

TRACTATENBLAD

VAN HET

KONINKRIJK DER NEDERLANDEN

JAARGANG 2025 Nr. 3

A. TITEL

*Verdrag tussen het Koninkrijk der Nederlanden en de Republiek Letland inzake de uitwisseling en wederzijdse beveiliging van gerubriceerde gegevens (met Bijlage);
's-Gravenhage, 15 januari 2025*

Voor een overzicht van de verdragsgegevens, zie verdragsnummer 012703 in de Verdragenbank.

B. TEKST¹⁾

Agreement between the Kingdom of the Netherlands and the Republic of Latvia concerning the exchange and mutual protection of classified information

The Kingdom of the Netherlands

and

the Republic of Latvia,

Hereinafter jointly referred to as "the Parties", and each individually as "Party".

Wishing to ensure the mutual protection of Classified Information have, in the interests of national security, agreed upon the following.

Article 1

Purpose

The purpose of this Agreement is to ensure the protection of Classified Information exchanged between the Parties or between legal entities or individuals under their jurisdiction. The Agreement sets out the security procedures and arrangements for such protection.

Article 2

Definitions

For the purpose of this Agreement:

a) "**Classified Contract**" means a contract, including any pre-contractual negotiations, to be entered into by one of the Parties or Contractor under its jurisdiction with a Contractor under jurisdiction of the other Party for the supply of goods, execution of works or provision of services, the performance of which requires or involves access or potential access to or the creation of Classified Information.

b) "**Classified Information**" means any information, material or object, regardless of its form or nature, or any parts thereof, marked with the security classification level by one of the Parties in accordance with national laws and regulations. The unauthorised disclosure, alteration, compromise or loss of such information could cause various degrees of damage or harm to the interests of one or both of the Parties.

c) "**Competent Security Authority**" means the government authority in a Party responsible for the implementation and supervision of this Agreement.

d) "**Contractor**" means any individual or legal entity under the jurisdiction of a Party with the capacity to

¹⁾ De Letse tekst is niet opgenomen.

enter into a Classified Contract.

e) **“Facility Security Clearance”** means the positive determination by the Competent Security Authority that a facility has in place appropriate security measures to access and handle Classified Information up to and including a specified security classification level, in accordance with national laws and regulations.

f) **“Need to know”** means the requirement for an individual or a legal entity for access to, knowledge of or possession of Classified Information to perform official tasks or services.

g) **“Originating Party”** means the government institution in a Party under whose authority Classified Information has been created.

h) **“Personnel Security Clearance”** means the positive determination by the Competent Security Authority that an individual has been security cleared to access and handle Classified Information up to and including a specified classification level, in accordance with its national laws and regulations.

i) **“Providing Party”** means the Party or Contractor under its jurisdiction, which provides Classified Information to the Receiving Party under this Agreement.

j) **“Receiving Party”** means the Party or Contractor under its jurisdiction, which receives Classified Information from the Providing Party under this Agreement.

k) **“Security Classification Guide”** means a document associated with a Classified Contract that identifies each part of that Classified Contract which contains Classified Information, specifying the applicable security classification levels.

l) **“Security Incident”** means an act or an omission, contrary to national laws and regulations, which results in the unauthorised access, disclosure, loss or compromise of Classified Information.

m) **“Third Party”** means any international organisation, government or state, including legal entities or individuals under its jurisdiction, which is not a Party to this Agreement.

Article 3

Competent Security Authorities

1. The Competent Security Authorities of the Parties are listed in Annex 1 of this Agreement.
2. The Competent Security Authority may delegate part of its responsibilities to a delegated Competent Security Authority.
3. The Competent Security Authorities shall provide each other with official contact details.
4. The Parties shall notify each other in writing of any changes in contact details of their respective Competent Security Authorities.

Article 4

Security classification levels

1. The following security classification levels of the Parties are equivalent and correspond to the security classification levels specified in their national legislation. The English equivalent is an informal translation, not part of the national laws and regulations of the Parties and should not be used to mark Classified Information.

For the Republic of Latvia	For the Kingdom of the Netherlands	Equivalent in English
SEVIŠĶI SLEPENI	Stg. ZEER GEHEIM	TOP SECRET
SLEPENI	Stg. GEHEIM	SECRET
KONFIDENCIĀLI	Stg. CONFIDENTIEEL	CONFIDENTIAL
DIENESTA VAJADŽĪBĀM	DEPARTEMENTAAL VERTROUWELIJK	RESTRICTED

2. In accordance with the provisions set in its national laws and regulations, Receiving Party shall mark all the Classified Information under this Agreement that it has received from the Providing Party with the security classification that corresponds to the security classification given by the Originating Party in accordance with the scheme contained in paragraph 1 of this article.

3. The Receiving Party may alter or revoke the security classification of received Classified Information under this Agreement only upon the written consent of the Originating Party.

Article 5

Access to Classified Information

1. Access to Classified Information at the level KONFIDENCIĀLI / Stg. CONFIDENTIEEL or above, shall be granted only to those individuals who have a Need to know, hold a Personnel Security Clearance or a national equivalent at the corresponding level, are briefed on their responsibilities and have signed a statement of confidentiality in accordance with national laws and regulations.
2. Access at the level DIENESTA VAJADZĪBĀM / DEPARTEMENTAAL VERTROUWELIJK shall be granted only to those individuals who have a Need to know, are briefed on their responsibilities and have signed a statement of confidentiality in accordance with national laws and regulations.

Article 6

Security measures

1. The Parties shall take all appropriate measures applicable under their national laws and regulations to protect Classified Information generated or provided under this Agreement.
2. The Parties shall take all appropriate measures to ensure that the Providing Party:
 - a) marks Classified Information with the appropriate security classification level in accordance with its national laws and regulations;
 - b) informs the Receiving Party of any conditions of release or limitations on the use of the Classified Information provided;
 - c) informs the Receiving Party of any subsequent change in the security classification level of the Classified Information provided.
3. The Parties shall take all appropriate measures to ensure that the Receiving Party:
 - a) affords the same level of protection to Classified Information as afforded to its national Classified Information of an equivalent security classification level;
 - b) ensures that Classified Information is marked with its own corresponding security classification level, if such marking is in accordance with its national laws and regulations;
 - c) ensures that the security classification levels assigned to Classified Information are not altered or revoked without the prior written consent of the Originating Party;
 - d) ensures that Classified Information is not disclosed or released to a Third Party without the prior written consent of the Originating Party;
 - e) uses Classified Information solely for the purpose it has been released for and in accordance with handling requirements of the Originating Party.

