security classification levels:

Republic of Croatia:	Republic of Austria:	Corresponding English expression:
VRLO TAJNO	STRENG GEHEIM	TOP SECRET
TAJNO	GEHEIM	SECRET
POVJERLJIVO	VERTRAULICH	CONFIDENTIAL
OGRANIČENO	EINGESCHRÄNKT	RESTRICTED

ARTICLE 3
MARKING

(1) Classified Information to be transmitted shall be marked by the Originator in accordance with the appropriate Security Classification Level. The Recipient shall mark received Classified Information with the Security Classification Level equivalent to the marking by the Originator.

(2) Classified Information generated, reproduced or translated in the course of cooperation under this Agreement shall also be marked.

(3) The Security Classification Level shall only be altered or revoked with the written consent of the Originator. The Originator shall inform the Recipient without delay about any alteration or revocation of the security classification level of the transmitted Classified Information.

ARTICLE 4
PRINCIPLES OF THE PROTECTION OF CLASSIFIED INFORMATION

(1) The Parties shall take all appropriate measures to ensure the protection of the transmitted Classified Information and shall provide for the necessary control of this protection.

(2) The Parties shall afford transmitted Classified Information at least the same level of protection as they afford their own Classified Information of the equivalent Security Classification Level.

(3) Transmitted Classified Information shall only be used for the purpose it has been released for.

(4) Transmitted Classified Information shall only be made accessible to persons who are authorized in accordance with national laws and regulations to have access to Classified Information of the equivalent Security Classification Level and who require this access for the exercise of their duties.

(5) A Party shall not make Classified Information accessible to a third party without the prior written consent of the Competent Authority of the Originator.

(6) Classified Information generated in the course of cooperation under this Agreement shall enjoy the same protection as Classified Information transmitted in the course of cooperation under this Agreement.

ARTICLE 5
PERSONNEL SECURITY CLEARANCE

(1) Within the scope of this Agreement, each Party shall recognize the Personnel Security Clearances issued by the other Party.

(2) The Competent Authorities shall assist each other upon request and in accordance with national laws and regulations in carrying out vetting procedures necessary for the application of this Agreement.

(3) Within the scope of this Agreement, the Competent Authorities shall inform each other without delay about any alteration with regard to Personnel Security Clearances, in particular about a revocation or an alteration of the Security Classification Level.

(4) Upon request of the Competent Authority of the Originator, the Competent Authority of the Recipient shall issue a written confirmation that an individual is authorized to access Classified Information.

ARTICLE 6
CLASSIFIED CONTRACTS

(1) A Classified Contract shall contain provisions on the security requirements and on the Security Classification Level of the information to be released. A copy of the provisions shall be sent to the Competent Authority.

(2) In the context of Classified Contracts, each Party shall recognize the Facility Security Clearances issued by the other Party.

(3) In the context of the preparation or conclusion of Classified Contracts, the Competent Authorities shall inform each other upon request whether a valid Facility Security Clearance has been issued or the relevant proceedings have been initiated and about the security requirements for the Classified Information involved.

(4) The Competent Authorities shall inform each other about any Classified Contracts falling under this Agreement.

(5) The Competent Authorities shall inform each other without delay about any alteration with regard to Facility Security Clearances falling under this Article, in particular about a revocation or an alteration of the Security Classification Level.

(6) The Originator shall transmit to the Recipient and to the Competent Authority of the Recipient a list of the Classified Information to be transmitted under the Classified Contract.

(7) A contractor may hire a subcontractor to fulfil a part of a Classified Contract. Subcontractors shall be subject to the same security requirements as those applicable for the contractor.

ARTICLE 7
TRANSMISSION

Classified Information shall be transmitted through diplomatic channels or any other channels as agreed upon between the Parties. Receipt of Classified Information marked POVJERLJIVO / VERTRAULICH / CONFIDENTIAL and above shall be acknowledged in writing. Upon the request of the Originator, receipt of Classified Information marked OGRANIČENO / EINGESCHRÄNKT / RESTRICTED shall also be acknowledged in writing.

ARTICLE 8
REPRODUCTION AND TRANSLATION

(1) The reproduction and translation of Classified Information may be restricted or excluded by the Originator. The number of copies shall be restricted to that required for official purposes.

(2) Classified Information marked as VRLO TAJNO / STRENG GEHEIM / TOP SECRET shall not be reproduced or translated without the prior written consent of the Originator.

(3) Classified Information shall only be translated by persons authorized to have access to Classified Information of the respective Security Classification Level.

(4) Copies and translations shall be protected in the same way as originals. The translation shall bear an appropriate note in the language into which it is translated that the translation contains Classified Information of the Originator.

ARTICLE 9
DESTRUCTION

(1) Classified Information shall be destroyed in a manner that does not permit a full or partial reconstruction. The destruction of Classified Information that has been registered in accordance with national laws and regulations shall be recorded.

(2) The Originator may, by additional marking or sending subsequent written notice to the Recipient, expressly prohibit the destruction of Classified Information. If the destruction of Classified Information is prohibited, it shall be returned to the Originator.

(3) In case of a crisis situation in which it is impossible to protect or return Classified Information transmitted or generated under this Agreement, the Classified Information shall be destroyed immediately. The Recipient shall inform the Competent Authority of the Originator about this destruction as soon as possible.

ARTICLE 10
VISITS

(1) Visits requiring access to Classified Information are subject to prior permission by the Competent Authority of the host Party. The permission shall be granted only to persons authorized in accordance with national laws and regulations to have access to Classified Information of the respective Security Classification Level.

(2) Requests for visits shall be submitted to the Competent Authority of the host Party at least ten working days prior to the visit, in urgent cases within a shorter period. The Competent Authorities shall inform each other about the details of the visit and ensure the protection of personal data.

(3) Requests for visits shall be made in English language and shall state in particular the following:

a) purpose and proposed date of the visit;

b) first name and family name, date and place of birth, citizenship and passport or ID card number of the visitor;

c) position of the visitor and name of the authority, agency or enterprise represented;

d) validity and level of the Personnel Security Clearance of the visitor;

e) name, address, phone and fax number, e-mail address and point of contact of the authorities, agencies or facilities to be visited;

f) date of the request and signature of the Competent Authority.

(4) The Competent Authorities of the Parties may draw up lists of individuals authorised to make recurring visits. The lists are valid for an initial period of twelve months. The terms of the respective visits shall be directly arranged with the appropriate points of contact in the legal entity to be visited by these individuals, in accordance with the terms and conditions agreed upon.

ARTICLE 11
BREACH OF SECURITY

(1) In the event of a Breach of Security, the Competent Authority of the Recipient shall immediately inform the Competent Authority of the Originator in writing.

(2) Violations of the provisions on the protection of Classified Information falling under this Agreement shall be investigated and prosecuted in accordance with national laws and regulations. The Parties shall assist each other upon request.

(3) The Parties shall inform each other about the result of the investigations and the measures taken.

ARTICLE 12
EXPENSES

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

ARTICLE 13
COMPETENT AUTHORITIES

The Parties shall notify each other through diplomatic channels of the Competent Authorities responsible for the implementation of this Agreement.

ARTICLE 14
CONSULTATIONS

(1) The Competent Authorities shall inform each other of the respective national laws and regulations on the protection of Classified Information and any significant amendments thereof.

(2) In order to ensure close cooperation in the implementation of this Agreement, the Competent Authorities shall consult each other and facilitate the necessary mutual visits.

ARTICLE 15
SETTLEMENT OF DISPUTES

Any dispute regarding the application or interpretation of this Agreement shall be resolved by direct consultations and negotiations between the Parties.

ARTICLE 16
FINAL PROVISIONS

(1) This Agreement is concluded for an indefinite period of time and shall enter into force on the first day of the second month following the day on which the Parties have notified each other in writing, through diplomatic channels, of the completion of the internal procedures necessary for the entry into force of this Agreement.

(2) This Agreement may be amended by mutual written consent of the Parties. Amendments shall enter into force in accordance with paragraph 1 of this Article.

(3) Each Party may terminate this Agreement at any time by giving written notice to the other Party through diplomatic channels. In such a case, the Agreement shall terminate six months after the receipt of the termination notice by the other Party. In the case of termination, all Classified Information transmitted or generated in application of this Agreement shall continue to be protected in accordance with the provisions set forth in this Agreement.

Done at Zagreb on 24 July 2018 in two originals in the Croatian, German and English languages, all texts being equally authentic. In case of any divergence of interpretation, the English text shall prevail.

For the Government of the Republic of Croatia

For the Austrian Federal Government

[GERMAN TEXT – TEXTE ALLEMAND]

ABKOMMEN

ZWISCHEN

DER REGIERUNG DER REPUBLIK KROATIEN

UND

DER ÖSTERREICHISCHEN BUNDESREGIERUNG

ÜBER DEN AUSTAUSCH UND GEGENSEITIGEN SCHUTZ KLASSIFIZIERTER INFORMATIONEN

Die Regierung der Republik Kroatien und die Österreichische Bundesregierung (im Weiteren „die Parteien" genannt),

In der Absicht, den Schutz aller klassifizierten Informationen zu gewährleisten, die gemäß dem innerstaatlichen Recht einer der Parteien als solche eingestuft und gekennzeichnet wurden und an die andere Partei übermittelt wurden,

Von dem Wunsch geleitet, Regeln zum gegenseitigen Schutz der übermittelten oder im Zuge der Zusammenarbeit zwischen den Parteien entstandenen klassifizierten Informationen vorzusehen,

sind wie folgt übereingekommen:

