No. 56206*

Croatia
and
Italy

Agreement between the Government of the Republic of Croatia and the Government of the Italian Republic on exchange and mutual protection of classified information. Zagreb, 9 July 2019

Entry into force: *17 January 2020 by notification, in accordance with article 16(1)*

Authentic texts: *Croatian, English and Italian*

Registration with the Secretariat of the United Nations: *Croatia, 16 March 2020*

**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
Italie

Accord entre le Gouvernement de la République de Croatie et le Gouvernement de la République italienne sur l'échange et la protection mutuelle des informations classifiées. Zagreb, 9 juillet 2019

Entrée en vigueur : *17 janvier 2020 par notification, conformément au paragraphe 1 de l'article 16*

Textes authentiques : *croate, anglais et italien*

Enregistrement auprès du Secrétariat de l'Organisation des Nations Unies : *Croatie, 16 mars 2020*

**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
VLADE TALIJANSKE REPUBLIKE
O RAZMJENI I UZAJAMNOJ ZAŠTITI KLASIFICIRANIH PODATAKA

Vlada Republike Hrvatske i Vlada Talijanske Republike (u daljnjem tekstu „stranke"),

prepoznajući važnu ulogu svoje uzajamne suradnje u svrhu stabilizacije mira, međunarodne sigurnosti i uzajamnog povjerenja,

prepoznajući interes i zajedničku potrebu da se osigura zaštita bilo kojih klasificiranih podataka u političkom, sigurnosnom, vojnom, gospodarskom i bilo kojem drugom području, koji se razmjenjuju između stranaka i njihovih javnih i privatnih subjekata, u skladu sa zakonima i propisima stranaka,

prepoznajući potrebu za utvrđivanjem zajedničkih sigurnosnih pravila za zaštitu podataka, također i u vezi s mogućnošću provedbe ugovora o tehničkoj suradnji i razrade ugovornih aktivnosti,

postigavši dogovor o vođenju razgovora o sigurnosnim pitanjima te širenju i jačanju svoje uzajamne suradnje,

shvaćajući da dobra suradnja može zahtijevati razmjenu klasificiranih podataka između stranaka,

sporazumjele su se kako slijedi:

Članak 1.
Predmet i primjenjivost

Predmet ovog Ugovora je osiguravanje zaštite klasificiranih podataka i utvrđivanje zajedničkih postupaka i pravila za zaštitu bilo kojih klasificiranih podataka koji se razmjenjuju između stranaka i između javnih i privatnih subjekata stranaka, a koji se odnose na međunarodne poslove, nacionalnu sigurnost i obranu, kao i na industrijske aktivnosti i operacije.

Članak 2.
Definicije

Za potrebe ovog Ugovora:

1. „**klasificirani podaci**" označava bilo koji podatak, zapis, aktivnost, dokument, materijal, uključujući objekte i pravne osobe, kojima je, u skladu s nacionalnim zakonima i propisima, dodijeljen stupanj tajnosti;
2. „**nužnost pristupa podacima za obavljanje poslova iz djelokruga**" označava načelo prema kojem je pristup klasificiranim podacima omogućen samo osobama kojima je to potrebno radi obavljanja njihovih službenih poslova i zadaća;
3. „**povreda sigurnosti**" označava posljedicu činjenja ili nečinjenja suprotnog odredbi koja se odnosi na zaštitu klasificiranih podataka, koja može dovesti do gubitka povjerljivosti, cjelovitosti ili dostupnosti takvih podataka;

4. „**stupanj tajnosti**" označava kategoriju, u skladu s nacionalnim zakonima i propisima, koja obilježava važnost klasificiranih podataka, stupanj ograničenja pristupa istima i stupanj zaštite koju im pružaju stranke, o čemu se odlučuje na temelju razmjera štete uzrokovane neovlaštenim pristupom;
5. „**oznaka tajnosti**" označava oznaku na bilo kojim klasificiranim podacima, koja prikazuje stupanj tajnosti;
6. „**stranka pošiljateljica**" označava stranku koja ustupa ili dostavlja klasificirane podatke stranci primateljici;
7. „**stranka primateljica**" označava stranku kojoj se dostavljaju klasificirani podaci;
8. „**nadležno sigurnosno tijelo**" označava sigurnosno tijelo koje, u skladu s nacionalnim zakonima i propisima odnosne stranke, provodi nacionalnu strategiju zaštite klasificiranih podataka, provodi cjelokupni nadzor u tom području te prati provedbu ovog Ugovora;
9. „**ugovaratelji i podugovaratelji**" označava fizičke ili pravne osobe koje posjeduju pravnu sposobnost za sklapanje ugovora;
10. „**klasificirani ugovor**" označava ugovor između dva ili više ugovaratelja, koji će zahtijevati pristup klasificiranim podacima ili stvaranje klasificiranih podataka;
11. „**uvjerenje o sigurnosnoj provjeri osobe**" označava potvrdu izdanu od nadležnog sigurnosnog tijela, u skladu s nacionalnim zakonima i propisima, kojom se potvrđuje da je fizičkoj osobi izdano uvjerenje o sigurnosnoj provjeri za pristup odnosnom stupnju tajnosti klasificiranih podataka;
12. „**uvjerenje o sigurnosnoj provjeri pravne osobe**" označava potvrdu izdanu od nadležnog sigurnosnog tijela, u skladu s nacionalnim zakonima i propisima, kojom se potvrđuje da je pravna osoba certificirana za postupanje i rukovanje s klasificiranim podacima odnosnog stupnja tajnosti;
13. „**treća strana**" označava bilo koju državu, organizaciju i pravnu osobu koja nije stranka ovog Ugovora.

Članak 3.
Stupnjevi tajnosti

Stranke su suglasne da su sljedeći stupnjevi tajnosti istoznačni i odgovaraju stupnjevima tajnosti propisanim nacionalnim zakonima i propisima odnosne stranke:

Za Republiku Hrvatsku	Za Talijansku Republiku	Engleski prijevod
VRLO TAJNO	SEGRETISSIMO	TOP SECRET
TAJNO	SEGRETO	SECRET
POVJERLJIVO	RISERVATISSIMO	CONFIDENTIAL
OGRANIČENO	RISERVATO	RESTRICTED

Članak 4.
Nadležna sigurnosna tijela

1. Nadležna sigurnosna tijela stranaka su:

   Za Republiku Hrvatsku:
   Ured Vijeća za nacionalnu sigurnost;

   Za Talijansku Republiku:
   Dipartimento delle Informazioni per la Sicurezza (DIS)
   Ufficio Centrale per la Segretezza (UCSe).

2. Nadležna sigurnosna tijela obavješćuju jedno drugo o važećim nacionalnim zakonima i propisima koji uređuju zaštitu klasificiranih podataka i razmjenjuju podatke o sigurnosnim standardima, postupcima i praksama u svrhu zaštite klasificiranih podataka, kao i o bilo kojim mogućim naknadnim izmjenama i dopunama nacionalnih zakona i propisa koji uređuju zaštitu klasificiranih podataka te bilo kojim promjenama koje se odnose na nazive i adrese nadležnih sigurnosnih tijela.

3. Kako bi se osigurala bliska suradnja u provedbi ovog Ugovora, nadležna sigurnosna tijela mogu održavati konzultacije.

4. Stranke uzajamno priznaju uvjerenja o sigurnosnoj provjeri pravne osobe i uvjerenja o sigurnosnoj provjeri osobe izdana u skladu s nacionalnim zakonima i propisima.

5. Nadležna sigurnosna tijela osiguravaju strogo i obvezno poštivanje ovog Ugovora od strane bilo kojeg javnog i privatnog subjekta stranaka, u skladu s nacionalnim zakonima i propisima.

Članak 5.
Načela za uzajamnu zaštitu klasificiranih podataka

1. U skladu sa svojim nacionalnim zakonima i propisima, stranke provode sve odgovarajuće mjere za zaštitu klasificiranih podataka koji se razmjenjuju ili nastaju u skladu s ovim Ugovorom. Svaka stranka osigurava da se bilo kojim klasificiranim podacima druge stranke dodjeljuje isti stupanj zaštite koji za njezine klasificirane podatke zahtijevaju nacionalni zakoni i propisi.

2. Stranka ne može dostaviti trećoj strani bilo koje klasificirane podatke druge stranke, niti može smanjiti stupanj tajnosti ili deklasificirati klasificirane podatke druge stranke bez prethodnog pisanog pristanka stranke pošiljateljice.

3. Obje se stranke obvezuju da se neće pozivati na ovaj Ugovor kako bi pribavile bilo koje klasificirane podatke koje je druga stranka pribavila od treće strane.

4. Pristup klasificiranim podacima omogućava se po načelu nužnosti pristupa podacima za obavljanje poslova iz djelokruga. Uvjerenje o sigurnosnoj provjeri osobe i uvjerenje o sigurnosnoj provjeri pravne osobe izdaje se u skladu s nacionalnim zakonima i propisima stranaka.

5. Stranka primateljica:

   a) dostavlja klasificirane podatke trećoj strani samo uz prethodni pisani pristanak stranke pošiljateljice;

   b) dodjeljuje klasificiranim podacima stupanj tajnosti jednak onome koji je dodijelila stranka pošiljateljica;

   c) koristi klasificirane podatke samo za svrhe za koje su ustupljeni.

6. Načela za uzajamnu zaštitu klasificiranih podataka dogovorena između stranaka primjenjuju se u svim drugim ugovorima i sporazumima koji zahtijevaju razmjenu klasificiranih podataka između stranaka.

Članak 6.
Dostava klasificiranih podataka

1. Podaci označeni do stupnja „TAJNO/SEGRETO/SECRET" dostavljaju se diplomatskim putem ili vojnim i drugim kurirskim službama koje su odobrila nadležna sigurnosna tijela stranaka. Stranka primateljica pisano potvrđuje primitak klasificiranih podataka od stupnja „POVJERLJIVO/RISERVATISSIMO/CONFIDENTIAL" naviše. Klasificirani podaci stupnja „VRLO TAJNO/SEGRETISSIMO/TOP SECRET" salju se samo certificiranim vojnim ili diplomatskim putem. U izvanrednim situacijama stranke mogu, na temelju procjene u svakom pojedinom slučaju, dogovoriti drugačije načine dostave klasificiranih podataka.