Article 7

Security co-operation

1. In order to maintain comparable standards of security, the Competent Security Authorities shall, on request, inform each other about their security regulations, policies and practices for protecting Classified Information.
2. On request of the Competent Security Authority of one Party, the Competent Security Authority of the other Party shall issue a written confirmation that a valid Personnel Security Clearance or Facility Security Clearance has been issued.
3. If a national of one Party requires a Personnel Security Clearance, the Competent Security Authority of the other Party may send a request to issue a Personnel Security Clearance, to the Competent Security Authority of the Party he or she is a national of, in accordance with national laws and regulations.
4. If a Contractor under the jurisdiction of one Party requires a Facility Security Clearance, the Competent Security Authority of the other Party may send a request to issue a Facility Security Clearance to the Competent Security Authority of the Contractor, in accordance with national laws and regulations.
5. The Competent Security Authorities shall carry out vetting procedures for their nationals and issue Personnel Security Clearances or provide information about vetting results and Facility Security Clearances for legal entities under their jurisdiction in accordance with national laws and regulations.
6. The Competent Security Authorities shall assist each other in carrying out Facility Security Clearance and Personnel Security Clearance vetting on request and in accordance with national laws and regulations.

7. The Competent Security Authorities shall promptly notify each other in writing about changes in recognised Personnel Security Clearances and Facility Security Clearances for which a confirmation has been provided.

8. The co-operation under this Agreement shall be effected in English.

Article 8

Classified Contracts

1. If a Party or a Contractor under its jurisdiction proposes to grant a Classified Contract at the level KONFIDENCIĀLI / Stg. CONFIDENTIEEL or above, with a Contractor under the jurisdiction of the other Party, it shall first obtain written confirmation from the other Party that the Contractor has been granted a Facility Security Clearance or Personnel Security Clearance(s) at the appropriate security classification level. For Classified Contracts at the security classification level DIENESTA VAJADŽIBAM / DEPARTEMENTAAL VERTROUWELIJK as mentioned in article 4 of this Agreement, a Facility Security Clearance may be required, if mandated by national laws and regulations.

2. The Competent Security Authority shall ensure that the Contractor:

- a) ensures that all individuals granted access to Classified Information are informed of their responsibilities to protect Classified Information in accordance with the conditions defined in this Agreement and with national laws and regulations;
- b) monitors the security conduct within its facilities;
- c) notifies promptly its Competent Security Authority of any Security Incident relating to the Classified Contract.
- d) For Classified Contracts at the level KONFIDENCIĀLI / Stg. CONFIDENTIEEL or above, the Competent Security Authority shall ensure that the Contractor holds a Facility Security Clearance at the appropriate security classification level in order to protect the Classified Information and that the individuals requiring access to Classified Information hold a Personnel Security Clearance at the appropriate security classification level.

3. Every Classified Contract concluded in accordance with this Agreement shall include a security requirements chapter which identifies at least the following aspects:

- a) a reference to this Agreement, the definition of the term "Classified Information" in accordance with Article 2 of this Agreement, and the table of the equivalent security classification levels of the Parties in accordance with the provisions of article 4 of this Agreement;
- b) a statement that Classified Information generated or provided in the framework of the Classified Contract shall be protected in accordance with the applicable national laws and regulations;
- c) a statement that the Contractor shall disclose the Classified Information only to individuals who have a Need to know, and, in case of Classified Information at the level KONFIDENCIĀLI / Stg. CONFIDENTIEEL or above, hold a Personnel Security Clearance at the appropriate Classification Level in accordance with the provisions specified in article 5 of this Agreement, and have been assigned to perform official tasks or services in relation to the Classified Contract;
- d) a statement that the Contractor shall not disclose, or permit the disclosure of Classified Information to a Third Party or any other party that is not part of the Classified Contract without the prior written consent of the Originating Party;
- e) a statement that Classified Information provided under the Classified Contract is to be used solely for the purpose for which it has been provided, or as further expressly authorised by the Originating Party in writing;
- f) a Security Classification Guide;
- g) a procedure for communication of changes in the security classification level, taking into account paragraph 3 of article 4, of this Agreement;
- h) the channels and procedures to be used for the transport, transmittal or transmission of Classified Information;
- i) a statement that Classified Information shall be stored and handled in premises and classified information systems that are accredited for storage and handling of Classified Information at the Classification Level foreseen in the particular Classified Contract. This statement is independent from the procedure for obtaining a confirmation regarding the granting of a Facility Security Clearance as foreseen in paragraph 1 of this article;
- j) contact details of the Competent Security Authorities responsible for overseeing the protection of Classified Information related to the Classified Contract;
- k) obligation to notify any Security Incidents.

4. The Competent Security Authority of the Party authorising the award of the Classified Contract shall forward a copy of the security requirements chapter, to the Competent Security Authority of the Receiving Party, to facilitate the security oversight of the contract.

5. The procedures for the approval of visits associated with Classified Contract activities by personnel of one Party to the other Party, shall be in accordance with article 11 of this Agreement.

6. If a Contractor sub-contracts parts of a Classified Contract, the Contractor and the sub-contractor shall ensure the observance of all their obligations arising from this Agreement.

Article 9

Transmission of Classified Information

1. Classified Information shall be transmitted in accordance with national laws and regulations of the Providing Party or as otherwise agreed between the Competent Security Authorities.

2. Classified Information at the level KONFIDENCIĀLI / Stg. CONFIDENTIEEL shall be transmitted by a courier or diplomatic pouch. Classified Information at the level SLEPENI / Stg. GEHEIM shall be transmitted by a diplomatic courier. The Competent Security Authorities may agree on alternative channels of transmission in accordance with national laws and regulations.

3. The person performing transmission of Classified Information must be authorized to have access to Classified Information of the corresponding security classification level.

4. Classified Information must be packed in accordance with the national laws and regulations of the Providing Party.

5. Large volumes of Classified Information at the level KONFIDENCIĀLI / Stg. CONFIDENTIEEL or above shall be transmitted in accordance with a transportation plan confirmed by the Competent Security Authorities of both Parties. Where applicable, the transportation plan shall contain at least the following information:

- a) description of the Classified Contract;
- b) description of consignment (including security classification level);
- c) identification of participating Parties' representatives (including facility security officers);
- d) delivery points, transfer points, or processing points;
- e) identification of commercial entities to be involved in each movement;
- f) transportation route.

6. Classified Information at the level DIENESTA VAJADZĪBĀM / DEPARTEMENTAAL VERTROUWELIJK may only be transmitted by registered mail or other delivery services in accordance with national laws and regulations.

7. The Parties may only electronically transmit Classified Information protected by cryptographic means in accordance with procedures to be approved by the Competent Security Authorities.

Article 10

Reproduction, translation and destruction of Classified Information

1. Reproductions and translations of Classified Information shall bear original classification markings and placed under the same protection as the original Classified Information.

2. Translations or reproductions shall be limited to the minimum required for use under this Agreement and shall be made only by individuals who are authorized in accordance with national laws and regulations to access Classified Information at the security classification level of the Classified Information being translated or reproduced.

3. Translations shall contain a suitable annotation in the language in which they have been translated, indicating that they contain Classified Information of the Providing Party.

4. Classified Information at the level SEVIŠĶI SLEPENI / Stg. ZEER GEHEIM shall not be translated or reproduced without the prior written consent of the Originating Party.

5. Classified Information marked at the security classification level SEVIŠĶI SLEPENI / Stg. ZEER GEHEIM shall not be destroyed without the prior written consent of the Originating Party. The Originating Party shall decide whether the information shall be returned to the Originating Party or destroyed after it is no longer considered necessary by the Providing and Receiving Parties.

6. Classified Information up to and including SLEPENI / Stg. GEHEIM shall be destroyed after it is no longer considered necessary by the Receiving Party, in accordance with its national laws and regulations. In the case of destruction of Classified Information at the level of SLEPENI / Stg. GEHEIM the Receiving Party shall inform the Originating Party.

7. If a crisis situation makes it impossible to protect Classified Information provided under this Agreement, the Classified Information shall be destroyed immediately. The Receiving Party shall notify as soon as possible in writing the Competent Security Authority of the Originating Party about the destruction of this Classified Information.

Article 11

Visits

1. Visits requiring access to Classified Information at the level KONFIDENCIĀLI / Stg. CONFIDENTIEEL or above are subject to the prior written consent of the respective Competent Security Authority, unless otherwise agreed between the Competent Security Authorities. If mandated by national laws and regulations of the host Party, DIENESTA VAJADZIBĀM / DEPARTEMENTAAL VERTROUWELIJK level visits may be subject to a prior written consent of the Competent Security Authority of the host Party.

2. The visitor shall submit the request for visit at least ten calendar days in advance of the proposed date of the visit to his Competent Security Authority, which shall forward it to the Competent Security Authority of the other Party. In urgent cases, the request for visit may be submitted at a shorter notice, subject to prior coordination between the Competent Security Authorities.

3. Request for visit shall include:

- a) full name of the visitor, date and place of birth, nationality and passport/ID card number;
- b) official title of the visitor and name of the organization the visitor represents;
- c) confirmation of the visitor's Personnel Security Clearance and its validity if required;
- d) date and duration of the visit. In the case of recurring visits the total period covered by the visits shall be stated;
- e) purpose of the visit and the anticipated security classification level of Classified Information to be discussed or accessed;
- f) name, address, phone number, e-mail address and point of contact of the facility to be visited;
- g) dated and stamped signature of a representative of the visitor's Competent Security Authority.

4. The Competent Security Authorities may agree on a list of visitors entitled to recurring visits. The Competent Security Authorities shall agree on the further details of the recurring visits.

5. Classified Information provided to or acquired by a visitor shall be treated in accordance with the provisions of this Agreement.

Article 12

Security incident

1. The Competent Security Authorities shall immediately inform each other in writing of any actual or potential Security Incident involving Classified Information of the other Party.

2. The Receiving Party shall investigate immediately any actual or potential Security Incident. The Competent Security Authority of the Originating Party shall, if required, cooperate in the investigation.

3. The Competent Security Authority shall take appropriate measures in accordance with its national laws and regulations to limit the consequences of the incident and to prevent a recurrence. The Competent Security Authority of the Originating Party shall be informed of the outcome of the investigation and of measures, if any, taken.

Article 13

Costs

Each Party shall bear its own costs incurred in the course of implementing and executing its obligations under this Agreement.

Article 14

Dispute resolution

Any dispute on the interpretation or application of this Agreement shall be settled through consultations or negotiations between the Parties and shall not be referred to any national or international tribunal or Third Party for resolution.

Article 15

Implementing arrangements

The Competent Security Authorities may conclude implementing arrangements pursuant to this Agreement.

Article 16

Final provisions

1. This Agreement is concluded for an indefinite period of time. Each Party shall notify the other Party through diplomatic channels once the national procedures necessary for entry into force of this Agreement have been completed. This Agreement shall enter into force on the first day of the second month following the receipt of the latter notification.
2. With regard to the Kingdom of the Netherlands, this Agreement shall apply to the European part of the Netherlands and the Caribbean part of the Netherlands (the islands of Bonaire, Sint Eustatius and Saba).
3. This Agreement may only be amended with the mutual consent of the Parties. Either Party may propose amendments to this Agreement at any time through diplomatic channels. Such amendments shall enter into force under the conditions laid down in paragraph 1 of this article.
4. Notwithstanding the provisions of paragraph 3 of this article, any amendment to the Annex 1 of this Agreement shall be agreed upon by the Competent Security Authorities of the Parties, shall be confirmed in writing through an exchange of diplomatic notes and shall enter into force on a date to be determined in the diplomatic notes.
5. A Party may terminate this Agreement in writing at any time through diplomatic channels. In this case, the Agreement shall expire six months after receipt of such notification.
6. Regardless of the termination of this Agreement, all Classified Information exchanged, released or generated under this Agreement shall be protected in accordance with the terms of this Agreement before it was terminated, for as long as the Classified Information remains classified.

IN WITNESS WHEREOF the representatives of the Parties, duly authorised thereto, have signed this Agreement.

DONE in The Hague on 15 January 2025 in two original copies in the Latvian, Dutch and English languages, all texts being equally authentic. In case of divergence of interpretation of this Agreement, the English text shall prevail.

For the Kingdom of the Netherlands,

C.C.J. VELDKAMP

For the Republic of Latvia,

B. BRAŽE

Annex I

The Competent Security Authority for the Republic of Latvia is:

National Security Authority
Constitution Protection Bureau

The Competent Security Authority for the Kingdom of the Netherlands is:

General Intelligence and Security Service
Ministry of the Interior and Kingdom Relations

The delegated Competent Security Authority for the Kingdom of the Netherlands in the military domain is:

Defence Security Authority
Directorate – General of Policy
Ministry of Defence

Verdrag tussen het Koninkrijk der Nederlanden en de Republiek Letland inzake de uitwisseling en wederzijdse beveiliging van gerubriceerde gegevens

Het Koninkrijk der Nederlanden

en

de Republiek Letland,

Hierna gezamenlijk te noemen „de partijen” en elk afzonderlijk „de partij”,

Geleid door de wens de wederzijdse beveiliging te waarborgen van gerubriceerde gegevens, in het belang van de nationale veiligheid, komen het volgende overeen:

Artikel 1

Doel

Dit Verdrag heeft ten doel de beveiliging te waarborgen van gerubriceerde gegevens die worden uitgewisseld tussen de partijen of tussen rechtspersonen of natuurlijke personen onder hun rechtsmacht. In het Verdrag worden de beveiligingsprocedures en regelingen voor deze beveiliging vastgelegd.

Artikel 2

Begripsomschrijvingen

Voor de toepassing van dit Verdrag wordt verstaan onder:

- a) „**Gerubriceerd contract**”, een contract, met inbegrip van eventuele voorafgaande contractonderhandelingen, dat een van de partijen of een opdrachtnemer onder haar rechtsmacht aangaat met een opdrachtnemer onder de rechtsmacht van de andere partij voor de levering van goederen, uitvoering van werkzaamheden of levering van diensten, waarbij voor de uitvoering toegang of mogelijk toegang tot gerubriceerde gegevens vereist is of waarbij deze gecreëerd worden.
- b) „**Gerubriceerde gegevens**”, gegevens, materiaal of voorwerpen, ongeacht de vorm of aard daarvan, of delen daarvan die of dat door een van de partijen is voorzien van een rubriceringsniveau in overeenstemming met de nationale wet- en regelgeving. De ongeoorloofde bekendmaking, verandering, compromittering of het verlies van dergelijke gegevens zou de belangen van een of beide partijen in meerdere of mindere mate kunnen schaden.
- c) „**Bevoegde beveiligingsautoriteit**”, de overheidsautoriteit in een partij die verantwoordelijk is voor de implementatie van en toezicht op dit Verdrag.
- d) „**Opdrachtnemer**”, elke natuurlijke persoon of rechtspersoon onder de rechtsmacht van een partij die bevoegd is gerubriceerde contracten aan te gaan.
- e) „**veiligheidsmachtiging bedrijfslocatie**”, de vaststelling door de bevoegde beveiligingsautoriteit dat een bedrijfslocatie passende beveiligingsmaatregelen heeft genomen voor de toegang tot en omgang met gerubriceerde gegevens tot en met een gespecificeerd rubriceringsniveau, in overeenstemming met de nationale wet- en regelgeving.
- f) „**Need to know**”, het vereiste voor een natuurlijke persoon of rechtspersoon voor toegang tot, kennis van of bezit van gerubriceerde gegevens voor het uitvoeren van officiële taken of diensten.
- g) „**Partij van herkomst**”, de overheidsinstelling in een partij onder wier gezag gerubriceerde gegevens zijn gecreëerd.
- h) „**Veiligheidsmachtiging personeel**”, de vaststelling door de bevoegde beveiligingsautoriteit dat een natuurlijke persoon toestemming heeft gekregen voor de toegang tot en omgang met gerubriceerde gegevens tot en met een gespecificeerd rubriceringsniveau, in overeenstemming met de nationale wet- en regelgeving.
- i) „**Verstrekkende partij**”, de partij of opdrachtnemer onder haar rechtsmacht die de gerubriceerde gegevens uit hoofde van dit Verdrag verstrekt aan de ontvangende partij.
- j) „**Ontvangende partij**”, de partij of opdrachtnemer onder haar rechtsmacht die de gerubriceerde gegevens

uit hoofde van dit Verdrag ontvangt van de verstreckende partij.

k) „**Rubriceringsgids**”, een document dat hoort bij een gerubriceerd contract waarin de van toepassing zijnde rubriceringsniveaus voor elk onderdeel van het gerubriceerde contract dat gerubriceerde gegevens bevat worden gespecificeerd.

l) „**Beveiligingsincident**”, elk handelen of nalaten te handelen, in strijd met de nationale wet- en regelgeving, dat resulteert in ongeoorloofde toegang tot of bekendmaking, verlies of compromittering van gerubriceerde gegevens.

m) „**Derde**”, elke internationale organisatie, regering of staat, met inbegrip van rechtspersonen of natuurlijke personen onder zijn rechtsmacht, die geen partij is bij dit Verdrag.

Artikel 3

Bevoegde beveiligingsautoriteiten

1. De bevoegde beveiligingsautoriteiten van de partijen staan vermeld in Bijlage 1 bij dit Verdrag.
2. De bevoegde beveiligingsautoriteit kan een deel van haar verantwoordelijkheden delegeren aan een gemachtigde bevoegde beveiligingsautoriteit.
3. De bevoegde beveiligingsautoriteiten voorzien elkaar van de officiële contactgegevens.
4. De partijen stellen elkaar schriftelijk in kennis van eventuele wijzigingen in de contactgegevens van hun respectieve bevoegde beveiligingsautoriteiten.

Artikel 4

Rubriceringsniveaus

1. De volgende rubriceringsniveaus van de partijen komen overeen en corresponderen met de rubriceringsniveaus die in hun nationale wetgeving staan vermeld. Het Engelse equivalent is een niet-officiële vertaling, die geen deel uitmaakt van de nationale wet- en regelgeving van de partijen en niet gebruikt dient te worden om gerubriceerde gegevens aan te duiden.

Voor de Republiek Letland	Voor het Koninkrijk der Nederlanden	Equivalent in het Engels
SEVIŠĶI SLEPENI	Stg. ZEER GEHEIM	TOP SECRET
SLEPENI	Stg. GEHEIM	SECRET
KONFIDENCIĀLI	Stg. CONFIDENTIEEL	CONFIDENTIAL
DIENESTA VAJADZĪBĀM	DEPARTEMENTAAL VERTROUWELIJK	RESTRICTED

2. In overeenstemming met de bepalingen in de nationale wet- en regelgeving voorziet de ontvangende partij alle gerubriceerde gegevens uit hoofde van dit Verdrag die zij ontvangen heeft van de verstreckende partij van het rubriceringsniveau dat overeenkomt met het door de partij van herkomst gegeven rubriceringsniveau in overeenstemming met de tabel in het eerste lid van dit artikel.

3. De ontvangende partij mag het rubriceringsniveau van uit hoofde van dit Verdrag ontvangen gerubriceerde gegevens uitsluitend veranderen of intrekken na de schriftelijke toestemming door de partij van herkomst.

Artikel 5

Toegang tot gerubriceerde gegevens

1. Toegang tot gerubriceerde gegevens op het niveau KONFIDENCIĀLI / Stg. CONFIDENTIEEL of hoger wordt uitsluitend verleend aan de natuurlijke personen die van de gegevens op de hoogte moeten zijn (need to know), een veiligheidsmachtiging personeel of een nationaal equivalent daarvan op het overeenkomstige niveau hebben, zijn ingelicht over hun verantwoordelijkheden en een geheimhoudingsverklaring hebben ondertekend in overeenstemming met de nationale wet- en regelgeving.

2. Toegang op het niveau DIENESTA VAJADZĪBĀM / DEPARTEMENTAAL VERTROUWELIJK wordt uitsluitend verleend aan de natuurlijke personen die van de gegevens op de hoogte moeten zijn (need to know), zijn ingelicht over hun verantwoordelijkheden en een geheimhoudingsverklaring hebben ondertekend in overeenstemming met de nationale wet- en regelgeving.

Artikel 6

Beveiligingsmaatregelen

1. De partijen nemen alle passende maatregelen die krachtens hun nationale wet- en regelgeving van toepassing zijn op de uit hoofde van dit Verdrag gegenereerde of verstrekte gerubriceerde gegevens.
2. De partijen nemen alle passende maatregelen om te waarborgen dat de verstreckende partij:
 - a) de gerubriceerde gegevens voorziet van de juiste rubriceringsmarkering in overeenstemming met haar nationale wet- en regelgeving;
 - b) de ontvangende partij in kennis stelt van mogelijke voorwaarden voor vrijgave of beperkingen gesteld aan het gebruik van de verstrekte gerubriceerde gegevens;
 - c) de ontvangende partij in kennis stelt van eventuele navolgende veranderingen van het rubriceringsniveau van de verstrekte gerubriceerde gegevens.
3. De partijen nemen alle passende maatregelen om te waarborgen dat de ontvangende partij:
 - a) hetzelfde beveiligingsniveau aan gerubriceerde gegevens toekent als aan haar nationale gerubriceerde gegevens met een vergelijkbaar rubriceringsniveau;
 - b) waarborgt dat gerubriceerde gegevens worden voorzien van haar eigen dienovereenkomstige rubriceringsniveau indien deze rubricering in overeenstemming is met haar nationale wet- en regelgeving;
 - c) waarborgt dat de aan de gerubriceerde gegevens toegekende rubriceringsniveaus niet worden veranderd of ingetrokken zonder de voorafgaande schriftelijke toestemming van de partij van herkomst;
 - d) waarborgt dat gerubriceerde gegevens niet bekend worden gemaakt of vrijgegeven aan een derde zonder de voorafgaande schriftelijke toestemming van de partij van herkomst;
 - e) de gerubriceerde gegevens uitsluitend gebruikt voor het doel waarvoor zij zijn vrijgegeven en in overeenstemming met de eisen voor gebruik van de partij van herkomst.

Artikel 7

Beveiligingssamenwerking

1. Teneinde vergelijkbare beveiligingsnormen te handhaven, verstrekken de bevoegde beveiligingsautoriteiten elkaar op verzoek informatie over hun beveiligingsvoorschriften, -beleid en -praktijken met betrekking tot de beveiliging van gerubriceerde gegevens.
2. Op verzoek van de bevoegde beveiligingsautoriteit van de ene partij bevestigt de bevoegde beveiligingsautoriteit van de andere partij schriftelijk dat er een geldige veiligheidsmachtiging personeel of veiligheidsmachtiging bedrijfslocatie is afgegeven.
3. Indien een onderdaan van een partij een veiligheidsmachtiging personeel nodig heeft, kan de bevoegde beveiligingsautoriteit van de andere partij een verzoek om afgifte van een veiligheidsmachtiging personeel sturen naar de bevoegde beveiligingsautoriteit van de partij waarvan hij of zij onderdaan is, in overeenstemming met de nationale wet- en regelgeving.
4. Indien een opdrachtnemer onder de rechtsmacht van een partij een veiligheidsmachtiging bedrijfslocatie nodig heeft, kan de bevoegde beveiligingsautoriteit van de andere partij een verzoek om afgifte van een veiligheidsmachtiging bedrijfslocatie sturen naar de bevoegde beveiligingsautoriteit van de opdrachtnemer, in overeenstemming met de nationale wet- en regelgeving.
5. De bevoegde beveiligingsautoriteiten voeren antecedentenonderzoeken op hun onderdanen uit en geven veiligheidsmachtigingen personeel af of verstrekken informatie over de resultaten van het antecedentenonderzoek en veiligheidsmachtigingen bedrijfslocaties voor rechtspersonen onder hun rechtsmacht in overeenstemming met de nationale wet- en regelgeving.
6. De bevoegde beveiligingsautoriteiten verlenen elkaar, op verzoek en in overeenstemming met de nationale wet- en regelgeving, bijstand bij het uitvoeren van (antecedenten)onderzoeken in verband met de afgifte van een veiligheidsmachtiging bedrijfslocatie of veiligheidsmachtiging personeel.
7. De bevoegde beveiligingsautoriteiten stellen elkaar onverwijld schriftelijk in kennis van veranderingen in erkende veiligheidsmachtigingen personeel of veiligheidsmachtigingen bedrijfslocatie waarvoor een bevestiging is verstrekt.
8. Bij de samenwerking uit hoofde van dit Verdrag wordt gebruikgemaakt van de Engelse taal.

Artikel 8

Gerubriceerde contracten

1. Indien een partij of een opdrachtnemer onder haar rechtsmacht voorstelt een gerubriceerd contract op het rubriceringsniveau KONFIDENCIÁLI / Stg. CONFIDENTIEEL of hoger te gunnen aan een opdrachtnemer onder de rechtsmacht van de andere partij, dient zij eerst de schriftelijke bevestiging te verkrijgen van de andere partij dat aan deze opdrachtnemer een veiligheidsmachtiging bedrijfslocatie of veiligheidsmachtiging(en) personeel is/zijn toegekend op het juiste rubriceringsniveau. Voor gerubriceerde contracten met het rubriceringsniveau DIENESTA VAJADZÍBAM / DEPARTEMENTAAL VERTROUWELIJK zoals vermeld in artikel 4 van dit Verdrag, kan een veiligheidsmachtiging bedrijfslocatie nodig zijn indien dit verplicht is volgens de nationale wet- en regelgeving.

2. De bevoegde beveiligingsautoriteit waarborgt dat de opdrachtnemer:

- a) waarborgt dat alle natuurlijke personen die toegang krijgen tot gerubriceerde gegevens in kennis worden gesteld van hun verantwoordelijkheid de gerubriceerde gegevens te beveiligen in overeenstemming met de voorwaarden omschreven in dit Verdrag en de nationale wet- en regelgeving;
- b) de beveiligingsuitvoering op zijn locaties in het oog houdt;
- c) zijn bevoegde beveiligingsautoriteit onverwijld in kennis stelt van elk beveiligingsincident dat betrekking heeft op het gerubriceerd contract.
- d) Voor gerubriceerde contracten op het niveau KONFIDENCIÁLI / Stg. CONFIDENTIEEL of hoger, waarborgt de bevoegde beveiligingsautoriteit dat de opdrachtnemer een veiligheidsmachtiging bedrijfslocatie bezit met het juiste rubriceringsniveau teneinde de gerubriceerde gegevens te beveiligen en dat de natuurlijke personen die toegang dienen te krijgen tot gerubriceerde gegevens, een veiligheidsmachtiging personeel met het juiste rubriceringsniveau hebben.

3. Elk gerubriceerd contract dat in overeenstemming met dit Verdrag wordt gesloten dient een hoofdstuk met beveiligingsvereisten te bevatten waarin ten minste de volgende aspecten vermeld staan:

- a) een verwijzing naar dit Verdrag, de omschrijving van het begrip „gerubriceerde gegevens” in overeenstemming met artikel 2 van dit Verdrag en de tabel met de equivalente rubriceringsniveaus van de partijen in overeenstemming met de bepalingen van artikel 4 van dit Verdrag;
- b) een verklaring dat de gerubriceerde gegevens die zijn gegenereerd of verstrekt in het kader van een gerubriceerd contract beschermd zijn in overeenstemming met de nationale wet- en regelgeving;
- c) een verklaring dat de opdrachtnemer de gerubriceerde gegevens alleen bekend maakt aan natuurlijke personen die van de gegevens op de hoogte moeten zijn (need to know) en, in het geval van gerubriceerde gegevens op het niveau KONFIDENCIÁLI / Stg. CONFIDENTIEEL of hoger, een veiligheidsmachtiging personeel bezitten met het juiste rubriceringsniveau in overeenstemming met de bepalingen gespecificeerd in artikel 5 van dit Verdrag en zijn aangewezen om officieel taken of diensten te verrichten in relatie tot het gerubriceerde contract;
- d) een verklaring dat de opdrachtnemer geen gerubriceerde gegevens bekendmaakt of de bekendmaking daarvan toestaat aan een derde partij of enige andere partij die geen onderdeel is van het gerubriceerde contract zonder de voorafgaande schriftelijke toestemming van de partij van herkomst;
- e) een verklaring dat gerubriceerde gegevens die zijn verstrekt uit hoofde van het gerubriceerde contract uitsluitend worden gebruikt voor het doel waarvoor zij zijn verstrekt, of zoals verder schriftelijk uitdrukkelijk toegestaan door de partij van herkomst;
- f) een rubriceringsgids;
- g) een procedure voor het doorgeven van wijzigingen van het rubriceringsniveau, rekening houdend met artikel 4, derde lid, van dit Verdrag;
- h) de kanalen en procedures die gebruikt dienen te worden voor het vervoer, de overdracht of de overbrenging van gerubriceerde gegevens;
- i) een verklaring dat de gerubriceerde gegevens worden opgeslagen en verwerkt op locaties en in gerubriceerde informatiesystemen die zijn geaccrediteerd voor de opslag en de verwerking van gerubriceerde gegevens op het rubriceringsniveau dat is voorzien in het specifieke gerubriceerde contract. Deze verklaring staat los van de procedure voor het verkrijgen van een bevestiging met betrekking tot de toekenning van een veiligheidsmachtiging bedrijfslocatie zoals voorzien in het eerste lid van dit artikel;
- j) contactgegevens van de bevoegde beveiligingsautoriteiten die verantwoordelijk zijn voor het toezicht op de beveiliging van gerubriceerde gegevens die betrekking hebben op het gerubriceerde contract;
- k) de verplichting elk beveiligingsincident te melden.

4. De bevoegde beveiligingsautoriteit van de partij die de toekenning van het gerubriceerde contract goedkeurt, stuurt een kopie van het hoofdstuk over de beveiligingsvereisten naar de bevoegde beveiligingsautoriteit van de ontvangende partij, om het beveiligingstoezicht op het contract te vergemakkelijken.

5. De procedure voor de goedkeuring van bezoeken die samenhangen met activiteiten onder een gerubriceerd contract door personeel van de ene partij aan de andere partij, dient in overeenstemming met artikel 11 van dit Verdrag te zijn.

6. Indien een opdrachtnemer delen van een gerubriceerd contract uitbesteedt aan een onderopdrachtnemer, waarborgen de opdrachtnemer en de onderopdrachtnemer de naleving van al hun verplichtingen die voortvloeien uit dit Verdrag.