ARTIKEL 1
BEGRIFFSBESTIMMUNGEN

Im Sinne dieses Abkommens bedeutet:

a) „Klassifizierte Informationen" Informationen, unabhängig von ihrer Form, die gemäß den innerstaatlichen Gesetzen und Verordnungen einer der Parteien als klassifiziert eingestuft und gekennzeichnet wurden, um ihren Schutz vor unberechtigter Preisgabe, widerrechtlicher Verwendung oder Verlust zu gewährleisten;

b) „Sicherheitsklassifizierungsstufe" eine Kategorie die, im Einklang mit innerstaatlichen Gesetzen und Verordnungen, den Level der Zugangsbeschränkung zu klassifizierten Informationen und das Mindestlevel des Schutzes durch die Parteien charakterisiert;

c) „Zuständige Behörde" die nationale Sicherheitsbehörde und jede andere zuständige Behörde oder Agentur, die gemäß Artikel 13 notifiziert wurde;

d) „Sicherheitsunbedenklichkeitsbescheinigung für Personen" die Feststellung durch eine zuständige Behörde, dass eine Person zum Zugang zu klassifizierten Informationen gemäß innerstaatlichem Recht berechtigt ist;

e) „Sicherheitsunbedenklichkeitsbescheinigung für Unternehmen" die Feststellung durch eine zuständige Behörde, dass eine juristische Person über die physische und organisatorische Fähigkeit verfügt, die Bedingungen für den Zugang zu und den Umgang mit klassifizierten Informationen gemäß den innerstaatlichen Gesetzen und Verordnungen zu erfüllen;

f) „Klassifizierter Vertrag" ein Vertrag oder Untervertrag zwischen einer juristischen oder natürlichen Person einer Partei und einer juristischen oder natürlichen Person der anderen Partei, dessen Erfüllung den Zugang zu oder die Herstellung von klassifizierten Informationen erfordert;

g) „Herausgeber" die herausgebende Partei sowie jede der Hoheitsgewalt der betreffenden Partei unterstehende juristische oder natürliche Person, die klassifizierte Informationen herausgibt;

h) „Empfänger" die empfangende Partei sowie jede der Hoheitsgewalt der betreffenden Partei unterstehende juristische oder natürliche Person, die klassifizierte Informationen empfängt;

i) „Dritter" eine juristische oder natürliche Person, die nicht Herausgeber oder Empfänger der klassifizierten Information ist, die gemäß diesem Abkommen übermittelt wurde, oder eine Regierung, die nicht Partei dieses Abkommens ist, oder eine internationale Organisation;

j) „Sicherheitsverletzung" ist die unberechtigte Preisgabe, widerrechtliche Verwendung, unberechtigte Änderung, Beschädigung oder Zerstörung von klassifizierten Informationen sowie jede andere Handlung oder Unterlassung, die den Verlust ihrer Vertraulichkeit, Integrität oder Verfügbarkeit nach sich zieht.

ARTIKEL 2
GLEICHWERTIGKEIT DER KLASSIFIZIERUNGSSTUFEN

Die Parteien legen fest, dass folgende Klassifizierungsstufen gleichwertig sind:

Republik Kroatien:	Republik Österreich:	Englische Entsprechung:
VRLO TAJNO	STRENG GEHEIM	TOP SECRET
TAJNO	GEHEIM	SECRET
POVJERLJIVO	VERTRAULICH	CONFIDENTIAL
OGRANIČENO	EINGESCHRÄNKT	RESTRICTED

ARTIKEL 3
KENNZEICHNUNG

(1) Zu übermittelnde klassifizierte Informationen werden vom Herausgeber in Übereinstimmung mit der entsprechenden Klassifizierungsstufe gekennzeichnet. Der Empfänger kennzeichnet erhaltene klassifizierte Informationen mit einer Klassifizierungsstufe, die der Kennzeichnung des Herausgebers entspricht.

(2) Die Kennzeichnungspflicht gilt auch für klassifizierte Informationen, die im Zuge der unter dieses Abkommen fallenden Zusammenarbeit erzeugt, vervielfältigt oder übersetzt werden.

(3) Die Klassifizierungsstufe darf ausschließlich mit schriftlicher Zustimmung des Herausgebers geändert oder aufgehoben werden. Der Herausgeber informiert den Empfänger unverzüglich über jede Änderung oder Aufhebung der Klassifizierungsstufe der übermittelten klassifizierten Informationen.

ARTIKEL 4
GRUNDSÄTZE DES SCHUTZES KLASSIFIZIERTER INFORMATIONEN

(1) Die Parteien treffen alle geeigneten Maßnahmen, um den Schutz der übermittelten klassifizierten Informationen zu gewährleisten, und sorgen für die erforderliche Kontrolle dieses Schutzes.

(2) Die Parteien gewähren den übermittelten klassifizierten Informationen mindestens den gleichen Schutzstandard, wie sie ihren eigenen klassifizierten Informationen der gleichwertigen Klassifizierungsstufe gewähren.

(3) Übermittelte klassifizierte Informationen dürfen nur zu dem Zweck, für den sie herausgegeben wurden, verwendet werden.

(4) Übermittelte klassifizierte Informationen werden nur Personen zugänglich gemacht, die gemäß dem innerstaatlichen Recht zum Zugang zu klassifizierten Informationen der gleichwertigen Klassifizierungsstufe ermächtigt sind und die den Zugang für die Ausübung ihrer Aufgaben benötigen.

(5) Eine Partei macht Dritten ohne vorherige schriftliche Zustimmung der zuständigen Behörde des Herausgebers klassifizierte Informationen nicht zugänglich.

