

No. 45131*

—
**Latvia
and
Israel**

Agreement between the Government of the Republic of Latvia and the Government of the State of Israel regarding mutual protection of classified information in the field of defence and military cooperation. Tel Aviv, 6 March 2006

Entry into force: *6 March 2006 by signature, in accordance with article 13*

Authentic texts: *English, Hebrew and Latvian*

Registration with the Secretariat of the United Nations: *Latvia, 21 July 2008*

—
**Lettonie
et
Israël**

Accord entre le Gouvernement de la République de Lettonie et le Gouvernement de l'État d'Israël relatif à la protection mutuelle des informations classifiées en matière de défense et de coopération militaire. Tel Aviv, 6 mars 2006

Entrée en vigueur : *6 mars 2006 par signature, conformément à l'article 13*

Textes authentiques : *anglais, hébreu et letton*

Enregistrement auprès du Secrétariat des Nations Unies : *Lettonie, 21 juillet 2008*

* *The texts reproduced below are the original texts of the agreement as submitted. For ease of reference, they were sequentially paginated. The relevant Treaty Series volume will be published in due course.*

Les textes reproduit ci-dessous sont les textes authentiques de l'accord tel que soumises pour l'enregistrement. Pour référence, ils ont été présentés sous forme de la pagination consécutive. Le volume correspondant du Recueil des Traités sera disponible en temps utile.

[ENGLISH TEXT – TEXTE ANGLAIS]

The Government of the Republic of Latvia and the Government of the State of Israel, hereinafter referred to as the Parties,
intending to ensure the mutual protection of all Classified Information, in the field of Defence and Military Cooperation which has been classified in the state of the one Party and transferred to the state of the other Party,
desiring to establish the rules of the mutual protection of Classified Information, which shall be extended to agreements relating to defense and military cooperation to be concluded between the Parties and the contracts to be signed between organizations and institutions of the states, legal entities and persons, if applicable, authorized to exchange Classified Information,
Have Agreed As Follows:

Article 1: Definitions

For the purpose of this Agreement:

1. Classified Information means:

- A. Any classified item, be it an oral communication of classified contents or the electrical or electronic transmission of a classified message, or a "material" as defined in (b) below;
B. "Material" includes "document" as defined in (c) below, and any item of machinery, equipment, weapon or weapon-systems either manufactured or in the process of manufacture;
C. "Document" means any form of recorded information regardless of type of recording media; Which in the interest of national security of either Party and in accordance with its national laws and regulations, requires protection against unauthorized disclosure and which has been classified in accordance with its national laws and legislation.
2. Contractor - an individual or legal entity possessing the legal capacity to undertake Classified Contracts.
3. Classified Contract - an agreement between two or more legal entities or individuals creating and defining enforceable rights and obligations between them, which contains or includes Classified Information.
4. Competent Security Authority - the authority of the State of the Party, which in compliance with national laws and regulations is responsible for the protection of Classified Information and for the implementation of this Agreement. Such authorities are listed in Article 4 of this Agreement.
5. Receiving Party- the Party to which the Classified Information is transferred as represented by the Competent Security Authority.
6. Originating Party - the Party initiating the Classified Information as represented by the Competent Security Authority.
7. Third Party - any state, organization, legal entity, and individual which is not a Party to this Agreement.
8. Need to Know - a principle that access to Classified Information may only be granted to a person who has a verified need to know by virtue of his/her duties, within the framework of which the information was released to the Receiving Party.

Article 2: Security Classifications

The security classifications and their equivalents of the Parties are:

REPUBLIC OF LATVIA	EQUIVALENT IN ENGLISH	STATE OF ISRAEL
SEVIŠĶI SLEPENI	TOP SECRET	SODI BEYOTER
SLEPENI	SECRET	SODI
KONFIDENCIALI	CONFIDENTIAL	SHAMUR
INFORMACIJA DIENESTA VAJADZIBĀM	RESTRICTED	SHAMUR

Article 3: Protection Of Classified Information

1. Access to Classified Information shall be limited to those persons who have a Need to Know, and who have been security cleared by the Competent Security Authority of the Receiving Party, in accordance with its national laws and regulations, corresponding to the required security classification of the information to be accessed.

2. The Originating Party shall ensure that the Receiving Party is informed of:
 - A. The security classification of the Classified Information and any conditions of release or limitations on its use, and that the Classified Information is so marked.
 - B. Any subsequent change in security classification.
3. The Receiving Party shall:
 - A. In accordance with its national laws and regulations, provide the same level of security protection to Classified Information as provided by the Originating Party, subject to Article 2 of this Agreement.
 - B. Ensure that security classification is not amended and Classified Information is not declassified unless authorized in writing by the Originating Party.

Article 4: Competent Security Authorities

1. The Competent Security Authorities of the states of the Parties are:

For the Republic of Latvia:

- The Constitution Protection Bureau- Miera street 85a Riga LV 1013, Latvia;

For the State of Israel:

- The Directorate of Security for the Defense Establishment - Hakiryia Tel-Aviv, Israel.

2. In order to achieve and maintain comparable standards of security, the respective Competent Security Authorities shall, on request, provide each other with information about the security standards, procedures and practices for safeguarding Classified Information in the respective state of the Party.

3. The respective Competent Security Authorities of the states of both Parties can conclude executive documents to this Agreement.

Article 5: Restrictions On Use Of Classified Information and Disclosure

1. Unless written consent of the Originating Party is given, the Receiving Party shall not disclose or use, or permit the disclosure or use of any Classified Information.
2. The Receiving Party shall not pass to any Third Party any Classified Information, provided under the provisions of this Agreement, nor shall it publicly disclose any Classified Information without the prior written permission of the Originating Party.

Article 6 Transfer Of Classified Information

1. Classified Information shall be transferred normally by means of diplomatic, military and/or other courier services approved by the Competent Security Authorities. The Receiving Party shall confirm in writing the receipt of Classified Information.
2. If a large consignment containing Classified Information is to be transferred the respective Competent Security Authorities shall mutually agree on and approve the means of transportation, the route and security measures for each such case.
3. Other approved means of transfer or exchange of Classified Information, including electromagnetic transmission may be used if agreed upon by the Competent Security Authorities.

Article 7 Translation, Reproduction, Destruction

1. Documents containing information classified SEVIŠĶI SLEPENI / TOP SECRET / SODI BEYOTER shall be allowed for translation and copying only on the written permission of the respective Competent Security Authority of the state of the Originating Party.
2. Translation of any Classified Information shall be made by appropriately security-cleared individuals. Such translation should bear appropriate security classification markings in the language into which it is translated indicating that the translation contains Classified Information of the state of the Originating Party.
3. Copies and translations of Classified Information of the state of the Originating Party shall be marked with the same classification markings as the originals and shall be handled as originals. Such reproduced information shall be placed under the same controls as the original information. The number of copies shall be limited to that required for official purposes.
4. Classified Documents shall be destroyed or modified in such a manner so as to prevent their reconstruction.
5. Document or material containing information, classified SEVIŠĶI SLEPENI / TOP SECRET/ SODI BEYOTER shall not be destroyed. It shall be returned to the respective Competent Security Authority of the state of the Originating Party.

Article 8 Classified Contracts

1. If there is a need to conclude a Classified Contract with a Contractor residing in the territory of the state of the other Party or with Contractor of the other Party residing in the territory of the state of the first men-

tioned Party, an assurance from the Competent Security Authority shall be obtained in advance that the proposed Contractor has a security clearance corresponding to the required classification level and has implemented appropriate security arrangements to ensure the protection of Classified Information. This assurance also involves the obligation to ensure that the security arrangements of the security cleared Contractor correspond to national laws and regulations on protection of Classified Information and that these arrangements are supervised by the Competent Security Authority.