Artikel 9

Overbrenging van gerubriceerde gegevens

1. Gerubriceerde gegevens worden overgebracht in overeenstemming met de nationale wet- en regelgeving van de verstreckende partij of zoals anderszins overeengekomen tussen de bevoegde beveiligingsautoriteiten.
2. Gerubriceerde gegevens op het niveau KONFIDENCIĀLI / Stg. CONFIDENTIEEL worden overgebracht per koerier of diplomatieke post. Gerubriceerde gegevens op het niveau SLEPENI / Stg. GEHEIM worden overgebracht per diplomatieke koerier. De bevoegde beveiligingsautoriteiten kunnen alternatieve kanalen voor overbrenging afspreken in overeenstemming met de nationale wet- en regelgeving.
3. De persoon die de gerubriceerde gegevens overbrengt dient toestemming hebben voor toegang tot gerubriceerde gegevens met het overeenkomstige rubriceringsniveau.
4. Gerubriceerde gegevens moeten verpakt zijn in overeenstemming met de nationale wet- en regelgeving van de verstreckende partij.
5. Grote hoeveelheden gerubriceerde gegevens op het niveau KONFIDENCIĀLI / Stg. CONFIDENTIEEL of hoger moeten worden overgebracht in overeenstemming met een vervoersplan dat wordt bevestigd door de bevoegde beveiligingsautoriteiten van beide partijen. Wanneer van toepassing dient het vervoersplan in ieder geval de volgende informatie te bevatten:
 - a) omschrijving van het gerubriceerde contract;
 - b) omschrijving van de zending (met inbegrip van het rubriceringsniveau);
 - c) identificatie van de vertegenwoordigers van de deelnemende partijen (met inbegrip van de beveiligingsfunctionarissen van de locatie);
 - d) afleveringspunten, overdrachtpunten of verwerkingspunten;
 - e) identificatie van commerciële entiteiten die bij elke beweging betrokken worden;
 - f) vervoersroute.
6. Gerubriceerde gegevens op het niveau DIENESTA VAJADZĪBĀM / DEPARTEMENTAAL VERTROUWELIJK mogen uitsluitend worden overgebracht per aangetekende post of via andere bezorgingsdiensten in overeenstemming met de nationale wet- en regelgeving.
7. De partijen kunnen gerubriceerde gegevens die door encryptie beveiligd zijn alleen langs elektronische weg overbrengen in overeenstemming met procedures die door de bevoegde beveiligingsautoriteiten dienen te worden goedgekeurd.

Artikel 10

Reproductie, vertaling en vernietiging van gerubriceerde gegevens

1. Reproducties en vertalingen van gerubriceerde gegevens krijgen dezelfde rubriceringsmarkeringen en beveiliging als de oorspronkelijke gerubriceerde gegevens.
2. Vertalingen of reproducties worden beperkt tot het minimumaantal dat nodig is voor gebruik uit hoofde van dit Verdrag en worden uitsluitend gemaakt door natuurlijke personen die in overeenstemming met de nationale wet- en regelgeving gemachtigd zijn om toegang te krijgen tot gerubriceerde gegevens met het rubriceringsniveau van de gerubriceerde gegevens die vertaald of gereproduceerd worden.
3. Vertalingen dienen te worden voorzien van een passende annotatie in de taal waarin zij zijn gesteld met de aanduiding dat zij gerubriceerde gegevens bevatten van de verstreckende partij.
4. Gerubriceerde gegevens op het niveau SEVIŠĶI SLEPENI / Stg. ZEER GEHEIM worden niet vertaald of gereproduceerd zonder de voorafgaande schriftelijke toestemming van de partij van herkomst.
5. Gerubriceerde gegevens op rubriceringsniveau SEVIŠĶI SLEPENI / Stg. ZEER GEHEIM worden niet vernietigd zonder de voorafgaande schriftelijke toestemming van de partij van herkomst. De partij van herkomst besluit of de gegevens dienen te worden geretourneerd aan de partij van herkomst of worden vernietigd nadat de verstreckende en de ontvangende partij ze niet meer nodig achten.

6. Gerubriceerde gegevens tot en met rubriceringsniveau SLEPENI / Stg. GEHEIM worden in overeenstemming met haar nationale wet- en regelgeving vernietigd nadat de ontvangende partij ze niet meer nodig acht. In geval van het vernietigen van gerubriceerde gegevens op het niveau SLEPENI / Stg. GEHEIM informeert de ontvangende partij de partij van herkomst.

7. Indien een crisissituatie het onmogelijk maakt de uit hoofde van dit Verdrag verstrekte gerubriceerde gegevens te beveiligen, dienen de gerubriceerde gegevens onmiddellijk vernietigd te worden. De ontvangende partij stelt de bevoegde beveiligingsautoriteit van de partij van herkomst zo spoedig mogelijk schriftelijk in kennis van de vernietiging van deze gerubriceerde gegevens.

Artikel 11

Bezoeken

1. Bezoeken waarbij toegang tot gerubriceerde gegevens op het niveau KONFIDENCIÁLI / Stg. CONFIDENTI-EEL of hoger vereist is, dienen vooraf schriftelijk te worden goedgekeurd door de respectieve bevoegde beveiligingsautoriteit, tenzij anderszins overeengekomen door de bevoegde beveiligingsautoriteiten. Indien dit verplicht is volgens de nationale wet- en regelgeving van de als gastheer optredende partij kunnen bezoeken op het niveau DIENESTA VAJADZIBAM / DEPARTEMENTAAL VERTROUWELIJK onderworpen zijn aan voorafgaande schriftelijke toestemming van de bevoegde beveiligingsautoriteit van de als gastheer optredende partij.

2. De bezoeker dient de aanvraag voor het bezoek ten minste tien dagen vóór de beoogde datum van het bezoek in bij zijn bevoegde beveiligingsautoriteit, die de aanvraag doorstuurt naar de bevoegde beveiligingsautoriteit van de andere partij. In dringende gevallen kan de aanvraag van een verzoek binnen een kortere termijn worden ingediend, mits hierover voorafgaande coördinatie tussen de bevoegde beveiligingsautoriteiten plaatsvindt.

3. Een aanvraag voor een bezoek dient de volgende gegevens te bevatten:

- a) volledige naam van de bezoeker, geboortedatum en -plaats, nationaliteit en nummer paspoort/ identiteitskaart;
- b) officiële functiebenaming van de bezoeker en de naam van de organisatie die de bezoeker vertegenwoordigt;
- c) bevestiging van de veiligheidsmachtiging personeel van de bezoeker en de geldigheid ervan indien nodig;
- d) datum en duur van het bezoek. In het geval van herhalingsbezoeken dient de volledige periode waarin de bezoeken plaatsvinden te worden vermeld;
- e) doel van het bezoek en het verwachte rubriceringsniveau van de gerubriceerde gegevens die besproken worden of waartoe toegang wordt verkregen;
- f) naam, adres, telefoonnummer, e-mailadres en contactpunt van de te bezoeken locatie;
- g) van een datum en stempel voorziene handtekening van een vertegenwoordiger van de bevoegde beveiligingsautoriteit van de bezoeker.

4. De bevoegde beveiligingsautoriteiten kunnen een lijst overeenkomen van bezoekers die herhalingsbezoeken mogen afleggen. De bevoegde beveiligingsautoriteiten komen nadere details van de herhalingsbezoeken overeen.

5. Gerubriceerde gegevens die aan een bezoeker worden verstrekt of door deze worden verkregen, worden behandeld in overeenstemming met de bepalingen van dit Verdrag.

Artikel 12

Beveiligingsincident

1. De bevoegde beveiligingsautoriteiten stellen elkaar onverwijld schriftelijk in kennis van een feitelijk of potentieel beveiligingsincident waarbij gerubriceerde gegevens van de andere partij betrokken zijn.

2. De ontvangende partij onderzoekt feitelijke of potentiële beveiligingsincidenten onmiddellijk. De bevoegde beveiligingsautoriteit van de partij van herkomst verleent, indien nodig, medewerking aan het onderzoek.

3. De bevoegde beveiligingsautoriteit neemt passende maatregelen in overeenstemming met zijn nationale wet- en regelgeving om de gevolgen van het incident te beperken en herhalingen te voorkomen. De bevoegde beveiligingsautoriteit van de partij van herkomst wordt in kennis gesteld van de uitkomsten van het onderzoek en de eventuele getroffen maatregelen.

Artikel 13

Kosten

Elke partij draagt haar eigen kosten die ontstaan in verband met de implementatie en tenuitvoerlegging van haar verplichtingen ingevolge dit Verdrag.

Artikel 14

Oplossing van geschillen

Elk geschil omtrent de uitlegging of toepassing van dit Verdrag wordt door middel van overleg of onderhandelingen tussen de partijen opgelost en niet ter beslechting voorgelegd aan een nationaal of internationaal scheidsgerecht of een andere derde.

Artikel 15

Uitvoeringsregelingen

De bevoegde beveiligingsautoriteiten kunnen uitvoeringsregelingen sluiten ingevolge dit Verdrag.

Artikel 16

Slotbepalingen

1. Dit Verdrag wordt gesloten voor onbepaalde tijd. Elke partij stelt de andere partij langs diplomatieke weg in kennis van de voltooiing van de nationale procedures die nodig zijn voor de inwerkingtreding van dit Verdrag. Dit Verdrag treedt in werking op de eerste dag van de tweede maand die volgt op de ontvangst van de laatste kennisgeving.
2. Ten aanzien van het Koninkrijk der Nederlanden is dit Verdrag van toepassing op het Europese deel van Nederland en op het Caribische deel van Nederland (de eilanden Bonaire, Sint Eustatius en Saba).
3. Dit Verdrag kan alleen met wederzijdse instemming van de partijen worden gewijzigd. Elke partij kan op elk moment langs diplomatieke weg wijzigingen van dit Verdrag voorstellen. Deze wijzigingen treden in werking in overeenstemming met de in het eerste lid van dit artikel vastgelegde voorwaarden.
4. Onverminderd de bepalingen van het derde lid van dit artikel, worden wijzigingen van de Bijlage 1 bij dit Verdrag die tussen de bevoegde beveiligingsautoriteiten van de partijen kunnen worden overeengekomen, bij diplomatieke notawisseling bevestigd, en worden van kracht op een in de diplomatieke notawisseling te bepalen datum.
5. Een partij kan dit Verdrag te allen tijde schriftelijk langs diplomatieke weg beëindigen. In dat geval eindigt het Verdrag zes maanden na ontvangst van deze kennisgeving.
6. Ongeacht de beëindiging van dit Verdrag blijven alle uit hoofde van dit Verdrag uitgewisselde, vrijgegeven of gegenereerde gerubriceerde gegevens beveiligd in overeenstemming met de bepalingen van dit Verdrag voor de beëindiging ervan, zolang deze gerubriceerde gegevens gerubriceerd blijven.

TEN BLIJKE WAARVAN de vertegenwoordigers van de partijen, daartoe naar behoren gemachtigd, dit Verdrag hebben ondertekend.

GEDAAN te 's-Gravenhage op 15 januari 2024, in twee oorspronkelijke exemplaren, in de Letse, de Nederlandse en de Engelse taal, waarbij alle teksten gelijkelijk authentiek zijn. In geval van verschillen in interpretatie van dit Verdrag is de Engelse tekst doorslaggevend.

Voor het Koninkrijk der Nederlanden,

C.C.J. VELDKAMP

Voor de Republiek Letland,

B. BRAŽE

Bijlage I

De bevoegde beveiligingsautoriteit van de Republiek Letland is:

De Nationale Beveiligingsautoriteit
Bureau Grondwetbescherming

De bevoegde beveiligingsautoriteit van het Koninkrijk der Nederlanden is:

De Algemene Inlichtingen- en Veiligheidsdienst (AIVD)
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

De gemachtigde bevoegde beveiligingsautoriteit van het Koninkrijk der Nederlanden voor het militaire domein is:

De Beveiligingsautoriteit
Directoraat-Generaal Beleid
Ministerie van Defensie

D. PARLEMENT

Het Verdrag, met Bijlage, behoeft ingevolge artikel 91 van de Grondwet de goedkeuring van de Staten-Generaal, alvorens het Koninkrijk aan het Verdrag, met Bijlage, kan worden gebonden.

G. INWERKINGTREDING

De bepalingen van het Verdrag, met Bijlage, zullen ingevolge artikel 16, eerste lid, van het Verdrag in werking treden op de eerste dag van de tweede maand die volgt op de ontvangst van de laatste kennisgeving waarin de partijen elkaar langs diplomatieke weg in kennis hebben gesteld van de voltooiing van de nationale procedures die nodig zijn voor de inwerkingtreding van het Verdrag.

Uitgegeven de *twintigste* januari 2025.

De Minister van Buitenlandse Zaken,

C.C.J. VELDKAMP