20 (2024) Nr. 1

TRACTATENBLAD

VAN HET

KONINKRIJK DER NEDERLANDEN

JAARGANG 2024 Nr. 150

A. TITEL

Verdrag tussen het Koninkrijk der Nederlanden en de Portugese Republiek inzake de uitwisseling en wederzijdse beveiliging van gerubriceerde gegevens (met Bijlage); 's-Gravenhage, 11 december 2024

Voor een overzicht van de verdragsgegevens, zie verdragsnummer 012025 in de Verdragenbank.

B. TEKST[1)]

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

The Kingdom of the Netherlands

and

the Portuguese Republic,

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

Recognizing the important role of their joint co-operation in ensuring peace, international security, and mutual confidence,

Considering that they share equivalent security standards for the protection of classified information and

In order to ensure the mutual protection of Classified Information, have, in the interests of national security, agreed upon the following:

Article 1

Purpose and scope

1. The purpose of this Agreement is to ensure the protection of Classified Information exchanged between the Parties, between one Party and a Contractor under the jurisdiction of the other Party, between Contractors under the respective Parties' jurisdiction, or generated in the framework of a bilateral program under this Agreement. This Agreement sets out the security procedures and arrangements for such protection.

2. The Parties shall take all appropriate measures under their internal law to ensure the protection of Classified Information in accordance with this Agreement.

3. This Agreement does not constitute a basis to compel the provision or exchange of Classified Information by the Parties.

[1)] De Portugese tekst is niet opgenomen.

Article 2

Definitions

For the purpose of this Agreement:
a) **"Agreement"** means this document, including its Annex;
b) **"Classified Contract"** means any legally binding instrument to provide goods and/or services to be entered into by one of the Parties or a Contractor under its jurisdiction with a Contractor under the jurisdiction of the other Party, which contains Classified Information or the performance of which requires access or potential access to Classified Information. This term includes pre-contractual activity;
c) **"Classified Information"** means any information regardless of its form that is assigned a security classification level by a Party, 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. This information may include reproductions, translations, and material in the process of development;
d) **"Competent Security Authority"** means the government authority in a Party responsible for the implementation and supervision 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), legal entity or other forms of organisation under the jurisdiction of a Party, entering into or bound by a Classified Contract. This term includes a sub-contractor;
f) **"Facility Security Clearance"** means the administrative determination by the Competent Security Authority that, from a security viewpoint, a facility can afford adequate security protection to Classified Information, in accordance with its internal law;
g) **"Need to Know"** means the requirement for an authorised individual, legal entity or other form of organisation to access, have knowledge of, or possess Classified Information in order to be able to perform their official duties or services;
h) **"Originating Party"** means the Party under whose authority Classified Information has been created;
i) **"Personnel Security Clearance"** means the administrative determination by the Competent Security Authority that an individual has been security cleared to access and handle Classified Information up to and including a specified classification level, in accordance with its internal law;
j) **Program/Project Security Instruction**" "means a compilation of security regulations and procedures based on national security policy and supporting directives, which are applied to a specific program or project in order to standardize security procedures;
k) **"Providing Party"** means the Party or Contractor under its jurisdiction, which provides Classified Information to the Receiving Party under this Agreement;
l) **"Receiving Party"** means the Party or Contractor 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 Incident"** means any unauthorised disclosure, alteration, compromise, loss, access, handling, storage or destruction of Classified Information, contrary to internal law of the Receiving Party and/or this Agreement;
o) **"Third Party"** means any international organisation, government or state, including individuals, legal entities or other forms of organisation under its jurisdiction, which is not a Party to this Agreement.

Article 3

Competent Security Authorities

1. The Competent Security Authorities of the Parties are listed in the Annex of this Agreement.

2. The Competent Security Authorities shall provide each other with official contact details and any changes thereof.

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' internal law. The English equivalent is an informal translation, not part of the internal law of the Parties and shall not be used to mark Classified Information.

TABLE 1

For the Kingdom of the Netherlands	For the Portuguese Republic	Equivalent in English
Stg. ZEER GEHEIM	MUITO SECRETO	TOP SECRET
Stg. GEHEIM	SECRETO	SECRET
Stg. CONFIDENTIEEL	CONFIDENCIAL	CONFIDENTIAL
DEPARTEMENTAAL VERTROUWELIJK	RESERVADO	RESTRICTED

2. Classified Contracts within the military domain at the security classification level equivalent to "DEPARTEMENTAAL VERTROUWELIJK" shall be treated as "CONFIDENCIAL" for the purpose of issuing a Facility Security Clearance pursuant to article 7.

Article 5

Security measures

1. The Originating Party shall assign a security classification level to Classified Information and shall mark the Classified Information according to its internal law.

2. The Receiving Party shall mark all the Classified Information that it has received from the Providing Party with the Receiving Party's security classification that corresponds to the security classification given by the Originating Party in accordance with article 4 and, where applicable, in accordance with paragraph 5 of this article.