2. The Classified Contracts between the legal entities of the states of the Parties shall be concluded in accordance with the national laws and regulations of the states of the Parties.

3. The Competent Security Authority is responsible for ensuring that Classified Information, which has been either released to the Contractor of the other Party or generated in connection with; a Classified Contract, has been assigned a security classification. On request of the Competent Security Authority of one Party, the Competent Security Authority of the other Party shall provide a security requirements list. The Competent Security Authority of one Party shall provide the Competent Security Authority of the other Party with a notification stating that the Contractor has undertaken to observe national laws and regulations on the protection of Classified Information.

4. At all events, the Competent Security Authority shall ensure that the Contractor will handle the parts of a contract which require classification, in the same manner as Classified Information of the state of the Contractor in compliance with the security classification defined in the Article 2 of this Agreement.

5. Should the Competent Security Authority approve a classified sub contract, this Article shall apply accordingly.

6. The Competent Security Authorities shall ensure that a Classified Contract is authorized only after the Contractor has implemented all the necessary security measures.

Article 9: Visits

1. Access to Classified Information and to premises where classified projects are carried out, will be granted by one Party to any person from the other Party's country if previous permission from the Competent Security Authority of the Hosting Party has been obtained. Such permission shall be granted only upon visit applications to persons who have been security cleared and authorized to deal with Classified Information (hereinafter referred to as: "the Visitors").

2. The Competent Security Authority of the Sending Party shall notify the Competent Security Authority of the Hosting Party of planned visits, at least three weeks in advance. In case of special needs, security authorization of the visit will be granted as soon as possible, subject to prior coordination.

3. Visit applications shall include at least the following data:

a. Name and last name of the visitor, dates and place of birth, nationality and passport number or other identity documents.

b. Official title of the visitor and the name of the entity, plant of the legal entity or organization represented by him/her.

c. Certification of security clearance of the visitor, given by the Competent Security Authorities of the Sending Party.

d. Planned date of visit.

e. Purpose of the visit.

f. Name of persons, plants, installations, organizations and premises requested to be visited.

4. Upon approval of the Competent Security Authority, the visit permission can be granted for a specific period of time, as necessary for a specific project. Multiple visit permissions will be granted for a period not exceeding 12 months. Such permission shall be granted by the relevant Competent Security Authorities of the Parties.

5. Each Party shall ensure the protection of personal data of the visitors according to its applicable national laws and regulations.

Article 10: Breach Of Security

1. In case of a breach of security aspects that results in certain or suspected compromise of Classified Information, originated or received from the other Party, the Competent Security Authority in whose state the compromise occurred shall inform the Competent Security Authority of the other Party as soon as possible and carry out the appropriate investigation. The other Party shall, if required, cooperate in the investigation.

2. In any case, the other Party shall be informed of the results of the investigation and shall receive the final report as to the compromised Classified Information, the reasons of the event and the corrective, meas-

ures undertaken.

Article 11: Coverage Of Expenses

Each Party shall waive claims to other Party for reimbursements of expenditures incurred under the implementation of this Agreement.

Article 12: Dispute Resolution

1. In the event of any dispute arising between the Parties to this Agreement, whether such dispute shall relate to the interpretation of the Agreement or to the execution of the terms hereof or any matter arising therefrom, the Parties shall, in the first instance, make every reasonable effort to reach an amicable settlement.

2. In the event, however, of the Parties failing to reach such settlement, the Parties agree to submit the dispute to the Director of the Constitution Protection Bureau for the Latvian Party and the Director of Security for Israel Defense Establishment for the Israeli Party. Any decision given shall be final and binding on the Parties to this Agreement.

3. During the pending of any dispute, and/or controversy, both Parties shall continue to fulfill all their obligations under this Agreement.

4. Under no circumstances, any disputes arising from the interpretation of this Agreement will be referred to any third country or to any National or International Tribunal.

Article 13: Final Provisions

1. This Agreement shall enter into force upon signing by the Parties.

2. This Agreement shall remain in effect until terminated by either Party giving the other Party six*(6) months prior written notice of termination, through diplomatic channels. Notwithstanding the termination of this Agreement, all Classified Information provided pursuant to this Agreement shall continue to be protected in accordance with the provisions set forth herein, until the Originating Party will dispense the Receiving Party from this obligation. In case of termination, the Parties shall enter into consultations in order to specify the security aspects of the existing projects.

3. Each Party shall promptly notify the other Party of any amendments to its national laws and regulations that may affect the protection of Classified Information under this Agreement. In such case, the Parties shall consult to consider possible amendments to this Agreement. In the meantime, Classified Information shall continue to be protected as described herein, unless requested otherwise in writing by the Originating Party.

4. This Agreement may be amended on the basis of mutual written consent of both Parties. Such amendments shall enter into force in accordance with paragraph 1 of this Article.

5. All communication generated by either Party to this Agreement shall be in writing in English.

6. All notices concerning termination of or amendments to the Agreement shall be effected through diplomatic channels.

7. All other notices shall be done through the following POCs:

Latvian Party

Republic of Latvia - Director of Constitution Protection Bureau

Israeli Party

The State of Israel -Ministry of Defense

Head of Security of Information for the Defense Establishment

Done in Tel Aviv on 6 March 2006 in two copies in the Latvian, Hebrew and English languages, all texts being equally authentic. In case of any divergence of interpretation of the provisions of this Agreement the English text shall prevail.

For the Government of the Republic of Latvia:

Jānis Kažociņš

Director of the Constitution Protection Bureau

For the Government of the State of Israel:

Yechiel Horev

Principal Deputy Director General

Director of Directorate of Security

of the Defense Establishment

- בינתיים, מידע מסווג ימשיך להיות מוגן כפי שתואר לעיל, אלא אם התבקש אחרת בכתב על ידי הצד היוזם.
4. הסכם זה יכול להיות מתוקן על בסיס הסכמה הדדית משותפת של שני הצדדים. תיקונים כאלו יכנסו לתוקף בהתאם לפסקה הראשונה של פרק זה.
5. כל תקשורת הנוצרה על ידי אחד משני הצדדים בנוגע להסכם זה תהיה בכתב באנגלית.
6. כל הודעות הנוגעות לסיום ההסכם או לתיקונים להסכם זה יבוצעו על ידי ערוצים דיפלומטיים.
7. כל הודעות אחרות יבוצעו באמצעות ה-POC הבאים:

הצד הישראלי

מדינת ישראל - משרד הבטחון
הממונה על הבטחון במערכת הבטחון

הצד הלטבי

רפובליקת לטביה
מנהל לשכת ההגנה החוקתית

נחתם ב Tel Aviv ביום 6 March 2006 בשני עותקים בשפות העברית, הלטבית והאנגלית, כל הטקסטים אותנטיים במידה שווה. במקרה של מחלוקת בפירוש התנאים להסכם זה, הגרסה האנגלית תהיה המנחה.

לממשלת רפובליקת לטביה



יאניס קאזוסינס
מנהל לשכת ההגנה החוקתית

לממשלת מדינת ישראל



יחיאל חורב
המשנה למנכ"ל
והממונה על הבטחון במערכת הבטחון

5. כל צד יבטיח את ההגנה על הנתונים האישיים של המבקרים, בהתאם לתקנות והחוקים המתאימים שלו.

פרק 10 - הפרת בטחונות

1. במקרה של הפרה של היבטים בטחוניים אשר עלולה לגרום לפגיעה בטחונות הצד האחר ישתף פעולה בחקירה, באם נדרש.
2. בכל מקרה, הצד האחר ייודע בתוצאות החקירה ויקבל את הדו"ח הסופי בדבר המידע המסווג עליו התבצעה התקלה, הסיבות לאירוע והצעדים המתקנים שננקטו.

פרק 11 - כיסויי הוצאות

- כל צד יוותר לצד האחר לגבי כיסויי הוצאות אשר הוצאו לשם יישום הסכם זה.

