

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

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

intending to ensure the security of all classified information designated as such in accordance with the applicable national law and transmitted to the other Party,

wishing to provide rules for the mutual protection of classified information applicable to every form of cooperation in the course of which such information is exchanged or generated,

have agreed upon the following:

**ARTICLE 1
DEFINITIONS**

For the purposes of this Agreement:

(1) "Classified information" means any information or object, regardless of its form of presentation and data storage medium, designated and marked as such in accordance with the applicable national law in order to ensure protection against any breach of security.

(2) "Applicable national law" means all the laws and regulations of either the Republic of Austria or the Republic of Latvia.

(3) "Breach of security" means any act or omission contrary to the applicable national law which results or may result in unauthorised disclosure, misappropriation or loss of classified information.

2

(4) “Receiver” means a Party as well as any public or private entity under its jurisdiction, to which classified information is transmitted.

(5) “Originator” means a Party as well as any public or private entity under its jurisdiction, which releases classified information.

(6) “Personnel security clearance” means a written determination based on a vetting procedure that an individual is duly authorised to have access to classified information up to the level defined in the clearance.

(7) “Facility security clearance” means a written determination based on an investigative procedure that a public or private entity is duly authorised to handle classified information up to the level defined in the clearance.

(8) “Contractor” means a public or private entity possessing the legal capacity to conclude contracts.

(9) “Classified contract” means a contract between a contractor from the State of one Party and a contractor from the State of the other Party, which contains classified information or the implementation of which requires access to and handling of classified information.

ARTICLE 2 SECURITY CLASSIFICATION LEVELS

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

| Republic of Austria: | Republic of Latvia: | Equivalent in English: |
|-----------------------------|----------------------------|-------------------------------|
| STRENG GEHEIM | SEVIŠĶI SLEPENI | TOP SECRET |
| GEHEIM | SLEPENI | SECRET |
| VERTRAULICH | KONFIDENCIĀLI | CONFIDENTIAL |
| EINGESCHRÄNKT | DIENESTA VAJADZĪBĀM | RESTRICTED |

(2) Classified information to be transmitted shall be marked by the originator with the appropriate security classification level.

(3) Classified information generated or reproduced in the course of cooperation under this Agreement shall also be marked in accordance with paragraph 2 of this Article.

(4) The security classification level shall only be altered or revoked by the originator. The receiver shall be informed without delay in writing about any alteration or revocation.

ARTICLE 3 COMPETENT SECURITY AUTHORITIES AND AGENCIES

The Parties shall notify each other through diplomatic channels of their security authorities and agencies competent for the implementation of this Agreement.

ARTICLE 4 SECURITY PRINCIPLES

(1) The Parties shall take all appropriate measures in accordance with this Agreement and the applicable national law to protect the transmitted classified information and shall ensure the necessary control of these measures.

(2) The Parties shall afford transmitted classified information at least the same level of protection as they afford their own classified information of the equivalent security classification level.

(3) Transmitted classified information shall only be used for the agreed purposes and shall only be made accessible to individuals duly authorised in accordance with the applicable national law.

(4) Transmitted classified information shall not be made accessible to a third party without the prior written consent of the originator.

(5) Classified information generated in the course of cooperation under this Agreement shall be protected in the same way as transmitted classified information.

ARTICLE 5 PERSONNEL SECURITY CLEARANCE

- (1) Access to information classified as VERTRAULICH/KONFIDENCIĀLI/CONFIDENTIAL and above shall only be granted on the basis of a personnel security clearance.
- (2) The competent security authorities and agencies shall assist each other upon written request and in accordance with the applicable national law when, under this Agreement, carrying out vetting procedures of individuals staying or having stayed in the other State.
- (3) Within the scope of this Agreement, the Parties shall mutually recognise the personnel security clearances.
- (4) Within the scope of this Agreement, the competent security authorities and agencies shall inform each other without delay in writing about any alteration with regard to personnel security clearances.