2. Ako se treba dostaviti velika pošiljka koja sadrži klasificirane podatke, nadležna sigurnosna tijela međusobno pisano dogovaraju i odobravaju prijevozno sredstvo, rutu i sigurnosne mjere, posebno za svaki slučaj.

3. Stranke dostavljaju klasificirane podatke drugim odobrenim načinima dostave u skladu sa sigurnosnim postupcima koje su dogovorila nadležna sigurnosna tijela.

Članak 7.
Uvjerenje o sigurnosnoj provjeri osobe

1. Ako osoba za obavljanje svojih službenih poslova i zadaća ima potrebu pristupa podacima označenim „POVJERLJIVO/RISERVATISSIMO/CONFIDENTIAL" ili više, ona treba posjedovati odgovarajuće uvjerenje o sigurnosnoj provjeri osobe i treba biti odgovarajuće informirana. Stranke izdaju uvjerenje o sigurnosnoj provjeri osobe, u skladu sa svojim nacionalnim zakonima i propisima.

2. Nadležna sigurnosna tijela, na zahtjev, pomažu jedno drugom u postupku provjere u svrhu izdavanja uvjerenja o sigurnosnoj provjeri osobe.

3. Nadležna sigurnosna tijela također osiguravaju uzajamnu suradnju u vezi s mogućim zahtjevima za podacima o državljanima druge stranke koji su živjeli ili boravili na njezinom državnom području.

Članak 8.
Označavanje klasificiranih podataka

1. Stranka primateljica označava primljene klasificirane podatke u skladu s nacionalnim zakonima i propisima te istoznačnim stupnjem tajnosti, kako je određeno u članku 3. ovog Ugovora.

2. Umnoženi primjerci i prijevodi primljenih klasificiranih podataka označavaju se i s njima se postupa na isti način kao s izvornicima.

Članak 9.
Umnožavanje i prevođenje klasificiranih podataka

1. Podaci označeni kao „VRLO TAJNO/SEGRETISSIMO/TOP SECRET" prevode se ili umnožavaju samo u iznimnim slučajevima, na temelju prethodnog pisanog pristanka stranke pošiljateljice.

2. Svi umnoženi primjerci klasificiranih podataka označavaju se izvornim oznakama tajnosti. Takvi umnoženi podaci stavljaju se pod isti nadzor kao izvorni podaci. Broj umnoženih primjeraka ograničen je na broj potreban za službene svrhe.

3. Sve prijevode klasificiranih podataka od stupnja „POVJERLJIVO/RISERVATISSIMO/ CONFIDENTIAL" naviše rade osobe kojima je izdano uvjerenje o sigurnosnoj provjeri.

4. Prijevod klasificiranih podataka označava se izvornom oznakom tajnosti i ima odgovarajuću naznaku, na jeziku na koji je preveden, da prijevod sadrži klasificirane podatke stranke pošiljateljice.

Članak 10.
Uništavanje klasificiranih podataka

1. Klasificirani podaci uništavaju se na način koji otklanja mogućnost njihovog djelomičnog ili potpunog obnavljanja.

2. Podaci označeni kao „VRLO TAJNO/SEGRETISSIMO/TOP SECRET" ne uništavaju se. Oni se vraćaju stranci pošiljateljici.

3. Stranka pošiljateljica može, dodatnim označavanjem ili slanjem naknadne pisane obavijesti, izričito zabraniti umnožavanje, izmjenu ili uništavanje klasificiranih podataka. Ako je uništavanje klasificiranih podataka zabranjeno, oni se vraćaju stranci pošiljateljici.

4. U slučaju nužde, klasificirani podaci koje je nemoguće zaštititi ili vratiti stranci pošiljateljici odmah se uništavaju. Stranka primateljica pisano obavješćuje stranku pošiljateljicu samo o uništavanju podataka označenih kao „VRLO TAJNO/SEGRETISSIMO/TOP SECRET".

Članak 11.
Klasificirani ugovori

1. Ugovaratelji i podugovaratelji koji sudjeluju u pregovorima i provedbi klasificiranih ugovora posjeduju odgovarajuće uvjerenje o sigurnosnoj provjeri pravne osobe stupnja koji je potreban za ugovor, kako bi se osigurala zaštita klasificiranih podataka.

2. U slučaju da javni ili privatni subjekt jedne stranke, koji posjeduje odgovarajuće uvjerenje o sigurnosnoj provjeri, dobije ugovor koji se treba provesti unutar državnih granica druge stranke, a taj ugovor u ključuje razmjenu klasificiranih podataka, stranka kod koje se ugovor treba provesti poduzima odgovarajuće sigurnosne mjere zaštite klasificiranih podataka, u skladu s nacionalnim zakonima i propisima.

3. Klasificirani ugovori sklapaju se i provode u skladu s nacionalnim zakonima i propisima svake stranke. Na zahtjev, nadležno sigurnosno tijelo svake stranke potvrđuje da je predloženom ugovaratelju izdano odgovarajuće nacionalno uvjerenje o sigurnosnoj provjeri pravne osobe.

4. Sigurnosni dodatak sastavni je dio svakog klasificiranog ugovora ili podugovora kojim ugovaratelj stranke pošiljateljice pobliže određuje koji će se klasificirani podaci ustupiti stranci primateljici i koji je stupanj tajnosti dodijeljen tim podacima.

5. Obveze ugovaratelja u vezi sa zaštitom klasificiranih podataka odnose se, najmanje, na sljedeće:

   a) ustupanje klasificiranih podataka isključivo osobama kojima je prethodno izdano odgovarajuće uvjerenje o sigurnosnoj provjeri osobe, kod kojih postoji nužnost pristupa podacima za obavljanje poslova iz djelokruga i koje su uključene u provedbu klasificiranog ugovora;

   b) dostavu klasificiranih podataka na način koji je u skladu s odredbama ovog Ugovora;

   c) postupke i mehanizme obavješćivanja o bilo kojim promjenama koje mogu nastupiti u vezi s klasificiranim podacima;

   d) korištenje klasificiranih podataka u skladu s klasificiranim ugovorom samo za svrhe vezane uz predmet ugovora;

   e) strogo poštivanje odredaba ovog Ugovora u vezi s postupcima za postupanje s klasificiranim podacima;

   f) obvezu obavješćivanja nadležnog sigurnosnog tijela ugovaratelja o bilo kojem stvarnom neovlaštenom pristupu klasificiranim podacima vezanim uz klasificirani ugovor i o svakom pokušaju ili sumnji u isti, u skladu s odredbama ovog Ugovora;

   g) ustupanje klasificiranih podataka vezanih uz klasificirani ugovor bilo kojoj trećoj strani samo uz prethodni pisani pristanak stranke pošiljateljice.

6. Mjere potrebne za zaštitu klasificiranih podataka, kao i postupak procjene u vezi s bilo kakvom odštetom za moguće gubitke koje ugovarateljima izazove neovlašteni pristup klasificiranim podacima, pobliže se određuju u odnosnom klasificiranom ugovoru.

7. Klasificirani ugovori stupnja tajnosti „OGRANIČENO/RISERVATO/RESTRICTED" sadrže odgovarajuću sigurnosnu klauzulu kojom se naznačuju minimalne sigurnosne mjere koje treba primijeniti za zaštitu klasificiranih podataka. Za takve ugovore, ugovaratelje se sigurnosno informira u skladu s nacionalnim zakonima i propisima.

Članak 12.
Posjeti

1. Posjeti državljana jedne stranke državnim tijelima ili pravnim osobama druge stranke, kojima je potreban pristup klasificiranim podacima, podliježu prethodnom pisanom ovlaštenju nadležnog sigurnosnog tijela stranke kod koje se posjet odvija.

2. Zahtjev za posjet dostavlja se najmanje 20 dana prije zakazanog datuma. U slučaju izuzetno važnih i žurnih posjeta, koji nisu unaprijed zakazani, zahtjev za posjet dostavlja se najmanje 5 dana prije posjeta.

3. Zaposlenici jedne od stranaka, koji službeno traže posjet drugoj stranci, u skladu s ovim Ugovorom:

   a) ovlašteni su za primanje klasificiranih podataka ili pristup klasificiranim podacima, po načelu nužnosti pristupa podacima za obavljanje poslova iz djelokruga, i

   b) trebaju posjedovati uvjerenje o sigurnosnoj provjeri osobe, najmanje jednakog stupnja tajnosti kao podaci kojima se treba pristupiti.

4. Zahtjev za posjet iz stavka 2. ovog članka sadrži:

   a) ime i prezime posjetitelja, datum i mjesto rođenja, državljanstvo;

   b) broj putovnice ili broj identifikacijske iskaznice posjetitelja;

   c) radno mjesto posjetitelja i naziv organizacije koju predstavlja;

d) odgovarajuću potvrdu o sigurnosnoj provjeri, na temelju uvjerenja o sigurnosnoj provjeri posjetitelja, ako je potrebno;

e) naznaku o stupnju tajnosti podataka kojima se treba pristupiti;

f) naznaku o kontakt osobi u javnom ili privatnom subjektu koji se posjećuje, uključujući ime i prezime, adresu elektroničke pošte i broj telefona;

g) svrhu i planirani datum posjeta;

h) nazive organizacija i državnih tijela ili pravnih osoba koje se posjećuje;

i) broj posjeta i traženo razdoblje;

j) ostale podatke, ako su ih dogovorila nadležna sigurnosna tijela.

5. Nadležno sigurnosno tijelo stranke domaćina obavješćuje nadležno sigurnosno tijelo druge stranke o svojoj odluci, na dogovoreni način, dovoljno unaprijed s obzirom na zakazani datum posjeta.

6. Posjeti zaposlenika javnog ili privatnog subjekta jedne od stranaka do stupnja „OGRANIČENO/RISERVATO/RESTRICTED" dogovaraju se izravno s javnim ili privatnim subjektom druge stranke. Javni ili privatni subjekt koji je domaćin obavješćuje svoje nadležno sigurnosno tijelo o posjetu.

7. U slučaju projekata ili ugovora koji zahtijevaju ponovljene posjete, a označeni su kao „POVJERLJIVO/RISERVATISSIMO/CONFIDENTIAL" i više, nadležna sigurnosna tijela stranaka obavješćuju jedno drugo slanjem popisa ovlaštenih zaposlenika. Takav popis ne može važiti dulje od 12 mjeseci.