פרק 12 - יישוב מחלוקות

1. בכל מקרה של מחלוקת על הסכם זה העולה בין הצדדים, בין אם מחלוקת שכזו נוגעת לפירוש ההסכם או להוצאתם לפועל של התנאים של זה או כל נושא העולה מכך, הצדדים יעשו כל מאמץ סביר, בהקדם האפשרי, על מנת להגיע ליישוב המחלוקת באופן ידידותי.
2. בכל מקרה, לעומת זאת, בו כשלו הצדדים להגיע ליישוב המחלוקת, יסכימו הצדדים להגיש את המחלוקת לממונה על הבטחון במערכת הבטחון הישראלית לצד הישראלי ולמנהל לשכת ההגנה החוקתית לצד הלטבי. כל החלטה שתיתן תהיה סופית ומחייבת את הצדדים להסכם זה.
3. בזמן בו מחלוקת ממתונה להכרעה, שני הצדדים ימשיכו למלא אחר כל חובותיהם תחת הסכם זה.
4. בשום נסיבות שהן, כל מחלוקת העולה כתוצאה מפירוש של הסכם זה לא תופנה לכל מדינה שלישית או לכל בית דין לאומי או בינלאומי.

פרק 13 - תנאים סופיים

1. הסכם זה ייכנס לתוקפו מיום חתימתו על ידי הצדדים.
2. הסכם זה יהיה תקף עד המועד בו יסתיים על ידי אחד משני הצדדים, הנותן לצד האחר הודעה כתובה על סיום ששה (6) חודשים קודם לכן, באמצעות הערוצים הדיפלומטיים. למרות סיום הסכם זה, כל מידע מסווג אשר סופק בעקבות הסכם זה ימשיך להיות מוגן, בהתאם לכל התנאים המוגדרים מכאן ואילך, עד שישחרר הצד היוזם את הצד המקבל מהתחייבות זו. במקרה של סיום ההסכם הצדדים יתכנסו להתייעצות על מנת לפרט את ההיבטים הבטחוניים של הפרויקטים הקיימים.
3. כל צד יודיע מיידית לצד האחר על כל תיקונים בחקיקה הלאומית שלו, אשר עלולים להשפיע על ההגנה של מידע מסווג תחת הסכם זה. במקרה כזה, הצדדים ייוועצו לשקול תיקונים אפשריים להסכם זה.

- הגנת המידע המסווג. הבטחה זו תכלול גם את ההתחייבות להבטיח כי סידורי הבטחון של הקבלן בעל הסיווג יתאימו לחקיקה הלאומית בהגנת המידע המסווג וכי על סידורים אלה קיים פיקוח על ידי הרשות הבטחונית המתאימה.
2. החוזים המסווגים בין היישויות החוקיות של מדינות הצדדים יסוכמו בהתאם לחקיקה הלאומית של מדינות הצדדים.
3. הרשות הבטחונית המתאימה אחראית להבטיח כי מידע מסווג, אשר הופץ לקבלן הצד האחר או נוצר בהקשר לחוזה מסווג, קיבל סיווג בטחוני. לפי בקשת הרשות הבטחונית המתאימה של צד אחד, הרשות הבטחונית המתאימה של הצד האחר תספק רשימת דרישות בטחוניות. הרשות הבטחונית המתאימה של הצד האחד תדאג לספק לרשות הבטחונית של הצד האחר הודעה המציינת כי הקבלן נטל על עצמו להקפיד על החקיקה הלאומית המתאימה להגנה על מידע מסווג.
4. בכל מקרה, הרשות הבטחונית המתאימה תבטיח כי הקבלן יתייחס לכל חלקי החוזה אשר זקוקים לסיווג באותו אופן כמו מידע וחומר מסווג של מדינת הקבלן בהתאם לסיווג הבטחוני המוגדר בפרק 2 להסכם זה.
5. באם תאשר הרשות הבטחונית המתאימה קיומו של תת-חוזה מסווג, יהיה פרק זה ישים לכך.
6. הרשות הבטחונית המתאימה תבטיח כי חוזה מסווג יאושר אך ורק לאחר שהקבלן יישם את כל האמצעים הבטחוניים הנחוצים.

פרק 9 - ביקורים

1. גישה למידע מסווג ולמתקנים בהם מתבצעים פרויקטים מסווגים תינתן על ידי צד אחד לכל אדם ממדינת הצד האחר אם ניתן אישור קודם מהרשות הבטחונית המתאימה של הצד המארח. אישור שכזה יינתן אך ורק לפי בקשות ביקורים לאישים בעלי סיווג ומורשים להתנהל עם מידע מסווג (להלן: "המבקרים").
2. הרשות הבטחונית המתאימה של הצד השולח תודיע לרשות הבטחונית המתאימה של הצד המארח על ביקורים מתוכננים, לפחות שלושה שבועות קודם להם. במקרה של צרכים מיוחדים, הרשאה בטחונית של הביקור תינתן מוקדם ככל האפשר, לפי תיאום קודם.
3. בקשות לביקורים יכללו לפחות את הנתונים הבאים:
- א. שם ושם משפחה של המבקר, תאריך ומקום לידה, אזרחות ומספר דרכון או מסמכי זהות אחרים.
 - ב. תואר רשמי של המבקר ושם הישות, מפעל הישות החוקית או ארגון המיוצג על ידה.
 - ג. סיווג בטחוני של המבקר, אשר ניתנה על ידי הרשות הבטחונית המתאימה של הצד השולח.
 - ד. תאריך מתוכנן של הביקור.
 - ה. מטרת הביקור.
 - ו. שמות אנשים, מפעלים, מתקנים, ארגונים ושטחים אותם חפצים לבקר.
4. בכפוף לאישור הרשות בטחונית המתאימה, אישור הביקור יינתן לתקופת מוגדרת של זמן, כפי שנחוץ לפרויקט מסוים. אישור ביקור רב-פעמי יינתן לתקופת זמן שלא עולה על 12 חודשים. אישור שכזה יינתן על ידי הרשות הבטחונית המתאימה הרלוונטית של הצדדים.

3. הרשות הבטחונית המתאימה של המדינות של שני הצדדים יוכלו לסכם מסמכים ביצועיים של הסכם זה.

פרק 5 - הגבלות על שימוש של מידע מסווג וחשיפה

1. אלא אם ניתנה הסכמה של הצד היוזם בכתב, הצד המקבל לא יחשוף או ישתמש, או יתיר חשיפה או שימוש של כל מידע מסווג.
2. הצד המקבל לא יעביר לכל צד שלישי כל מידע מסווג, אשר סופק תחת תנאי הסכם זה, וגם לא יחשוף לציבור כל מידע מסווג מבלי לקבל היתר כתוב קודם של הצד היוזם.

פרק 6 - העברת מידע מסווג

1. מידע מסווג יועבר בדרך כלל באמצעים דיפלומטיים, צבאיים ו/או שירותי שליחות המאושרים על ידי הרשות הבטחונית המתאימה. הצד המקבל יאשר בכתב את קבלת המידע המסווג.
2. באם יש לשלוח משגור גדול המכיל מידע מסווג יסכימו הרשויות הבטחוניות המתאימות ויאשרו את אמצעי ההעברה, מסלולם והצעדים הבטחוניים לכל מקרה שכזה.
3. אמצעי העברה או החלפה של מידע מסווג אתרים המאושרים, כולל תשדורת אלקטרומגנטית, יכולים להיות ברי שימוש אם הוסכם כך על ידי הרשויות הבטחוניות המתאימות.