(6) Klassifizierte Informationen, die im Zuge der unter dieses Abkommen fallenden Zusammenarbeit erzeugt werden, genießen den gleichen Schutz wie übermittelte klassifizierte Informationen.

ARTIKEL 5
SICHERHEITSUNBEDENKLICHKEITSBESCHEINIGUNGEN FÜR PERSONEN

(1) Im Rahmen dieses Abkommens anerkennt jede Partei die von der anderen Partei ausgestellten Sicherheitsunbedenklichkeitsbescheinigungen für Personen.

(2) Die zuständigen Behörden unterstützen einander auf Ersuchen und im Einklang mit den jeweiligen innerstaatlichen Gesetzen und Verordnungen bei den für die Anwendung dieses Abkommens notwendigen Sicherheitsüberprüfungen.

(3) Im Rahmen dieses Abkommens informieren die zuständigen Behörden einander unverzüglich über alle Änderungen von Sicherheitsunbedenklichkeits-bescheinigungen für Personen, insbesondere über einen Widerruf oder eine Änderung der Klassifizierungsstufe.

(4) Auf Ersuchen der zuständigen Behörde des Herausgebers stellt die zuständige Behörde des Empfängers eine schriftliche Bestätigung aus, dass eine Person zum Zugang zu klassifizierten Informationen berechtigt ist.

ARTIKEL 6
KLASSIFIZIERTE VERTRÄGE

(1) Ein klassifizierter Vertrag enthält Bestimmungen über die Sicherheitsanforderungen und Klassifizierungsstufe der herauszugebenden Information. Eine Kopie der Bestimmungen wird an die zuständige Behörde der Partei weitergeleitet.

(2) Im Zusammenhang mit klassifizierten Verträgen anerkennt jede Partei die Sicherheitsunbedenklichkeitsbescheinigungen für Unternehmen, die von der anderen Partei ausgestellt wurden.

(3) Im Zuge der Vorbereitung oder des Abschlusses klassifizierter Verträge informieren einander die zuständigen Behörden der beiden Parteien auf deren Ersuchen über die Ausstellung der erforderlichen Sicherheitsunbedenklichkeitsbescheinigungen für Unternehmen sowie über den Beginn entsprechender Verfahren und über sonstige zusätzliche Sicherheitserfordernisse.

(4) Die zuständigen Behörden informieren einander über klassifizierte Verträge, die unter dieses Abkommen fallen.

(5) Die zuständigen Behörden informieren einander unverzüglich über jegliche Änderung von den unter diesen Artikel fallenden Sicherheitsunbedenklichkeitsbescheinigungen für Unternehmen, vor allem über alle Änderungen oder Aufhebungen bezüglich deren Sicherheitsklassifizierungsstufe.

(6) Der Herausgeber übermittelt dem Empfänger und der zuständigen Behörde des Empfängers eine Liste der klassifizierten Informationen, die gemäß dem klassifizierten Vertrag zu übermitteln sind.

(7) Ein Auftragnehmer kann einen Subunternehmer heranziehen, um einen Teil des klassifizierten Vertrags zu erfüllen. Subunternehmer unterliegen den gleichen Sicherheitserfordernissen wie der Auftragnehmer.

ARTIKEL 7
ÜBERMITTLUNG

Klassifizierte Informationen werden auf diplomatischem Weg oder auf jedem anderen zwischen den Vertragsparteien vereinbarten Weg übermittelt. Der Empfang von als POVJERLJIVO / VERTRAULICH / CONFIDENTIAL oder höher gekennzeichneten klassifizierten Informationen ist schriftlich zu bestätigen. Auf Ersuchen des Herausgebers kann auch der Empfang von als OGRANIČENO / EINGESCHRÄNKT / RESTRICTED markierten Informationen schriftlich bestätigt werden.

ARTIKEL 8
VERVIELFÄLTIGUNG UND ÜBERSETZUNG

(1) Die Vervielfältigung und Übersetzung klassifizierter Informationen kann vom Herausgeber eingeschränkt oder ausgeschlossen werden. Die Anzahl der Kopien kann auf jene Anzahl eingeschränkt werden, die für öffentliche Zwecke erforderlich ist.

(2) Als VRLO TAJNO / STRENG GEHEIM / TOP SECRET gekennzeichnete klassifizierte Informationen dürfen nur mit schriftlicher Zustimmung des Herausgebers vervielfältigt oder übersetzt werden.

(3) Klassifizierte Informationen werden nur von Personen übersetzt, die zum Zugang zu klassifizierten Informationen der jeweiligen Klassifizierungsstufe berechtigt sind.

(4) Kopien und Übersetzungen sind wie Originale zu schützen. Die Übersetzung enthält einen Hinweis in der Sprache, in die übersetzt wurde, dass die Übersetzung klassifizierte Informationen des Herausgebers enthält.

ARTIKEL 9
VERNICHTUNG

(1) Klassifizierte Informationen werden auf eine Weise vernichtet, die eine vollständige oder teilweise Wiederherstellung nicht zulässt. Die Vernichtung von klassifizierten Informationen die im Einklang mit nationalen Gesetzen und Verordnungen registriert wurde wird aufgezeichnet.

(2) Der Herausgeber kann mittels zusätzlicher Kennzeichnung oder nachträglicher schriftlicher Mitteilung an den Empfänger die Vernichtung von klassifizierten Informationen ausdrücklich verbieten. Wenn die Vernichtung von klassifizierten Informationen verboten wurde, sind diese an den Herausgeber zurückzustellen.

(3) Im Falle einer Krisensituation, in der es unmöglich ist klassifizierte Informationen, die in Anwendung dieses Abkommens übermittelt oder erzeugt wurden, zu schützen oder rückzuübermitteln, werden die klassifizierten Informationen umgehend vernichtet. Der Empfänger informiert die zuständige Behörde des Herausgebers sobald wie möglich über diese Vernichtung.

ARTIKEL 10
BESUCHE

(1) Besuche, die den Zugang zu klassifizierten Informationen erfordern, unterliegen der vorherigen Genehmigung durch die zuständige Behörde der gastgebenden Partei. Die Genehmigung wird nur Personen erteilt, die gemäß den innerstaatlichen Gesetzen und Verordnungen zum Zugang zu klassifizierten Informationen der entsprechenden Klassifizierungsstufe ermächtigt sind.

(2) Besuchsanträge werden mindestens zehn Arbeitstage vor dem Besuch bei der zuständigen Behörde der gastgebenden Partei gestellt, in dringenden Fällen innerhalb eines kürzeren Zeitraums. Die zuständigen Behörden informieren einander über die Einzelheiten des Besuchs und gewährleisten den Schutz personenbezogener Daten.

(3) Besuchsanträge werden in englischer Sprache gestellt und enthalten insbesondere folgende Angaben:

a) Zweck, vorgesehenes Datum und Dauer des Besuchs;

b) Vor- und Familienname, Geburtsdatum und -ort, Staatsangehörigkeit und Pass- oder Personalausweisnummer des Besuchers;

c) Funktion des Besuchers und Name der vertretenen Behörde oder Stelle oder des vertretenen Unternehmens;

d) Gültigkeit und Klassifizierungsstufe der Sicherheitsunbedenklichkeits-bescheinigung für Personen des Besuchers;

e) Name, Adresse, Telefon- und Faxnummer, E-Mail-Adresse und Ansprechpartner der Behörden, Stellen oder Einrichtungen, die besucht werden sollen;

f) Datum des Antrags und Unterschrift der zuständigen Behörde.

(4) Die zuständigen Behörden der Parteien können Listen von Personen erstellen, die zu wiederholten Besuchen ermächtigt sind. Diese Listen sind für einen anfänglichen Zeitraum von 12 Monaten gültig. Die Bedingungen für die jeweiligen Listen werden direkt mit den passenden Ansprechpartnern in der juristischen Person, die von diesen Personen besucht werden soll, gemäß den vereinbarten Modalitäten und Bedingungen vorgesehen.

ARTIKEL 11
SICHERHEITSVERLETZUNGEN

(1) Im Falle einer Sicherheitsverletzung informiert die zuständige Behörde des Empfängers unverzüglich die zuständige Behörde des Herausgebers schriftlich.

(2) Verletzungen der Bestimmungen über den Schutz von unter dieses Abkommen fallenden klassifizierten Informationen werden gemäß den innerstaatlichen Gesetzen und Verordnungen untersucht und verfolgt. Die Parteien unterstützen einander auf Ersuchen.

(3) Die Parteien informieren einander über das Ergebnis der Untersuchungen und über die getroffenen Maßnahmen.

ARTIKEL 12
KOSTEN

Jede Partei trägt die Kosten, die ihr im Zuge der Durchführung dieses Abkommens entstehen.

ARTIKEL 13
ZUSTÄNDIGE BEHÖRDEN

Die Parteien teilen einander auf diplomatischem Weg die zuständigen Behörden mit, die für die Durchführung dieses Abkommens verantwortlich sind.

ARTIKEL 14
KONSULTATIONEN

(1) Die zuständigen Behörden informieren einander über das jeweilige innerstaatliche Recht über den Schutz klassifizierter Informationen und alle wesentlichen Änderungen.

(2) Um eine enge Zusammenarbeit bei der Durchführung dieses Abkommens zu gewährleisten, konsultieren die zuständigen Behörden einander und erleichtern die notwendigen gegenseitigen Besuche.

ARTIKEL 15
STREITBEILEGUNG

Streitigkeiten über die Anwendung oder Auslegung dieses Abkommens werden im Wege direkter Konsultationen und Verhandlungen beigelegt.

ARTIKEL 16
SCHLUSSBESTIMMUNGEN

(1) Dieses Abkommen wird auf unbestimmte Zeit geschlossen und tritt am ersten Tag des zweiten Monats nach dem Tag in Kraft, an dem die Parteien einander auf diplomatischem Wege schriftlich den Abschluss der für das Inkrafttreten des Abkommens erforderlichen innerstaatlichen Verfahren mitgeteilt haben.

(2) Dieses Abkommen kann im gegenseitigen schriftlichen Einvernehmen beider Parteien geändert werden. Änderungen treten gemäß Absatz 1 in Kraft.