8. Nadležno sigurnosno tijelo stranke domaćina, na zahtjev nadležnog sigurnosnog tijela stranke posjetitelja, posjetiteljima omogućuje pristup klasificiranim podacima ili prostorima gdje se postupa s klasificiranim podacima, u skladu s nacionalnim zakonima i propisima.

9. Svaka stranka jamči zaštitu osobnih podataka posjetitelja u skladu sa svojim nacionalnim zakonima i propisima.

Članak 13.
Povreda sigurnosti

1. U slučaju stvarne povrede sigurnosti ili sumnje u povredu sigurnosti, nadležno sigurnosno tijelo stranke kod koje se ona dogodila bez odgode obavješćuje stranku pošiljateljicu i, u skladu s nacionalnim zakonima i propisima, pokreće odgovarajući postupak, kako bi se utvrdile okolnosti povrede. Rezultati postupka, kao i popratnih provedenih mjera, dostavljaju se stranci pošiljateljici.

2. Kada se povreda sigurnosti dogodi kod treće strane, nadležno sigurnosno tijelo stranke pošiljateljice, ako je moguće, bez odgode poduzima radnje iz stavka 1. ovog članka.

Članak 14.
Troškovi

1. Provedba ovog Ugovora ne uključuje nikakve troškove.

2. U slučaju da troškove prouzroči jedna stranka, njih ne podmiruje druga stranka.

Članak 15.
Rješavanje sporova

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

2. U međuvremenu, stranke nastavljaju ispunjavati odredbe navedene u ovom Ugovoru.

Članak 16.
Završne odredbe

1. Ovaj Ugovor stupa na snagu datumom primitka posljednje pisane obavijesti kojom stranke obavješćuju jedna drugu, diplomatskim putem, da su ispunjeni njihovi unutarnji pravni uvjeti potrebni za njegovo stupanje na snagu.

2. Ovaj Ugovor može se izmijeniti i dopuniti uzajamnim pisanim pristankom stranaka. Izmjene i dopune stupaju na snagu u skladu s odredbom stavka 1. ovog članka.

3. Ovaj Ugovor sklapa se na neodređeno vrijeme. Svaka od stranaka može otkazati ovaj Ugovor pisanom obaviješću drugoj stranci, diplomatskim putem. U tom slučaju, ovaj Ugovor prestaje šest (6) mjeseci nakon datuma na koji je druga stranka primila obavijest o otkazu.

4. U slučaju prestanka ovog Ugovora, svi klasificirani podaci dostavljeni u skladu s ovim Ugovorom nastavljaju se štititi u skladu s ovdje sadržanim odredbama.

Sastavljeno u Zagrebu dana 9. srpnja 2019. u dva izvornika, svaki na hrvatskom, talijanskom i engleskom jeziku, pri čemu su svi tekstovi jednako vjerodostojni. U slučaju razlika u tumačenju, mjerodavan je engleski tekst.

ZA VLADU
REPUBLIKE HRVATSKE

ZA VLADU
TALIJANSKE REPUBLIKE

[ENGLISH TEXT – TEXTE ANGLAIS]

AGREEMENT
BETWEEN
THE GOVERNMENT OF THE REPUBLIC OF CROATIA
AND
THE GOVERNMENT OF THE ITALIAN REPUBLIC
ON EXCHANGE AND MUTUAL PROTECTION OF CLASSIFIED INFORMATION

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

Recognising the important role of their mutual co-operation for the stabilisation of peace, international security and mutual confidence,

Recognising the interest and the common necessity to ensure the protection of any Classified Information in the political, security, military, economic and any other field exchanged between the Parties and their public and private entities, in accordance with the laws and regulations of the Parties,

Recognising the need to establish common security regulations for the safeguarding of information, also in relation to the possibility of implementing technical cooperation agreements and developing contractual activities,

Having agreed to hold talks on security related issues and to broaden and tighten their mutual co-operation,

Realising that good co-operation may require exchange of Classified Information between the Parties,

Have agreed as follows:

Article 1
Objective and Applicability

The objective of this Agreement is to ensure protection of Classified Information and to establish common procedures and rules for the protection of any Classified Information exchanged between the Parties and between the public and private entities of the Parties concerning international affairs, national security and defence, as well as industrial activities and operations.

Article 2
Definitions

For the purposes of this Agreement:

1. "**Classified Information**" means any information, record, activity, document, material, including objects and facilities, that a security classification level has been assigned to in accordance with the national laws and regulations;
2. "**Need-to-know**" means the principle upon which access to Classified Information is authorized only to individuals in relation to their need to perform their official functions and duties;
3. "**Breach of Security**" means the consequence of actions or omissions contrary to a provision concerning the protection of Classified Information that may result in a loss of confidentiality, integrity or availability of such information;

4. "**Security classification level**" means the category, in accordance with the national laws and regulations, which characterises the importance of Classified Information, level of restriction of access to it and level of its protection by the Parties, decided on the basis of the extent of the damage caused by an unauthorized access;
5. "**Classification marking**" means a mark on any Classified Information, which shows the security classification level;
6. "**Originating Party**" means the Party that originates or transmits the Classified Information to the Receiving Party;
7. "**Receiving Party**" means the Party to which Classified Information is transmitted;
8. "**Competent Security Authority**" means the security authority which, in accordance with the national laws and regulations of the respective Party, performs the national policy for the protection of Classified Information, exercises overall control in this sphere as well as conducts the implementation of this Agreement;
9. "**Contractors and Subcontractors**" means individuals or legal entities possessing the legal capacity to conclude contracts;
10. "**Classified Contract**" means an agreement between two or more Contractors, that will require access to or generation of Classified Information;
11. "**Personnel Security Clearance Certificate**" means a positive determination granted by the Competent Security Authority in accordance with the national laws and regulations, confirming that the individual is security cleared for access to the respective level of Classified Information;
12. **"Facility Security Clearance Certificate"** means a positive determination granted by the Competent Security Authority in accordance with the national laws and regulations, confirming that the legal entity is certified to handle and manage Classified Information to the respective level of classification;
13. "**Third Party**" means any State, organization and legal entity which is not a party to this Agreement.

Article 3
Security Classification Levels

The Parties agree that the following security classification levels are equivalent and correspond to the security classification levels prescribed by the national laws and regulations of the respective Party:

For the Republic of Croatia	For the Italian Republic	English translation
VRLO TAJNO	SEGRETISSIMO	TOP SECRET
TAJNO	SEGRETO	SECRET
POVJERLJIVO	RISERVATISSIMO	CONFIDENTIAL
OGRANIČENO	RISERVATO	RESTRICTED

Article 4
Competent Security Authorities

1. The Competent Security Authorities of the Parties are:

   For the Republic of Croatia:
   Ured Vijeca za nacionalnu sigurnost;

   For the Italian Republic:
   Dipartimento delle Informazioni per la Sicurezza (DIS)
   Ufficio Centrale per la Segretezza (UCSe).

2. The Competent Security Authorities shall inform each other of the national laws and regulations in force regulating the protection of Classified Information and shall exchange information about the security standards, procedures and practices for the protection of Classified Information, as well as on any subsequent possible amendment to the national laws and regulations which govern the protection of Classified Information and any changes concerning the names and addresses of the Competent Security Authorities.

3. In order to ensure close co-operation in the implementation of this Agreement, the Competent Security Authorities may hold consultations.

4. The Parties shall mutually recognize the Facility and Personnel Security Clearance Certificates, released in accordance with the national laws and regulations.

5. The Competent Security Authorities shall ensure a strict and binding adherence to this Agreement by any public and private entity of the Parties, in accordance with national laws and regulations.

Article 5
Principles for the Mutual Protection of Classified Information

1. In accordance with their national laws and regulations, the Parties shall implement all appropriate measures for the protection of Classified Information which is exchanged or generated under this Agreement. Each Party shall ensure that any Classified Information of the other Party is assigned the same level of protection required by national laws and regulations for its Classified Information.

2. The Party cannot release to a Third Party any Classified Information of the other Party, nor downgrade or declassify the security classification level of Classified Information of the other Party, without the prior written consent of the Originating Party.

3. Both Parties are committed not to appeal to this Agreement to obtain any Classified Information which the other Party has obtained by a Third Party.

4. Access to Classified Information shall be granted on the basis of the need-to-know principle. Personnel Security Clearance Certificate and Facility Security Clearance Certificate shall be issued in accordance with the national laws and regulations of the Parties.

5. The Receiving Party shall:

   a) submit Classified Information to a Third Party only upon prior written consent of the Originating Party;

   b) grant Classified Information a security classification level equivalent to that provided by the Originating Party;

   c) use Classified Information only for the purposes it has been provided for.

6. Principles for the mutual protection of Classified Information agreed between the Parties shall be applied in all other agreements and arrangements entailing the exchange of Classified Information between the Parties.

Article 6
Transmission of Classified Information

1. Information classified up to "TAJNO/SEGRETO/SECRET" level shall be transmitted through diplomatic channels or by military and other courier services approved by the Competent Security Authorities of the Parties. The Receiving Party shall confirm the receipt of Classified Information in writing from "POVJERLJIVO/RISERVATISSIMO/CONFIDENTIAL" level and above. Classified Information "VRLO TAJNO/SEGRETISSIMO/TOP SECRET" shall be sent only through certified military or diplomatic channels. In case of emergency, the Parties may arrange, on a case by case evaluation, different modalities of transmission of Classified Information.

2. If a large consignment, containing Classified Information, is to be transmitted, the Competent Security Authorities shall mutually agree and approve in writing the means of transportation, the route and security measures on case-by-case basis.

3. The Parties shall transmit Classified Information by other approved means of transmission in accordance with the security procedures agreed upon by the Competent Security Authorities.

Article 7
Personnel Security Clearance Certificate

1. If an individual needs access to information classified as "POVJERLJIVO/RISERVATISSIMO/ CONFIDENTIAL" or above, to perform his/her official functions and duties, he/she shall hold an appropriate Personnel Security Clearance Certificate and need to be briefed accordingly. The Parties shall grant a Personnel Security Clearance Certificate, in compliance with their national laws and regulations.

2. The Competent Security Authorities shall assist each other, on request, during the vetting procedure for the release of Personnel Security Clearance Certificate.

3. The Competent Security Authorities shall also ensure mutual cooperation for possible requests for information on citizens of the other Party who lived or stayed in its territory.

Article 8
Marking of Classified Information

1. The Receiving Party shall mark the received Classified Information in accordance with the national laws and regulations and with the equivalent security classification level as defined in Article 3 of this Agreement.

2. Copies and translations of the received Classified Information shall be marked and handled in the same manner as the originals.

Article 9
Reproduction and Translation of Classified Information

1. Information classified as "VRLO TAJNO/SEGRETISSIMO/TOP SECRET" shall be translated or reproduced only in exceptional cases upon prior written consent of the Originating Party.

2. All reproduced copies of Classified Information shall be marked with the original classification marking. Such reproduced information shall be placed under the same control as the original information. The number of copies shall be restricted to that required for official purposes.

3. All translations of Classified Information from "POVJERLJIVO/RISERVATISSIMO/ CONFIDENTIAL" level and above shall be made by security cleared individuals.

4. The translation of Classified Information shall be marked with the original classification marking and shall bear an appropriate note in the language into which it is translated that the translation contains Classified Information of the Originating Party.

Article 10
Destruction of Classified Information

1. Classified Information shall be destroyed in such a manner as to eliminate the possibility of its partial or total reconstruction.

2. Information classified as "VRLO TAJNO/SEGRETISSIMO/TOP SECRET" shall not be destroyed. It shall be returned to the Originating Party.

3. The Originating Party may by additional marking or sending subsequent written notice expressly prohibit reproduction, alteration or destruction of Classified Information. If destruction of Classified Information is prohibited, it shall be returned to the Originating Party.

4. In case of an emergency, Classified Information, impossible to be protected or returned to the Originating Party, shall be destroyed immediately. The Receiving Party shall notify the Originating Party in writing only about the destruction of information classified as "VRLO TAJNO/SEGRETISSIMO/TOP SECRET".

Article 11
Classified Contracts

1. Contractors and Subcontractors which participate in negotiation and performing of classified contracts shall hold an appropriate Facility Security Clearance Certificate to the level required for the contract, to ensure the protection of Classified Information.

2. In the event that a public or private entity of one Party, duly cleared, awarded a contract to be performed within the national borders of the other Party, and such contract includes the exchange of Classified Information, the Party where the contract is to be performed, shall take appropriate security measures for the protection of Classified Information, in accordance with the national laws and regulations.

3. Classified Contracts shall be concluded and implemented in accordance with the national laws and regulations of each Party. Upon request the Competent Security Authority of each Party shall confirm that a proposed Contractor has been granted an appropriate national Facility Security Clearance Certificate.

4. A security annex shall be an integral part of each Classified Contract or sub-contract by which the Contractor of the Originating Party shall specify which Classified Information is to be released to the Receiving Party, and which security classification level has been assigned to this information.

5. The Contractor's obligations to protect the Classified Information shall refer, at least, to the following:

   a) release of Classified Information exclusively to persons who have been previously granted the appropriate Personnel Security Clearance Certificate, who have "need-to-know" and who are engaged in the carrying out of the Classified Contract;

   b) transmission of Classified Information by the means in accordance with the provisions of this Agreement;

   c) the procedures and mechanisms for communicating any changes that may arise in respect of Classified Information;

   d) usage of Classified Information under the Classified Contract only for the purposes related to the subject of the contract;

   e) strict adherence to the provisions of this Agreement related to the procedures for handling of Classified Information;

   f) the obligation to notify the Contractor's Competent Security Authority of any actual, attempted or suspected unauthorised access to Classified Information related to the Classified Contract in accordance with the provisions of this Agreement;

   g) release of Classified Information related to the Classified Contract to any Third Party only with the prior written consent of the Originating Party.

6. The measures required for the protection of Classified Information, as well as the procedure for assessment of any indemnification for possible losses caused to the Contractors by unauthorised access to Classified Information, shall be specified in more detail in the respective Classified Contract.

7. Classified Contracts of security classification level "OGRANIČENO/RISERVATO/ RESTRICTED" shall contain an appropriate security clause identifying the minimum security measures to be applied for the protection of Classified Information. For such contracts the Contractors shall be security briefed in accordance with the national laws and regulations.

Article 12
Visits

1. Visits carried out by citizens of one Party to facilities of the other Party, who need access to Classified Information, shall be submitted to prior written authorization by the Competent Security Authority of the Party where the visit takes place.

2. Request for visit shall be forwarded at least 20 days in advance of the scheduled date. In case of visits of utmost importance and urgency and not previously scheduled, the request for visit shall be forwarded at least 5 days before the visit takes place.

3. Personnel of one of the Parties, making an official request for visit to the other Party, pursuant to this Agreement shall:

   a) be authorized to receive or access to Classified Information according to the need-to-know principle, and

   b) hold a Personnel Security Clearance Certificate, at least equal to the classification level of the information which needs to be accessed to.

4. The request for visit referred to in paragraph 2 of this Article shall include:

   a) visitor's name and surname, date and place of birth, citizenship;

   b) passport number or identification card number of the visitor;

   c) position of the visitor and name of the organisation represented;

d) appropriate security clearance assurance on the basis of the Personnel Security Clearance Certificate of the visitor, if necessary;

e) indication of the security classification level of the information that needs to be accessed to;

f) indication of the point of contact at the public or private entity to be visited, including name and surname, e-mail address and telephone number;

g) purpose and planned date of the visit;

h) names of organisations and facilities to be visited;

i) number of visits and period required;

j) other data, if agreed upon by the Competent Security Authorities.

5. The Competent Security Authority of the host Party notifies the Competent Security Authority of the other Party, through the channels agreed, about its decision, with sufficient advance in respect of the scheduled date for visit.

6. Visits of personnel of the public or private entity of one of the Parties up to the level "OGRANIČENO/RISERVATO/RESTRICTED" shall be agreed directly with the public or private entity of the other Party. The hosting public or private entity shall notify its Competent Security Authority about the visit.

7. In case of projects or contracts which require recurring visits classified as "POVJERLJIVO/RISERVATISSIMO/CONFIDENTIAL" and above, the Competent Security Authorities of the Parties shall notify each other by sending a list of authorized personnel. Such list can not be valid more than 12 months.

8. The Competent Security Authority of the host Party shall, upon request of the Competent Security Authority of the visiting Party, allow access to Classified Information or to premises where Classified Information is handled to the visitors in accordance with the national laws and regulations.

9. Each Party shall guarantee the protection of personal data of the visitors in accordance with its national laws and regulations.

Article 13
Breach of Security

1. In case of actual or suspected Breach of Security, the Competent Security Authority of the Party where it has occurred shall, without delay, inform the Originating Party and, in accordance with the national laws and regulations, initiate appropriate proceedings, in order to determine the circumstances of the breach. The results of the proceedings as well as the following measures adopted shall be forwarded to the Originating Party.

2. When the Breach of Security has occurred in a Third Party, the Competent Security Authority of the sending Party, if possible, shall take the actions referred to in paragraph 1 of this Article without delay.

Article 14
Expenses

1. The implementation of this Agreement does not include any cost.

2. In the event of costs incurred by one Party, these shall not be supported by the other Party.

Article 15
Settlement of Disputes

1. Any dispute regarding the interpretation or implementation of this Agreement shall be settled by consultations and negotiations between the Parties.

2. Meanwhile, the Parties shall continue to fulfil the provisions set forth in this Agreement.

Article 16
Final Provisions

1. This Agreement shall enter into force on the date of receipt of the last written notification by which the Parties have informed each other, through diplomatic channels, that their internal legal requirements necessary for its entry into force have been fulfilled.

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

3. This Agreement is concluded for an indefinite period of time. Each of the Parties may denounce this Agreement by giving the other Party notice in writing through diplomatic channels. In that case, this Agreement shall terminate six (6) months after the date on which the other Party has received the denunciation notice.

4. In case of termination of this Agreement, all Classified Information transmitted pursuant to this Agreement shall continue to be protected in accordance with the provisions set forth herein.

Done at Zagreb on 9 July 2019 in two originals, each in the Croatian, Italian 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 GOVERNMENT OF THE ITALIAN REPUBLIC

[ITALIAN TEXT – TEXTE ITALIEN]

ACCORDO

TRA

IL GOVERNO DELLA REPUBBLICA DI CROAZIA

ED

IL GOVERNO DELLA REPUBBLICA ITALIANA

PER LO SCAMBIO E LA RECIPROCA PROTEZIONE DELLE INFORMAZIONI CLASSIFICATE

Il Governo della Repubblica di Croazia ed il Governo della Repubblica Italiana (di seguito denominate "le Parti"),

Riconoscendo l'importante ruolo della loro reciproca cooperazione per il consolidamento della pace, della sicurezza internazionale e della reciproca fiducia,

Riconoscendo l'interesse e la comune necessità di assicurare la protezione di ogni Informazione Classificata scambiata nei settori politico, di sicurezza, militare, economico ed in ogni altro settore tra le Parti e tra i relativi enti pubblici e privati, in conformità con le leggi ed i regolamenti delle Parti,

Riconoscendo la necessità di stabilire comuni regole di sicurezza per la salvaguardia delle informazioni, anche in relazione alla possibilità di attuare accordi di cooperazione tecnica e di sviluppare attività contrattuali,

Avendo convenuto di avviare un dialogo sulle tematiche di sicurezza e di sviluppare e rafforzare la loro reciproca collaborazione,

Riconoscendo che una buona cooperazione può richiedere scambio di Informazioni Classificate tra le Parti,

Hanno concordato quanto segue:

Articolo 1
Scopo e applicabilità

L'obiettivo di questo Accordo è di assicurare la protezione delle Informazioni Classificate e stabilire comuni procedure e regole per la protezione di ciascuna Informazione Classificata scambiata tra le Parti e tra Enti pubblici e privati delle Parti, riguardante affari internazionali, sicurezza nazionale e difesa, nonché attività e operazioni industriali.

Articolo 2
Definizioni

Per gli scopi di questo Accordo:

1. "**Informazione Classificata**" indica ogni informazione, atto, attività, documento, materiale inclusi oggetti e infrastrutture cui è stato assegnato un livello di classifica di segretezza in conformità con le leggi ed i regolamenti nazionali;
2. **"Necessità di conoscere"** indica il principio secondo il quale l'accesso alle Informazioni Classificate è consentito soltanto ad individui in relazione alla loro necessità di svolgere le loro funzioni ed incarichi ufficiali;
3. "**Violazione di Sicurezza**" indica la conseguenza di azioni o di omissioni contrarie a una disposizione relativa alla protezione delle Informazioni Classificate dalle quali può derivare una perdita di riservatezza, integrità o disponibilità di tali informazioni;

4. "**Livello di classifica di segretezza**" indica la categoria, in conformità con le leggi ed i regolamenti nazionali, che contraddistingue la rilevanza dell'informazione classificata, il livello di restrizione di accesso alla stessa ed il livello di protezione assegnato dalle Parti sulla base dell'entità del danno causato da un accesso non autorizzato;
5. "**Contrassegno di classifica**" indica un contrassegno apposto su ogni informazione classificata che ne attesta il livello di classifica di segretezza;
6. "**Parte Originatrice**" indica la Parte che origina o trasmette le Informazioni Classificate alla Parte Ricevente;
7. "**Parte Ricevente**" indica la Parte alla quale l'Informazione Classificata è trasmessa;
8. "**Autorità Competente per la Sicurezza**" indica l'autorità di sicurezza, che, in conformità con le leggi ed i regolamenti nazionali delle Parti, attua la politica nazionale per la protezione delle Informazioni Classificate, esercita un generale controllo in questo ambito e cura l'attuazione del presente Accordo;
9. "**Contraenti e Subcontraenti**" indica persone fisiche o giuridiche in possesso della capacità legale di concludere contratti;
10. "**Contratto Classificato**" indica un accordo tra due o più Contraenti che richiede l'accesso o la produzione di Informazioni Classificate;
11. "**Certificato di Abilitazione di Sicurezza Personale**" indica una positiva determinazione adottata dall'Autorità Competente per la Sicurezza, in conformità con le leggi ed i regolamenti nazionali, attestante che l'individuo è abilitato all'accesso al corrispondente livello di Informazione Classificata;
12. "**Certificato di Abilitazione di Sicurezza Industriale**" indica una positiva determinazione adottata dall'Autorità Competente per la Sicurezza, in conformità con le leggi ed i regolamenti nazionali, attestante che la persona giuridica è abilitata a gestire e trattare l'Informazione Classificata al corrispondente livello di classifica;
13. "**Parte Terza**" indica qualsiasi Stato, Organizzazione e persona giuridica che non è parte di questo Accordo.

Articolo 3
Livelli di Classifica di Segretezza

Le Parti concordano che i seguenti livelli di classifica di segretezza sono equivalenti e corrispondono ai livelli di classifica di segretezza contemplati dalle leggi e dai regolamenti nazionali delle rispettive Parti:

Per la Repubblica di Croazia	Per la Repubblica Italiana	Equivalente in inglese
VRLO TAJNO	SEGRETISSIMO	TOP SECRET
TAJNO	SEGRETO	SECRET
POVJERLJIVO	RISERVATISSIMO	CONFIDENTIAL
OGRANIČENO	RISERVATO	RESTRICTED

Articolo 4
Autorità Competenti per la Sicurezza

1. Le Autorità Competenti per la Sicurezza delle Parti sono:

   Per la Repubblica di Croazia:
   Ured Vijeća za nacionalnu sigurnost;

   Per la Repubblica Italiana:
   Dipartimento delle Informazioni per la Sicurezza (DIS)
   Ufficio Centrale per la Segretezza (UCSe).

2. Le Autorità Competenti per la Sicurezza si informano reciprocamente in merito alle leggi e ai regolamenti nazionali in vigore che disciplinano la protezione delle Informazioni Classificate e si scambiano informazioni inerenti le norme, le procedure e le prassi di sicurezza per la protezione delle Informazioni Classificate, ogni eventuale successivo emendamento alle leggi ed ai regolamenti nazionali che disciplinano la protezione delle Informazioni Classificate nonché le modifiche relative ai nomi ed agli indirizzi delle Competenti Autorità per la Sicurezza.

3. Allo scopo di assicurare una stretta cooperazione nell'attuazione del presente Accordo, le Autorità Competenti per la Sicurezza possono avviare delle consultazioni.

4. Le Parti riconoscono reciprocamente i Certificati di Abilitazione di Sicurezza Industriale e Personale, rilasciati in conformità con le leggi ed i regolamenti nazionali.

5. Le Autorità Competenti per la Sicurezza assicurano una rigorosa e vincolante osservanza di questo Accordo da parte di ogni ente pubblico o privato delle Parti, in conformità con le leggi ed i regolamenti nazionali.

Articolo 5
Principi sulla Reciproca Protezione delle Informazioni Classificate

1. In conformità con le leggi ed i regolamenti nazionali, le Parti applicano tutte le misure necessarie per la protezione delle Informazioni Classificate generate o scambiate in applicazione del presente Accordo. Ogni Parte assicura che ad ogni Informazione Classificata dell'altra Parte è assegnato lo stesso livello di protezione previsto dalle leggi e dai regolamenti nazionali per le proprie Informazioni Classificate.

2. Una Parte non può rilasciare ad una Parte Terza alcuna Informazione Classificata dell'altra Parte, né ridurre o eliminare il livello di classifica di segretezza dell'informazione classificata dell'altra Parte, senza il preventivo consenso scritto della Parte Originatrice.

3. Entrambe le Parti si impegnano a non invocare questo Accordo al fine di ottenere Informazioni Classificate che l'altra Parte ha ricevuto da una Parte Terza.

4. L'accesso alle Informazioni Classificate è assicurato sulla base del principio della "necessità di conoscere". Il Certificato di Abilitazione di Sicurezza Personale e il Certificato di Abilitazione di Sicurezza Industriale sono rilasciati in conformità con le leggi ed i regolamenti nazionali delle Parti.

5. La Parte Ricevente deve:

   a) cedere Informazioni Classificate a Parti Terze solo previo consenso scritto della Parte Originatrice;

   b) assicurare all'Informazione Classificata un livello di classifica di segretezza equivalente a quello assegnato dalla Parte Originatrice;

   c) utilizzare l'Informazione Classificata solo per gli scopi per cui è stata rilasciata.

6. I principi per la reciproca protezione delle Informazioni Classificate concordati tra le Parti devono essere applicati in tutti gli altri accordi e intese, che implicano lo scambio di Informazioni Classificate tra le Parti.

Articolo 6
Trasmissione di Informazioni Classificate

1. Le informazioni classificate fino al livello "TAJNO/SEGRETO/SECRET" sono trasmesse attraverso canali diplomatici o militari e altri servizi di corrieri approvati dalle Competenti Autorità per la Sicurezza delle Parti. La Parte Ricevente conferma la ricezione dell'Informazione Classificata per iscritto dal livello "POVJERLJIVO/ RISERVATISSIMO/CONFIDENTIAL" e superiore. L'Informazione Classificata "VRLO TAJNO/SEGRETISSIMO/TOP SECRET", deve essere trasmessa solo attraverso canali diplomatici o militari certificati. In caso di emergenza, le Parti possono concordare, valutando caso per caso, differenti modalità di trasmissione delle Informazioni Classificate.

2. In caso debba essere effettuata una consegna di grande volume, contenente Informazioni Classificate, le Competenti Autorità Nazionali per la Sicurezza concordano reciprocamente e approvano per iscritto, caso per caso, i mezzi di trasporto, il percorso e le misure di sicurezza.

3. Le Parti trasmettono Informazioni Classificate tramite altri sistemi di trasmissioni approvati in conformità con le procedure di sicurezza concordate tra le Competenti Autorità Nazionali per la Sicurezza.

Articolo 7
Certificato di Abilitazione di Sicurezza Personale

1. Se un individuo ha necessità di accedere ad Informazioni Classificate di livello "POVJERLJIVO/RISERVATISSIMO/CONFIDENTIAL" o superiore, per svolgere i propri incarichi e funzioni, lo stesso deve essere in possesso di una appropriata Certificazione di Abilitazione di Sicurezza Personale e deve essere stato adeguatamente istruito. Le Parti rilasciano un Certificato di Abilitazione di Sicurezza Personale, in conformità con le leggi ed i regolamenti nazionali.

2. Le Competenti Autorità per la Sicurezza, su richiesta, si prestano reciproca assistenza durante le procedure di investigazione finalizzate al rilascio di Certificati di Abilitazione di Sicurezza Personale.

3. Le Competenti Autorità per la Sicurezza devono anche assicurare una reciproca cooperazione per eventuali richieste di informazioni su cittadini dell'altra Parte che hanno vissuto o soggiornato sul proprio territorio.

Articolo 8
Contrassegno delle Informazioni Classificate

1. La Parte ricevente contrassegna l'Informazione Classificata ricevuta in conformità con le leggi ed i regolamenti nazionali con il livello di classifica di segretezza equivalente così come previsto nell'articolo 3 di questo Accordo.

2. Le copie e le traduzioni delle Informazioni Classificate ricevute devono essere contrassegnate e trattate allo stesso modo degli originali.

Articolo 9
Riproduzione e traduzione delle Informazioni Classificate

1. Le Informazioni Classificate di livello "VRLO TAJNO/SEGRETISSIMO/TOP SECRET" devono essere tradotte o riprodotte solo in casi eccezionali previo consenso scritto della Parte Originatrice.

2. Tutte le copie riprodotte di Informazioni Classificate devono essere contrassegnate con il livello di classifica originale. Tali informazioni riprodotte devono essere sottoposte allo stesso tipo di controllo previsto per l'informazione originale. Il numero di copie deve essere limitato a quello richiesto per gli scopi ufficiali.

3. Tutte le traduzioni di Informazioni Classificate di livello "POVJERLJIVO/RISERVATISSIMO/ CONFIDENTIAL" e superiore devono essere eseguite da persone in possesso di una abilitazione di sicurezza.

4. La traduzione di Informazioni Classificate deve essere contrassegnata con il livello originale di classifica e deve recare un'appropriata nota nella lingua di traduzione, attestante che la traduzione contiene Informazioni Classificate della Parte Originatrice.

Articolo 10
Distruzione di Informazioni Classificate

1. L'Informazione Classificata deve essere distrutta in modo da eliminare la possibilità di una sua parziale o totale ricostruzione.