פרק 7 - תרגום, שעתוק, השמדה

1. מסמכים הכוללים מידע מסווג סודי ביותר/ טופ סיקרט/ סבסקי סלפני יאושרו לתרגום והעתקה אך ורק על היתר כתוב של הרשות הבטחונית המתאימה של מדינת הצד היוזם.
2. תרגום של כל מידע מסווג יבוצע על ידי אישים בעלי סיווג מתאים. תרגום שכזה יהיה בעל סימונים הולמים של סיווג בטחוני בשפה אליה הוא מתורגם, המורים כי התרגום מכיל מידע מסווג של מדינת הצד היוזם.
3. עותקים ותרגומים של מידע מסווג של מדינת הצד היוזם יסומנו באותם סימוני סיווג כמו המקוריים ויקבלו את אותו היחס כמו המקוריים. מידע משועתק שכזה יהיה תחת אותה שליטה כמו המידע המקורי. מספר העותקים יוגבל לאלה הנדרשים למטרות רשמיות.
4. מסמכים מסווגים יושמדו או ישונו באופן שלא יאפשר את שחזורם.
5. מסמך או חומר המכילים מידע, המסווג כסודי ביותר/ טופ סיקרט/ סבסקי סלפני לא יושמדו. אלה יוחזרו לרשות הבטחונית המתאימה במדינת הצד היוזם.

פרק 8 - חוזים מסווגים

1. אם קיים צורך לסכם חוזה מסווג עם קבלן המתגורר בשטחי המדינה של הצד האחר או עם קבלן של הצד האחר המתגורר בשטחי המדינה של הצד המצוין לעיל, תושג מראש הבטחה מהרשות הבטחונית המתאימה כי הקבלן המוצע הוא בעל סיווג בטחוני המתאים לרמת הסיווג וכי יישם את סידורי הבטחון המתאימים על מנת להבטיח את

פרק 2 - סיווג בטחוני

הסיווגים הבטחוניים והמונחים המקבילים להם של הצדדים הם :

מדינת ישראל	שווה ערך באנגלית	רפובליקת לטביה
סודי ביותר	טופ סיקרט	סבסקי סלפני
סודי	סיקרט	סלפני
שמור	קונפידנשיאל	קונפידנציאלי
שמור	רסטריקטד	אינפורמסייה דינסטה ואיאדזיבאם

פרק 3 - הגנה על מידע מסווג

1. גישה למידע מסווג תהיה מוגבלת לאנשים המסוימים להם יש צורך לדעת, ואשר נבדקו מבחינה בטחונית על ידי הרשות הבטחונית המתאימה של הצד המקבל, בהתאם לחקיקה הלאומית שלו, בהתאמה לסיווג הבטחוני הנדרש של המידע אליו תהיה גישה.
2. הצד היוזם יבטיח כי הצד המקבל מודע לנייל:
 - א. הסיווג הבטחוני של המידע המסווג וכל תנאי שחרור או מגבלות שהם בשימוש, וכי המסמכים המסווגים והחומרים המסווגים מסומנים.
 - ב. כל שינוי נוסף בסיווג בטחוני.
3. על הצד המקבל:
 - א. בהתאם לחקיקה הלאומית שלו, לספק את אותה רמת הגנה בטחונית למידע המסווג אשר תסופק על ידי הצד היוזם, הנתון לפרק 2 להסכם זה.
 - ב. להבטיח כי סיווגים בטחוניים אינם משונים וכי אין מורידים רמת סיווג של מידע מסווג אלא אם מורשה בכתב על ידי הצד היוזם.

פרק 4 - רשות בטחונית מתאימה

1. הרשויות הבטחוניות המתאימות של מדינות הצדדים הן:
 - למדינת ישראל:
 - הממונה על הבטחון במערכת הבטחון - הקירייה, תל אביב, ישראל;
 - לרפובליקת לטביה:
 - לשכת ההגנה החוקתית - רחוב מיירה 85 א', ריגה, ל.ב. 1013, לטביה;
2. על מנת להשיג ולשמור על סטנדרטים ברי השוואה של בטחון, הרשויות הבטחוניות המתאימות יספקו, על פי בקשה, אחת לשנייה את המידע לגבי הסטנדרטים, ההליכים וההוראות הבטחוניים המיועדים להגן על מידע מסווג במדינת כל אחד מהצדדים.

[HEBREW TEXT – TEXTE HÉBREU]

ממשלת מדינת ישראל וממשלת רפובליקת לטביה, להלן הצדדים,

מתוך כוונה להבטיח את ההגנה ההדדית של כל מידע מסווג, בתחומי שיתוף פעולה בטחוני וצבאי, אשר סווג במדינת צד אחד והועבר למדינת הצד השני,

מתוך רצון לבסס את כללי ההגנה ההדדית של המידע המסווג, אשר יהיו תקפים להסכמים הנוגעים לשיתוף פעולה בטחוני וצבאי שיסוכמו בין הצדדים והחוזים אשר יחתמו בין ארגונים ומוסדות של המדינות, יישויות ואנשים בהתאמה, המורשים להחליף ביניהם מידע מסווג,

הסכימו הצדדים כדלהלן:

פרק 1 – הגדרות

למטרת הסכם זה:

1. משמעותו של 'מידע מסווג' היא:
 - א. כל פריט מסווג, בין אם תקשורת שבעל פה של תוכן מסווג או תשדורת אלקטרונית או חשמלית של הודעה מסווגת, או "חומר" כפי שמוגדר בסעיף ב' הנ"ל;
 - ב. "חומר" כולל "מסמך" כפי שמוגדר בג' הנ"ל, וכל פריט מכני, ציוד, נשק, או מערכות נשק אשר יוצרו או תחת תהליך ייצור;
 - ג. "מסמך" הוא כל צורה של מידע מתועד, בלא תלות בסוג המדיה המתעדת;
 אשר במניעי הבטחון הלאומיים של כל צד ובהתאם לחוקיו ותקנותיו הלאומיים, דורש הגנה כנגד חשיפה לא מורשית ואשר סווג בהתאם לחקיקה הלאומית של כל צד.
2. קבלן – יישות פרטית או חוקית המחזיקה את היכולת החוקית לקחת על עצמה ביצוע חוזים מסווגים.
3. חוזה מסווג – הסכם בין שתי יישויות חוקיות או אישים פרטיים או יותר היוצר ומגדיר זכויות וחובות. ברות אכיפה ביניהם, הכולל בתוכו מידע מסווג.
4. רשות בטחונית מתאימה - רשות מדינת הצד, אשר בהתאם לחקיקה הלאומית אחראית להגנה על מידע מסווג ויישום של הסכם זה. רשויות מסוג זה רשומות בפרק 4 להסכם זה.
5. הצד המקבל - הצד אליו מועבר המידע המסווג, כפי שמיוצג על ידי הרשות הבטחונית המתאימה.
6. הצד היוזם - הצד אשר מהווה את מקור המידע המסווג כפי שמיוצג על ידי הרשות הבטחונית המתאימה.
7. צד שלישי - כל מדינה, ארגון או יישות חוקית ופרטית שלא מהווה צד בהסכם זה.
8. צורך לדעת - עקרון לפיו גישה למידע מסווג תינתן אך ורק לאדם אשר לו צורך ממשי לדעת מכוח חובותיו/ה, במסגרת בה המידע ניתן מהצד המקבל.

[LATVIAN TEXT – TEXTE LETTON]

Latvijas Republikas valdība un Izraēlas Valsts valdība, turpmāk sauktas Puses,

Ar mērķi nodrošināt savstarpēju klasificētās informācijas aizsardzību aizsardzības un militārās sadarbības jomā, kura ir klasificēta vienas Puses valstī un nodota otras Puses valstij,

Vēloties nostiprināt savstarpējas klasificētās informācijas aizsardzības noteikumus, kas attiektos uz līgumiem aizsardzības un militārās sadarbības jomā, kas tiktu noslēgti starp Pusēm, un līgumiem, kas tiktu parakstīti starp valstu organizācijām un institūcijām, juridiskajām un, ja nepieciešams, fiziskajām personām, kas ir pilnvarotas apmainīties ar klasificēto informāciju,

IR VIENOJUŠĀS PAR SEKOJOŠO:

1. PANTS DEFINĪCIJAS

Šī Līguma mērķiem:

1. Klasificētā informācija nozīmē:

A. Jebkuru klasificētu objektu, kas var būt gan mutisks paziņojums ar klasificētu saturu, gan arī elektriski vai elektroniski nosūtīts klasificēts ziņojums, vai arī “materiāls”, kā definēts punktā (b),

B. Termins “materiāls” ietver “dokumentu”, kā definēts punktā (c), kā arī jebkuru mašīnu, iekārtu, ieroču vai ieroču sistēmu vienību, kas ir izgatavota vai ir izgatavošanas procesā,

C. Termins “dokuments” nozīmē jebkuru pierakstītas informācijas formu, neatkarīgi no ierakstīšanas vides veida,

kurai katras Puses nacionālās drošības interesēs un saskaņā ar tās nacionālajiem normatīvajiem aktiem ir nepieciešama aizsardzība pret nesankcionētu izpaušanu un kura ir klasificēta saskaņā ar tās nacionālajiem normatīvajiem aktiem.

2. Līgumslēdzējs – fiziska vai juridiska persona, kas ir tiesīga uzņemties klasificētu līgumu izpildi.

3. Klasificēts līgums – līgums starp divām vai vairākām juridiskām vai fiziskām personām, kas rada un nosaka izpildāmas tiesības un pienākumus starp tām un kas satur vai ietver klasificēto informāciju.

4. Kompetentā drošības iestāde – Puses valsts institūcija, kas saskaņā ar nacionālajiem normatīvajiem aktiem ir atbildīga par klasificētās informācijas aizsardzību un šī Līguma ieviešanu. Šīs institūcijas ir uzskaitītas šī Līguma 4. pantā.

5. Saņēmēja Puse – Puse, kurai klasificētā informācija tiek nosūtīta un kuru pārstāv Kompetentā drošības iestāde.

6. Izcelsmes Puse – Puse, kura rada klasificēto informāciju un kuru pārstāv Kompetentā drošības iestāde.

7. Trešā puse – jebkura valsts, organizācija, juridiska vai fiziska persona, kas nav šī Līguma puse.

8. Nepieciešamība zināt – princips, ka pieeja klasificētajai informācijai var tikt piešķirta vienīgi personai, kurai ir pārbaudīta nepieciešamība to zināt saistībā ar viņa/viņas darba pienākumiem, kuru ietvaros informācija ir tikusi nodota saņēmējai Pusei.

2. PANTS KLASIFIKĀCIJAS PAKĀPES

Pušu klasifikācijas pakāpes un to ekvivalenti ir šādi:

LATVIJAS REPUBLIKA	ANĢĻU VALODAS EKVIVALENTS	IZRAĒLAS VALSTS
SEVIŠĶI SLEPENI	TOP SECRET	SODI BEYOTER
SLEPENI	SECRET	SODI
KONFIDENCIĀLI	CONFIDENTIAL	SHAMUR
INFORMĀCIJA DIENESTA VAJADZĪBĀM	RESTRICTED	SHAMUR

3. PANTS

KLASIFICĒTĀS INFORMĀCIJAS AIZSARDZĪBA

1. Pieeja klasificētajai informācijai tiek piešķirta vienīgi personām, kurām ir ‘nepieciešamība zināt’ un kurām saņēmējas Puses Kompetentā drošības iestāde saskaņā ar nacionālajiem normatīvajiem aktiem ir piešķīrusi speciālo atļauju, kas atbilst tās informācijas klasifikācijai, kurai ir nepieciešama pieeja.

2. Izcelsmes Puse nodrošina, ka saņēmēja Puse tiek informēta par:

A. klasificētās informācijas klasifikācijas pakāpi un jebkādiem informācijas izpaušanas nosacījumiem vai lietošanas ierobežojumiem, un ka klasificētā informācija ir atbilstoši apzīmēta.

B. jebkādām turpmākām izmaiņām klasifikācijas pakāpē.

3. Saņēmēja Puse:

A. saskaņā ar nacionālajiem normatīvajiem aktiem klasificētajai informācijai nodrošina tādu pašu aizsardzības pakāpi, kā izcelsmes Puse, pamatojoties uz šī Līguma 2. pantu.

B. nodrošina, ka klasifikācijas pakāpe netiek mainīta, un klasificētā informācija netiek deklasificēta bez iepriekšējas rakstiskas izcelsmes Puses piekrišanas.

4. PANTS

KOMPETENTĀS DROŠĪBAS IESTĀDES

1. Pušu valstu Kompetentās drošības iestādes ir:

Latvijas Republikā:

Satversmes aizsardzības birojs
Miera iela 85a
Rīga LV 1013
Latvija.

Izraēlas Valstī:

Aizsardzības iestādes Drošības direktorāts
Hakirya
Telaviva
Izraēla.

2. Lai sasniegtu un ievērotu līdzīgus drošības standartus, attiecīgās Kompetentās drošības iestādes pēc pieprasījuma iesniedz viena otrai informāciju par drošības standartiem, procedūrām un praksi klasificētās informācijas aizsardzībai attiecīgās Puses valstī.

3. Abu Pušu valstu attiecīgās Kompetentās drošības iestādes var noslēgt izpildes dokumentus šim Līgumam.

5. PANTS

KLASIFICĒTĀS INFORMĀCIJAS IZMANTOŠANAS IEROBEŽOJUMI UN INFORMĀCIJAS ATKLĀŠANA

1. Saņēmēja Puse bez iepriekšējas rakstiskas izcelsmes Puses piekrišanas neatklāj, neizmanto vai nepieļauj jebkādas klasificētās informācijas atklāšanu un izmantošanu.

2. Saņēmēja Puse nenodod šī Līguma ietvaros saņemto klasificēto informāciju Trešajai pusei un nepublico jebkādu klasificēto informāciju bez iepriekšējas rakstiskas izcelsmes Puses piekrišanas.

6. PANTS

KLASIFICĒTĀS INFORMĀCIJAS NODOŠANA

1. Klasificētā informācija tiek nodota ar diplomātisko, militāro un/vai citu kurjeru starpniecību, kurus ir apstiprinājušas Kompetentās drošības iestādes. Saņēmēja Puse rakstiski apstiprina klasificētās informācijas saņemšanu.

2. Ja ir nepieciešams nodod liela apjoma sūtījumu, kas satur klasificēto informāciju, attiecīgās Kompetentās drošības iestādes savstarpēji vienojas un apstiprina transportēšanas veidu, maršrutu un drošības pasākumus katrā šādā gadījumā.

3. Citi klasificētās informācijas nodošanas vai apmaiņas veidi, tai skaitā elektromagnētiskā nosūtīšana, var tikt izmantoti, ja par to vienojas Kompetentās drošības iestādes.

7. PANTS **TULKOŠANA, PAVAIROŠANA, IZNĪCINĀŠANA**

1. Dokumentus, kas satur informāciju, kas klasificēta kā SEVIŠĶI SLEPENI / TOP SECRET / SODI BEYOTER, var tulkot un pavairot tikai ar izcelsmes Puses valsts attiecīgās Kompetentās drošības iestādes rakstisku atļauju.

2. Klasificētās informācijas tulkošanu veic personas, kurām ir atbilstoša speciālā atļauja. Uz šādiem tulkojumiem tiek izdarīts klasifikācijas pakāpes apzīmējums valodā, uz kuru tulkojums ir veikts, kas norāda, ka tulkojums satur izcelsmes Puses valsts klasificēto informāciju.