3. The Receiving Party shall not modify or revoke the security classification of received or generated Classified Information under this Agreement without the written approval of the Originating Party.

4. The Originating Party shall ensure that the Receiving Party will be informed of any change in the security classification level of the Classified Information provided.

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

6. Classified Information jointly originated by the Parties shall be assigned a security classification that is mutually determined by the Parties.

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

8. In accordance with article 1, paragraph 2 of this Agreement, the Parties shall take all appropriate measures to ensure that the Providing Party:
a) marks Classified Information with the appropriate security classification in accordance with its internal law;
b) informs the Receiving Party of any conditions of release or limitations on the use of the Classified Information provided.

9. In accordance with article 1, paragraph 2 of this Agreement, the Parties shall take all appropriate measures to ensure that the Receiving Party:
a) affords the same level of protection to Classified Information as afforded to its national Classified Information of an equivalent security classification level;
b) ensures that Classified Information is not disclosed or released to a Third Party without the prior written consent of the Originating Party and, if deemed necessary, on conditions;
c) uses Classified Information solely for the purpose it has been released for and in accordance with handling requirements of the Originating Party.

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 their responsibilities for the protection of Classified Information, and have signed a statement of confidentiality in accordance with the internal law of the Receiving Party.

2. In addition to the requirements in paragraph 1 of this article, access to Classified Information at the security classification levels equivalent to "CONFIDENTIAL" and above as mentioned in article 4 of this Agreement, shall be granted only to those individuals who hold a Personnel Security Clearance at the corresponding level or who are otherwise duly authorised to access Classified Information by virtue of their function, in accordance with the internal law of the Receiving Party.

Article 7

Classified contracts

1. Upon request of the Originating Party, the Competent Security Authority of the Receiving Party shall inform the Competent Security Authority of the Originating Party whether a Contractor, under jurisdiction of the Receiving Party and participating in 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 receiving the request shall inform the requesting Competent Security Authority of that fact.

2. If a Party or a Contractor under its jurisdiction proposes to grant a Classified Contract at a security classification level equivalent to "CONFIDENTIAL" or above as mentioned in article 4 of this Agreement, with a Contractor under the jurisdiction of the other Party, it shall first obtain written confirmation from the Competent Security Authority of the other Party that the Contractor has been granted a Facility Security Clearance at the appropriate security classification level. For Classified Contracts at the security classification level equivalent to "RESTRICTED" as mentioned in article 4 of this Agreement, a Facility Security Clearance may be required, if mandated by respective internal law of the Contractor.

3. In accordance with article 1, paragraph 2 of this Agreement, the Party under whose jurisdiction the Classified Contract is to be performed shall ensure that the Contractor:
a) ensures that all individuals granted access to Classified Information are informed of their responsibilities to protect Classified Information in accordance with the conditions defined in this Agreement and in accordance with their internal law;
b) monitors the security conduct within its facilities;
c) notifies promptly its Competent Security Authority of any Security Incident relating to the Classified Contract.

4. In addition to article 7, paragraph 3, subparagraphs a), b) and c) of this Agreement, for Classified Contracts at the security classification levels equivalent to "CONFIDENTIAL" or above as mentioned in article 4 of this Agreement, the Competent Security Authority shall ensure that the Contractor holds a Facility Security Clearance at the appropriate security classification level in order to protect the Classified Information and that the individuals requiring access to Classified Information hold a Personnel Security Clearance at the appropriate security classification level.

5. Every Classified Contract shall include security requirements which identify the following aspects:
a) a Security Classification Guide;
b) a procedure for notification of changes in the security classification level;
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 Incidents 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 violation, in consultation with the Competent Security Authority;
g) in case a Classified Contract in whole or in part is sub-contracted, 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.

6. The Competent Security Authority of the Party or a Contractor under its jurisdiction awarding the Classified Contract shall forward a copy of the security requirements to the Competent Security Authority of the Receiving Party, to facilitate the security oversight of the Classified Contract.

7. When the size or complexity of a program or project and the Classified Information involved require the application of additional security requirements, the Parties, through their respective Competent Security Authorities, shall jointly determine a Program/Project Security Instruction and include it in the Classified Contract as an annex.

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

Article 8

International visits

1. Visits requiring access to Classified Information at a security classification level equivalent to "CONFIDENTIAL" or above as mentioned in article 4 of this Agreement are subject to the prior written consent of the Competent Security Authority of the host Party, unless otherwise agreed between 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 the appropriate level or who are otherwise duly authorised to access Classified Information by virtue of their function, in accordance with the internal law of the Receiving Party. If mandated by internal law of the host Party, "RESTRICTED" level visits may be subject to the prior written consent of the Competent Security Authority of the host Party.