2. L'Informazione Classificata di livello "VRLO TAJNO/SEGRETISSIMO/TOP SECRET" non deve essere distrutta. Essa deve essere restituita alla Parte Originatrice.

3. La Parte Originatrice può espressamente proibire, attraverso contrassegni addizionali o attraverso l'invio successivo di nota scritta, la riproduzione, la modifica o la distruzione delle Informazioni Classificate. Se la distruzione dell'Informazione Classificata è proibita, la stessa deve essere riconsegnata alla Parte Originatrice.

4. In caso di emergenza le Informazioni Classificate che non possono essere protette o riconsegnate alla Parte Originatrice devono essere distrutte immediatamente. La Parte Ricevente deve notificare per iscritto alla Parte Originatrice solo la distruzione dell'Informazione Classificata di livello "VRLO TAJNO/SEGRETISSIMO/TOP SECRET".

Articolo 11
Contratti classificati

1. I Contraenti e Subcontraenti che partecipano alla negoziazione e all'esecuzione di contratti classificati devono essere in possesso di un'adeguata Abilitazione di Sicurezza Industriale del livello richiesto per il contratto, allo scopo di assicurare la protezione delle Informazioni Classificate.

2. Nell'eventualità che un ente pubblico o privato di una delle Parti, debitamente abilitato, risulti aggiudicatario di un contratto la cui esecuzione debba aver luogo all'interno dei confini dell'altra Parte, e tale contratto implichi lo scambio di Informazioni Classificate, la Parte ove il contratto deve essere eseguito deve adottare adeguate misure di sicurezza per la protezione delle Informazioni Classificate, in conformità con le leggi ed i regolamenti nazionali.

3. I Contratti Classificati devono essere conclusi ed eseguiti in conformità con le leggi ed i regolamenti nazionali di ogni Parte. Su richiesta, la Competente Autorità per la Sicurezza di ciascuna Parte deve confermare che ad un potenziale Contraente è stato rilasciato un adeguato Certificato nazionale di Abilitazione di Sicurezza Industriale.

4. L'annesso di sicurezza è parte integrante di ogni Contratto o subcontratto Classificato nel quale il Contraente della Parte Originatrice deve indicare quale Informazione Classificata debba essere rilasciata alla Parte Ricevente e quale livello di classifica di segretezza è stato assegnato a questa informazione.

5. Gli obblighi del Contraente relative alla protezione delle Informazioni Classificate devono almeno prevedere quanto segue:

   a) il rilascio dell'Informazione Classificata solo alle persone cui sia stato rilasciato un Certificato di Abilitazione di Sicurezza Personale di livello adeguato, in possesso di "necessità di conoscere" e che siano coinvolti nell'esecuzione del Contratto Classificato;

   b) la trasmissione dell'Informazione Classificata mediante strumenti conformi alle disposizioni di questo Accordo;

   c) le procedure ed i meccanismi di comunicazione delle modifiche che possono riguardare le Informazioni Classificate;

   d) l'utilizzo di Informazioni Classificate nell'ambito del Contratto Classificato solamente per gli scopi concernenti l'oggetto del Contratto;

   e) la rigorosa conformità alle disposizioni di questo Accordo concernenti le procedure per la trattazione delle Informazioni Classificate;

   f) l'obbligo di notificare alla Competente Autorità per la Sicurezza del Contraente ogni effettivo, tentato o sospetto accesso non autorizzato alle Informazioni Classificate riguardanti il Contratto Classificato, in conformità con le disposizioni del presente Accordo;

   g) il rilascio di Informazioni Classificate riguardanti il Contratto Classificato ad una Parte Terza solo previo consenso scritto della Parte Originatrice.

6. Le misure richieste per la protezione delle Informazioni Classificate, come pure le procedure per la valutazione del risarcimento per eventuali perdite causate ai Contraenti da accesso non autorizzato alle Informazioni Classificate devono essere specificate dettagliatamente nel rispettivo Contratto Classificato.

7. I Contratti Classificati di livello di segretezza "OGRANIČENO/RISERVATO/ RESTRICTED" devono contenere una specifica clausola di sicurezza che identifica le misure di sicurezza minime che devono essere applicate per la protezione delle Informazioni Classificate. Per tali contratti i Contraenti devono ricevere un'istruzione di sicurezza in conformità con le leggi ed i regolamenti nazionali.

Articolo 12
Visite

1. Le visite effettuate dai cittadini di una Parte presso le infrastrutture dell'altra Parte che prevedono l'accesso ad Informazioni Classificate devono essere subordinate alla previa autorizzazione scritta della Competente Autorità per la Sicurezza della Parte dove la visita deve avere luogo.

2. La richiesta di visita deve essere inviata con un anticipo di almeno 20 giorni rispetto alla data pianificata. In caso di visite della massima importanza e urgenza, non preventivamente pianificate, la richiesta di visita deve essere inviata almeno 5 giorni prima che la visita abbia luogo.

3. Il personale di una delle Parti, che ha presentato una richiesta di visita ufficiale all'altra Parte, in conformità con il presente accordo, deve:

   a) essere autorizzato a ricevere o ad avere accesso a Informazioni Classificate in conformità al principio della "necessità di conoscere", e

b) essere in possesso di un Certificato di Abilitazione di Sicurezza Personale di livello almeno equivalente al livello di classifica dell'informazione a cui deve avere accesso.

4. La richiesta di visita di cui al paragrafo 2 di questo Articolo deve riportare:
   a) il nome e cognome, la data e il luogo di nascita, la cittadinanza del visitatore;
   b) il numero del passaporto o del documento di identità del visitatore;
   c) l'incarico del visitatore e il nome dell'organizzazione rappresentata;
   d) un'idonea assicurazione concernente l'abilitazione di sicurezza rilasciata sulla base del Certificato di Abilitazione di Sicurezza Personale del visitatore, se necessario;
   e) l'indicazione del livello di classifica di segretezza dell'informazione cui è necessario avere accesso;
   f) l'indicazione del punto di contatto dell'ente pubblico o privato che deve essere visitato, comprensivo del nome e cognome, indirizzo di posta elettronica e numero telefonico;
   g) lo scopo e la data programmata della visita;
   h) i nomi delle organizzazioni e infrastrutture da visitare;
   i) il numero delle visite e il periodo richiesto;
   j) altri dati, se così concordato tra le Competenti Autorità per la Sicurezza.

5. La Competente Autorità per la Sicurezza della Parte ospitante comunica, mediante i canali concordati, alla Competente Autorità per la Sicurezza dell'altra Parte la propria decisione, con sufficiente anticipo rispetto alla programmata data di visita.

6. Le visite del personale di enti pubblici o privati di una delle Parti con livello di classifica "OGRANIČENO/RISERVATO/RESTRICTED" sono concordate direttamente tra gli enti pubblici o privati dell'altra Parte. L'ente pubblico o privato ospitante notifica la visita alla propria Competente Autorità per la Sicurezza.

7. Nei casi di progetti o contratti che richiedono visite classificate ricorrenti di livello di classifica "POVJERLJIVO/RISERVATISSIMO/CONFIDENTIAL" e superiori, le Competenti Autorità per la Sicurezza delle Parti si informano reciprocamente con l'invio di una lista di personale autorizzato. Tale lista non può essere valida per un periodo superiore a 12 mesi.

8. La Competente Autorità per la Sicurezza della Parte ospitante, su richiesta della Competente Autorità per la Sicurezza della Parte che effettua la visita, autorizza l'accesso alle Informazioni Classificate o alle infrastrutture ove tali Informazioni Classificate saranno mostrate ai visitatori in conformità con le leggi ed i regolamenti nazionali.

9. Ogni Parte deve garantire la protezione dei dati personali dei visitatori in conformità con le proprie leggi e regolamenti nazionali.

Articolo 13
Violazione della Sicurezza

1. In caso di effettiva o sospetta Violazione della Sicurezza, la Competente Autorità per la Sicurezza della Parte dove si è verificata la violazione deve tempestivamente informare la Parte Originatrice e, in conformità con le proprie leggi e regolamenti nazionali, avviare idonei procedimenti allo scopo di determinare le circostanze della violazione. I risultati dei procedimenti, nonché le successive misure adottate devono essere comunicate alla Parte Originatrice.

2. Nel caso in cui la violazione della sicurezza sia avvenuta in una Parte Terza, la Competente Autorità per la Sicurezza della Parte che ha inviato l'Informazione Classificata, deve, ove possibile, adottare tempestivamente le azioni previste al paragrafo 1 di questo Articolo.

Articolo 14
Costi

1. L'attuazione di questo Accordo non prevede alcun costo.

2. Nell'eventualità che una Parte debba sostenere dei costi, questi non devono essere posti a carico dell'altra Parte.

Articolo 15
Risoluzione delle Controversie

1. Ogni controversia concernente l'interpretazione o l'attuazione di questo Accordo è definita attraverso consultazioni e negoziazioni tra le Parti.

2. Nel frattempo, le Parti continuano ad adempiere alle disposizioni previste in questo Accordo.

Articolo 16
Disposizioni Finali

1. Questo Accordo entra in vigore alla data di ricezione dell'ultima notifica scritta con la quale le Parti si sono informate reciprocamente, attraverso canali diplomatici, che le loro procedure legali interne necessarie per l'entrata in vigore sono state completate.

2. Questo Accordo può essere modificato con il reciproco consenso scritto delle Parti. Gli emendamenti entrano in vigore in conformità con le disposizioni del paragrafo 1 di questo Articolo.

3. Questo Accordo rimane in vigore per un periodo di tempo indeterminato. Ciascuna Parte può denunciare questo Accordo informandone l'altra Parte per iscritto, tramite canali diplomatici. In tal caso, questo Accordo termina sei (6) mesi dopo la data in cui l'altra Parte ha ricevuto la comunicazione della denuncia.

4. In caso di termine del presente Accordo, tutte le Informazioni Classificate trasmesse sulla base di questo Accordo devono continuare ad essere protette in conformità con le disposizioni qui stabilite.

Fatto a Zagabria il 9 luglio 2019 in due originali, ognuno in lingua Croata, Italiana e Inglese, essendo tutti i testi egualmente autentici. In caso di divergenze di interpretazione, prevale il testo Inglese.

PER IL GOVERNO DELLA REPUBBLICA DI CROAZIA

PER IL GOVERNO DELLA REPUBBLICA ITALIANA

[TRANSLATION – TRADUCTION]

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

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

Reconnaissant l'importance du rôle que joue leur coopération mutuelle en matière de stabilisation de la paix, de sécurité internationale et de confiance mutuelle,

Reconnaissant l'intérêt et la nécessité commune d'assurer la protection des informations classifiées échangées dans les domaines politique, sécuritaire, militaire, économique et tout autre domaine entre les Parties et leurs entités publiques et privées, conformément aux législations et réglementations des Parties,

Reconnaissant la nécessité d'établir des règles de sécurité communes pour la protection des informations, notamment en ce qui concerne la possibilité d'appliquer des accords de coopération technique et d'initier des activités contractuelles,

Ayant convenu de tenir des discussions sur les questions de sécurité ainsi que d'élargir et de renforcer leur coopération mutuelle,

Conscients qu'une coopération de qualité peut exiger des échanges d'informations classifiées entre les Parties,

Sont convenus de ce qui suit :

Article premier. Objectif et applicabilité

L'objectif du présent Accord est d'assurer la protection des informations classifiées et d'établir des procédures et des règles communes pour la protection de toutes les informations classifiées échangées entre les Parties et entre les entités publiques et privées des Parties concernant les affaires internationales, la sécurité et la défense nationales, ainsi que les activités et opérations industrielles.

Article 2. Définitions

Aux fins du présent Accord :

1. le terme « Informations classifiées » désigne toute information, tout enregistrement, toute activité, tout document, tout matériel, y compris les objets et les établissements, auxquels un niveau de classification de sécurité a été attribué conformément à la législation et à la réglementation nationales ;

2. le terme « Besoin d'en connaître » désigne le principe selon lequel l'accès à des informations classifiées n'est accordé qu'à des personnes qui ont un besoin de connaître lesdites informations dans le cadre de leurs fonctions et missions officielles ;

3. le terme « Atteinte à la sécurité » désigne les actions ou omissions contraires à une disposition relative à la protection des informations classifiées qui peuvent entraîner une perte de confidentialité, d'intégrité ou de disponibilité desdites informations ;

4. le terme « Niveau de classification de sécurité » désigne la catégorie, conformément à la législation et à la réglementation nationales, qui caractérise l'importance des informations classifiées, leur niveau de restriction d'accès et le niveau de leur protection par les Parties, déterminés en fonction de l'étendue du préjudice causé par un accès non autorisé ;

5. le terme « Marque de classification » désigne une marque apposée sur toute information classifiée et montrant le niveau de classification de sécurité ;

6. le terme « Partie d'origine » désigne la Partie qui communique ou transmet les informations classifiées à la Partie destinataire ;

7. le terme « Partie destinataire » désigne la Partie à laquelle les informations classifiées sont transmises ;

8. le terme « Autorité de sécurité compétente » désigne l'autorité chargée de la sécurité qui, conformément à la législation et à la réglementation nationales de la Partie concernée, met en œuvre la politique nationale de protection des informations classifiées, exerce un contrôle complet dans ce domaine et supervise la mise en œuvre du présent Accord ;

9. le terme « Contractants et sous-traitants » désigne des personnes physiques ou morales dotées de la capacité juridique de conclure des contrats ;

10. le terme « Contrat classifié » désigne un accord entre deux ou plusieurs contractants, qui requiert l'accès à des informations classifiées ou leur génération ;

11. le terme « Certificat d'habilitation de sécurité personnelle » désigne la décision positive prise par l'autorité de sécurité compétente, conformément aux législations et réglementations nationales, selon laquelle une personne est autorisée à accéder à des informations classifiées au niveau de classification respectif ;

12. le terme « Certificat d'habilitation de sécurité d'établissement » désigne la décision positive prise par l'autorité de sécurité compétente conformément aux législations et réglementations nationales, selon laquelle une personne morale est autorisée à traiter et à gérer des informations classifiées au niveau de classification respectif ;

13. le terme « Tierce partie » désigne tout État, toute organisation ou toute personne morale qui n'est pas partie au présent Accord.

Article 3. Niveaux de classification de sécurité

Les Parties conviennent que les niveaux de classification de sécurité suivants sont équivalents et correspondent aux niveaux de classification de sécurité prévus par la législation et la réglementation nationales de la Partie concernée :

Pour la République de Croatie	Pour la République italienne	Équivalent en français
VRLO TAJNO	SEGRETISSIMO	TRÈS SECRET
TAJ NO	SEGRETO	SECRET

POVJERLJIVO	RISERVATISSIMO	CONFIDENTIEL
OGRANIČENO	RISERVATO	RESTREINT

Article 4. Autorités de sécurité compétentes

1. Les autorités de sécurité compétentes des Parties sont les suivantes :

Pour la République de Croatie :

le Bureau du Conseil de sécurité nationale (« Ured Vijeca za nacionalnu sigurnost ») ;

Pour la République italienne :

le Département des informations pour la Sécurité (DIS) (« Dipartimento delle Informazioni per la Sicurezza ») ;

Ufficio Centrale per la Segretezza (UCSe).

2. Les autorités de sécurité compétentes s'informent mutuellement de la législation et de la réglementation nationales en vigueur régissant la protection des informations classifiées et échangent des informations sur les normes, procédures et pratiques en matière de sécurité pour la protection des informations classifiées, ainsi que sur toute modification ultérieure éventuelle de la législation et de la réglementation nationales régissant la protection des informations classifiées et toute modification concernant les noms et adresses des autorités de sécurité compétentes.

3. Pour garantir une étroite coopération aux fins de l'application du présent Accord, les autorités de sécurité compétentes peuvent entamer des consultations.

4. Les Parties reconnaissent mutuellement les certificats d'habilitation de sécurité personnelle et d'établissement délivrés conformément aux dispositions législatives et réglementaires nationales.

5. Les autorités de sécurité compétentes veillent au respect strict et contraignant du présent Accord par toute entité publique et privée des Parties, conformément à leur législation et réglementation nationales.

Article 5. Principes relatifs à la protection mutuelle des informations classifiées

1. Conformément à leur législation et réglementation nationales, les Parties prennent toutes les mesures appropriées pour protéger les informations classifiées qui sont échangées ou générées dans le cadre du présent Accord. Chaque Partie s'assure que toute information classifiée de l'autre Partie se voie attribuer le même niveau de protection que celui requis par la législation et la réglementation nationales pour ses propres informations classifiées.

2. La Partie ne peut communiquer à une tierce partie aucune information classifiée de l'autre Partie, ni diminuer ou déclasser le niveau de classification de sécurité des informations classifiées de l'autre Partie, sans le consentement écrit préalable de la Partie d'origine.

3. Les deux Parties s'engagent à ne pas recourir au présent Accord pour obtenir l'accès à toute information classifiée que l'autre Partie a obtenue d'une tierce partie.

4. L'accès aux informations classifiées est accordé sur la base du principe du besoin d'en connaître. Le certificat d'habilitation de sécurité personnelle et le certificat d'habilitation de

sécurité d'établissement sont délivrés conformément aux dispositions législatives et réglementaires nationales des Parties.

5. La Partie destinataire :

a) ne soumet des informations classifiées à une tierce partie qu'avec l'accord écrit préalable de la Partie d'origine ;

b) attribue aux informations classifiées un niveau de classification de sécurité équivalent à celui accordé par la Partie d'origine ;

c) utilise les informations classifiées aux seules fins pour lesquelles celles-ci ont été fournies.

6. Les principes de protection mutuelle des informations classifiées convenus entre les Parties sont appliqués dans tous les autres accords et arrangements impliquant l'échange d'informations classifiées entre les Parties.

Article 6. Transmission des informations classifiées

1. Les informations classifiées de niveau « TAJNO/SEGRETO/SECRET » ou inférieur sont transmises par la valise diplomatique, par courrier militaire ou par d'autres services approuvés par les autorités de sécurité compétentes des Parties. La Partie destinataire confirme par écrit la réception d'informations classifiées de niveau « POVJERLJIVO/RISERVATISSIMO/CONFIDENTIEL » et supérieur. Les informations classifiées « VRLO TAJNO/SEGRETISSIMO/TRÈS SECRET » ne sont transmises que par des voies militaires ou diplomatiques certifiées. En cas d'urgence, les Parties peuvent convenir, au cas par cas, de modalités différentes de transmission des informations classifiées.

2. En cas de transmission d'un volume important d'informations classifiées, les autorités de sécurité compétentes conviennent mutuellement par écrit des moyens de transport, de l'itinéraire et des mesures de sécurité applicables au cas par cas.

3. Les Parties transmettent les informations classifiées par d'autres moyens de transmission approuvés conformément aux procédures de sécurité convenues par les autorités de sécurité compétentes.

Article 7. Certificat d'habilitation de sécurité personnelle

1. Si une personne a besoin d'accéder à des informations classifiées de niveau « POVJERLJIVO/RISERVATISSIMO/CONFIDENTIEL » ou supérieur dans le cadre de ses fonctions et missions officielles, ladite personne est titulaire d'un certificat d'habilitation de sécurité personnelle approprié et doit être informée en conséquence. Les Parties délivrent un certificat d'habilitation de sécurité personnelle conformément à leur législation et réglementation nationales.

2. Les autorités de sécurité compétentes se prêtent mutuellement assistance, sur demande, au cours de la procédure de contrôle préalable à la délivrance du certificat d'habilitation de sécurité personnelle.

3. Les autorités de sécurité compétentes assurent également une coopération mutuelle pour les éventuelles demandes d'informations sur les citoyens de l'autre Partie qui ont vécu ou séjourné sur leur territoire.

Article 8. Marquage des informations classifiées

1. La Partie destinataire attribue aux informations classifiées reçues conformément aux législation et réglementation nationales un niveau de classification de sécurité équivalent, tel que défini à l'article 3 du présent Accord.

2. Les reproductions et les traductions des informations classifiées reçues portent les marques de classification de sécurité des originaux et sont traitées de la même manière que les originaux.

Article 9. Reproduction et traduction des informations classifiées

1. Les informations classifiées de niveau « VRLO TAJNO/SEGRETISSIMO/TRÈS SECRET » ne sont traduites ou reproduites que dans des cas exceptionnels, moyennant l'accord écrit préalable de la Partie d'origine.