ARTICLE 6

CLASSIFIED CONTRACTS

- (1) In the context of the preparation or conclusion of classified contracts, the competent security authorities and agencies shall inform each other upon written request, whether a valid facility security clearance has been issued or the relevant proceedings have been initiated.
- (2) Within the scope of this Agreement, the Parties shall mutually recognise the facility security clearances.
- (3) A classified contract shall contain provisions on the security requirements and on the classification of each of its aspects or elements in accordance with the applicable national law. A copy of these provisions shall be submitted to the competent security authority or agency.
- (4) The competent security authority or agency of one Party may request that a security inspection of a contractor in the State of the other Party is carried out to ensure continuing compliance with the security requirements in accordance with the applicable national law. The request shall provide the reasons for such an inspection.

(5) With the prior written consent of its competent security authority or agency, a contractor is entitled to involve sub-contractors, if the classified contract so provides. Prospective sub-contractors shall meet the same security requirements as the contractor.

(6) Within the scope of this Agreement, the competent security authorities and agencies shall inform each other without delay in writing about any alteration with regard to facility security clearances.

ARTICLE 7 TRANSMISSION

Classified information shall be transmitted through diplomatic channels or in any other way protected against any breach of security and agreed upon between the competent security authorities and agencies of both Parties. Receipt of information classified as VERTRAULICH/KONFIDENCIĀLI/CONFIDENTIAL and above shall be acknowledged in writing.

ARTICLE 8 REPRODUCTION AND TRANSLATION

(1) Classified information shall be reproduced in accordance with the applicable national law. The reproduction of classified information by the receiver may be restricted or excluded by the originator. Information classified as STRENG GEHEIM/SEVIŠŖKI SLEPENI/TOP SECRET shall not be reproduced.

(2) Classified information shall only be translated by individuals duly authorised to have access to the information concerned.

(3) Copies and translations shall be protected in the same way as originals.

ARTICLE 9 DESTRUCTION

Classified information shall be destroyed in accordance with the applicable national law in a verifiable way and in a manner that does not permit a full or partial reconstruction. Information classified as STRENG

GEHEIM/SEVIŠKI SLEPENI/TOP SECRET shall not be destroyed but shall be returned to the originator.

ARTICLE 10 VISITS

(1) Visitors shall be granted access to classified information as well as to facilities in which classified information is handled only to the extent necessary and with the permission of the competent security authority or agency of the host State. The permission shall be granted only to individuals duly authorised to have access to the information concerned.

(2) Requests for visits shall be submitted to the competent security authority or agency at least two weeks prior to the visit, in urgent cases within a shorter period. The competent security authorities and agencies inform each other about the details of the visit and ensure the protection of personal data of the visitors.

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

- a. purpose of the visit;
- b. proposed date and duration of the visit or requested period for recurring visits;
- c. first name and family name, date and place of birth, nationality and passport or ID card number of the visitor;
- d. position of the visitor and name of the authority, agency or enterprise represented;
- e. validity and level of the personnel security clearance of the visitor;
- f. name, address, phone and fax number, e-mail address and point of contact of the authorities, agencies or facilities to be visited;
- g. date of the request and signature of the competent security authority or agency.

ARTICLE 11 BREACH OF SECURITY

(1) In case of a suspected or established breach of security, the competent security authority or agency of the State in which the breach occurred shall inform the competent security authority or agency of the other State without delay in writing.

(2) Breaches of security shall be investigated and prosecuted in accordance with the applicable national law. The competent security authority or agency of the other Party shall provide assistance upon request.

(3) The competent security authorities and agencies shall inform each other about the result of the investigation and the measures taken.

ARTICLE 12 EXPENSES

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

ARTICLE 13 CONSULTATIONS

(1) The competent security authorities and agencies inform each other of the national law on the protection of classified information and any amendments thereto.

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

ARTICLE 14 SETTLEMENT OF DISPUTES

Any disputes regarding the application or interpretation of this Agreement shall be resolved by direct consultations between the competent security authorities and agencies or through diplomatic channels.

ARTICLE 15 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 date of signature.

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

(3) Each Party may terminate this Agreement 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 under this Agreement shall continue to be protected under the provisions of this Agreement until the originator dispenses the receiver from this obligation.

Done in Vienna, on 31 October 2008 in two original copies, each in the German, Latvian and English languages, all texts being equally authentic. In case of any divergence of interpretation, the English text shall prevail.

For the Austrian Federal
Government:

For the Government of the Republic
of Latvia:

Ferdinand TRAUTTMANSDORFF m.p.

Aivars GROZA m.p.