(3) Jede Partei kann dieses Abkommen jederzeit auf diplomatischem Wege kündigen. In einem solchen Fall tritt das Abkommen sechs Monate nach Erhalt der Kündigungsnote durch die andere Partei außer Kraft. Im Fall der Kündigung bleiben klassifizierte Informationen, die in Anwendung dieses Abkommens übermittelt oder hergestellt wurden, weiterhin nach den Bestimmungen dieses Abkommens geschützt.

Geschehen zu Zagreb am 24. Juli 2018 in zwei Urschriften in kroatischer, deutscher und englischer Sprache, wobei alle Texte gleichermaßen authentisch sind. Im Fall unterschiedlicher Auslegungen geht der englische Wortlaut vor.

Für die Regierung der Republik Kroatien

Für die Österreichische Bundesregierung

[TRANSLATION – TRADUCTION]

ACCORD ENTRE LE GOUVERNEMENT DE LA RÉPUBLIQUE DE CROATIE ET LE GOUVERNEMENT FÉDÉRAL AUTRICHIEN SUR L'ÉCHANGE ET LA PROTECTION MUTUELLE DES INFORMATIONS CLASSIFIÉES

Le Gouvernement de la République de Croatie et le Gouvernement fédéral autrichien (ci-après dénommés les « Parties »),

Aux fins d'assurer la protection de toutes les informations classifiées désignées et marquées comme telles conformément à la législation et aux réglementations internes de chacune des Parties et transmises à l'autre Partie,

Souhaitant établir des directives réglementant la protection mutuelle des informations classifiées transmises ou générées au cours de la coopération entre les Parties,

Sont convenus de ce qui suit :

ARTICLE PREMIER. DÉFINITIONS

Aux fins du présent Accord :

a) le terme « information classifiée » désigne toute information, quelle que soit sa forme, qui est considérée et marquée comme telle conformément à la législation et à la réglementation internes de l'une des Parties afin d'assurer sa protection contre toute divulgation non autorisée, tout détournement ou toute perte ;
b) le terme « niveau de classification de sécurité » désigne une catégorie qui, conformément à la législation et à la réglementation internes, caractérise le niveau de restriction d'accès aux informations classifiées et le niveau minimal de protection de ces informations par les Parties ;
c) le terme « autorité compétente » désigne l'Agence nationale de sécurité et toute autre autorité compétente et agence notifiée conformément à l'article 13 du présent Accord ;
d) le terme « habilitation de sécurité personnelle » désigne la décision d'une autorité compétente selon laquelle une personne est autorisée à accéder à des informations classifiées conformément à la législation et à la réglementation internes des Parties ;
e) le terme « habilitation de sécurité d'établissement » désigne la décision d'une autorité compétente selon laquelle une personne morale dispose de capacités physiques et organisationnelles suffisantes pour satisfaire aux critères d'accès et de traitement des informations classifiées conformément à la législation et à la réglementation internes des Parties ;
f) le terme « contrat classifié » désigne un contrat ou un contrat de sous-traitance entre une personne morale ou une personne physique de l'État d'une Partie et une personne morale ou une personne physique de l'État de l'autre Partie dont l'exécution nécessite l'accès à des informations classifiées ou la création de telles informations ;
g) le terme « auteur » désigne la Partie d'origine ainsi que les personnes morales ou physiques placées sous sa juridiction, qui communiquent des informations classifiées ;
h) le terme « destinataire » désigne la Partie destinataire ainsi que les personnes morales ou physiques placées sous sa juridiction, qui reçoivent des informations classifiées ;
i) le terme « tierce partie » désigne une personne morale ou une personne physique qui n'est ni l'auteur ni le destinataire des informations classifiées transmises en vertu du présent Accord, un gouvernement qui n'est pas une Partie au présent Accord, ou une organisation internationale ;

j) le terme « atteinte à la sécurité »

désigne toute forme de divulgation, d'utilisation abusive, de modification non autorisée, de détérioration ou de destruction d'informations classifiées, ainsi que toute autre mesure ou inaction susceptible d'entraîner la perte de leur confidentialité, de leur intégrité ou de leur disponibilité ;

ARTICLE 2. NIVEAUX DE CLASSIFICATION DE SÉCURITÉ

Les Parties conviennent de l'équivalence des niveaux de classification de sécurité suivants :

République de Croatie :	République d'Autriche :	Équivalent en français :
VRLO TAJNO	STRENG GEHEIM	TRÈS SECRET
TAJNO	GEHEIM	SECRET
POVJERLJIVO	VERTRAULICH	CONFIDENTIEL
OGRANIČENO	EINGESCHRÄNKT	RESTREINT

ARTICLE 3. MARQUAGE

1) L'auteur appose sur les informations classifiées à transmettre la marque correspondant au niveau de classification de sécurité approprié. Le destinataire appose sur les informations classifiées reçues la marque correspondant au niveau de classification de sécurité équivalent au marquage de l'auteur.

2) Les informations classifiées générées, reproduites ou traduites dans le cadre de la coopération visée dans le présent Accord doivent également porter une marque de classification.

3) Le niveau de classification de sécurité ne peut être modifié ou révoqué qu'avec le consentement écrit préalable de l'auteur. L'auteur informe sans délai le destinataire de toute modification ou révocation du niveau de classification de sécurité des informations classifiées transmises.

ARTICLE 4. PRINCIPES RELATIFS À LA PROTECTION DES INFORMATIONS CLASSIFIÉES

1) Les Parties prennent toutes les mesures appropriées pour assurer la protection des informations classifiées transmises et fournissent l'appui nécessaire au contrôle de cette protection.

2) Les Parties accordent aux informations classifiées transmises au moins le même niveau de protection que celui qu'elles accordent à leurs propres informations classifiées de niveau de classification de sécurité équivalent.

3) Les informations classifiées transmises ne sont utilisées qu'aux fins pour lesquelles elles ont été transmises.

4) L'accès aux informations classifiées transmises n'est accordé qu'aux personnes qui sont autorisées, conformément à la législation et à la réglementation internes, à avoir accès à des informations classifiées de niveau de classification de sécurité équivalent et qui ont besoin de cet accès dans l'exercice de leurs fonctions.

5) La Partie destinataire ne rend pas les informations classifiées accessibles à une tierce partie sans le consentement écrit préalable de l'autorité compétente de l'auteur.

6) Les informations classifiées générées dans le cadre de la coopération en vertu du présent Accord bénéficient de la même protection que les informations classifiées transmises dans le cadre de la coopération en vertu du présent Accord.

ARTICLE 5. HABILITATION DE SÉCURITÉ PERSONNELLE

1) Dans le cadre du présent Accord, chaque Partie reconnaît les habilitations de sécurité personnelles délivrées par l'autre Partie.

2) Les autorités compétentes se prêtent mutuellement assistance, sur demande et conformément à la législation et à la réglementation internes, pour l'exécution des procédures de vérification nécessaires à l'application du présent Accord.

3) Dans le cadre du présent Accord, les autorités compétentes s'informent sans délai de toute modification concernant les habilitations de sécurité personnelles, en particulier de toute révocation ou modification du niveau de classification de sécurité.

4) Sur demande de l'autorité compétente de l'auteur, l'autorité compétente du destinataire donne une confirmation écrite qu'une personne est autorisée à accéder aux informations classifiées.

ARTICLE 6. CONTRATS CLASSIFIÉS

1) Un contrat classifié contient des dispositions relatives aux exigences de sécurité et au niveau de classification de sécurité des informations à divulguer. Une copie des dispositions est adressée aux autorités compétentes.

2) Dans le cadre des contrats classifiés, chaque Partie reconnaît les habilitations de sécurité d'établissement délivrées par l'autre Partie.

3) Dans le cadre de la préparation ou de la conclusion de contrats classifiés, les autorités compétentes s'informent mutuellement, sur demande, de la délivrance d'une habilitation de sécurité d'établissement ou de l'exécution des procédures appropriées, et des exigences de sécurité pour les informations classifiées concernées.

4) Les autorités compétentes s'informent mutuellement de tout contrat classifié visé par le présent Accord.

5) Les autorités compétentes s'informent sans délai de toute modification concernant les habilitations de sécurité d'établissement visées par le présent Accord, en particulier de toute révocation ou modification du niveau de classification de sécurité.

6) L'auteur transmet au destinataire et à l'autorité compétente du destinataire une liste des informations classifiées à transmettre en vertu du contrat classifié.

7) Une entreprise prestataire peut engager un sous-traitant pour exécuter une partie d'un contrat classifié. Les sous-traitants se conforment aux mêmes exigences de sécurité que celles établies pour l'entreprise prestataire.

ARTICLE 7. TRANSMISSION

Les informations classifiées sont transmises par la voie diplomatique ou selon toute autre voie convenue par les Parties. La réception d'informations classifiées de niveau POVJERLJIVO / VERTRAULICH / CONFIDENTIEL ou d'un niveau supérieur requiert un accusé de réception écrit. À la demande de l'auteur, la réception d'informations classifiées de niveau OGRANlCENO / EINGESCHRANKT / RESTREINT requiert également un accusé de réception écrit.

ARTICLE 8. REPRODUCTION ET TRADUCTION

1) La reproduction et la traduction d'informations classifiées peuvent être limitées ou exclues par l'auteur. Le nombre d'exemplaires est limité à celui requis à des fins officielles.

2) Les informations classifiées de niveau VRLO TAJNO / STRENG GEHEIM / TRÈS SECRET ne sont reproduites ou traduites qu'avec le consentement écrit préalable de l'auteur.

3) Les informations classifiées sont traduites exclusivement par des personnes autorisées à accéder aux informations classifiées de niveau de classification de sécurité correspondant.

4) Les copies et les traductions sont protégées de la même manière que les originaux. La traduction porte une mention appropriée, rédigée dans la langue de la traduction, indiquant qu'elle contient des informations classifiées de l'auteur.

ARTICLE 9. DESTRUCTION

1) Les informations classifiées sont détruites de manière à empêcher leur reconstitution intégrale ou partielle. La destruction des informations classifiées enregistrées conformément à la législation et à la réglementation internes est consignée.

2) L'auteur peut, au moyen d'un marquage supplémentaire ou de l'envoi ultérieur d'une notification écrite au destinataire, interdire expressément la destruction d'informations classifiées. Si la destruction des informations classifiées est interdite, ces informations sont restituées à leur auteur.

3) En cas de situation de crise rendant impossible la protection ou la restitution des informations classifiées transmises ou générées dans le cadre du présent Accord, les informations classifiées sont immédiatement détruites. Le destinataire informe l'autorité compétente de l'auteur de cette destruction dans les meilleurs délais.

ARTICLE 10. VISITES

1) Les visites qui nécessitent l'accès à des informations classifiées sont soumises à l'autorisation préalable de l'autorité compétente de la Partie hôte. Cette autorisation n'est accordée qu'aux personnes habilitées, en vertu de la législation et de la réglementation internes, à accéder aux informations classifiées du niveau de classification de sécurité correspondant.

2) Les demandes de visite sont soumises à l'autorité compétente de la Partie hôte au moins dix jours ouvrables avant la visite, ou, en cas d'urgence, dans un délai plus court. Les autorités compétentes s'informent mutuellement des détails de la visite et veillent à la protection des données à caractère personnel.

3) Les demandes de visite sont rédigées en langue anglaise et mentionnent notamment les éléments suivants :

a) l'objectif de la visite et sa date envisagée ;
b) le prénom, le nom de famille, la date et le lieu de naissance, la nationalité ainsi que le numéro du passeport ou de la carte d'identité du visiteur ;
c) la fonction du visiteur et le nom de l'autorité, de l'agence ou de l'entité qu'il représente ;
d) la validité et le niveau de l'habilitation de sécurité personnelle du visiteur ;
e) le nom, l'adresse, les numéros de téléphone et de télécopieur, l'adresse électronique et le point de contact des autorités, des agences ou des établissements à visiter ;
f) la date de la demande et la signature de l'autorité compétente.

4) Les autorités compétentes des Parties peuvent établir des listes de personnes autorisées à effectuer des visites régulières. Les listes sont valables pour une période initiale de 12 mois. Les modalités des différentes visites sont définies directement avec les points de contact compétents de la personne morale qui fera l'objet de visites par ces personnes, conformément aux clauses et conditions convenues.

ARTICLE 11. ATTEINTE À LA SÉCURITÉ

1) En cas d'atteinte à la sécurité, l'autorité compétente du destinataire en informe immédiatement par écrit l'autorité compétente de l'auteur.

2) Les violations des dispositions relatives à la protection des informations classifiées visées par le présent Accord font l'objet d'enquêtes et de poursuites conformément aux législations et réglementations internes. Les Parties se prêtent mutuellement assistance sur demande.

3) Les Parties s'informent mutuellement du résultat des enquêtes et des mesures prises.

ARTICLE 12. FRAIS

Chaque Partie prend en charge les dépenses qu'elle a engagées dans le cadre de la mise en œuvre du présent Accord.

ARTICLE 13. AUTORITÉS COMPÉTENTES

Les Parties s'informent mutuellement par la voie diplomatique des autorités compétentes responsables de l'application du présent Accord.

ARTICLE 14. CONSULTATIONS

1) Les autorités compétentes s'informent mutuellement de leurs législation et réglementation internes relatives à la protection des informations classifiées et de toute modification importante de celles-ci.

2) Afin de garantir une étroite collaboration dans la mise en application du présent Accord, les autorités compétentes se consultent et facilitent les visites mutuelles nécessaires.

ARTICLE 15. RÈGLEMENT DES DIFFÉRENDS

Tout différend relatif à l'application ou à l'interprétation du présent Accord est réglé au moyen de consultations et de négociations directes entre les Parties.

ARTICLE 16. DISPOSITIONS FINALES

1) Le présent Accord est conclu pour une durée indéterminée et entre en vigueur le premier jour du deuxième mois suivant le jour où les Parties se sont mutuellement informées, par écrit et par la voie diplomatique, de l'accomplissement des procédures internes nécessaires à cette fin.

2) Le présent Accord peut être modifié par consentement mutuel écrit des Parties. Les modifications entrent en vigueur conformément aux dispositions du paragraphe 1 du présent article.

3) Chaque Partie peut, à tout moment, dénoncer le présent Accord par une notification écrite adressée à l'autre Partie par la voie diplomatique. Dans ce cas, la dénonciation prend effet six mois après réception de la notification de dénonciation par l'autre Partie. En cas de dénonciation, toutes les informations classifiées transmises ou générées dans le cadre de l'application du présent Accord continuent à être protégées en vertu des dispositions établies dans le présent Accord.

FAIT à Zagreb le 24 juillet 2018, en deux exemplaires originaux, chacun en langue croate, allemande et anglaise, tous les textes faisant également foi. En cas de divergence d'interprétation, le texte anglais prévaut.

Pour le Gouvernement de la République de Croatie :

[SIGNÉ]

Pour le Gouvernement fédéral autrichien :

[SIGNÉ]