2. Toutes les copies d'informations classifiées reproduites portent la marque de classification d'origine. Les informations reproduites font l'objet du même contrôle que les informations d'origine. Le nombre de copies se limite au nombre requis à des fins officielles.

3. Toutes les traductions d'informations classifiées de niveau « POVJERLJIVO/RISERVATISSIMO/CONFIDENTIEL » et supérieur sont réalisées par des personnes dotées d'une habilitation de sécurité.

4. Les informations classifiées traduites portent la marque de classification d'origine et contiennent une note appropriée dans la langue dans laquelle elles sont traduites indiquant que la traduction contient des informations classifiées de la Partie d'origine.

Article 10. Destruction des informations classifiées

1. Les informations classifiées sont détruites de manière à empêcher leur reconstitution intégrale ou partielle.

2. Les informations classifiées de niveau « VRLO TAJNO/ SEGRETISSIMO/TRÈS SECRET » ne sont pas détruites. Elles sont restituées à la Partie d'origine.

3. La Partie d'origine peut, par une marque supplémentaire ou l'envoi d'une notification écrite ultérieure, interdire expressément la reproduction, l'altération ou la destruction des informations classifiées. Si la destruction des informations classifiées est interdite, celles-ci sont restituées à la Partie d'origine.

4. En cas de situation d'urgence dans laquelle il est impossible de protéger les informations classifiées ou de les restituer à la Partie d'origine, celles-ci sont immédiatement détruites. La Partie destinataire ne notifie par écrit à la Partie d'origine que la destruction des informations classifiées de niveau « VRLO TAJNO/SEGRETISSIMO/TRÈS SECRET ».

Article 11. Contrats classifiés

1. Les contractants et sous-traitants qui participent à la négociation et à l'exécution de contrats classifiés sont titulaires d'un certificat d'habilitation de sécurité d'établissement approprié au niveau requis pour le contrat, afin de garantir la protection des informations classifiées.

2. Dans le cas où une entité publique ou privée d'une Partie, dûment habilitée, a attribué un contrat à exécuter à l'intérieur des frontières nationales de l'autre Partie, et que ledit contrat inclut l'échange d'informations classifiées, la Partie où le contrat doit être exécuté prend les mesures de sécurité appropriées pour la protection des informations classifiées, conformément aux législations et réglementations nationales.

3. Les contrats classifiés sont conclus et exécutés conformément à la législation et à la réglementation nationales de chaque Partie. Sur demande, l'autorité de sécurité compétente de chaque Partie confirme qu'un contractant proposé s'est vu délivrer un certificat d'habilitation de sécurité d'établissement approprié.

4. Une annexe relative à la sécurité fait partie intégrante de chaque contrat ou sous-contrat classifié par lequel le contractant de la Partie d'origine précise les informations classifiées à transmettre à la Partie destinataire, ainsi que le niveau de classification de sécurité attribué auxdites informations.

5. Les obligations du contractant en matière de protection des informations classifiées se réfèrent, au moins, aux éléments suivants :

a) la divulgation d'informations classifiées exclusivement aux personnes ayant préalablement obtenu le certificat d'habilitation de sécurité personnelle approprié, qui ont « besoin d'en connaître » et qui sont engagées dans l'exécution du contrat classifié ;

b) la transmission d'informations classifiées par les moyens prévus par les dispositions du présent Accord ;

c) les procédures et mécanismes de communication de toute modification relative aux informations classifiées ;

d) l'utilisation d'informations classifiées dans le cadre du contrat classifié uniquement aux fins liées à l'objet du contrat ;

e) le strict respect des dispositions du présent Accord relatives aux procédures de traitement des informations classifiées ;

f) l'obligation de notifier à l'autorité de sécurité compétente du contractant tout accès réel, tenté ou présumé non autorisé à des informations classifiées liées au contrat classifié, conformément aux dispositions du présent Accord ;

g) la divulgation d'informations classifiées liées au contrat classifié à toute tierce partie uniquement avec le consentement écrit préalable de la Partie d'origine.

6. Les mesures requises pour la protection des informations classifiées, ainsi que la procédure d'évaluation de toute indemnisation de pertes éventuelles subies par les contractants du fait d'un accès non autorisé à des informations classifiées, sont spécifiées plus précisément dans le contrat classifié correspondant.

7. Les contrats classifiés de niveau « OGRANICENO/RISERVATO/RESTREINT » comportent une clause de sécurité appropriée définissant les mesures de sécurité minimales à adopter afin d'assurer la protection des informations classifiées. Pour ces contrats, les contractants sont informés sur les questions de sécurité conformément aux législations et réglementations nationales.

Article 12. Visites

1. Les visites effectuées par des citoyens d'une Partie dans des établissements de l'autre Partie qui nécessitent l'accès à des informations classifiées, sont soumises à l'autorisation écrite préalable de l'autorité de sécurité compétente de la Partie au sein de laquelle la visite a lieu.

2. La demande de visite est transmise au moins vingt jours avant la date prévue. En cas de visites de la plus haute importance et d'urgence qui ne sont pas programmées au préalable, la demande de visite est transmise au moins cinq jours avant la visite.

3. Le personnel de l'une des Parties qui présente une demande de visite officielle à l'autre Partie, conformément au présent Accord :

a) est autorisé à recevoir ou à accéder à des informations classifiées selon le principe du besoin d'en connaître ;

b) est titulaire d'un certificat d'habilitation de sécurité personnelle, au moins égal au niveau de classification des informations auxquelles il faut accéder.

4. La demande de visite, telle que visée au paragraphe 2 du présent article, comprend :

a) le nom et le prénom du visiteur, sa date et son lieu de naissance, ainsi que sa nationalité ;

b) le numéro de son passeport ou de sa carte d'identité ;

c) la fonction du visiteur et le nom de l'organisation qu'il représente ;

d) l'assurance d'une habilitation de sécurité appropriée sur la base du certificat d'habilitation de sécurité personnelle du visiteur, si nécessaire ;

e) l'indication du niveau de classification de sécurité des informations auxquelles il faut accéder ;

f) l'indication du point de contact de l'entité publique ou privée à visiter, y compris le nom et le prénom, l'adresse électronique et le numéro de téléphone ;

g) l'objectif de la visite et sa date envisagée ;

h) les noms des organisations et des établissements à visiter ;

i) le nombre de visites et la durée requise ;

j) tout autre renseignement, si approuvé par les autorités de sécurité compétentes.

5. L'autorité de sécurité compétente de la Partie hôte informe l'autorité de sécurité compétente de l'autre Partie, par les voies convenues, de sa décision, suffisamment à l'avance par rapport à la date prévue de la visite.

6. Les visites du personnel de l'entité publique ou privée de l'une des Parties de niveau « OGRANlCENO/RISERVATO/RESTREINT » et inférieur sont convenues directement avec l'entité publique ou privée de l'autre Partie. L'entité publique ou privée hôte informe son autorité de sécurité compétente de la visite.

7. Dans le cas de projets ou de contrats qui nécessitent des visites récurrentes de niveau « POVJERLJIVO/RISERVATISSIMO/CONFIDENTIEL » ou supérieur, les autorités de sécurité compétentes des Parties se notifient mutuellement par l'envoi d'une liste du personnel autorisé. Ladite liste ne peut être valable plus de douze mois.

8. L'autorité de sécurité compétente de la Partie hôte autorise, à la demande de l'autorité de sécurité compétente de la Partie en visite, l'accès des visiteurs aux informations classifiées ou aux

locaux dans lesquels des informations classifiées sont traitées, conformément aux législations et réglementations nationales.

9. Chaque Partie garantit la protection des données à caractère personnel des visiteurs conformément à ses législation et réglementation nationales.

Article 13. Atteinte à la sécurité

1. En cas d'atteinte à la sécurité, réelle ou présumée, l'autorité de sécurité compétente de la Partie sur le territoire de laquelle l'atteinte à la sécurité a été commise en informe sans délai l'autorité de sécurité compétente de la Partie d'origine et, conformément aux dispositions législatives et réglementaires nationales, engage les poursuites appropriées afin de déterminer les circonstances de l'atteinte à la sécurité. Les résultats des poursuites ainsi que les mesures adoptées suivantes sont transmis à la Partie d'origine.

2. Lorsque l'atteinte à la sécurité s'est produite dans une tierce partie, l'autorité de sécurité compétente de la Partie expéditrice prend, sans tarder et dans la mesure du possible, les mesures visées au paragraphe 1 du présent article.

Article 14. Dépenses

1. La mise en œuvre du présent Accord n'entraîne aucun frais.

2. En cas de frais engagés par une Partie, ceux-ci ne sont pas pris en charge par l'autre Partie.

Article 15. Règlement des différends

1. Tout différend relatif à l'interprétation ou à l'application du présent Accord est réglé par voie de consultations et de négociations entre les Parties.

2. Entre-temps, les Parties continuent d'appliquer les dispositions énoncées dans le présent Accord.

Article 16. Dispositions finales

1. Le présent Accord entre en vigueur à la date de réception de la dernière notification écrite par laquelle les Parties se notifient mutuellement, par la voie diplomatique, l'accomplissement de leurs procédures légales internes nécessaires à cet effet.

2. Le présent Accord peut être modifié sur accord écrit des Parties. Toute modification entre en vigueur selon les dispositions du paragraphe 1 du présent article.

3. Le présent Accord est conclu pour une durée indéterminée. Chacune des Parties peut dénoncer le présent Accord par notification écrite adressée à l'autre Partie par la voie diplomatique. Le cas échéant, le présent Accord prend fin six mois à compter de la date à laquelle l'autre Partie a reçu la notification de dénonciation.

4. En cas de dénonciation du présent Accord, toutes les informations classifiées transmises dans le cadre du présent Accord continuent à être protégées conformément aux présentes dispositions.

FAIT à Zagreb le 9 juillet 2019 en deux exemplaires originaux, chacun en langues croate, italienne et anglaise, tous les textes faisant également foi. En cas de divergence d'interprétation, la version anglaise prévaut.

Pour le Gouvernement de la République de Croatie :

[SIGNÉ]

Pour le Gouvernement de la République italienne :

[SIGNÉ]