

# TRACTATENBLAD

VAN HET

KONINKRIJK DER NEDERLANDEN

---

JAARGANG 2026 Nr. 80

---

## A. TITEL

*Verdrag tussen de Regering van het Koninkrijk der Nederlanden en de Regering van de Italiaanse Republiek  
inzake de uitwisseling en wederzijdse beveiliging van gerubriceerde gegevens (met Bijlage);  
Rome, 2 juli 2026*

Voor een overzicht van de verdragsgegevens, zie verdragsnummer 014113 in de Verdragenbank.

## B. TEKST

### **Agreement between the Government of the Kingdom of the Netherlands and the Government of the Italian Republic concerning the exchange and mutual protection of classified information**

The Government of the Kingdom of the Netherlands

and

the Government of the Italian Republic,

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

Wishing to ensure the mutual protection of Classified Information, in accordance with their national laws and regulations and in line with their respective interests of national security as well as their international commitments,

Have agreed upon the following:

#### Article 1

##### *Purpose and scope*

1. The purpose of this Agreement is to ensure the protection of Classified Information either exchanged between the Parties, between a Party and a Contractor under the jurisdiction of the other Party or between Contractors under the respective Parties' jurisdictions, or generated by the Parties, Contractors or Legal Entities within the scope of this Agreement. This Agreement sets out the security procedures and arrangements for such protection.
2. The provisions set out in this Agreement shall apply to any agreement, arrangement, contract or other form of co-operation involving Classified Information that will be concluded or conducted between the Parties, Contractors or Legal Entities under their jurisdiction.
3. The Parties shall take all appropriate measures under their national laws and regulations to ensure the protection of Classified Information in accordance with this Agreement.
4. This Agreement does not constitute a basis to compel the provision or exchange of Classified Information by the Parties.

## Article 2

### *Definitions*

For the purpose of this Agreement:

- a) "Agreement" means this document, including its Annex, which forms an integral part thereof.
- b) "Classified Contract" means any legally enforceable agreement to provide goods or services to be entered into by one of the Parties, a Contractor or Legal Entity under its jurisdiction, with the other Party, a Contractor, or Legal Entity under its jurisdiction, which contains Classified Information or the performance of which requires access, potential access to or generation of Classified Information. This includes pre-contractual activity.
- c) "Classified Information" means any information, material or object, regardless of its form or nature, or any parts thereof, marked with a security classification by one of the Parties or with a security classification mutually determined by both Parties in accordance with this Agreement, the unauthorised disclosure, alteration, compromise or loss of which could cause varying degrees of damage or harm to the interests of one or both of the Parties.
- d) "Competent Security Authority" means the government authority in a Party responsible for the supervision or the implementation of this Agreement. The Competent Security Authority may delegate part of its responsibilities to a delegated competent security authority.
- e) "Contractor" means any individual (other than those engaged by a Party under a contract of employment) or legal person, under the jurisdiction of a Party, engaging in any form of bidding process relating to, entering into or bound by a Classified Contract. This definition includes sub-contractors.
- f) "Facility Security Clearance" means the positive determination by the Competent Security Authority of one Party, following a vetting procedure carried out in accordance with its national laws and regulations, that a facility has in place appropriate security measures to access and handle Classified Information up to and including a specified security classification level.
- g) "Legal Entity" means any public or private body to which the national laws and regulations concerning the protection of Classified Information of a Party apply.
- h) "Need to Know" means the principle by which access to Classified Information may be granted to an individual only in connection with his/her official duties and for the performance of specific tasks.
- i) "Originator" means the Party under whose authority Classified Information has been created.
- j) "Personnel Security Clearance" means the positive determination by the Competent Security Authority of one Party, following a vetting procedure assessing the loyalty, trustworthiness and reliability of an individual, that such individual has been security cleared to access and handle Classified Information up to and including a specified classification level, in accordance with the national laws and regulations of that Party.
- k) "Providing Party" means the Party, including Contractors or Legal Entities under its jurisdiction, which provides Classified Information to the Receiving Party under this Agreement.
- l) "Receiving Party" means the Party, including Contractors or Legal Entities under its jurisdiction, which receives Classified Information from the Providing Party under this Agreement.
- m) "Security Classification Guide" means a document associated with a Classified Contract specifying the applicable security classification levels of each part of that Classified Contract.
- n) "Security Breach" means any act or omission contrary to national laws and regulations of the Receiving Party and/or this Agreement which may result in loss, unauthorised disclosure, misappropriation, alteration, or any other form of compromise, of Classified Information.
- o) "Third Party" means any international organisation, government or state, including individuals, legal persons or other forms of organisation under its jurisdiction, which is not a Party, a Contractor or a Legal Entity under this Agreement.

## Article 3

### *Competent security authorities*

1. The Competent Security Authorities of the Parties are listed in the Annex of this Agreement.
2. The Competent Security Authorities shall provide each other with official contact details and shall timely communicate each other any changes thereof.
3. The Competent Security Authorities shall notify each other of any other security authority responsible for the implementation of this Agreement.

## Article 4

### *Security classification levels*

1. The following security classifications of the Parties are equivalent and correspond to the security classification levels specified in the Parties' national laws and regulations. The English translation is not part of the national laws and regulations of the Parties and shall not be used to mark Classified Information.

| For the Italian Republic | For the Kingdom of the Netherlands | Translation in English |
|--------------------------|------------------------------------|------------------------|
| SEGRETISSIMO             | Stg. ZEER GEHEIM                   | TOP SECRET             |
| SEGRETO                  | Stg. GEHEIM                        | SECRET                 |
| RISERVATISSIMO           | Stg. CONFIDENTIEEL                 | CONFIDENTIAL           |
| RISERVATO                | DEPARTEMENTAAL VERTROUWELIJK       | RESTRICTED             |

2. Classified Information jointly originated by the Parties shall be assigned a security classification marking that is mutually agreed upon by the Parties.

3. The Originator may additionally mark, in English, the Classified Information with handling requirements, to specify any limitations on its use, disclosure, release and access by the Receiving Party.

## Article 5

### *Security measures*

1. The Parties shall afford Classified Information exchanged or generated under this Agreement at least the same protection as they afford to their national Classified Information at the corresponding security classification level.

2. The Providing Party shall mark Classified Information with the appropriate security classification, in accordance with its national laws and regulations. The Receiving Party may add an indication in order to ensure that Classified Information received from the Providing Party is protected at the corresponding security classification level in accordance with its own national laws and regulations. In any case, it shall always be clear who the Originator is.

3. The Receiving Party shall ensure that the security classification of Classified Information received under this Agreement is not modified or revoked without the written approval of the Originator.

4. The Providing Party shall inform the Receiving Party of any change in the security classification level of the Classified Information provided.

5. The Receiving Party shall ensure that Classified Information is not disclosed or released to a Third Party without the prior written consent and in accordance with any conditions required by the Originator.

6. The Receiving Party shall ensure that Classified Information is used solely for the purpose it has been released for and in accordance with handling requirements of the Originator. In particular, the Receiving Party shall not release Classified Information received from the Providing Party to a Contractor or a Legal Entity without the prior written consent of the Originator.

## Article 6

### *Access to Classified Information*

1. Access to Classified Information shall be granted only to those individuals who have a Need to Know, are briefed on and have acknowledged in writing their responsibilities on the protection of Classified Information, in accordance with the national laws and regulations of the Receiving Party.

2. In addition to the requirements in paragraph 1 of this article, access to Classified Information at RISERVATISSIMO / Stg. CONFIDENTIEEL and above shall be granted only to those individuals who hold a Personnel Security Clearance at least at the corresponding level or who are otherwise duly authorized to access Classified Information by virtue of their function, in accordance with the national laws and regulations of the Receiving Party.

## Article 7

### *Classified Contracts*

1. If a Party, a Contractor or Legal Entity under its jurisdiction proposes to place a Classified Contract at RISERVATISSIMO / Stg. CONFIDENTIEEL or above as mentioned in article 4 of this Agreement, to a Contractor under the jurisdiction of the other Party, it shall first obtain written confirmation from the Competent Security Authority of such Party that the Contractor has been granted a Facility Security Clearance at the appropriate security classification level.

2. For Classified Contracts at the security classification level equivalent to RISERVATO / DEPARTEMENTAAL VERTROUWELIJK a Facility Security Clearance may be required, if stipulated by national laws and regulations of the Party under whose jurisdiction the Contractor operates. In case a Facility Security Clearance is required under national laws and regulations of one Party, such a requirement for Facility Security Clearance shall not impose on the other Party additional obligations than those established by its own national laws and regulations.

3. Notwithstanding paragraph 2, upon request by the Competent Security Authority of the Dutch Party, the Competent Security Authority of the Italian Party shall initiate the procedure for granting a Facility Security Clearance to Contractors who may have access to Classified Information at DEPARTEMENTAAL VERTROUWELIJK level in the context of Classified Contracts in the military domain. The Competent Security Authority of the Dutch Party shall be informed of the outcome of such procedure.

4. Upon request, the Competent Security Authority of the Receiving Party shall inform the Competent Security Authority of the Providing Party whether a Contractor under its jurisdiction and participating in a Classified Contract or precontractual negotiations regarding a Classified Contract has been issued a Facility Security Clearance at the required security classification level. If the Contractor does not, at that point, hold a Facility Security Clearance, or the Facility Security Clearance is at a lower level than that required, the Competent Security Authority of the Receiving Party shall inform the Competent Security Authority of the Providing Party of that fact.

5. The Party under whose jurisdiction a Classified Contract is to be performed shall ensure that:

- a) all individuals who may be 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) the Contractor has the organizational capability to monitor the security conduct within its facilities;
- c) the Contractor notifies promptly its Competent Security Authority of any Security Breach relating to the Classified Contract.

6. In addition to the requirements in paragraph 5 of this Article, for Classified Contracts at RISERVATISSIMO / Stg. CONFIDENTIEEL or above the Competent Security Authority having jurisdiction over the Contractor shall ensure that, prior to accessing such Classified Information, it holds a Facility Security Clearance at the corresponding 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 least at the corresponding security classification level.

7. Every Classified Contract shall include security clauses referring to:

- a) a Security Classification Guide;
- b) a procedure for notification of changes in the security classification level, taking into account article 5, paragraph 4 of this Agreement;
- c) the channels and procedures to be used for the transport and/or transmission of Classified Information;
- d) instructions for the handling, storage, destruction and returning of Classified Information;
- e) contact details of the Competent Security Authorities responsible for overseeing the protection of Classified Information related to the Classified Contract;
- f) the obligation to notify any security incident to the Competent Security Authority of the Contractor and the obligation for Contractors to take all reasonable steps to assist in mitigating the effect of such a Security Breach, in consultation with the Competent Security Authority;
- g) in case a Classified Contract in whole or in part is sub-contracted to a sub-Contractor, the obligation to impose all the stipulations concerning Contractors in this Agreement to the sub-Contractor;
- h) a reference to this Agreement;
- i) a statement that Classified Information exchanged or generated pursuant to the Classified Contract shall be protected by the Contractor in accordance with this Agreement and applicable laws and regulations.

8. If a Classified Contract is awarded, the Party, the Contractor or Legal Entity shall, via its Competent Security Authority, forward a copy of the security clauses to the Competent Security Authority of the Receiving Party, to facilitate the security oversight of the Classified Contract.

9. The procedures for the approval of visits associated with Classified Contract activities by personnel under the jurisdiction of one Party to premises of the other Party or of a Contractor or Legal Entity under its jurisdiction shall be in accordance with article 8 of this Agreement.

## Article 8

### *Visits*

1. Visits requiring access to Classified Information at RISERVATISSIMO / Stg. CONFIDENTIEEL or above are subject to the prior written consent of the Competent Security Authority of the host Party, unless otherwise

jointly decided by the Competent Security Authorities. Such consent shall be given only to persons who have a Need to Know and who hold a valid Personnel Security Clearance at least at the corresponding level or who are otherwise duly authorised to access Classified Information by virtue of their function, in accordance with the national laws and regulations of the Receiving Party.

2. Visits to premises under the jurisdiction of the Italian Party requiring access to Classified Information at RISERVATO level are subject to the prior written consent of the Competent Security Authority of the Italian Party.

3. The visitors shall submit the request for visit at least twenty working days in advance of the proposed date of the visit to their Competent Security Authority, which shall forward it to the Competent Security Authority of the other Party. In urgent cases, the Competent Security Authorities may jointly consent to a shorter period.

4. 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 and present position of the visitor and name of the organization the visitor represents or to which the visitor belongs;
- c) confirmation of the visitor's Personnel Security Clearance and its level and validity;
- 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 highest security classification level of Classified Information to be discussed or accessed;
- f) name, address, phone number, e-mail address of the point of contact of the facility to be visited;
- g) dated and stamped signature of a representative of the visitor's Competent Security Authority.

5. The Competent Security Authority of the host Party shall inform the security officials of the facility to be visited of the details of those individuals whose visit request has been approved.

6. The Competent Security Authorities may agree on a list of visitors entitled to recurring visits for a period not exceeding twelve months. The Competent Security Authorities shall agree on the further details of the recurring visits. Requests for recurring visits shall be submitted in accordance with paragraph 3 of this article. Once the list has been approved, visits may be arranged directly between the facilities involved.

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

8. The Parties shall ensure, pursuant to their national laws and regulations, the protection of the personal data of the individuals requesting for a visit requiring access to Classified Information. This personal data shall not be used for any other purpose than determining on the request for the visit.

## Article 9

### *Transfer of Classified Information*

1. Classified Information shall be transferred in accordance with national laws and regulations of the Providing Party.

2. Classified Information at RISERVATISSIMO / Stg. CONFIDENTIEL and above shall be transferred through governmental channels or through other channels as otherwise agreed between the Competent Security Authorities of the Parties.

3. Classified Information at SEGRETISSIMO / Stg. ZEER GEHEIM level shall be sent only through diplomatic or military channels in accordance with national laws and regulations.

4. In case of transportation of a substantial volume of Classified Information, procedures for transport shall be jointly agreed and evaluated on a case-by-case basis by the Competent Security Authorities of the Parties.

5. Electronic transmission of Classified Information may take place only by using cryptographic means in accordance with procedures mutually approved by the Competent Security Authorities.

## Article 10

### *Reproduction, translation and destruction of Classified Information*

1. Reproductions and translations of Classified Information shall be marked and placed under the same protection as the original Classified Information.

2. Reproductions and translations shall be limited to the minimum amount required for use under this Agreement.
3. Translations shall contain a suitable annotation in the language of translation, indicating that they contain Classified Information of the Originator.
4. Classified Information marked at the security classification level equivalent to "TOP SECRET" as mentioned in article 4 of this Agreement, shall not be reproduced or translated without the prior written consent of the Originator.
5. Classified Information marked up to and including RISERVATISSIMO / Stg. CONFIDENTIEEL as mentioned in article 4 of this Agreement, shall be destroyed after it is no longer considered necessary by the Receiving Party.
6. Classified Information marked at SEGRETO / Stg. GEHEIM and above as mentioned in article 4 of this Agreement shall be destroyed only with the prior written consent of the Originator. The Receiving Party shall inform the Providing Party of such destruction.
7. By default, SEGRETISSIMO / Stg. ZEER GEHEIM shall be returned to the Providing Party after it is no longer considered necessary by the Receiving Party.
8. If a crisis situation makes it impossible for a Receiving Party to protect Classified Information provided under this Agreement, the Classified Information shall be destroyed immediately. The Receiving Party shall, via its Competent Security Authority, notify the Competent Security Authority of the Providing Party as soon as possible and in writing of the destruction of this Classified Information.

#### Article 11

##### *Protection of Classified Information in communication and information systems*

1. Each Party shall ensure that appropriate measures are implemented for the protection of Classified Information processed, stored and transmitted through communication and information systems in accordance with its national laws and regulations.
2. The Parties shall mutually recognise equipment and mechanisms related to communication and information systems used to process Classified Information as approved under their applicable national laws and regulations.

#### Article 12

##### *Security co-operation*

1. The Competent Security Authorities shall, on request, inform each other about changes in their national laws and 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. The Competent Security Authorities of the Parties shall recognize Personnel Security Clearances and Facility Security Clearances which are issued in accordance with the national laws and regulations of the other Party and within the scope of this Agreement.
4. The Competent Security Authorities shall assist each other in carrying out Facility Security Clearance and Personnel Security Clearance investigations on request and in accordance with their national laws and regulations.
5. 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.
6. The Competent Security Authorities of the Parties shall ensure that a foreign ownership, control and influence assessment is carried out in the respective procedures for the release of Facility Security Clearances.
7. A Competent Security Authority may request security assessment visits to be carried out by the Competent Security Authority of the other Party at private or public facilities under the latter Party's jurisdiction handling Classified Information provided or generated pursuant to this Agreement, in order to ensure that



best practices are employed and security standards are observed. Such security assessment visits are jointly decided by the Competent Security Authorities in advance.

8. In order to pursue the objectives of this Agreement, the Competent Security Authorities may visit each other, provided that prior adequate notice is given.

9. The Competent Security Authorities shall inform each other without undue delay of exceptional security risks that may endanger the Classified Information released by the Parties.

10. The co-operation under this Agreement shall be effected in the English language.

#### Article 13

##### *Security Breach*

1. In case a Security Breach involving the Classified Information of the Providing Party is suspected or ascertained by the Receiving Party, the Competent Security Authority of the Receiving Party shall inform the Competent Security Authority of the Providing Party in writing as soon as possible. The notice must contain sufficient details for the Originator to assess the consequences and circumstances of the suspected or actual violation.

2. The Receiving Party shall immediately investigate any actual or potential Security Breach. The Competent Security Authority of the Providing Party shall, if required, cooperate in the investigation. The Originator shall be informed of the outcome of the proceedings and the measures undertaken in connection with the Security Breach.

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

4. In case a Security Breach occurs outside of the jurisdiction of one of the Parties when Classified Information is sent from one Party to the other Party via Third Parties' territories or from one Party to a Third Party with the prior written consent of the Providing Party, the Competent Security Authority of the sending Party, shall, to the extent possible, take the actions referred to in paragraph 1 of this Article without undue delay.

#### Article 14

##### *Applicable law*

Each Party shall implement this Agreement in accordance with their own legislation, as well as applicable international law and the obligations arising from each Party' membership of the European Union.

#### Article 15

##### *Costs*

Each Party shall bear its own costs incurred in the course of implementing and executing its obligations under this Agreement. The expenses deriving from the implementation of this Agreement shall be covered by the Italian Party within the limits of its ordinary budget availability, without any additional costs for the State budget of the Italian Republic.

#### Article 16

##### *Dispute resolution*

Any dispute arising from the interpretation and/or implementation of this Agreement shall be settled exclusively through direct consultation or negotiations between the Parties and shall not be referred to any national or international tribunal or other entity for resolution.

#### Article 17

##### *Implementing arrangements*

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

## Article 18

### *Final provisions*

1. This Agreement is concluded for an indefinite period of time. Each Party shall notify the other Party through diplomatic channels once its 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 date of receipt of the last of the two notifications.
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, including its Annex, may be amended in writing 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, with the exception of an amendment to the Annex, which shall enter into force on a date to be agreed upon by the Parties.
4. Either Party may terminate this Agreement in writing at any time by notifying the other Party through diplomatic channels. In this case, the Agreement shall expire six months after receipt of such notification.
5. In case of termination of this Agreement, all Classified Information exchanged, released or generated under this Agreement shall remain protected in accordance with the terms of this Agreement before it was terminated, for as long as the Classified Information remains classified. Upon request, Classified Information shall be returned to the Providing Party in accordance with the provisions of this Agreement.

IN WITNESS whereof the undersigned, duly authorised thereto, have signed this Agreement.

DONE at Rome on July 2<sup>nd</sup> 2026, in two originals, each in the English, Dutch and Italian languages, all texts being equally authentic. In case of divergence of interpretation, the English text shall prevail.

*For the Government of the Kingdom of the Netherlands,*

MICHAEL STIBBE

*For the Government of the Italian Republic,*

VITTORIO RIZZI

---

### **ANNEX**

The Competent Security Authority for the Italian Republic is:

Presidency of the Council of Ministers  
Security Intelligence Department (DIS)  
Central Secrecy Office (UCSe)

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 de Regering van het Koninkrijk der Nederlanden en de Regering van de Italiaanse Republiek inzake de uitwisseling en wederzijdse beveiliging van gerubriceerde gegevens**

De Regering van het Koninkrijk der Nederlanden

en

de Regering van de Italiaanse Republiek,

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

Geleid door de wens de wederzijdse beveiliging te waarborgen van gerubriceerde gegevens, in overeenstemming met hun nationale wet- en regelgeving en in lijn met hun respectieve nationale veiligheidsbelangen en hun internationale verplichtingen,

Zijn het volgende overeengekomen:

## **Artikel 1**

### *Doel en reikwijdte*

1. Dit Verdrag heeft ten doel de beveiliging te waarborgen van gerubriceerde gegevens die ofwel worden uitgewisseld tussen de partijen, tussen een partij en een opdrachtnemer onder de rechtsmacht van de andere partij, of tussen opdrachtnemers onder de rechtsmacht van de respectieve partijen, of die worden gegenereerd door de partijen, opdrachtnemers of rechtspersonen binnen de reikwijdte van dit Verdrag. In dit Verdrag worden de beveiligingsprocedures en regelingen voor deze beveiliging vastgelegd.
2. De bepalingen van dit Verdrag zijn van toepassing op elke overeenkomst, regeling, contract of andere vorm van samenwerking waarbij gerubriceerde gegevens betrokken zijn, die of dat worden gesloten of uitgevoerd tussen de partijen, opdrachtnemers of rechtspersonen onder hun rechtsmacht.
3. De partijen nemen alle passende maatregelen krachtens hun nationale wet- en regelgeving om de beveiliging van gerubriceerde gegevens in overeenstemming met dit Verdrag te waarborgen.
4. Dit Verdrag vormt geen basis om de partijen ertoe te verplichten gerubriceerde gegevens te verstrekken of uit te wisselen.

## **Artikel 2**

### *Begripsomschrijvingen*

Voor de toepassing van dit Verdrag wordt verstaan onder:

- a. „Verdrag”, dit document, met inbegrip van de Bijlage erbij, die een integrerend onderdeel ervan uitmaakt.
- b. „Gerubriceerd contract”, elke wettelijk afdwingbare overeenkomst om goederen of diensten te leveren die een van de partijen of een opdrachtnemer of rechtspersoon onder haar rechtsmacht aangaat met de andere partij, een opdrachtnemer, of een rechtspersoon onder haar rechtsmacht, die gerubriceerde gegevens bevat of waarbij voor de uitvoering toegang of mogelijk toegang vereist is tot gerubriceerde gegevens of waarbij deze gegenereerd worden. Dit omvat tevens precontractuele activiteiten.
- c. „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 of van een rubriceringsniveau dat gezamenlijk wordt bepaald door beide partijen in overeenstemming met dit Verdrag, waarvan de ongeoorloofde bekendmaking, verandering, compromittering of het verlies de belangen van een of beide partijen in meerdere of mindere mate zou kunnen schaden.
- d. „Bevoegde beveiligingsautoriteit”, de overheidsautoriteit in een partij die verantwoordelijk is voor het toezicht op en de implementatie van dit Verdrag. De bevoegde beveiligingsautoriteit kan een deel van zijn verantwoordelijkheden delegeren aan een gemachtigde bevoegde beveiligingsautoriteit.
- e. „Opdrachtnemer”, elke persoon (anders dan degenen die door een partij in dienst zijn genomen op grond van een arbeidsovereenkomst) of rechtspersoon, onder de rechtsmacht van een partij, die meedoet aan een aanbestedingsprocedure in welke vorm dan ook, die een gerubriceerd contract aangaat of er door gebonden is. Dit begrip omvat tevens onderopdrachtnemers.
- f. „Veiligheidsmachtiging bedrijfslocatie”, de vaststelling door de bevoegde beveiligingsautoriteit van een partij, na een antecedentenonderzoek uitgevoerd in overeenstemming met haar nationale wet- en regelgeving, dat een bedrijfslocatie passende beveiligingsmaatregelen heeft genomen voor de toegang tot en omgang met gerubriceerde gegevens tot en met een gespecificeerd rubriceringsniveau.
- g. „Rechtspersoon”, elk publiek of privaat lichaam waarop de nationale wet- en regelgeving inzake de beveiliging van gerubriceerde gegevens van een partij van toepassing is.
- h. „Need to know”, het beginsel dat toegang tot gerubriceerde gegevens alleen aan een natuurlijke persoon

mag worden toegestaan in verband met zijn/haar officiële werkzaamheden en voor het uitvoeren van specifieke taken.

i. „Partij van herkomst”, de partij onder wier gezag gerubriceerde gegevens zijn gecreëerd.

j. „Veiligheidsmachtiging personeel”, de vaststelling door de bevoegde beveiligingsautoriteit van een partij, na een antecedentenonderzoek waarin de loyaliteit, integriteit en betrouwbaarheid van een natuurlijke persoon wordt beoordeeld, 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 van die partij.

k. „Verstreckende partij”, de partij, met inbegrip van opdrachtnemers of rechtspersonen onder haar rechtsmacht, die de gerubriceerde gegevens uit hoofde van dit Verdrag verstrekt aan de ontvangende partij.

l. „Ontvangende partij”, de partij, met inbegrip van opdrachtnemers of rechtspersonen onder haar rechtsmacht, die de gerubriceerde gegevens uit hoofde van dit Verdrag ontvangt van de verstreckende partij.

m. „Rubriceringsgids”, een document dat hoort bij een gerubriceerd contract waarin de van toepassing zijnde rubriceringsniveaus voor elk onderdeel van dat gerubriceerd contract worden gespecificeerd.

n. „Inbreuk op de beveiliging”, elk handelen of nalaten te handelen, in strijd met de nationale wet- en regelgeving van de ontvangende partij en/of dit Verdrag, dat kan resulteren in verlies, ongeoorloofde bekendmaking, onrechtmatig gebruik, verandering of enige andere vorm van compromittering van gerubriceerde gegevens.

o. „Derde”, elke internationale organisatie, regering of staat, met inbegrip van natuurlijke personen, rechtspersonen of andere organisatievormen onder zijn rechtsmacht die geen partij, opdrachtnemer of rechtspersoon is ingevolge dit Verdrag.

### Artikel 3

#### *Bevoegde beveiligingsautoriteiten*

1. De bevoegde beveiligingsautoriteiten van de partijen staan vermeld in de Bijlage bij dit Verdrag.
2. De bevoegde beveiligingsautoriteiten voorzien elkaar van de officiële contactgegevens en stellen elkaar tijdig in kennis van eventuele veranderingen daarvan.
3. De bevoegde beveiligingsautoriteiten stellen elkaar in kennis van enige andere beveiligingsautoriteit die verantwoordelijk is voor de implementatie van dit Verdrag.

### Artikel 4

#### *Rubriceringsniveaus*

1. De volgende rubriceringsniveaus van de partijen komen overeen en corresponderen met de rubriceringsniveaus die in de nationale wet- en regelgeving van de partijen staan vermeld. De Engelse vertaling maakt geen deel uit van de nationale wet- en regelgeving van de partijen en dient niet gebruikt te worden om gerubriceerde gegevens aan te duiden.

| Voor de Italiaanse Republiek | Voor het Koninkrijk der Nederlanden | Engelse vertaling |
|------------------------------|-------------------------------------|-------------------|
| SEGRETISSIMO                 | Stg. ZEER GEHEIM                    | TOP SECRET        |
| SEGRETO                      | Stg. GEHEIM                         | SECRET            |
| RISERVATISSIMO               | Stg. CONFIDENTIEEL                  | CONFIDENTIAL      |
| RISERVATO                    | DEPARTEMENTAAL VERTROUWELIJK        | RESTRICTED        |

2. Gerubriceerde gegevens die gezamenlijk worden aangemaakt door de partijen krijgen een rubriceringsniveau toegekend dat gezamenlijk wordt overeengekomen door de partijen.
3. De partij van herkomst kan de gerubriceerde gegevens tevens voorzien, in het Engels, van vereisten voor de omgang ermee, om eventuele beperkingen te stellen aan het gebruik, de bekendmaking, vrijgave en toegang door de ontvangende partij.

### Artikel 5

#### *Beveiligingsmaatregelen*

1. De partijen kennen aan gerubriceerde gegevens die uit hoofde van dit Verdrag worden uitgewisseld of gegenereerd ten minste dezelfde beveiliging toe als aan hun nationale gerubriceerde gegevens met een overeenkomstig rubriceringsniveau.
2. De verstreckende partij voorziet de gerubriceerde gegevens van de juiste rubriceringsmarkering, in overeenstemming met haar nationale wet- en regelgeving. De ontvangende partij kan een indicatie toevoegen om

te waarborgen dat de gerubriceerde gegevens die van de verstreckende partij worden ontvangen worden beveiligd op het overeenkomstige rubriceringsniveau in overeenstemming met haar eigen wet- en regelgeving. Het dient in elk geval steeds duidelijk te zijn wie de partij van herkomst is.

3. De ontvangende partij waarborgt dat het rubriceringsniveau van de uit hoofde van dit Verdrag ontvangen gerubriceerde gegevens niet wordt gewijzigd of ingetrokken zonder de schriftelijke toestemming van de partij van herkomst.

4. De verstreckende partij stelt de ontvangende partij op de hoogte van elke verandering van het rubriceringsniveau van de verstrekte gerubriceerde gegevens.

5. De ontvangende partij waarborgt dat de gerubriceerde gegevens niet bekend worden gemaakt of vrijgegeven aan een derde zonder de voorafgaande schriftelijke toestemming van de partij van herkomst en in overeenstemming met de voorwaarden die deze daar eventueel aan heeft verbonden.

6. De ontvangende partij waarborgt dat gerubriceerde gegevens uitsluitend worden gebruikt voor het doel waarvoor zij zijn verstrekt en in overeenstemming met de eisen voor gebruik van de partij van herkomst. De ontvangende partij geeft met name geen gerubriceerde gegevens die van de verstreckende partij zijn ontvangen vrij aan een opdrachtnemer of een rechtspersoon zonder de voorafgaande schriftelijke toestemming van de partij van herkomst.

## Artikel 6

### *Toegang tot gerubriceerde gegevens*

1. Toegang tot gerubriceerde gegevens wordt uitsluitend verleend aan de natuurlijke personen die van de gegevens op de hoogte moeten zijn (Need to know), zijn ingelicht over hun verantwoordelijkheden voor de beveiliging van gerubriceerde gegevens en deze schriftelijk hebben bevestigd, in overeenstemming met de nationale wet- en regelgeving van de ontvangende partij.

2. In aanvulling op de vereisten van het eerste lid van dit artikel wordt toegang tot gerubriceerde gegevens op niveau RISERVATISSIMO / Stg. CONFIDENTIEEL en hoger uitsluitend verleend aan de natuurlijke personen die een veiligheidsmachtiging personeel hebben op ten minste het overeenkomstige niveau of die anderszins gemachtigd zijn om toegang te krijgen tot gerubriceerde gegevens uit hoofde van hun functie, in overeenstemming met de nationale wet- en regelgeving van de ontvangende partij.

## Artikel 7

### *Gerubriceerde contracten*

1. Indien een partij, een opdrachtnemer of rechtspersoon onder haar rechtsmacht voorstelt een gerubriceerd contract op niveau RISERVATISSIMO / Stg. CONFIDENTIEEL of hoger, zoals vermeld in artikel 4 van dit Verdrag, te plaatsen bij een opdrachtnemer onder de rechtsmacht van de andere partij, dient zij eerst de schriftelijke bevestiging te verkrijgen van de bevoegde beveiligingsautoriteit van deze partij dat aan de opdrachtnemer een veiligheidsmachtiging bedrijfslocatie is toegekend op het juiste rubriceringsniveau.

2. Voor gerubriceerde contracten met het rubriceringsniveau dat overeenkomt met RISERVATO / DEPARTEMENTAAL VERTROUWELIJK kan een veiligheidsmachtiging bedrijfslocatie nodig zijn indien dit verplicht is volgens de nationale wet- en regelgeving van de partij onder wier rechtsmacht de opdrachtnemer zijn activiteiten uitvoert. In het geval een veiligheidsmachtiging bedrijfslocatie vereist is ingevolge de nationale wet- en regelgeving van een partij, legt een dergelijke vereiste voor een veiligheidsmachtiging bedrijfslocatie de andere partij geen aanvullende verplichtingen op dan die welke in haar eigen nationale wet- en regelgeving zijn vastgesteld.

3. Niettegenstaande het tweede lid, initieert de bevoegde beveiligingsautoriteit van de Italiaanse partij op verzoek van de bevoegde beveiligingsautoriteit van de Nederlandse partij de procedure voor het verlenen van een veiligheidsmachtiging bedrijfslocatie aan opdrachtnemers die mogelijk toegang hebben tot gerubriceerde gegevens op DEPARTEMENTAAL VERTROUWELIJK-niveau in het kader van gerubriceerde contracten op militair gebied. De bevoegde beveiligingsautoriteit van de Nederlandse partij wordt in kennis gesteld van de uitkomsten van deze procedure.

4. Op verzoek deelt de bevoegde beveiligingsautoriteit van de ontvangende partij de bevoegde beveiligingsautoriteit van de verstreckende partij mee of een opdrachtnemer die onder haar rechtsmacht valt en deelneemt aan een gerubriceerd contract of aan precontractuele onderhandelingen over een gerubriceerd contract, een veiligheidsmachtiging bedrijfslocatie heeft gekregen op het vereiste rubriceringsniveau. Indien de opdrachtnemer niet, op dat moment, over een veiligheidsmachtiging bedrijfslocatie beschikt, of de veilig-

heidsmachtiging bedrijfslocatie van een lager niveau is dan vereist, stelt de bevoegde beveiligingsautoriteit van de ontvangende partij de bevoegde beveiligingsautoriteit van de verstreckende partij van dat feit in kennis.

5. De partij onder wier rechtsmacht een gerubriceerd contract dient te worden uitgevoerd 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;
  - de opdrachtnemer over de organisatorische capaciteit beschikt om de beveiligingsuitvoering op zijn locaties in het oog te houden;
  - de opdrachtnemer zijn bevoegde beveiligingsautoriteit onverwijld in kennis stelt van elke inbreuk op de beveiliging die betrekking heeft op het gerubriceerd contract.

6. In aanvulling op de vereisten van het vijfde lid van dit artikel, waarborgt de bevoegde beveiligingsautoriteit onder wier rechtsmacht de opdrachtnemer valt, bij gerubriceerde contracten met beveiligingsniveau RISERVATISSIMO / Stg. CONFIDENTIEEL of hoger, dat deze, alvorens toegang te krijgen tot dergelijke gerubriceerde gegevens, een veiligheidsmachtiging bedrijfslocatie bezit met het overeenkomstige rubriceringsniveau teneinde de gerubriceerde gegevens te beveiligen en dat de natuurlijke personen die toegang dienen te krijgen tot gerubriceerde gegevens, een veiligheidsmachtiging personeel met ten minste het overeenkomstige rubriceringsniveau hebben.

7. Elk gerubriceerd contract bevat bepalingen inzake beveiliging die verwijzen naar:
- een rubriceringsgids;
  - een procedure voor kennisgeving van wijzigingen van het rubriceringsniveau, rekening houdend met artikel 5, vierde lid, van dit Verdrag;
  - de kanalen en procedures die gebruikt dienen te worden voor het vervoer en/of de overbrenging van gerubriceerde gegevens;
  - instructies voor de omgang met, opslag, vernietiging en retourneren van gerubriceerde gegevens;
  - contactgegevens van de bevoegde beveiligingsautoriteiten die verantwoordelijk zijn voor het toezicht op de beveiliging van gerubriceerde gegevens die betrekking hebben op het gerubriceerde contract;
  - de verplichting om de bevoegde beveiligingsautoriteit van de opdrachtnemer in kennis te stellen van elk beveiligingsincident en de verplichting voor opdrachtnemers om alle redelijke stappen te nemen om de gevolgen van een dergelijke beveiligingsinbreuk te beperken in samenspraak met de bevoegde beveiligingsautoriteit;
  - wanneer een gerubriceerd contract geheel of gedeeltelijk wordt uitbesteed aan een onderaannemer, de verplichting om alle bepalingen betreffende onderaannemers in dit Verdrag op te leggen aan de onderaannemer;
  - een verwijzing naar dit Verdrag;
  - een verklaring dat gerubriceerde gegevens die in het kader van het gerubriceerde contract worden uitgewisseld of gegenereerd, door de opdrachtnemer worden beschermd in overeenstemming met dit Verdrag en de toepasselijke wet- en regelgeving.

8. Indien een gerubriceerd contract wordt toegekend, stuurt de partij, via haar bevoegde beveiligingsautoriteit, de opdrachtnemer of de rechtspersoon, een kopie van de beveiligingsvereisten naar de bevoegde beveiligingsautoriteit van de ontvangende partij, om het toezicht op de beveiliging op het gerubriceerde contract te vergemakkelijken.

9. De procedure voor de goedkeuring van bezoeken die samenhangen met activiteiten onder een gerubriceerd contract door personeel onder de rechtsmacht van een partij op de locatie van de andere partij of van een opdrachtnemer of rechtspersoon onder haar rechtsmacht dient in overeenstemming met artikel 8 van dit Verdrag te zijn.

## Artikel 8

### *Bezoeken*

1. Bezoeken waarbij toegang tot gerubriceerde gegevens op niveau RISERVATISSIMO / Stg. CONFIDENTIEEL of hoger vereist is, dienen vooraf schriftelijk te worden goedgekeurd door de bevoegde beveiligingsautoriteit van de als gastheer optredende partij, tenzij anderszins gezamenlijk overeengekomen door de bevoegde beveiligingsautoriteiten. Deze goedkeuring wordt uitsluitend verleend aan de natuurlijke personen die van de gegevens op de hoogte moeten zijn (Need to know) en die een veiligheidsmachtiging personeel hebben op ten minste het overeenkomstige niveau of die anderszins gemachtigd zijn om toegang te krijgen tot gerubriceerde gegevens uit hoofde van hun functie, in overeenstemming met de nationale wet- en regelgeving van de ontvangende partij.

2. Bezoeken aan locaties onder de rechtsmacht van de Italiaanse partij waarbij toegang tot gerubriceerde gegevens nodig is op het niveau RISERVATO dienen vooraf schriftelijk te worden goedgekeurd door de bevoegde beveiligingsautoriteit van de Italiaanse partij.
3. De bezoekers dienen de aanvraag voor het bezoek ten minste twintig werkdagen vóór de beoogde datum van het bezoek in bij hun bevoegde beveiligingsautoriteit, die de aanvraag doorstuurt naar de bevoegde beveiligingsautoriteit van de andere partij. In dringende gevallen kunnen de bevoegde beveiligingsautoriteiten gezamenlijk een kortere termijn overeenkomen.
4. 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 en huidige functie van de bezoeker en de naam van de organisatie die de bezoeker vertegenwoordigt of waartoe de bezoeker behoort;
  - c. bevestiging van de veiligheidsmachtiging personeel van de bezoeker en het niveau en de geldigheid ervan;
  - 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 hoogste 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.
5. De bevoegde beveiligingsautoriteit van de partij die als gastheer optreedt stelt de beveiligingsbeambten van de te bezoeken locatie in kennis van de gegevens van de natuurlijke personen van wie het bezoek is goedgekeurd.
6. De bevoegde beveiligingsautoriteiten kunnen een lijst overeenkomen van bezoekers die herhalingsbezoeken mogen afleggen gedurende een periode van niet langer dan twaalf maanden. De bevoegde beveiligingsautoriteiten komen nadere details van de herhalingsbezoeken overeen. Verzoeken voor herhalingsbezoeken dienen in overeenstemming met het derde lid van dit artikel te worden ingediend. Wanneer de lijst eenmaal is goedgekeurd, mogen bezoeken rechtstreeks geregeld worden tussen de betrokken bedrijfslocaties.
7. Gerubriceerde gegevens die aan een bezoeker worden verstrekt of door deze worden verkregen, worden behandeld in overeenstemming met de bepalingen van dit Verdrag.
8. De partijen waarborgen, in overeenstemming met hun nationale wet- en regelgeving, de beveiliging van de persoonsgegevens van de individuen die een bezoek willen brengen waarbij toegang tot gerubriceerde gegevens nodig is. Deze persoonsgegevens worden niet gebruikt voor enig ander doel dan het besluit over de aanvraag voor het bezoek.

## Artikel 9

### *Overbrenging van gerubriceerde gegevens*

1. Gerubriceerde gegevens worden overgebracht in overeenstemming met de nationale wet- en regelgeving van de verstreckende partij.
2. Gerubriceerde gegevens op niveau RISERVATISSIMO / Stg. CONFIDENTIEEL en hoger worden overgebracht via overheidskanalen of via andere kanalen zoals anderszins overeengekomen door de bevoegde beveiligingsautoriteiten van de partijen.
3. Gerubriceerde gegevens op niveau SEGRETISSIMO / Stg. ZEER GEHEIM dienen alleen via diplomatieke of militaire kanalen te worden verzonden in overeenstemming met de nationale wet- en regelgeving.
4. In het geval van het vervoer van een aanzienlijk volume aan gerubriceerde gegevens, worden de vervoersprocedures gezamenlijk overeengekomen en per geval geëvalueerd door de bevoegde beveiligingsautoriteiten van de partijen.
5. De elektronische overbrenging van gerubriceerde gegevens mag alleen geschieden met gebruikmaking van cryptografische middelen in overeenstemming met procedures die door de bevoegde beveiligingsautoriteiten wederzijds dienen te worden goedgekeurd.

## Artikel 10

### *Reproductie, vertaling en vernietiging van gerubriceerde gegevens*

1. Reproducties en vertalingen van gerubriceerde gegevens krijgen dezelfde markering en beveiliging als de oorspronkelijke gerubriceerde gegevens.
2. Reproducties en vertalingen worden beperkt tot het minimumaantal dat nodig is voor gebruik uit hoofde van dit Verdrag.
3. Vertalingen worden voorzien van een passende annotatie in de taal waarin zij zijn gesteld met de aanduiding dat zij gerubriceerde gegevens bevatten van de partij van herkomst.
4. Gerubriceerde gegevens met het rubriceringsniveau dat overeenkomt met „TOP SECRET” zoals vermeld in artikel 4 van dit Verdrag worden niet gereproduceerd of vertaald zonder voorafgaande schriftelijke toestemming van de partij van herkomst.
5. Gerubriceerde gegevens tot en met rubriceringsniveau RISERVATISSIMO / Stg. CONFIDENTIEEL zoals vermeld in artikel 4 van dit Verdrag worden vernietigd nadat de ontvangende partij ze niet meer nodig acht.
6. Gerubriceerde gegevens met het rubriceringsniveau SEGRETO / Stg. GEHEIM en hoger zoals vermeld in artikel 4 van dit Verdrag worden uitsluitend vernietigd met de voorafgaande schriftelijke toestemming van de partij van herkomst. De ontvangende partij stelt de verstreckende partij in kennis van een dergelijke vernietiging.
7. Gerubriceerde gegevens met niveau SEGRETISSIMO / Stg. ZEER GEHEIM worden standaard geretourneerd aan de verstreckende partij nadat de ontvangende partij ze niet meer nodig acht.
8. Indien een crisissituatie het een ontvangende partij 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, via haar bevoegde beveiligingsautoriteit, de bevoegde beveiligingsautoriteit van de verstreckende partij zo spoedig mogelijk schriftelijk in kennis van de vernietiging van deze gerubriceerde gegevens.

## Artikel 11

### *Beveiliging van gerubriceerde gegevens in communicatie- en informatiesystemen*

1. Elke partij waarborgt dat passende maatregelen worden genomen voor de beveiliging van de gerubriceerde gegevens die worden verwerkt, opgeslagen en overgebracht door communicatie- en informatiesystemen, in overeenstemming met haar nationale wet- en regelgeving.
2. De partijen erkennen wederzijds apparatuur en mechanismen met betrekking tot communicatie- en informatiesystemen die worden gebruikt voor de verwerking van gerubriceerde gegevens, zoals goedgekeurd krachtens hun toepasselijke nationale wet- en regelgeving.

## Artikel 12

### *Beveiligingssamenwerking*

1. De bevoegde beveiligingsautoriteiten stellen elkaar, op verzoek, in kennis van veranderingen in hun nationale wet- en regelgeving, 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. De bevoegde beveiligingsautoriteiten van de partijen erkennen de veiligheidsmachtigingen personeel en veiligheidsmachtigingen bedrijfslocatie die overeenkomstig de nationale wet- en regelgeving van de andere partij en binnen de reikwijdte van dit Verdrag zijn afgegeven.
4. De bevoegde beveiligingsautoriteiten verlenen elkaar, op verzoek en in overeenstemming met hun nationale wet- en regelgeving, bijstand bij het uitvoeren van onderzoeken in verband met de afgifte van een veiligheidsmachtiging bedrijfslocatie en veiligheidsmachtiging personeel.



5. De bevoegde beveiligingsautoriteiten stellen elkaar onverwijld schriftelijk in kennis van veranderingen in erkende veiligheidsmachtigingen personeel en veiligheidsmachtigingen bedrijfslocatie waarvoor een bevestiging is verstrekt.
6. De bevoegde beveiligingsautoriteiten van de partijen waarborgen dat een FOCI-onderzoek (Foreign Ownership, Control and Influence) wordt uitgevoerd tijdens de respectieve procedures voor de afgifte van veiligheidsmachtigingen bedrijfslocatie.
7. Een bevoegde beveiligingsautoriteit kan verzoeken dat de bevoegde beveiligingsautoriteit van de andere partij beveiligingsbeoordelingsbezoeken aflegt in particuliere of openbare faciliteiten onder de rechtsmacht van laatstgenoemde partij die op grond van dit Verdrag verstrekte of gegenereerde gerubriceerde gegevens behandelen, om ervoor te zorgen dat beste praktijken worden toegepast en beveiligingsnormen worden nageleefd. Dergelijke beveiligingsbeoordelingsbezoeken worden vooraf gezamenlijk overeengekomen door de bevoegde beveiligingsautoriteiten.
8. Met het oog op de verwezenlijking van de doelstellingen van dit Verdrag kunnen de bevoegde beveiligingsautoriteiten elkaar bezoeken, mits vooraf een passende kennisgeving wordt gedaan.
9. De bevoegde beveiligingsautoriteiten stellen elkaar onverwijld in kennis van uitzonderlijke veiligheidsrisico's die de door de partijen vrijgegeven gerubriceerde gegevens in gevaar kunnen brengen.
10. Bij de samenwerking uit hoofde van dit Verdrag wordt gebruikgemaakt van de Engelse taal.

### Artikel 13

#### *Inbreuk op de beveiliging*

1. Indien een inbreuk op de beveiliging met betrekking tot de gerubriceerde gegevens van de verstreckende partij wordt vermoed of vastgesteld door de ontvangende partij, stelt de bevoegde beveiligingsautoriteit van de ontvangende partij de bevoegde beveiligingsautoriteit van de verstreckende partij daarvan zo spoedig mogelijk schriftelijk in kennis. De kennisgeving dient voldoende gedetailleerde informatie te bevatten om de partij van herkomst in staat te stellen de consequenties en omstandigheden van de vermoede of vastgestelde inbreuk te beoordelen.
2. De ontvangende partij onderzoekt feitelijke of vermoedelijke inbreuken op de beveiliging onmiddellijk. De bevoegde autoriteit van de verstreckende partij verleent, indien vereist, medewerking aan het onderzoek. De partij van herkomst wordt in kennis gesteld van de uitkomst van de procedure en van de maatregelen die worden getroffen in verband met de inbreuk op de beveiliging.
3. De bevoegde beveiligingsautoriteit van de ontvangende partij neemt passende maatregelen in overeenstemming met haar nationale wet- en regelgeving om de gevolgen van het beveiligingsincident te beperken en om herhaling ervan te voorkomen. De bevoegde beveiligingsautoriteit van de verstreckende partij wordt in kennis gesteld van de uitkomsten van het onderzoek en de eventuele getroffen maatregelen.
4. Indien zich buiten de rechtsmacht van een van de partijen een inbreuk op de beveiliging voordoet wanneer gerubriceerde gegevens van de ene partij naar de andere partij wordt verzonden via het grondgebied van een derde of van de ene partij naar een derde met voorafgaande schriftelijke toestemming van de verstreckende partij, neemt de bevoegde beveiligingsautoriteit van de verzendende partij, voor zover mogelijk, onverwijld de in het eerste lid van dit artikel bedoelde maatregelen.

### Artikel 14

#### *Toepasselijk recht*

Elke partij implementeert dit Verdrag in overeenstemming met haar eigen wetgeving alsmede met het toepasselijke internationale recht en de verplichtingen die voortvloeien uit het lidmaatschap van elke partij van de Europese Unie.

### Artikel 15

#### *Kosten*

Elke partij draagt haar eigen kosten die ontstaan bij de implementatie en tenuitvoerlegging van haar verplichtingen ingevolge dit Verdrag. De kosten die voortvloeien uit de implementatie van dit Verdrag worden door de Italiaanse partij gedekt binnen de grenzen van haar gewone beschikbare begroting, zonder extra kosten voor de staatsbegroting van de Italiaanse Republiek.

## Artikel 16

### *Oplossing van geschillen*

Elk geschil omtrent de uitlegging en/of implementatie van dit Verdrag wordt uitsluitend door middel van rechtstreeks overleg of onderhandelingen tussen de partijen opgelost en niet ter beslechting voorgelegd aan een nationaal of internationaal scheidsrecht of andere entiteit.

## Artikel 17

### *Uitvoeringsregelingen*

De bevoegde beveiligingsautoriteiten van de partijen kunnen uitvoeringsregelingen sluiten ingevolge dit Verdrag.

## Artikel 18

### *Slotbepalingen*

1. Dit Verdrag wordt gesloten voor onbepaalde tijd. Elke partij stelt de andere partij langs diplomatieke weg in kennis van de voltooiing van haar nationale procedures die nodig zijn voor de inwerkingtreding van dit Verdrag. Dit Verdrag treedt in werking op de eerste dag van de tweede maand na de datum van ontvangst van de laatste van de twee kennisgevingen.
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, met inbegrip van de Bijlage daarbij, kan met wederzijdse instemming van de partijen schriftelijk worden gewijzigd. Elke partij kan op elk moment langs diplomatieke weg wijzigingen van dit Verdrag voorstellen. Dergelijke wijzigingen treden in werking onder de voorwaarden vervat in het eerste lid van dit artikel, met uitzondering van een wijziging van de Bijlage, welke in werking treedt op een door de partijen overeen te komen datum.
4. Elk van de partijen kan dit Verdrag te allen tijde beëindigen door de andere partij daarvan langs diplomatieke weg schriftelijk kennis te geven. In dat geval eindigt het Verdrag zes maanden na ontvangst van deze kennisgeving.
5. In geval van 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. Op verzoek worden gerubriceerde gegevens geretourneerd aan de verstrekende partij in overeenstemming met de bepalingen van dit Verdrag.

TEN BLIJKE WAARVAN de ondergetekenden, daartoe naar behoren gemachtigd, dit Verdrag hebben ondertekend.

GEDAAN te Rome op 2 juli 2026, in twee oorspronkelijke exemplaren, elk in de Engelse, de Nederlandse en de Italiaanse taal, waarbij alle teksten gelijkelijk authentiek zijn. In geval van verschil in interpretatie is de Engelse tekst doorslaggevend.

*Voor de Regering van het Koninkrijk der Nederlanden,*

MICHAEL STIBBE

*Voor de Regering van de Italiaanse Republiek,*

VITTORIO RIZZI

---

## BIJLAGE

De bevoegde beveiligingsautoriteit van de Italiaanse Republiek is:  
Het Ufficio Centrale per la Segretezza (UCSe) (Centraal Bureau voor Veiligheid)  
van het Dipartimento delle Informazioni per la Sicurezza (DIS) (Departement Veiligheidsinlichtingen) van het Presidenza del Consiglio dei Ministri (Voorzitterschap van de Raad van Ministers)

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

---

**Accordo tra il Governo del Regno dei Paesi Bassi e il Governo della Repubblica Italiana relativo allo scambio e alla reciproca protezione delle informazioni classificate**

Il Governo del Regno dei Paesi Bassi

e

il Governo della Repubblica Italiana,

di seguito denominati collettivamente come „Parti”, e individualmente come „Parte”,

DESIDERANDO assicurare la reciproca protezione delle Informazioni Classificate, in conformità alle proprie leggi e regolamenti nazionali, in linea con i rispettivi interessi di sicurezza nazionale, nonché con i propri impegni internazionali,

Hanno concordato quanto segue:

**Articolo 1**

*Finalità e ambito applicativo*

1. La finalità del presente Accordo è assicurare la protezione delle Informazioni Classificate scambiate tra le Parti, tra una Parte e un Contraente sotto la giurisdizione dell'altra Parte o tra Contraenti sotto la giurisdizione delle rispettive Parti, ovvero generate dalle Parti, dai Contraenti o dalle Persone Giuridiche nell'ambito del presente Accordo. Il presente Accordo definisce le procedure e le disposizioni di sicurezza per tale protezione.
2. Le disposizioni del presente Accordo si applicano a ogni accordo, intesa, contratto o altra forma di cooperazione che coinvolga Informazioni Classificate conclusi o effettuati tra le Parti, i Contraenti o le Persone Giuridiche sotto la loro giurisdizione.
3. Le Parti adottano tutte le misure adeguate, ai sensi delle rispettive leggi e regolamenti nazionali, per assicurare la protezione delle Informazioni Classificate in conformità al presente Accordo.
4. Il presente Accordo non costituisce base giuridica idonea a obbligare le Parti alla cessione o allo scambio delle Informazioni Classificate.

**Articolo 2**

*Definizioni*

Ai fini del presente Accordo:

- a) „Accordo” indica il presente documento, incluso il suo Annesso che ne costituisce parte integrante.
- b) „Contratto Classificato” indica qualsiasi accordo giuridicamente vincolante per la fornitura di beni o servizi concluso da una delle Parti, da un Contraente o da una Persona Giuridica sotto la sua giurisdizione, con l'altra Parte, con un Contraente o con una Persona Giuridica sotto la sua giurisdizione, che contenga Informazioni Classificate o la cui esecuzione richieda l'accesso, il potenziale accesso o la produzione di Informazioni Classificate. Ciò include l'attività precontrattuale.
- c) „Informazione Classificata” indica qualunque informazione, materiale od oggetto, indipendentemente dalla sua forma o natura, o qualsiasi parte di essi, contrassegnati con una classifica di segretezza da una delle Parti o con una classifica di segretezza determinata reciprocamente da entrambe le Parti in conformità al presente Accordo, la cui divulgazione non autorizzata, alterazione, compromissione o perdita potrebbe causare diversi livelli di danno o lesione agli interessi di una o entrambe le Parti.
- d) „Autorità di Sicurezza Competente” indica l'autorità governativa di una Parte responsabile per la supervi-

sione o l'attuazione del presente Accordo. L'Autorità di Sicurezza Competente può delegare parte delle sue responsabilità a un'autorità di sicurezza competente delegata.

e) "Contraente" indica qualsiasi persona fisica (diversa da quelle impiegate da una Parte mediante contratto di lavoro) o giuridica, sotto la giurisdizione di una Parte, che partecipi a qualsiasi forma di procedura di gara relativa a un Contratto Classificato, ovvero che stipuli o sia vincolata da un Contratto Classificato. Questa definizione include i sub-contraenti.

f) "Abilitazione di Sicurezza Industriale" indica la determinazione positiva da parte dell'Autorità di Sicurezza Competente di una Parte, a seguito di una procedura di indagine eseguita in conformità alle proprie leggi e regolamenti nazionali, secondo la quale una struttura applica misure di sicurezza adeguate ad accedere a e trattare Informazioni Classificate fino a un determinato livello di classifica di segretezza.

g) "Persona Giuridica" indica qualsiasi ente pubblico o privato al quale si applicano le leggi e i regolamenti nazionali di una Parte relativi alla protezione delle Informazioni Classificate.

h) "Necessità di Conoscere" indica il principio in base al quale l'accesso alle Informazioni Classificate può essere concesso a un individuo solo in relazione alle proprie funzioni ufficiali e per l'esecuzione di compiti specifici.

i) "Originatore" indica la Parte sotto la cui autorità sono state create le Informazioni Classificate.

j) "Abilitazione di Sicurezza Personale" indica la determinazione positiva da parte dell'Autorità di Sicurezza Competente di una Parte, rilasciata all'esito di una procedura di indagine volta a valutare la fedeltà, la lealtà e l'affidabilità un individuo, che attesta che tale individuo è autorizzato ad accedere a e trattare Informazioni Classificate fino a un determinato livello di classifica, in conformità alle leggi e ai regolamenti nazionali di tale Parte.

k) "Parte Fornitrice" indica la Parte che fornisce Informazioni Classificate alla Parte Ricevente ai sensi del presente Accordo, ivi compresi i Contraenti o le Persone Giuridiche sotto la sua giurisdizione.

l) "Parte Ricevente" indica la Parte che riceve Informazioni Classificate dalla Parte Fornitrice ai sensi del presente Accordo, ivi compresi i Contraenti o le Persone Giuridiche sotto la sua giurisdizione.

m) "Guida alle Classifiche di Segretezza" indica un documento annesso a un Contratto Classificato che specifica i livelli di classifica di segretezza applicabili a ciascuna attività da esso prevista.

n) "Violazione di Sicurezza" indica qualsiasi atto od omissione contrario alle leggi e ai regolamenti nazionali della Parte Ricevente e/o al presente Accordo, che possa comportare la perdita, la divulgazione non autorizzata, l'appropriazione indebita, l'alterazione o qualsiasi altra forma di compromissione di Informazioni Classificate.

o) "Parte Terza" indica qualsiasi organizzazione internazionale, governo o stato, compresi individui, persone giuridiche o altre forme di organizzazione sotto la relativa giurisdizione, che non siano una Parte del presente Accordo, né un Contraente o una Persona Giuridica ai sensi dello stesso.

### Articolo 3

#### *Autorità di Sicurezza Competenti*

1. Le Autorità di Sicurezza Competenti delle Parti sono elencate nell'Annesso al presente Accordo.
2. Le Autorità di Sicurezza Competenti si forniscono reciprocamente i recapiti ufficiali e si comunicano tempestivamente eventuali modifiche degli stessi.
3. Le Autorità di Sicurezza Competenti si danno reciproca informazione in merito a qualsiasi altra autorità di sicurezza responsabile per l'attuazione del presente Accordo.

### Articolo 4

#### *Livelli di classifica di segretezza*

1. Le seguenti classifiche di segretezza delle Parti sono equivalenti e corrispondono ai livelli di classifica di segretezza individuati dalle leggi e dai regolamenti nazionali delle Parti. La traduzione in inglese non fa parte delle leggi e dei regolamenti nazionali delle Parti e non deve essere utilizzata per contrassegnare le Informazioni Classificate.

| Per la Repubblica Italiana | Per il Regno dei Paesi Bassi | Traduzione in inglese |
|----------------------------|------------------------------|-----------------------|
| SEGRETISSIMO               | Stg. ZEER GEHEIM             | TOP SECRET            |
| SEGRETO                    | Stg. GEHEIM                  | SECRET                |
| RISERVATISSIMO             | Stg. CONFIDENTIEEL           | CONFIDENTIAL          |
| RISERVATO                  | DEPARTEMENTAAL VERTROUWELIJK | RESTRICTED            |

2. Alle Informazioni Classificate generate congiuntamente dalle Parti è assegnato un contrassegno di classifica di segretezza concordato dalle Parti medesime.

3. L'Originatore può apporre un contrassegno in lingua inglese sulle Informazioni Classificate con requisiti di gestione, al fine di specificare ogni eventuale limitazione di utilizzo, divulgazione, rilascio e accesso per la Parte Ricevente.

## Articolo 5

### *Misure di sicurezza*

1. Le Parti garantiscono alle Informazioni Classificate scambiate o generate ai sensi del presente Accordo almeno la stessa protezione assegnata alle proprie Informazioni Classificate nazionali con livello di classifica di segretezza corrispondente.

2. La Parte Fornitrice contrassegna le Informazioni Classificate con la classifica di segretezza adeguata, in conformità alle leggi e ai regolamenti nazionali. La Parte Ricevente può aggiungere un'indicazione al fine di garantire che le Informazioni Classificate ricevute dalla Parte Fornitrice siano protette al corrispondente livello di classifica di segretezza, in conformità alle leggi e ai regolamenti nazionali. In ogni caso, l'Originatore è sempre chiaramente individuato.

3. La Parte Ricevente assicura che la classifica di segretezza attribuita alle Informazioni Classificate ricevute ai sensi del presente Accordo non sia modificata o revocata senza l'approvazione scritta dell'Originatore.

4. La Parte Fornitrice informa la Parte Ricevente di qualsiasi modifica al livello di classifica di segretezza delle Informazioni Classificate fornite.

5. La Parte Ricevente assicura che le Informazioni Classificate non siano divulgate o rilasciate a Terze Parti senza il previo consenso scritto dell'Originatore e in conformità alle condizioni poste da esso.

6. La Parte Ricevente assicura che le Informazioni Classificate siano utilizzate esclusivamente per lo scopo per cui sono state rilasciate e in conformità ai requisiti di gestione indicati dall'Originatore. In particolare, la Parte Ricevente non divulga le Informazioni Classificate ricevute dalla Parte Fornitrice a un Contraente o a una Persona Giuridica senza il previo consenso scritto dell'Originatore.

## Articolo 6

### *Accesso alle Informazioni Classificate*

1. L'accesso alle Informazioni Classificate è concesso solo agli individui che hanno Necessità di Conoscere, sono stati istruiti e hanno accettato per iscritto le proprie responsabilità in materia di protezione delle Informazioni Classificate, in conformità alle leggi e ai regolamenti nazionali della Parte Ricevente.

2. In aggiunta ai requisiti di cui al paragrafo 1 del presente articolo, l'accesso alle Informazioni Classificate al livello RISERVATISSIMO / Stg. CONFIDENTIEEL e superiore è concesso solo agli individui in possesso di un'Abilitazione di Sicurezza Personale al livello almeno corrispondente o che, in alternativa, siano stati debitamente autorizzati ad accedere ad Informazioni Classificate in virtù della loro funzione, in conformità alle leggi e ai regolamenti nazionali della Parte Ricevente.

## Articolo 7

### *Contratti classificati*

1. Se una Parte, un Contraente o una Persona Giuridica sotto la sua giurisdizione propone di assegnare un Contratto Classificato al livello RISERVATISSIMO / Stg. CONFIDENTIEEL o superiore ai sensi dell'articolo 4 del presente Accordo a un Contraente sotto la giurisdizione dell'altra Parte, essa deve ottenere conferma scritta, dall'Autorità di Sicurezza Competente di tale Parte, che al Contraente sia stata rilasciata un'Abilitazione di Sicurezza Industriale al livello di classifica di segretezza adeguato.

2. Per i Contratti Classificati a un livello di classifica di segretezza equivalente a RISERVATO / DEPARTEMENTAAL VERTROUWELIJK, può essere richiesta un'Abilitazione di Sicurezza Industriale ove prevista dalle leggi e dai regolamenti nazionali della Parte sotto la cui giurisdizione opera il Contraente. Qualora un'Abilitazione di Sicurezza Industriale sia richiesta dalle leggi e dai regolamenti nazionali di una Parte, tale requisito non impone all'altra Parte obblighi aggiuntivi rispetto a quelli stabiliti dalle proprie leggi e dai propri regolamenti nazionali.

3. Fermo restando quanto stabilito nel paragrafo 2, su richiesta dell'Autorità di Sicurezza Competente della Parte neerlandese, l'Autorità di Sicurezza Competente della Parte italiana avvia la procedura per il rilascio di un'Abilitazione di Sicurezza Industriale ai Contraenti che potrebbero avere accesso a Informazioni Classificate

al livello DEPARTEMENTAAL VERTROUWELIJK nell'ambito di Contratti Classificati relativi al settore militare. L'Autorità di Sicurezza Competente della Parte neerlandese è informata dell'esito di tale procedura.

4. Su richiesta, l'Autorità di Sicurezza Competente della Parte Ricevente informa l'Autorità di Sicurezza Competente della Parte Fornitrice sul possesso un'Abilitazione di Sicurezza Industriale al livello di classifica di segretezza richiesto da parte di un Contraente sotto la propria giurisdizione che partecipi a un Contratto Classificato o a trattative precontrattuali relative a un Contratto Classificato. Se il Contraente non è in possesso di un'Abilitazione di Sicurezza Industriale, ovvero se l'Abilitazione di Sicurezza Industriale è di un livello inferiore a quello richiesto, l'Autorità di Sicurezza Competente della Parte Ricevente ne informa l'Autorità di Sicurezza Competente della Parte Fornitrice.

5. La Parte sotto la cui giurisdizione è eseguito un Contratto Classificato assicura che:

- d) tutti gli individui cui può essere consentito l'accesso alle Informazioni Classificate siano informati delle loro responsabilità in relazione alla protezione di tali Informazioni, in conformità alle condizioni definite nel presente Accordo e alle leggi e ai regolamenti nazionali;
- e) il Contraente abbia la capacità organizzativa di monitorare la condotta di sicurezza all'interno delle proprie strutture;
- f) il Contraente notifichi tempestivamente alla propria Autorità di Sicurezza Competente qualsiasi Violazione di Sicurezza afferente al Contratto Classificato.

6. In aggiunta ai requisiti di cui al paragrafo 5 del presente articolo, per i Contratti Classificati al livello RISERVATISSIMO / Stg. CONFIDENTIEEL o superiore, l'Autorità di Sicurezza Competente che ha giurisdizione sul Contraente garantisce che, prima di accedere a tali Informazioni Classificate, quest'ultimo sia in possesso di un'Abilitazione di Sicurezza Industriale al corrispondente livello di classifica di segretezza al fine di proteggere le Informazioni Classificate e che gli individui che richiedono l'accesso a dette Informazioni Classificate siano in possesso di un'Abilitazione di Sicurezza Personale almeno al corrispondente livello di classifica di segretezza.

7. Ogni Contratto Classificato include clausole di sicurezza relative a:

- a) una Guida alle Classifiche di Segretezza;
- b) una procedura per la notifica delle modifiche del livello di classifica di segretezza, tenendo conto dell'articolo 5, paragrafo 4 del presente Accordo;
- c) i canali e le procedure da utilizzare per il trasporto e/o la trasmissione delle Informazioni Classificate;
- d) istruzioni per la gestione, la custodia, la distruzione e la restituzione delle Informazioni Classificate;
- e) i recapiti delle Autorità di Sicurezza Competenti responsabili per il monitoraggio della protezione delle Informazioni Classificate relative al Contratto Classificato;
- f) l'obbligo di notificare ogni incidente di sicurezza all'Autorità di Sicurezza Competente del Contraente e l'obbligo per i Contraenti di adottare tutte le misure utili per contribuire a mitigare l'effetto di tale Violazione di Sicurezza, in consultazione con l'Autorità di Sicurezza Competente;
- g) nel caso in cui un Contratto Classificato venga subappaltato in tutto o in parte a un sub-Contraente, l'obbligo di imporre al sub-Contraente tutte le disposizioni relative ai Contraenti previste dal presente Accordo;
- h) un riferimento al presente Accordo;
- i) una dichiarazione secondo cui le Informazioni Classificate scambiate o generate ai sensi del Contratto Classificato saranno protette dal Contraente in conformità al presente Contratto e alle leggi e ai regolamenti in vigore.

8. Ove si aggiudichi un Contratto Classificato, la Parte, il Contraente o la Persona Giuridica inoltra, tramite la propria Autorità di Sicurezza Competente, una copia delle clausole di sicurezza all'Autorità di Sicurezza Competente della Parte Ricevente, al fine agevolare la supervisione degli aspetti di sicurezza di detto Contratto Classificato.

9. Le procedure per l'approvazione delle visite correlate alle attività di un Contratto Classificato da parte di personale sotto la giurisdizione di una Parte presso i locali dell'altra Parte, o di un Contraente o Persona Giuridica sotto la sua giurisdizione, avvengono in conformità all'articolo 8 del presente Accordo.

## Articolo 8

### *Visite*

1. Le visite che richiedono l'accesso a Informazioni Classificate al livello RISERVATISSIMO / Stg. CONFIDENTIEEL o superiore sono soggette al previo consenso scritto dell'Autorità di Sicurezza Competente della Parte ospitante, salvo diversa decisione congiunta delle Autorità di Sicurezza Competenti. Tale consenso è rilasciato esclusivamente agli individui che hanno Necessità di Conoscere e che sono in possesso di un'Abilitazione di Sicurezza del Personale valida al livello almeno corrispondente o che, in alternativa, sono debitamente autorizzati ad accedere alle Informazioni Classificate in virtù della loro funzione, in conformità alle leggi e ai regolamenti nazionali della Parte Ricevente.



2. Le visite che richiedono l'accesso a Informazioni Classificate di livello RISERVATO presso locali sotto la giurisdizione della Parte italiana sono soggette al previo consenso scritto dell'Autorità di Sicurezza Competente della suddetta Parte italiana.
3. I visitatori presentano la richiesta di visita almeno venti giorni lavorativi prima della data prevista per detta visita alla propria Autorità di Sicurezza Competente, che la inoltra all'Autorità di Sicurezza Competente dell'altra Parte. In casi urgenti, le Autorità di Sicurezza Competenti possono concordare congiuntamente un termine più breve.
4. Le richieste di visita includono:
- a) nome del visitatore, data e luogo di nascita, nazionalità e numero di passaporto/ documento d'identità;
  - b) titolo ufficiale, carica attuale del visitatore e nome dell'organizzazione che il visitatore rappresenta o alla quale il visitatore appartiene;
  - c) conferma dell'Abilitazione di Sicurezza Personale del visitatore e del suo livello e validità;
  - d) data e durata della visita. In caso di visite ricorrenti, deve essere indicato il periodo complessivo coperto dalle visite;
  - e) finalità della visita e livello di classifica di segretezza più elevato previsto per le Informazioni Classificate oggetto di discussione o accesso;
  - f) nome, indirizzo, numero di telefono, indirizzo e-mail del punto di contatto della struttura da visitare;
  - g) data, timbro e firma di un rappresentante dell'Autorità di Sicurezza Competente del visitatore.
5. L'Autorità di Sicurezza Competente della Parte ospitante comunica ai responsabili per la sicurezza della struttura da visitare le informazioni sulle persone la cui richiesta di visita è stata approvata.
6. Le Autorità di Sicurezza Competenti possono concordare un elenco di visitatori autorizzati a visite ricorrenti per un periodo non superiore a dodici mesi. Le Autorità di Sicurezza Competenti concordano ulteriori dettagli relativi alle visite ricorrenti. Le richieste di visite ricorrenti devono essere presentate in conformità al paragrafo 3 del presente articolo. Una volta approvato l'elenco, le visite possono essere organizzate direttamente tra le strutture interessate.
7. Le Informazioni Classificate fornite o acquisite da un visitatore sono trattate come disposto dalle previsioni del presente Accordo.
8. Le Parti assicurano, in conformità alle proprie leggi e regolamenti nazionali, la protezione dei dati personali degli individui che chiedono di svolgere visite che possano comportare l'accesso a Informazioni Classificate. Tali dati personali non sono impiegati per finalità diverse dalla decisione in merito alla richiesta di visita.

## Articolo 9

### *Trasmissione delle Informazioni Classificate*

1. Le Informazioni Classificate sono trasmesse in conformità alle leggi e ai regolamenti nazionali della Parte Fornitrice.
2. Le Informazioni Classificate al livello RISERVATISSIMO / Stg. CONFIDENTIEL e superiore sono trasmesse tramite canali governativi o tramite altri canali alternativamente concordati tra le Autorità di Sicurezza Competenti delle Parti.
3. Le Informazioni Classificate al livello SEGRETISSIMO / Stg. ZEER GEHEIM sono trasmesse unicamente attraverso canali diplomatici o militari, in conformità alle leggi e ai regolamenti nazionali.
4. In caso di trasmissione di un volume considerevole di Informazioni Classificate, le procedure di trasporto sono concordate congiuntamente e valutate caso per caso dalle Autorità di Sicurezza Competenti delle Parti.
5. La trasmissione elettronica di Informazioni Classificate può avvenire solo con l'impiego di mezzi crittografici in conformità alle procedure reciprocamente approvate dalle Autorità di Sicurezza Competenti.

## Articolo 10

### *Riproduzione, traduzione e distruzione delle Informazioni Classificate*

1. Le riproduzioni e le traduzioni di Informazioni Classificate sono contrassegnate alla stregua delle Informazioni Classificate originali e sottoposte alla medesima protezione.
2. Le riproduzioni e le traduzioni sono limitate al numero minimo richiesto per l'uso previsto dal presente Accordo.

3. Le traduzioni recano un'annotazione adeguata nella lingua della traduzione, che indica la presenza di Informazioni Classificate dell'Originatore.
4. Le Informazioni Classificate contrassegnate con un livello di classifica di segretezza equivalente a "TOP SECRET", ai sensi dell'articolo 4 del presente Accordo, non sono riprodotte o tradotte senza il previo consenso scritto dell'Originatore.
5. Le Informazioni Classificate contrassegnate al livello RISERVATISSIMO / Stg. CONFIDENTIEL e inferiore ai sensi dell'articolo 4 del presente Accordo sono distrutte quando ritenute non più necessarie dalla Parte Ricevente.
6. Le Informazioni Classificate contrassegnate SEGRETO / Stg. GEHEIM e superiore ai sensi dell'articolo 4 del presente Accordo sono distrutte solo con il previo consenso scritto dell'Originatore. La Parte Ricevente informa la Parte Fornitrice di tale distruzione.
7. Di regola, le Informazioni Classificate al livello SEGRETISSIMO / Stg. ZEER GEHEIM sono restituite alla Parte Fornitrice quando ritenute non più necessarie dalla Parte Ricevente.
8. Qualora una situazione di crisi renda impossibile per la Parte Ricevente proteggere le Informazioni Classificate fornite ai sensi del presente Accordo, le Informazioni Classificate sono immediatamente distrutte. La Parte Ricevente, tramite la propria Autorità di Sicurezza Competente, notifica il prima possibile e per iscritto all'Autorità di Sicurezza Competente della Parte Fornitrice la distruzione di tali Informazioni Classificate.

## Articolo 11

### *Protezione delle informazioni classificate nei sistemi di comunicazione e informazione*

1. Ciascuna Parte garantisce l'attuazione di misure adeguate per la protezione delle Informazioni Classificate elaborate, archiviate e trasmesse tramite sistemi di comunicazione e informazione, in conformità alle proprie leggi e regolamenti nazionali.
2. Le Parti riconoscono reciprocamente le apparecchiature e i meccanismi relativi ai sistemi di comunicazione e informazione utilizzati per elaborare le Informazioni Classificate, come approvati dalle rispettive leggi e regolamenti nazionali applicabili.

## Articolo 12

### *Cooperazione di sicurezza*

1. Le Autorità di Sicurezza Competenti, su richiesta, si informano reciprocamente in merito alle modifiche apportate alle rispettive leggi e regolamenti nazionali, alle direttive e alle prassi per la protezione delle Informazioni Classificate.
2. Su richiesta dell'Autorità di Sicurezza Competente di una Parte, l'Autorità di Sicurezza Competente dell'altra Parte fornisce conferma scritta dell'avvenuto rilascio di un'Abilitazione di Sicurezza Personale o di un'Abilitazione di Sicurezza Industriale.
3. Le Autorità di Sicurezza Competenti delle Parti riconoscono le Abilitazioni di Sicurezza Personali e le Abilitazioni di Sicurezza Industriali rilasciate in conformità alle leggi e ai regolamenti nazionali dell'altra Parte e nell'ambito del presente Accordo.
4. Su richiesta e in conformità alle rispettive leggi e regolamenti nazionali, le Autorità di Sicurezza Competenti si prestano reciproca assistenza nello svolgimento delle indagini relative alle Abilitazioni di Sicurezza Industriali e alle Abilitazioni di Sicurezza Personali.
5. Le Autorità di Sicurezza Competenti si notificano tempestivamente per iscritto circa le modifiche alle Abilitazioni di Sicurezza Personali e alle Abilitazioni di Sicurezza Industriali riconosciute per le quali è stata fornita conferma.
6. Le Autorità di Sicurezza Competenti delle Parti garantiscono lo svolgimento di una valutazione sugli assetti proprietari, sul controllo e sull'influenza stranieri nell'ambito delle rispettive procedure per il rilascio delle Abilitazioni di Sicurezza Industriali.
7. Un'Autorità di Sicurezza Competente può richiedere che l'Autorità di Sicurezza Competente dell'altra Parte effettui visite di valutazione della sicurezza presso strutture private o pubbliche soggette alla giurisdizione di quest'ultima Parte che trattano Informazioni Classificate fornite o generate ai sensi del presente Accordo, al

fine di garantire l'impiego delle migliori prassi e il rispetto degli standard di sicurezza. Tali visite di valutazione della sicurezza sono decise congiuntamente in anticipo dalle Autorità di Sicurezza Competenti.

8. Al fine di perseguire gli obiettivi del presente Accordo, le Autorità di Sicurezza Competenti possono scambiarsi visite, a condizione che sia dato adeguato preavviso.

9. Le Autorità di Sicurezza Competenti si informano reciprocamente, senza ingiustificato ritardo, in merito a rischi di sicurezza straordinari che potrebbero mettere a repentaglio le Informazioni Classificate rilasciate dalle Parti.

10. Le attività di cooperazione nell'ambito del presente Accordo sono effettuate in lingua inglese.

### Articolo 13

#### *Violazione di Sicurezza*

1. In caso di Violazione di Sicurezza sospetta o accertata dalla Parte Ricevente che riguarda le Informazioni Classificate della Parte Fornitrice, l'Autorità di Sicurezza Competente della Parte Ricevente informa per iscritto il prima possibile l'Autorità di Sicurezza Competente della Parte Fornitrice. La notifica include dettagli sufficienti a consentire all'Originatore di valutare le conseguenze e le circostanze della sospetta o effettiva violazione.

2. La Parte Ricevente indaga immediatamente su qualsiasi Violazione di Sicurezza, effettiva o potenziale. L'Autorità di Sicurezza Competente della Parte Fornitrice, ove necessario, collabora all'indagine. L'Originatore è informato dell'esito del procedimento e delle misure adottate in relazione alla Violazione di Sicurezza.

3. L'Autorità di Sicurezza Competente della Parte Ricevente adotta misure adeguate, in conformità alle proprie leggi e regolamenti nazionali, per limitare le conseguenze e impedire il ripetersi dell'incidente di sicurezza. L'Autorità di Sicurezza Competente della Parte Fornitrice è informata dell'esito dell'indagine e, se del caso, delle misure adottate.

4. Nel caso in cui si verifichi una Violazione di Sicurezza al di fuori della giurisdizione di una delle Parti quando le Informazioni Classificate sono inviate da una Parte all'altra tramite il territorio di una Parte Terza, ovvero da una Parte a una Parte Terza con il previo consenso scritto della Parte Fornitrice, l'Autorità di Sicurezza Competente della Parte trasmittente, nei limiti del possibile, adotta le misure di cui al paragrafo 1 del presente articolo senza ingiustificato ritardo.

### Articolo 14

#### *Normativa applicabile*

Ciascuna Parte applica il presente Accordo nel rispetto della propria legislazione, del diritto internazionale vigente e degli obblighi derivanti dall'appartenenza all'Unione europea.

### Articolo 15

#### *Costi*

Ciascuna Parte si fa carico delle spese sostenute nel corso dell'attuazione e dell'esecuzione dei propri obblighi derivanti dal presente Accordo. Le spese derivanti dall'attuazione del presente Accordo sono coperte dalla Parte italiana nei limiti delle proprie disponibilità di bilancio ordinarie, senza alcun onere aggiuntivo per il bilancio dello Stato della Repubblica Italiana.

### Articolo 16

#### *Risoluzione delle controversie*

Ogni controversia derivante dall'interpretazione e/o dall'attuazione del presente Accordo è risolta esclusivamente mediante consultazione diretta o negoziazione tra le Parti e non è deferita ad alcun tribunale nazionale o internazionale né ad altro soggetto per la risoluzione.

### Articolo 17

#### *Intese implementative*

Le Autorità di Sicurezza Competenti delle Parti possono concludere intese implementative ai sensi del presente Accordo.

## Articolo 18

### *Disposizioni finali*

1. Il presente Accordo è concluso per un periodo di tempo indeterminato. Ciascuna Parte notifica all'altra Parte, tramite canali diplomatici, l'avvenuto completamento delle procedure nazionali necessarie per l'entrata in vigore dello stesso Accordo. L'Accordo entra in vigore il primo giorno del secondo mese successivo alla data di ricezione dell'ultima delle due notifiche.
2. Per il Regno dei Paesi Bassi, il presente Accordo si applica alla parte europea e alla parte caraibica dei suddetti Paesi Bassi (isole di Bonaire, Sint Eustatius e Saba).
3. Il presente Accordo, incluso il suo Annesso, può essere modificato per iscritto con il reciproco consenso delle Parti. Ciascuna Parte può proporre emendamenti a detto Accordo in qualsiasi momento attraverso canali diplomatici. Tali emendamenti entrano in vigore alle condizioni stabilite al paragrafo 1 del presente articolo, ad eccezione degli emendamenti all'Annesso, che entrano in vigore alla data concordata tra le Parti.
4. Ciascuna Parte può denunciare il presente Accordo in qualsiasi momento per iscritto, dandone comunicazione all'altra Parte attraverso i canali diplomatici. In tal caso, l'Accordo cessa di produrre effetti sei mesi dopo la ricezione di tale comunicazione.
5. In caso di risoluzione del presente Accordo, tutte le Informazioni Classificate scambiate, diffuse o generate ai sensi dello stesso sono protette in conformità alle disposizioni in esso contenute prima della denuncia, per tutto il tempo in cui le Informazioni Classificate restano classificate. Su richiesta, le Informazioni Classificate sono restituite alla Parte Fornitrice in conformità alle disposizioni di detto Accordo.

IN FEDE DI CHE i sottoscritti, debitamente autorizzati, hanno firmato il presente Accordo

FATTO a Roma il 2 luglio 2026, in due copie originali, ciascuna in lingua inglese, neerlandese e italiana, tutti i testi facendo ugualmente fede.

In caso di divergenze nell'interpretazione, il testo in inglese prevale.

*Per il Governo del Regno dei Paesi Bassi,*

MICHAEL STIBBE

*Per il Governo della Repubblica Italiana,*

VITTORIO RIZZI

---

### **ANNESSO**

L'Autorità di Sicurezza Competente per la Repubblica Italiana è:

Ufficio Centrale per la Segretezza (UCSe)  
Dipartimento Informazioni per la Sicurezza (DIS)  
Presidenza del Consiglio dei Ministri

L'Autorità di Sicurezza Competente per il Regno dei Paesi Bassi è:

De Algemene Inlichtingen- en Veiligheidsdienst (AIVD) (Servizio di Intelligence e Sicurezza Civile)  
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (Ministero dell'Interno e delle Relazioni con il Regno)

L'Autorità di Sicurezza Competente Delegata per il Regno dei Paesi Bassi nell'ambito militare è:

De Beveiligingsautoriteit (Autorità di Sicurezza Competente)  
Directoraat-Generaal Beleid (Direzione generale-Politiche strategiche)  
Ministerie van Defensie (Ministero della Difesa)

---

#### D. PARLEMENT

Het Verdrag, met Bijlage, heeft 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 18, eerste lid, van het Verdrag in werking treden op de eerste dag van de tweede maand na de datum van ontvangst van de laatste van de twee kennisgevingen 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 *zestiende* juli 2026.

*De Minister van Buitenlandse Zaken,*

T.B.W. BERENDSEN