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

The Austrian Federal Government and the Government of the Italian Republic (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 exchanged by the Parties,

Wishing to provide rules for the mutual protection of Classified Information generated or exchanged in the course of the cooperation between the Parties,

Having regard to national interests and security as well as industrial activities,

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) “Competent Authority” means the National Security Authority of one of the Parties and any other competent security authority or agency, notified in accordance with Article 2, responsible for the implementation of this Agreement;

c) “Personnel Security Clearance” means a statement by a Competent Authority of either Party, which is made following completion of a security investigation in accordance with the national laws and regulations and which certifies that an individual is granted access to Classified Information up to a specific level until a specified date;

d) “Facility Security Clearance” means a statement by a Competent Authority of either Party in accordance with national laws and regulations that, from the security viewpoint, a facility has the organisational capability to afford an adequate level of protection to Classified Information of a specific security classification level until a specified date;

e) “Classified Contract” means a contract or subcontract between a legal entity under the jurisdiction of one Party and a legal entity under the jurisdiction of the other Party, the implementation of which requires access to or generation of Classified Information;

f) “Contractor” means a public or private entity having the legal capacity to conclude Classified Contracts;

g) “Originator” means the originating Party as well as any legal entity under its jurisdiction which creates or provides Classified Information;

h) “Receiver” means the receiving Party as well as any legal entity under its jurisdiction which receives Classified Information;

i) “Need to Know” means the principle by which access to Classified Information is granted exclusively to a person if such access is required for the fulfilment of his or her duties;

j) “Third Party” means a legal entity or an individual which is not an Originator or Receiver of the Classified Information exchanged in accordance with this Agreement, a government not Party to this Agreement or an international organisation;

k) “Visit” means the access to the premises of public or private entities under the jurisdiction of either Party, for the purpose of executing this Agreement, which includes access to and handling of Classified Information;

l) “Security Breach” means an act or omission contrary to the provisions of this Agreement or to the national laws and regulations of the Parties, which may result in unauthorised disclosure, loss, misappropriation or any other form of compromise of Classified Information.

ARTICLE 2
COMPETENT AUTHORITIES

(1) The Competent Authorities designated by the Parties as responsible for the implementation of this Agreement are:

In the Federal Republic of Austria:
Federal Chancellery
Federal Office for Information Security

In the Italian Republic:
Presidenza del Consiglio dei Ministri
Dipartimento delle Informazioni per la Sicurezza
Ufficio Centrale per la Segretezza

(2) The Parties shall notify each other through diplomatic channels of any other Competent Authorities responsible for the implementation of this Agreement, as well as any subsequent changes of the respective Competent Authorities.

ARTICLE 3
EQUIVALENCE OF SECURITY CLASSIFICATION LEVELS

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

Republic of Austria	Italian Republic	English translation
STRENG GEHEIM	SEGRETISSIMO	TOP SECRET
GEHEIM	SEGRETO	SECRET
VERTRAULICH	RISERVATISSIMO	CONFIDENTIAL
EINGESCHRÄNKT	RISERVATO	RESTRICTED

ARTICLE 4
MARKING

(1) Classified Information generated, exchanged and released under this Agreement shall be marked by the Receiver with the appropriate security classification level in accordance with Article 3 under the national laws and regulations of the Parties.

(2) Classified Information generated, reproduced or translated by the Receiver in the course of cooperation under this Agreement shall also be marked with the appropriate classification level in accordance with Article 3 under the national laws and regulations of the Parties.

(3) The security classification level assigned to Classified Information exchanged under this Agreement shall only be altered or withdrawn with the written consent of the Originator. The Originator shall inform the Receiver without delay about any alteration or withdrawal of the security classification level of such Classified Information.

ARTICLE 5
PRINCIPLES OF THE PROTECTION OF CLASSIFIED INFORMATION

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

(2) The Parties shall afford exchanged Classified Information at least the same level of protection as they afford their own Classified Information of the equivalent security classification level.

(3) Exchanged Classified Information shall only be used for the purpose for which it has been released and with the limitations stated by the Originator.

(4) Received Classified Information shall only be made accessible to persons who are duly authorized in accordance with national laws and regulations to have access to Classified Information of the equivalent security classification level and who have the Need to Know.

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

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

ARTICLE 6
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 implementation of this Agreement.

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

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

(5) Access to Classified Information designated and marked as RISERVATO / EINGESCHRÄNKT / RESTRICTED shall be limited to persons having the Need to Know and who have been briefed accordingly.

(6) Access to Classified Information designated and marked as RISERVATISSIMO / VERTRAULICH / CONFIDENTIAL and above, shall be allowed only to those individuals having the Need to Know, holding a Personnel Security Clearance at the appropriate level and who are regularly briefed accordingly.