2. The visitor shall submit the request for visit at least ten calendar days in advance of the proposed date of the visit to his Competent Security Authority, which shall forward it to the Competent Security Authority of the other Party. In urgent cases, the Competent Security Authorities may agree on a shorter period.

3. Request for visit shall include:
a) full name of the visitor, date and place of birth, nationality and passport/ID card number;
b) official title 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 facility's point of contact to be visited;
g) dated and stamped signature of a representative of the visitor's Competent Security Authority.

4. The Competent Security Authorities may agree on a list of visitors entitled to recurring visits for a period not exceeding twelve months. The Competent Security Authorities shall agree on the further details of the recurring visits.

5. The Competent Security Authority of the host Party shall inform the security officials of the organization to be visited, of the details of those individuals whose visit request has been approved. Once approval has been given, visit arrangements for individuals who have been given approval for recurring visits may be made directly with the agency, facility or organization concerned.

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

7. The parties shall ensure, pursuant to their internal law, 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 (recurring) visits.

Article 9

Transmission of Classified Information

1. Classified Information shall be transmitted in accordance with internal law of the Originating Party or as otherwise agreed between the Competent Security Authorities.

2. Electronic transmission of Classified Information may take place only by using cryptographic means in accordance with procedures to be approved jointly by the Competent Security Authorities.

3. At the request of the Originating Party, the Receiving Party shall provide the Originating Party with confirmation, in writing, that it has received Classified Information.

4. The Parties, through their respective Competent Security Authority, shall advise a contractor of the means and the packaging standards that the Parties have jointly approved for the transmission of Classified Information.

5. If Classified Information is too voluminous to be transmitted by approved courier, the Parties, through their respective Competent Security Authority, shall jointly approve a transportation plan that describes how they intend to transmit the Classified Information. That plan may include the type of transport, the route, and the type of escort for the Classified Information.

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 number 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 Originating Party.

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 Originating Party.

5. Classified Information marked at the security classification level equivalent to "TOP SECRET" as mentioned in article 4 of this Agreement shall be returned to the Originating Party after it is no longer considered necessary by the Receiving Party, or it may be destroyed solely with the prior written consent of the Originating Party.

6. Classified Information marked up to and including the security classification level equivalent to "SECRET" as mentioned in article 4 of this Agreement, shall be destroyed after it is no longer considered necessary by the Receiving Party.

7. 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 notify promptly in writing the Competent Security Authority of the Originating Party about the destruction of this Classified Information.

Article 11

Security co-operation

1. The Competent Security Authorities shall inform each other about changes in their internal law, 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 issued in accordance with the internal law of the other Party and in 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 internal law.

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

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

Article 12

Security Incident

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

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

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

4. The Competent Security Authority of the Receiving Party shall take appropriate measures in accordance with its internal law to limit the consequences and to prevent a recurrence of the Security Incident. The Competent Security Authority of the Originating Party shall be informed of the outcome of the investigation and, if any, of the measures taken.

Article 13

Costs

Each Party shall bear its own costs incurred in the course of implementing and executing its obligations under this Agreement, unless otherwise mutually determined by the Parties.

Article 14

Dispute resolution

Any dispute arising from the interpretation, implementation or application of this Agreement shall be settled through consultation or negotiations between the Parties, through diplomatic channels.

Article 15

Implementing arrangements

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

Article 16

Final provisions

1. This Agreement is concluded for an indefinite period of time.

2. Each Party shall notify the other Party, through diplomatic channels, once the respective national procedures necessary for entry into force of this Agreement have been completed. This Agreement shall enter into force on the first day of the second month following the receipt of the latter notification.

3. 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).

4. This Agreement, including its Annex, may be amended at any time by mutual written 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 2 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.

5. Either Party may terminate this Agreement in writing at any time through diplomatic channels. In this case, the Agreement shall expire six months after the receipt of such notification.

6. 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, unless the Parties mutually agree otherwise.

7. After the entry into force of this Agreement, the Party in whose territory it is signed shall transmit it for registration to the Secretariat of the United Nations, according to Article 102 of the Charter of the United Nations and Article 80 of the Vienna Convention on the Law of Treaties and shall notify the other Party of the conclusion of this proceeding, indicating the respective number of registration.

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

DONE in the Hague, on 11 December 2024, in two original copies, in the Portuguese, Dutch, and English languages, all texts being equally authentic. In case of divergence of interpretation, the English text shall prevail.

For the Kingdom of the Netherlands,

CASPAR VELDKAMP

For the Portuguese Republic,

INÊS DOMINGOS

Annex

The Competent Security Authority for the Portuguese Republic is:
National Security Authority
Presidency of the Council of Ministers

The Competent Security Authority for the Kingdom of the Netherlands is:
General Intelligence and Security Service
Ministry of the Interior and Kingdom Relations

The delegated Competent Security Authority for the Kingdom of the Netherlands in the military domain is:
Defence Security Authority
Directorate-General of Policy
Ministry of Defence

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

Het Koninkrijk der Nederlanden

en

de Portugese Republiek,

Hierna gezamenlijk te noemen „partijen" en elk afzonderlijk „partij",

Erkennend de belangrijke rol die hun samenwerking speelt bij het waarborgen van vrede, internationale veiligheid en wederzijds vertrouwen,

Overwegend dat zij vergelijkbare beveiligingsnormen delen voor de bescherming van gerubriceerde gegevens en

Teneinde de wederzijdse beveiliging van gerubriceerde gegevens te waarborgen;

Zijn, in het belang van de nationale veiligheid, het volgende overeengekomen:

Artikel 1

Doel en reikwijdte

1. Dit Verdrag heeft ten doel de beveiliging te waarborgen van gerubriceerde gegevens die worden uitgewisseld tussen de partijen, tussen een partij en een opdrachtnemer onder de rechtsmacht van de andere partij, tussen opdrachtnemers onder de rechtsmacht van de respectieve partijen, of die worden gegenereerd in het kader van een bilateraal programma uit hoofde van dit Verdrag. In dit Verdrag worden de beveiligingsprocedures en regelingen voor deze beveiliging vastgelegd.

2. De partijen nemen alle passende maatregelen krachtens hun interne wetgeving om de beveiliging van gerubriceerde gegevens in overeenstemming met dit Verdrag te waarborgen.

3. 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 daarbij;
b) **„Gerubriceerd contract"**, elk juridisch bindend instrument tot het leveren van goederen en/of diensten dat een van de partijen of een opdrachtnemer onder haar rechtsmacht aangaat met een opdrachtnemer onder de rechtsmacht van de andere partij, die gerubriceerde gegevens bevat of waarbij voor de uitvoering toegang of mogelijk toegang vereist is tot gerubriceerde gegevens. Dit begrip omvat tevens precontractuele activiteiten;
c) **„Gerubriceerde gegevens"**, gegevens, ongeacht de vorm daarvan, die van een van de partijen een rubricering krijgen toegekend, waarvan de ongeoorloofde bekendmaking, verandering, compromittering of het verlies de belangen van een of beide partijen in meer of mindere mate zou kunnen schaden. Deze gegevens kunnen reproducties, vertalingen en materiaal dat nog ontwikkeld wordt omvatten;
d) **„Bevoegde beveiligingsautoriteit"**, de overheidsautoriteit in een partij die verantwoordelijk is voor de implementatie van en toezicht op 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), rechtspersoon of andere vorm van organisatie onder de rechtsmacht van een partij, die een gerubriceerd contract aangaat of er door gebonden is. Dit begrip omvat tevens een onderopdrachtnemer;
f) **„Veiligheidsmachtiging bedrijfslocatie**", de administratieve vaststelling door de bevoegde beveiligingsautoriteit dat, vanuit beveiligingsoogpunt, een faciliteit gerubriceerde gegevens afdoende kan beveiligen, in overeenstemming met haar interne wetgeving;
g) **„Need to know"**, het vereiste voor een bevoegde natuurlijke persoon, rechtspersoon of andere organisatievorm voor toegang tot, kennis van of bezit van gerubriceerde gegevens om hun officiële werkzaamheden of taken te kunnen uitvoeren;
h) **„Partij van herkomst"**, de partij onder wier gezag gerubriceerde gegevens zijn gecreëerd;
i) **„Veiligheidsmachtiging personeel**", de administratieve vaststelling door de bevoegde beveiligingsautoriteit dat een natuurlijke persoon toestemming heeft gekregen voor de toegang tot en omgang met gerubriceerde gegevens tot en met een gespecificeerd rubriceringsniveau, in overeenstemming met haar interne wetgeving;
j) **„Programma-/Projectbeveiligingsinstructie**" een samenstelling van beveiligingsvoorschriften en -procedures gebaseerd op een nationaal beveiligingsbeleid en ondersteunende richtlijnen, die worden toegepast op een specifiek programma of project teneinde de beveiligingsprocedures te standaardiseren;
k) **„Verstrekkende partij"**, de partij of opdrachtnemer onder haar rechtsmacht die de gerubriceerde gegevens uit hoofde van dit Verdrag verstrekt aan de ontvangende partij;
l) **„Ontvangende partij"**, de partij of opdrachtnemer onder haar rechtsmacht die de gerubriceerde gegevens uit hoofde van dit Verdrag ontvangt van de verstrekkende 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) **„Veiligheidsincident"**, elk(e) ongeoorloofd(e) bekendmaking, verandering, compromittering, verlies, opslag of vernietiging van, toegang tot of omgang met gerubriceerde gegevens in strijd met de interne wetgeving en/of dit Verdrag;
o) **„Derde"**, elke internationale organisatie, regering of staat, met inbegrip van natuurlijke personen, rechtspersonen of andere organisatievormen onder zijn rechtsmacht die geen partij is bij 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 eventuele veranderingen daarvan.

Artikel 4

Rubriceringsniveaus

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

TABEL 1

Voor het Koninkrijk der Nederlanden	Voor de Portugese Republiek	Equivalent in het Engels
Stg. ZEER GEHEIM	MUITO SECRETO	TOP SECRET
Stg. GEHEIM	SECRETO	SECRET
Stg. CONFIDENTIEEL	CONFIDENCIAL	CONFIDENTIAL
DEPARTEMENTAAL VERTROUWELIJK	RESERVADO	RESTRICTED

2. Gerubriceerde contracten binnen het militaire domein met een rubriceringsniveau dat overeenkomt met „DEPARTEMENTAAL VERTROUWELIJK" worden behandeld als „CONFIDENCIAL" ten behoeve van het verstrekken van een veiligheidsmachtiging bedrijfslocatie ingevolge artikel 7.

Artikel 5

Beveiligingsmaatregelen

1. De partij van herkomst kent een rubriceringsniveau toe aan gerubriceerde gegevens en voorziet de gerubriceerde gegevens van een markering in overeenstemming met haar interne wetgeving.

2. De ontvangende partij voorziet alle gerubriceerde gegevens die zij ontvangen heeft van de verstrekkende partij van het rubriceringsniveau van de ontvangende partij dat overeenkomt met het door de partij van herkomst gegeven rubriceringsniveau in overeenstemming met artikel 4 en, wanneer van toepassing, in overeenstemming met het vijfde lid van dit artikel.

3. De ontvangende partij zal het rubriceringsniveau van uit hoofde van dit Verdrag ontvangen of gegenereerde gerubriceerde gegevens niet veranderen of intrekken zonder de schriftelijke goedkeuring van de partij van herkomst.

4. De partij van herkomst waarborgt dat de ontvangende partij op de hoogte wordt gebracht van elke verandering van het rubriceringsniveau van de verstrekte gerubriceerde gegevens.

5. De partij van herkomst kan de gerubriceerde gegevens tevens voorzien van vereisten voor de omgang ermee, om eventuele beperkingen te stellen aan het gebruik, de bekendmaking, vrijgave en toegang door de ontvangende partij.

6. Gerubriceerde gegevens die gezamenlijk worden aangemaakt door de partijen krijgen een rubriceringsniveau dat gezamenlijk wordt bepaald door de partijen.

7. De partijen kennen aan gerubriceerde gegevens die uit hoofde van dit Verdrag worden uitgewisseld of gegenereerd ten minste dezelfde beveiliging toe als aan hun eigen gerubriceerde gegevens met een vergelijkbaar rubriceringsniveau.

8. In overeenstemming met artikel 1, tweede lid, van dit Verdrag nemen de partijen alle passende maatregelen om te waarborgen dat de verstrekkende partij:
a. de gerubriceerde gegevens voorziet van de juiste rubriceringsmarkering in overeenstemming met haar interne wetgeving;
b. de ontvangende partij in kennis stelt van mogelijke voorwaarden voor vrijgave of beperkingen gesteld aan het gebruik van de verstrekte gerubriceerde gegevens.

9. In overeenstemming met artikel 1, tweede lid, van dit Verdrag nemen de partijen alle passende maatregelen om te waarborgen dat de verstrekkende partij:
a. hetzelfde beveiligingsniveau aan gerubriceerde gegevens toekent als aan haar nationale gerubriceerde gegevens met een vergelijkbaar rubriceringsniveau;

b. waarborgt dat gerubriceerde gegevens niet bekend worden gemaakt of vrijgegeven aan een derde zonder de voorafgaande schriftelijke toestemming van de partij van herkomst en, indien dit noodzakelijk wordt geacht, over de voorwaarden;
c. de gerubriceerde gegevens uitsluitend gebruikt voor het doel waarvoor zij zijn vrijgegeven en in overeenstemming met de eisen voor gebruik van de partij van herkomst.

Artikel 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 een geheimhoudingsverklaring hebben ondertekend in overeenstemming met de interne wetgeving van de ontvangende partij.

2. In aanvulling op de vereisten van het eerste lid van dit artikel, wordt toegang tot gerubriceerde gegevens met een rubriceringsniveau dat overeenkomt met „CONFIDENTIAL" en hoger, zoals vermeld in artikel 4 van dit Verdrag, uitsluitend verleend aan de natuurlijke personen die een veiligheidsmachtiging personeel hebben op het overeenkomstige niveau of die anderszins gemachtigd zijn om toegang te krijgen tot gerubriceerde gegevens uit hoofde van hun functie, in overeenstemming met de interne wetgeving van de ontvangende partij.

Artikel 7

Gerubriceerde contracten

1. Op verzoek van de partij van herkomst deelt de bevoegde beveiligingsautoriteit van de ontvangende partij mee of een opdrachtnemer die onder de rechtsmacht van de ontvangende partij valt en deelneemt aan een gerubriceerd contract, een veiligheidsmachtiging bedrijfslocatie heeft gekregen op het vereiste rubriceringsniveau. Indien de opdrachtnemer niet, op dat punt, over een veiligheidsmachtiging bedrijfslocatie beschikt, of de veiligheidsmachtiging bedrijfslocatie van een lager niveau is dan vereist, stelt de bevoegde beveiligingsautoriteit die het verzoek ontvangt de verzoekende bevoegde beveiligingsautoriteit van dat feit in kennis.

2. Indien een partij of een opdrachtnemer onder haar rechtsmacht voorstelt een gerubriceerd contract met een rubriceringsniveau dat overeenkomt met „CONFIDENTIAL" of hoger, zoals vermeld in artikel 4 van dit Verdrag, te gunnen aan een opdrachtnemer onder de rechtsmacht van de andere partij, dient zij eerst de schriftelijke bevestiging te verkrijgen van de bevoegde beveiligingsautoriteit van de andere partij dat aan deze opdrachtnemer een veiligheidsmachtiging bedrijfslocatie met het juiste rubriceringsniveau is toegekend. Voor gerubriceerde contracten met het rubriceringsniveau dat overeenkomt met „RESTRICTED" zoals vermeld in artikel 4 van dit Verdrag, kan een veiligheidsmachtiging bedrijfslocatie vereist zijn indien dit verplicht wordt gesteld in de desbetreffende interne wetgeving van de opdrachtnemer.

3. In overeenstemming met artikel 1, tweede lid, van dit Verdrag waarborgt de partij onder wier rechtsmacht het gerubriceerde contract dient te worden uitgevoerd dat de opdrachtnemer:
a. waarborgt dat alle natuurlijke personen die toegang krijgen tot gerubriceerde gegevens in kennis worden gesteld van hun verantwoordelijkheid de gerubriceerde gegevens te beveiligen in overeenstemming met de voorwaarden omschreven in dit Verdrag en in overeenstemming met hun interne wetgeving;
b. de beveiligingsuitvoering op zijn locaties in het oog houdt;
c. zijn bevoegde beveiligingsautoriteit onverwijld in kennis stelt van elk beveiligingsincident dat betrekking heeft op het gerubriceerd contract.

4. In aanvulling op artikel 7, derde lid, onderdelen a, b en c van dit Verdrag, met betrekking tot gerubriceerde contracten met een rubriceringsniveau dat overeenkomt met „CONFIDENTIAL" of hoger, zoals vermeld in artikel 4 van dit Verdrag, waarborgt de bevoegde beveiligingsautoriteit dat de opdrachtnemer een veiligheidsmachtiging bedrijfslocatie bezit met het juiste rubriceringsniveau teneinde de gerubriceerde gegevens te beveiligen en dat de natuurlijke personen die toegang dienen te krijgen tot gerubriceerde gegevens, een veiligheidsmachtiging personeel met het juiste rubriceringsniveau hebben.

5. Elk gerubriceerd contract dient beveiligingsvereisten te bevatten waarin de volgende aspecten vermeld staan:
a. een rubriceringsgids;
b. een procedure voor het melden van wijzigingen van het rubriceringsniveau;
c. de kanalen en procedures die gebruikt dienen te worden voor het vervoer en/of de overbrenging van gerubriceerde gegevens;
d. instructies voor de omgang met, opslag, vernietiging en retourneren van gerubriceerde gegevens;

e. contactgegevens van de bevoegde beveiligingsautoriteiten die verantwoordelijk zijn voor het toezicht op de beveiliging van gerubriceerde gegevens die betrekking hebben op het gerubriceerde contract;
f. 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;
g. wanneer een gerubriceerd contract geheel of gedeeltelijk wordt onderuitbesteed, de verplichting om alle bepalingen betreffende opdrachtnemers in dit Verdrag op te leggen aan de onderaannemer;
h. een verwijzing naar dit Verdrag;
i. 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.

6. De bevoegde beveiligingsautoriteit van de partij of een opdrachtnemer onder haar rechtsmacht die de toekenning van het gerubriceerde contract goedkeurt, stuurt een kopie van de beveiligingsvereisten naar de bevoegde beveiligingsautoriteit van de ontvangende partij, om het beveiligingstoezicht op het gerubriceerde contract te vergemakkelijken.

7. Wanneer de omvang of complexiteit van een programma of project en de betrokken gerubriceerde gegevens aanvullende beveiligingsvereisten nodig maken, stellen de partijen, via hun onderscheiden bevoegde beveiligingsautoriteiten, gezamenlijk een programma-/projectbeveiligingsinstructie op en voegen deze als bijlage toe aan het gerubriceerde contract.

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

Artikel 8

Internationale bezoeken

1. Internationale bezoeken waarbij toegang tot gerubriceerde gegevens op het rubriceringsniveau dat overeenkomt met „CONFIDENTIAL" of hoger zoals vermeld in artikel 4 van dit Verdrag vereist is, dienen vooraf schriftelijk te worden goedgekeurd door de bevoegde beveiligingsautoriteit van de ontvangende partij, tenzij anderszins 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 het juiste niveau of die anderszins gemachtigd zijn om toegang te krijgen tot gerubriceerde gegevens uit hoofde van hun functie, in overeenstemming met de interne wetgeving van de ontvangende partij. Indien dit verplicht is volgens de interne wetgeving van de als gastheer optredende partij kunnen bezoeken op het niveau „RESTRICTED" onderworpen zijn aan voorafgaande schriftelijke toestemming van de bevoegde beveiligingsautoriteit van de als gastheer optredende partij.

2. De bezoeker dient de aanvraag voor het bezoek ten minste tien dagen vóór de beoogde datum van het bezoek in bij zijn bevoegde beveiligingsautoriteit, die de aanvraag doorstuurt naar de bevoegde beveiligingsautoriteit van de andere partij. In dringende gevallen kunnen de bevoegde beveiligingsautoriteiten een kortere termijn overeenkomen.

3. Een aanvraag voor een bezoek dient de volgende gegevens te bevatten:
a. volledige naam van de bezoeker, geboortedatum en -plaats, nationaliteit en nummer paspoort/identiteitskaart;
b. officiële functiebenaming 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 van het contactpunt van de te bezoeken locatie;
g. van een datum en stempel voorziene handtekening van een vertegenwoordiger van de bevoegde beveiligingsautoriteit van de bezoeker.

4. De bevoegde beveiligingsautoriteiten kunnen een lijst overeenkomen van bezoekers die herhalingsbezoeken mogen afleggen gedurende een periode van niet langer dan twaalf maanden. De bevoegde beveiligingsautoriteiten komen nadere details van de herhalingsbezoeken overeen.

5. De bevoegde beveiligingsautoriteit van de partij die als gastheer optreedt stelt de beveiligingsbeambten van de te bezoeken organisatie in kennis van de gegevens van de natuurlijke personen van wie de bezoekaanvraag is goedgekeurd. Wanneer de goedkeuring eenmaal is verleend, kunnen de praktische aspecten van het bezoek van natuurlijke personen die herhalingsbezoeken mogen afleggen rechtstreeks geregeld worden met het betrokken agentschap of de betrokken locatie of organisatie.

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

7. De partijen waarborgen, in overeenstemming met hun interne wetgeving, de beveiliging van de persoonsgegevens van de natuurlijke personen die een bezoek aanvragen waarbij toegang tot gerubriceerde gegevens nodig is. Deze persoonsgegevens worden niet gebruikt voor enig ander doel dan het besluit over de aanvraag voor (herhalings)bezoeken.

Artikel 9

Overbrenging van gerubriceerde gegevens

1. Gerubriceerde gegevens worden overgebracht in overeenstemming met de interne wetgeving van de partij van herkomst of zoals anderszins overeengekomen tussen de bevoegde beveiligingsautoriteiten.

2. De elektronische overbrenging van gerubriceerde gegevens mag alleen geschieden met gebruikmaking van cryptografische middelen in overeenstemming met procedures die door de bevoegde beveiligingsautoriteiten gezamenlijk dienen te worden goedgekeurd.

3. Op verzoek van de partij van herkomst voorziet de ontvangende partij de partij van herkomst van een schriftelijke bevestiging dat zij de gerubriceerde gegevens heeft ontvangen.

4. De partijen stellen, via hun onderscheiden bevoegde autoriteit, een opdrachtnemer in kennis van de middelen en verpakkingsnormen die de partijen gezamenlijk hebben goedgekeurd voor de overbrenging van gerubriceerde gegevens.

5. Indien de gerubriceerde gegevens te omvangrijk zijn om door de goedgekeurde koerier te worden overgebracht, komen de partijen, via hun onderscheiden bevoegde beveiligingsautoriteit, gezamenlijk een vervoersplan overeen waarin wordt beschreven hoe zij de gerubriceerde gegevens willen overbrengen. Dit plan kan het soort vervoer, de route en het soort begeleiding van de gerubriceerde gegevens omvatten.

Artikel 10

Reproductie, vertaling en vernietiging van gerubriceerde gegevens

1. Reproducties en vertalingen van gerubriceerde gegevens krijgen dezelfde rubriceringsmarkering 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 met het rubriceringsniveau dat overeenkomt met „TOP SECRET” zoals vermeld in artikel 4 van dit Verdrag worden geretourneerd aan de partij van herkomst nadat de ontvangende partij ze niet meer nodig acht, of kunnen worden vernietigd, echter uitsluitend met voorafgaande schriftelijke toestemming van de partij van herkomst.

6. Gerubriceerde gegevens tot en met het rubriceringsniveau dat overeenkomt met „SECRET” zoals vermeld in artikel 4 van dit Verdrag worden vernietigd nadat de ontvangende partij ze niet meer nodig acht.

7. 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 de bevoegde beveiligingsautoriteit van de partij van herkomst onverwijld in kennis van de vernietiging van deze gerubriceerde gegevens.

Artikel 11

Beveiligingssamenwerking

1. De bevoegde beveiligingsautoriteiten stellen elkaar in kennis van veranderingen in hun interne wetgeving, 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 interne wetgeving 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 interne wetgeving, 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 bedrijfslocatie en veiligheidsmachtigingen personeel waarvoor een bevestiging is verstrekt.

6. Bij de samenwerking uit hoofde van dit Verdrag wordt gebruikgemaakt van de Engelse taal.

Artikel 12

Beveiligingsincident

1. Indien een beveiligingsincident met betrekking tot de gerubriceerde gegevens van de partij van herkomst wordt vermoed of vastgesteld door de ontvangende partij, stelt zij haar bevoegde beveiligingsautoriteit 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 bevoegde beveiligingsautoriteiten stellen elkaar onverwijld schriftelijk in kennis van een feitelijk of vermoedelijk beveiligingsincident waarbij gerubriceerde gegevens van de andere partij betrokken zijn.

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

4. De bevoegde beveiligingsautoriteit van de ontvangende partij neemt passende maatregelen in overeenstemming met zijn interne wetgeving om de gevolgen van het beveiligingsincident te beperken en om herhaling ervan te voorkomen. De bevoegde beveiligingsautoriteit van de partij van herkomst wordt in kennis gesteld van de uitkomsten van het onderzoek en de eventuele getroffen maatregelen.

Artikel 13

Kosten

Elke partij draagt haar eigen kosten die ontstaan in verband met de implementatie en tenuitvoerlegging van haar verplichtingen ingevolge dit Verdrag, tenzij de partijen gezamenlijk anders bepalen.

Artikel 14

Oplossing van geschillen

Elk geschil dat voortvloeit uit de uitlegging, uitvoering of toepassing van dit Verdrag wordt langs diplomatieke weg beslecht door middel van overleg of onderhandelingen tussen de partijen.

Artikel 15

Uitvoeringsregelingen

De bevoegde beveiligingsautoriteiten van de partijen kunnen uitvoeringsregelingen sluiten ingevolge dit Verdrag. Deze regelingen zijn ondergeschikt aan dit Verdrag.

Artikel 16

Slotbepalingen

1. Dit Verdrag wordt gesloten voor onbepaalde tijd.

2. Elke partij stelt de andere partij langs diplomatieke weg in kennis van de voltooiing van de respectieve nationale procedures die nodig zijn voor de inwerkingtreding van dit Verdrag. Dit Verdrag treedt in werking op de eerste dag van de tweede maand die volgt op de ontvangst van de laatste kennisgeving.

3. 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).

4. Dit Verdrag, met inbegrip van de Bijlage erbij, kan met de wederzijdse schriftelijke instemming van de partijen te allen tijde 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 tweede 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.

5. Elke partij kan dit Verdrag te allen tijde schriftelijk langs diplomatieke weg beëindigen. In dat geval eindigt het Verdrag zes maanden na de ontvangst van deze kennisgeving.

6. Bij 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, tenzij de partijen anderszins overeenkomen.

7. Na de inwerkingtreding van dit Verdrag zendt de partij op het grondgebied waarvan het is ondertekend het Verdrag ter registratie naar het Secretariaat van de Verenigde Naties, overeenkomstig artikel 102 van het Handvest van de Verenigde Naties en artikel 80 van het Verdrag van Wenen inzake het verdragenrecht, en stelt zij de andere partij in kennis van de afronding van deze procedure, met vermelding van het respectieve registratienummer.

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

GEDAAN te 's-Gravenhage op 11 december 2024, in twee oorspronkelijke exemplaren, elk in de Portugese, de Nederlandse, en de Engelse taal, waarbij alle teksten gelijkelijk authentiek zijn. In geval van verschil in interpretatie is de Engelse tekst doorslaggevend.

Voor het Koninkrijk der Nederlanden,

CASPAR VELDKAMP

Voor de Portugese Republiek,

INÊS DOMINGOS

Bijlage

De bevoegde beveiligingsautoriteit van de Portugese Republiek is:
De Nationale Beveiligingsautoriteit
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

D. PARLEMENT

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

G. INWERKINGTREDING

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

Uitgegeven de *negentiende* december 2024.

De Minister van Buitenlandse Zaken,

C.C.J. VELDKAMP

trb-2024-150
ISSN 0920 - 2218
's-Gravenhage 2024