3. Uz izcelsmes Puses valsts klasificētās informācijas kopijām un tulkojumiem tiek izdarīti tādi paši klasifikācijas pakāpes apzīmējumi, kā uz oriģināliem, un tie tiek aizsargāti kā oriģināli. Šādi pavairotai informācijai tiek nodrošināta tāda pati kontrole, kā oriģinālajai informācijai. Kopijas tiek izgatavotas tādā apjomā, kāds nepieciešams oficiāliem mērķiem.

4. Klasificētie dokumenti tiek iznīcināti vai pārveidoti tā, lai novērstu to rekonstruēšanu.

5. Dokuments vai materiāls, kas satur informāciju, kas klasificēta kā SEVIŠĶI SLEPENI / TOP SECRET/ SODI BEYOTER, netiek iznīcināts. Tas tiek atgriezts izcelsmes Puses valsts Kompetentajai drošības iestādei.

8. PANTS

KLASIFICĒTI LĪGUMI

1. Ja kādai no Pusēm ir nepieciešams slēgt klasificētu līgumu ar līgumslēdzēju, kas atrodas otras Puses teritorijā, vai ar otras Puses līgumslēdzēju, kas atrodas pirmās Puses valsts teritorijā, tad iepriekš tiek saņemts Kompetentās drošības iestādes apstiprinājums, ka attiecīgajam līgumslēdzējam ir industriālās drošības sertifikāts, kas atbilst nepieciešamajai klasifikācijas pakāpei, un ka tas ir veicis nepieciešamos drošības pasākumus, lai nodrošinātu klasificētās informācijas aizsardzību. Šis apstiprinājums iekļauj arī pienākumu nodrošināt, ka līgumslēdzēja veiktie drošības pasākumi atbilst nacionālajiem normatīvajiem aktiem par klasificētās informācijas aizsardzību un ka šos pasākumus uzrauga Kompetentā drošības iestāde.

2. Klasificēti līgumi starp Pušu valstu juridiskajām personām tiek noslēgti saskaņā ar Pušu valstu nacionālajiem normatīvajiem aktiem.

3. Kompetentā drošības iestāde ir atbildīga par to, lai klasificētajai informācijai, kas tiek nodota otras Puses līgumslēdzējam vai radīta saistībā ar klasificētu līgumu, tiek piešķirta atbilstoša klasifikācijas pakāpe. Pamatojoties uz vienas Puses Kompetentās drošības iestādes līgumu, otras Puses Kompetentā drošības iestāde iesniedz drošības prasību uzskaitījumu. Vienas Puses Kompetentā drošības iestāde iesniedz otras Puses Kompetentajai drošības iestādei paziņojumu par to, ka līgumslēdzējs ir apņēmis ievērot nacionālos normatīvos aktus par klasificētās informācijas aizsardzību.

4. Visos gadījumos Kompetentā drošības iestāde nodrošina, ka līgumslēdzējs rīkojas ar līguma daļām, kuras ir klasificējamas, tāpat kā ar līgumslēdzēja valsts klasificēto informāciju atbilstoši klasifikācijas pakāpei, kā noteikts šī Līguma 2. pantā.

5. Ja Kompetentā drošības iestāde apstiprina klasificētu apakšlīgumu, attiecīgi tiek piemērots šis pants.

6. Kompetentās drošības iestādes nodrošina, ka klasificēts līgums tiek noslēgts tikai pēc tam, kad līgumslēdzējs ir veicis visus nepieciešamos drošības pasākumus.

9. PANTS VIZĪTES

1. Pieeju klasificētajai informācijai un vietām, kur tiek izpildīti klasificēti projekti, viena Puse piešķir otras Puses valsts pilsonim, ja ir saņemta iepriekšēja atļauja no uzņēmējas Puses Kompetentās drošības iestādes. Iesniedzot vizītes pieprasījumu, šāda atļauja tiek piešķirta personām, kuras ir saņēmušas atbilstošu speciālo atļauju un ir pilnvarotas strādāt ar klasificēto informāciju (turpmāk tekstā - apmeklētāji).

2. Vizītes pieprasītājas Puses Kompetentā drošības iestāde informē uzņēmējas Puses Kompetento drošības iestādi par plānotajām vizītēm vismaz trīs nedēļas iepriekš. Īpašos gadījumos vizītes atļauja tiek izsniegta pēc iespējas ātrāk un pamatojoties uz iepriekšēju saskaņošanu.

3. Vizītes pieprasījumā iekļauj vismaz šādu informāciju:

- a. Apmeklētāja vārds un uzvārds, dzimšanas datums un vieta, pilsonība un pases numurs vai citi identifikācijas dokumenti.
- b. Apmeklētāja oficiālais amats un institūcijas, juridiskās personas struktūras vai organizācijas nosaukums, ko apmeklētājs pārstāv.
- c. Apmeklētāja speciālās atļaujas apstiprinājums, ko ir izsniegusi nosūtītājas Puses Kompetentā drošības iestāde.
- d. Plānotais vizītes datums.
- e. Vizītes mērķis.
- f. Apmeklējamo personu, uzņēmumu, objektu, organizāciju un telpu vārds/nosaukums.

4. Pēc Kompetentās drošības iestāde apstiprinājuma atļauja veikt vizīti var tikt piešķirta uz noteiktu laika periodu, ja tas ir nepieciešams konkrēta projekta ietvaros. Atļauja veikt vairākkārtējas vizītes tiek piešķirta uz laika periodu, kas nepārsniedz 12 mēnešus. Šādas atļaujas izsniedz attiecīgās Puses Kompetentās drošības iestādes.

5. Katra Puse nodrošina apmeklētāju personu datu aizsardzību saskaņā ar tās attiecīgajiem nacionālajiem normatīvajiem aktiem.

10. PANTS DROŠĪBAS PĀRKĀPUMS

1. Ja drošības aspektu pārkāpuma rezultātā ir notikusi vai iespējama klasificētās informācijas, kura ir izcēlusies vai saņemta no otras Puses, nesankcionēta izpaušana, Kompetentā drošības iestāde, kuras valstī tā ir notikusi, nekavējoties informē otras Puses Kompetentā drošības iestādi un veic nepieciešamo izmeklēšanu. Ja nepieciešams, otra Puse piedalās izmeklēšanā.

2. Jebkurā gadījumā otra Puse tiek informēta par izmeklēšanas rezultātiem un saņem nobeiguma ziņojumu par izpausto klasificēto informāciju, notikuma iemesliem un veiktajiem pasākumiem.

11. PANTS IZDEVUMU SEGŠANA

Neviena no Pusēm nepieprasa otrai Pusei atbildzināt izdevumus, kas radušies saistībā ar šī Līguma izpildi.

12. PANTS STRĪDU IZŠKIRŠANA

1. Jebkura strīda gadījumā, kas ir radies starp šī Līguma Pusēm, ja šis strīds ir saistīts ar Līguma interpretāciju vai tā noteikumu vai no tā izrietošo jebkuru jautājumu izpildi, Puses sākotnēji veic visu iespējamo, lai panāktu kopīgu risinājumu.

2. Ja Puses nevar kopīgi atrisināt strīdu, Puses vienojas iesniegt strīda jautājumu Satversmes aizsardzības biroja direktoram no Latvijas

puses un Izraēlas Aizsardzības iestādes Drošības direktoram no Izraēlas puses. Jebkurš lēmums šādā gadījumā ir galīgs un saistošs šī Līguma Pusēm.

3. Strīda un/vai pretrunu izskatīšanas laikā abas Puses turpina pildīt savas saistības šī Līguma ietvaros.

4. Strīdu, kas saistīti ar šī Līguma interpretāciju, izšķiršanā netiek iesaistīta trešā valsts vai cits nacionāls vai starptautisks tribunāls.

13. PANTS NOBEIGUMA NOTEIKUMI

1. Šis Līgums stājas spēkā ar brīdi, kad to ir parakstījušas abas Puses.

2. Šis Līgums ir spēkā līdz brīdim, kamēr kāda no Pusēm Līguma darbību neizbeidz, iesniedzot otrai Pusei sešus (6) mēnešus iepriekš pa diplomātiskiem kanāliem rakstisku paziņojumu. Neatkarīgi no šī Līguma izbeigšanas, visa klasificētā informācija, kas ir nodota saskaņā ar šo Līgumu, arī turpmāk tiek aizsargāta saskaņā ar šī Līguma noteikumiem, līdz izcelsmes Puse neatbrīvo saņēmēju Pusi no šī pienākuma. Līguma izbeigšanas gadījumā Puses konsultējas, lai noteiktu esošo projektu drošības pasākumus.

3. Katra Puse nekavējoties informē otru Pusi par jebkādiem grozījumiem tās nacionālajos normatīvajos aktos, kas var ietekmēt klasificētās informācijas aizsardzību šī Līguma ietvaros. Šādā gadījumā Puses konsultējas, lai apsvērtu šī Līguma iespējamos grozījumus. Tikmēr klasificētā informācija tiek aizsargāta, kā tas ir noteikts šajā Līgumā, ja vien izcelsmes Puse rakstiski nelūdz rīkoties savādāk.

4. Šis Līgums var tikt grozīts, abām Pusēm par to savstarpēji rakstiski vienojoties. Šādi grozījumi stājas spēkā saskaņā ar šī panta pirmo daļu.

5. Visa sazināšanās, kas tiek veikta starp šī Līguma Pusēm, notiek rakstiski angļu valodā.

6. Visi paziņojumi par Līguma izbeigšanu vai tā grozīšanu tiek nosūtīti pa diplomātiskiem kanāliem.

7. Visi pārējie paziņojumi tiek nosūtīti starp šādām iestādēm:

Latvijas Puse

Latvijas Republika, Satversmes aizsardzība biroja direktors

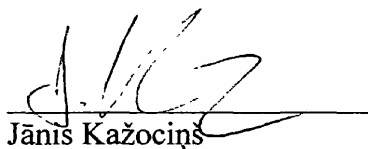
Izraēlas Puse

Izraēlas Valsts, Aizsardzības ministrija

Aizsardzības iestādes Informācijas drošības vadītājs

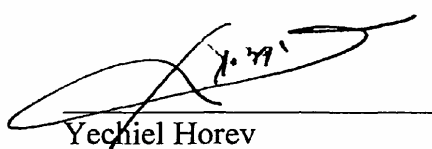
Paraksts *Telavivā* *2006. gada 6. martā* divos eksemplāros latviešu valodā, ivritā un angļu valodā. Atšķirīgas šī Līguma noteikumu interpretācijas gadījumā noteicošais ir teksts angļu valodā.

Latvijas Republikas
valdības vārdā



Jānis Kažociņš
Satversmes aizsardzības biroja
direktors

Izraēlas Valsts
valdības vārdā



Yecheil Horev
Ģenerāldirektora pirmais vietnieks
Aizsardzības iestādes Drošības
direktorāta direktors

[ENGLISH TEXT – TEXTE ANGLAIS]

The Government of the Republic of Latvia and the Government of the State of Israel, hereinafter referred to as the Parties,

intending to ensure the mutual protection of all Classified Information, in the field of Defence and Military Cooperation which has been classified in the state of the one Party and transferred to the state of the other Party,

desiring to establish the rules of the mutual protection of Classified Information, which shall be extended to agreements relating to defense and military cooperation to be concluded between the Parties and the contracts to be signed between organizations and institutions of the states, legal entities and persons, if applicable, authorized to exchange Classified Information,

HAVE AGREED AS FOLLOWS:

**ARTICLE 1
DEFINITIONS**

For the purpose of this Agreement:

1. Classified Information means:

A. Any classified item, be it an oral communication of classified contents or the electrical or electronic transmission of a classified message, or a "material" as defined in (b) below;

B. "Material" includes "document" as defined in (c) below, and any item of machinery, equipment, weapon or weapon-systems either manufactured or in the process of manufacture;

C. "Document" means any form of recorded information regardless of type of recording media;

Which in the interest of national security of either Party and in accordance with its national laws and regulations, requires protection against unauthorized disclosure and which has been classified in accordance with its national laws and legislation.

2. Contractor - an individual or legal entity possessing the legal capacity to undertake Classified Contracts.

3. Classified Contract - an agreement between two or more legal entities or individuals creating and defining enforceable rights and obligations between them, which contains or includes Classified Information.

4. Competent Security Authority - the authority of the State of the Party, which in compliance with national laws and regulations is responsible for the protection of Classified Information and for the implementation of this Agreement. Such authorities are listed in Article 4 of this Agreement.

5. Receiving Party - the Party to which the Classified Information is transferred as represented by the Competent Security Authority.

6. Originating Party - the Party initiating the Classified Information as represented by the Competent Security Authority.

7. Third Party - any state, organization, legal entity and individual which is not a Party to this Agreement.

8. Need to Know - a principle that access to Classified Information may only be granted to a person who has a verified need to know by virtue of his/her duties, within the framework of which the information was released to the Receiving Party.

ARTICLE 2 SECURITY CLASSIFICATIONS

The security classifications and their equivalents of the Parties are:

REPUBLIC OF LATVIA	EQUIVALENT IN ENGLISH	STATE OF ISRAEL
SEVIŠKI SLEPENI	TOP SECRET	SODI BEYOTER
SLEPENI	SECRET	SODI
KONFIDENCIĀLI	CONFIDENTIAL	SHAMUR

INFORMĀCIJA DIENESTA VAJADZĪBĀM	RESTRICTED	SHAMUR
---------------------------------------	------------	--------

**ARTICLE 3
PROTECTION OF CLASSIFIED INFORMATION**

1. Access to Classified Information shall be limited to those persons who have a Need to Know, and who have been security cleared by the Competent Security Authority of the Receiving Party, in accordance with its national laws and regulations, corresponding to the required security classification of the information to be accessed.

2. The Originating Party shall ensure that the Receiving Party is informed of:

A. The security classification of the Classified Information and any conditions of release or limitations on its use, and that the Classified Information is so marked.

B. Any subsequent change in security classification.

3. The Receiving Party shall:

A. In accordance with its national laws and regulations, provide the same level of security protection to Classified Information as provided by the Originating Party, subject to Article 2 of this Agreement.

B. Ensure that security classification is not amended and Classified Information is not declassified unless authorized in writing by the Originating Party.

**ARTICLE 4
COMPETENT SECURITY AUTHORITIES**

1. The Competent Security Authorities of the states of the Parties are:

For the Republic of Latvia:

- The Constitution Protection Bureau- Miera street 85a Riga LV 1013, Latvia;

For the State of Israel:

- The Directorate of Security for the Defense Establishment – Hakiryia Tel-Aviv, Israel.

2. In order to achieve and maintain comparable standards of security, the respective Competent Security Authorities shall, on request, provide each other with information about the security standards, procedures and practices for safeguarding Classified Information in the respective state of the Party.

3. The respective Competent Security Authorities of the states of both Parties can conclude executive documents to this Agreement.

ARTICLE 5
RESTRICTIONS ON USE OF CLASSIFIED INFORMATION
AND DISCLOSURE

1. Unless written consent of the Originating Party is given, the Receiving Party shall not disclose or use, or permit the disclosure or use of any Classified Information.

2. The Receiving Party shall not pass to any Third Party any Classified Information, provided under the provisions of this Agreement, nor shall it publicly disclose any Classified Information without the prior written permission of the Originating Party.

ARTICLE 6
TRANSFER OF CLASSIFIED INFORMATION

1. Classified Information shall be transferred normally by means of diplomatic, military and/or other courier services approved by the Competent Security Authorities. The Receiving Party shall confirm in writing the receipt of Classified Information.

2. If a large consignment containing Classified Information is to be transferred the respective Competent Security Authorities shall mutually agree on and approve the means of transportation, the route and security measures for each such case.

3. Other approved means of transfer or exchange of Classified Information, including electromagnetic transmission may be used if agreed upon by the Competent Security Authorities.

ARTICLE 7 TRANSLATION, REPRODUCTION, DESTRUCTION

1. Documents containing information classified SEVIŠKI SLEPENI / TOP SECRET / SODI BEYOTER shall be allowed for translation and copying only on the written permission of the respective Competent Security Authority of the state of the Originating Party.

2. Translation of any Classified Information shall be made by appropriately security-cleared individuals. Such translation should bear appropriate security classification markings in the language into which it is translated indicating that the translation contains Classified Information of the state of the Originating Party.

3. Copies and translations of Classified Information of the state of the Originating Party shall be marked with the same classification markings as the originals and shall be handled as originals. Such reproduced information shall be placed under the same controls as the original information. The number of copies shall be limited to that required for official purposes.

4. Classified Documents shall be destroyed or modified in such a manner so as to prevent their reconstruction.

5. Document or material containing information, classified SEVIŠKI SLEPENI / TOP SECRET / SODI BEYOTER shall not be destroyed. It shall be returned to the respective Competent Security Authority of the state of the Originating Party.

**ARTICLE 8
CLASSIFIED CONTRACTS**

1. If there is a need to conclude a Classified Contract with a Contractor residing in the territory of the state of the other Party or with Contractor of the other Party residing in the territory of the state of the first mentioned Party, an assurance from the Competent Security Authority shall be obtained in advance that the proposed Contractor has a security clearance corresponding to the required classification level and has implemented appropriate security arrangements to ensure the protection of Classified Information. This assurance also involves the obligation to ensure that the security arrangements of the security cleared Contractor correspond to national laws and regulations on protection of Classified Information and that these arrangements are supervised by the Competent Security Authority.

2. The Classified Contracts between the legal entities of the states of the Parties shall be concluded in accordance with the national laws and regulations of the states of the Parties.

3. The Competent Security Authority is responsible for ensuring that Classified Information, which has been either released to the Contractor of the other Party or generated in connection with a Classified Contract, has been assigned a security classification. On request of the Competent Security Authority of one Party, the Competent Security Authority of the other Party shall provide a security requirements list. The Competent Security Authority of one Party shall provide the Competent Security Authority of the other Party with a notification stating that the Contractor has undertaken to observe national laws and regulations on the protection of Classified Information.

4. At all events, the Competent Security Authority shall ensure that the Contractor will handle the parts of a contract which require classification, in the same manner as Classified Information of the state of the Contractor in compliance with the security classification defined in the Article 2 of this Agreement.

5. Should the Competent Security Authority approve a classified sub contract, this Article shall apply accordingly.

6. The Competent Security Authorities shall ensure that a Classified Contract is authorized only after the Contractor has implemented all the necessary security measures.

ARTICLE 9 VISITS

1. Access to Classified Information and to premises where classified projects are carried out, will be granted by one Party to any person from the other Party's country if previous permission from the Competent Security Authority of the Hosting Party has been obtained. Such permission shall be granted only upon visit applications to persons who have been security cleared and authorized to deal with Classified Information (hereinafter referred to as: "the Visitors").

2. The Competent Security Authority of the Sending Party shall notify the Competent Security Authority of the Hosting Party of planned visits, at least three weeks in advance. In case of special needs, security authorization of the visit will be granted as soon as possible, subject to prior coordination.

3. Visit applications shall include at least the following data:

- a. Name and last name of the visitor, dates and place of birth, nationality and passport number or other identity documents.
- b. Official title of the visitor and the name of the entity, plant of the legal entity or organization represented by him/her.
- c. Certification of security clearance of the visitor, given by the Competent Security Authorities of the Sending Party.
- d. Planned date of visit.
- e. Purpose of the visit.

f. Name of persons, plants, installations, organizations and premises requested to be visited.

4. Upon approval of the Competent Security Authority, the visit permission can be granted for a specific period of time, as necessary for a specific project. Multiple visit permissions will be granted for a period not exceeding 12 months. Such permission shall be granted by the relevant Competent Security Authorities of the Parties.

5. Each Party shall ensure the protection of personal data of the visitors according to its applicable national laws and regulations.

ARTICLE 10 BREACH OF SECURITY

1. In case of a breach of security aspects that results in certain or suspected compromise of Classified Information, originated or received from the other Party, the Competent Security Authority in whose state the compromise occurred shall inform the Competent Security Authority of the other Party as soon as possible and carry out the appropriate investigation. The other Party shall, if required, cooperate in the investigation.

2. In any case, the other Party shall be informed of the results of the investigation and shall receive the final report as to the compromised Classified Information, the reasons of the event and the corrective measures undertaken.

ARTICLE 11 COVERAGE OF EXPENSES

Each Party shall waive claims to other Party for reimbursements of expenditures incurred under the implementation of this Agreement.

ARTICLE 12 DISPUTE RESOLUTION

1. In the event of any dispute arising between the Parties to this Agreement, whether such dispute shall relate to the interpretation of the Agreement or to the execution of the terms hereof or any matter

arising therefrom, the Parties shall, in the first instance, make every reasonable effort to reach an amicable settlement.

2. In the event, however, of the Parties failing to reach such settlement, the Parties agree to submit the dispute to the Director of the Constitution Protection Bureau for the Latvian Party and the Director of Security for Israel Defense Establishment for the Israeli Party. Any decision given shall be final and binding on the Parties to this Agreement.

3. During the pending of any dispute, and/or controversy, both Parties shall continue to fulfill all their obligations under this Agreement.

4. Under no circumstances, any disputes arising from the interpretation of this Agreement will be referred to any third country or to any National or International Tribunal.

ARTICLE 13 FINAL PROVISIONS

1. This Agreement shall enter into force upon signing by the Parties.

2. This Agreement shall remain in effect until terminated by either Party giving the other Party six (6) months prior written notice of termination, through diplomatic channels. Notwithstanding the termination of this Agreement, all Classified Information provided pursuant to this Agreement shall continue to be protected in accordance with the provisions set forth herein, until the Originating Party will dispense the Receiving Party from this obligation. In case of termination, the Parties shall enter into consultations in order to specify the security aspects of the existing projects.

3. Each Party shall promptly notify the other Party of any amendments to its national laws and regulations that may affect the protection of Classified Information under this Agreement. In such case, the Parties shall consult to consider possible amendments to this Agreement. In the meantime, Classified Information shall continue to be protected as described herein, unless requested otherwise in writing by the Originating Party.

4. This Agreement may be amended on the basis of mutual written consent of both Parties. Such amendments shall enter into force in accordance with paragraph 1 of this Article.
5. All communication generated by either Party to this Agreement shall be in writing in English.
6. All notices concerning termination of or amendments to the Agreement shall be effected through diplomatic channels.
7. All other notices shall be done through the following POCs:

Latvian Party

Republic of Latvia – Director of Constitution Protection Bureau


Israeli Party

The State of Israel -Ministry of Defense

Head of Security of Information for the Defense Establishment

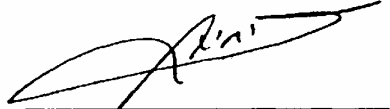
Done in.....*Tel Aviv*..... on...*6 March 2006*..... in two copies in the Latvian, Hebrew and English languages, all texts being equally authentic. In case of any divergence of interpretation of the provisions of this Agreement the English text shall prevail.

For the Government of
the Republic of Latvia



Jānis Kažociņš
Director of
the Constitution Protection Bureau

For the Government of
the State of Israel



Yechiel Horev
Principal Deputy Director General
Director of Directorate of Security
of the Defense Establishment