ARTICLE 7
FACILITY SECURITY CLEARANCES AND CLASSIFIED CONTRACTS

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

(2) Before providing Classified Information designated and marked as RISERVATISSIMO / VERTRAULICH / CONFIDENTIAL and above which is related to a Classified Contract to Contractors or prospective Contractors, the receiving Party shall ensure that:

a) such Contractors or prospective Contractors and their facilities have the organisational capability to protect Classified Information adequately;
b) Contractors and respective subcontractors and their facilities hold an appropriate Facility Security Clearance at the adequate level before the execution of the contract;

c) persons who perform functions requiring access to Classified Information hold an appropriate Personnel Security Clearance;
d) persons having access to the Classified Information are informed of their responsibilities and obligations to protect the Classified Information in accordance with the relevant laws and regulations of the receiving Party.

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

(4) 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 as well as about the security requirements for the Classified Information involved.

(5) The Competent Authorities shall inform each other about the conclusion of Classified Contracts falling under this Agreement.

(6) The Competent Authorities shall inform each other without delay about any withdrawal or alteration with regard to Facility Security Clearances falling under this Article, in particular about any alteration of the security classification level.

(7) The Competent Authority of the Originator shall transmit to the Receiver and to its Competent Authority the Programme Security Instructions and the Security Classification Guide generated under the Classified Contract.

(8) 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 8
PROTECTION OF CLASSIFIED INFORMATION IN COMMUNICATION AND INFORMATION SYSTEMS

Each Party shall ensure that appropriate measures are implemented under its national laws and regulations and in accordance with Article 5 for the protection of Classified Information processed, stored and transmitted through communication and information systems. Such measures shall ensure *inter alia* the confidentiality, integrity, availability and, where applicable, non-repudiation and authenticity of Classified Information, as well as an appropriate level of accountability and traceability of actions in relation to that Classified Information.

ARTICLE 9
TRANSMISSION

(1) Classified Information shall be transmitted through diplomatic channels or any other secure channel agreed upon by the Competent Authorities of the Parties.

(2) Receipt of Classified Information designated and marked as RISERVATISSIMO / VERTRAULICH / CONFIDENTIAL and above shall be acknowledged in writing.

(3) Classified Information designated and marked as SEGRETISSIMO / STRENG GEHEIM / TOP SECRET shall be sent only through diplomatic channels in accordance with national laws and regulations.

ARTICLE 10
REPRODUCTION AND TRANSLATION

(1) All reproductions, translations and copies shall bear appropriate security classification marking and shall be protected as the original Classified Information. The translations and the number of reproductions and copies shall be limited to a minimum. The reproduction, translation and copying of Classified Information may be limited or excluded by the Originator.

(2) Classified Information designated and marked as SEGRETISSIMO / STRENG GEHEIM / TOP SECRET shall not be reproduced, translated or copied without the prior written consent of the Originator.

(3) Classified Information shall only be translated by persons authorized to have access, in accordance with national laws and regulations of the Parties, to Classified Information of the respective security classification level.

ARTICLE 11
DESTRUCTION

(1) Classified Information designated and marked as RISERVATISSIMO / VERTRAULICH / CONFIDENTIAL or SEGRETO / GEHEIM / SECRET shall be destroyed in a verifiable way and in a manner that does not permit a full or partial reconstruction.

(2) Classified Information designated and marked as SEGRETISSIMO /STRENG GEHEIM / TOP SECRET shall not be destroyed. It shall be returned to the Originator after it is no longer considered necessary by the Receiver.

(3) In case of a crisis situation in which it is impossible to protect or return Classified Information exchanged or generated under this Agreement, the Classified Information shall be destroyed immediately. The Receiver shall inform the Competent Authority of the Originator about this destruction without undue delay.

ARTICLE 12
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 fifteen working days prior to the Visit, or 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 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 13
SECURITY BREACH

(1) In the event of a Security Breach resulting in a suspected or established unauthorized disclosure, misappropriation or loss of Classified Information falling under this Agreement, the Competent Authority of the Receiver 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) When a Security Breach occurs in the territory of a Third Party, the Competent Authorities shall immediately inform each other and, if possible, take the actions referred to in Paragraph 2 of this article.

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

ARTICLE 14
EXPENSES

Each Party shall bear its own expenses regarding the implementation of this Agreement in accordance with its national laws and regulations and without exceeding its ordinary budget availability.

ARTICLE 15
CONSULTATIONS

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

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

ARTICLE 16
SETTLEMENT OF DISPUTES

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

ARTICLE 17
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 of the completion of their respective internal procedures necessary for the entry into force of this Agreement.

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

(3) Each Party may terminate this Agreement through diplomatic channels at any time. In such a case, the Agreement shall expire six months after the receipt of the termination notice by the other Party. In the case of termination, Classified Information transmitted or generated in application of this Agreement shall continue to be protected under the provisions of this Agreement or, alternatively, returned to the Originator.

Done at ..... on ..... in two originals, each in the German, Italian and English languages, all texts being equally authentic. In case of divergence of interpretation, the text in English shall prevail.

For the Austrian Federal Government: For the Government of the Italian Republic: