12 (2023) Nr. 1

TRACTATENBLAD

VAN HET

KONINKRIJK DER NEDERLANDEN

JAARGANG 2023 Nr. 120

A. TITEL

Verdrag tussen het Koninkrijk der Nederlanden en de Federatieve Republiek Brazilië inzake de uitwisseling en wederzijdse beveiliging van gerubriceerde gegevens (met Bijlage); Brasilia, 9 oktober 2023

Voor een overzicht van de verdragsgegevens, zie verdragsnummer 013949 in de Verdragenbank.

B. TEKST

Agreement between the Kingdom of the Netherlands and the Federative Republic of Brazil on exchange and mutual protection of classified information

The Kingdom of the Netherlands

and

the Federative Republic of Brazil,

Hereinafter referred to together as "Parties", or separately, as "Party",

In the interests of national security and in order to ensure the protection of Classified Information exchanged within the scope of cooperation instruments, contracts and other agreements signed between the Parties, their accredited individuals, bodies, as well as public and private entities,

Desiring to establish a framework of rules and procedures related to Classified Information in accordance with the national laws and regulations of the Parties,

Confirming that this Agreement will not affect the commitments of both Parties that derive from other international agreements and that it will not be used against the interests, security and territorial integrity of other States,

Have agreed upon the following:

Article I

Purpose

1. This Agreement establishes rules and procedures for the protection of Classified Information exchanged between the aforementioned Parties, their accredited individuals, bodies, as well as public or private entities under their jurisdiction.

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

Article II

Definitions

For the purposes of this Agreement, the term:
a. Agreement means this agreement including its Annexes;
b. Annex means an attachment to this Agreement;

c. Classified Contract means an agreement, including any pre-contractual negotiations, the performance of which requires or involves access or potential access to or the creation of Classified Information;
d. Classified Information means the information, material or object, regardless of its form or nature or any parts thereof, with a certain Security Classification Level, which regardless of how it is presented must be protected against unauthorized access, disclosure or other type of Compromise for which it was designated, to prevent damage or harm in the interests of one or both of the Parties, in accordance with the respective laws and regulations of each Party and this Agreement;
e. Competent Security Authority (CSA) means the authority of each Party responsible for the security of Classified Information under this Agreement;
f. Compromise means any form of misuse, damage or unauthorized access, alteration, disclosure or destruction of Classified Information, as well as any other action or non-action that results in the loss of its confidentiality, integrity, availability or authenticity;
g. Contractor means any legal entity under the jurisdiction of a Party, entering into or otherwise bound by a Classified Contract;
h. Facility Security Clearance means the determination by the Competent Security Authority that a public or private entity has in place appropriate security measures and has therefore been accredited for the Handling of Classified Information, in accordance with the national laws and regulations of each Party;
i. Handling of Classified Information means a set of actions related to the production, reception, classification, use, access, reproduction, transport, transmission, distribution, archiving, storage, disposal, destination or control of Classified Information at a certain Security Classification Level;
j. Need to Know means the requirement for an individual to access, have knowledge of or possess Classified Information for the performance of official functions and tasks;
k. Originating Party means the Party under whose authority Classified Information has been created;
l. Personnel Security Clearance means the determination that a given individual has been security cleared and has therefore been accredited for the Handling of Classified Information, at a given Security Classification Level, in accordance with the national laws and regulations of each Party;
m. Providing Entity means the Party, or a Contractor, which provides Classified Information to the Receiving Entity under this Agreement;
n. Receiving Entity means the Party, or a Contractor, which receives Classified Information under this Agreement;
o. Security Breach means any intentional or accidental action or omission that result in an actual or possible Compromise of Classified Information provided or generated under this Agreement;
p. Security Classification Level means the level of protection assigned to Classified Information, in accordance with the national laws and regulations of each Party and as incorporated in article IV, paragraph 1 of this Agreement; and
q. Third Party means any organization, state, government or individual that is not a Party to this Agreement.

Article III

Competent Security Authorities

1. The Competent Security Authorities, responsible for the implementation and supervision of this Agreement, are listed in the Annex to this Agreement.

2. The Competent Security Authority may delegate parts of its responsibilities to a delegated competent security authority.

3. Each Party shall provide the other with the contact details of their respective Competent Security Authority, in writing. The Competent Security Authorities of the Parties shall inform each other in writing about changes in their contact details.

4. In order to ensure close cooperation in the implementation of this Agreement, the Competent Security Authorities may consult each other whenever necessary.

5. Representatives of both Competent Security Authorities may mutually visit their facilities with the intention of acquiring knowledge of security procedures and measures applicable to Classified Information, subject to the approval of the host Competent Security Authority.

6. Upon request, the Competent Security Authorities may assist each other in carrying out the procedures for the award of Facility Security Clearances and Personnel Security Clearances, on request and in accordance with their national laws and regulations.

7. Upon 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 and/or Facility Security Clearance has been issued.

8. The Competent Security Authorities of the Parties shall mutually recognize their Personnel Security Clearances and Facility Security Clearances issued in accordance with their respective laws and regulations and within the scope of this Agreement.

9. The Competent Security Authorities shall promptly notify each other in writing about changes in recognized Personnel Security Clearances and Facility Security Clearances for whom or for which a confirmation has been provided according to paragraph 8 of this article.

Article IV

Security Classification Levels

1. The Parties agree that the Security Classification Levels, in accordance with their respective national laws and regulations, shall correspond to each other in the following form of equivalence:

Classification Originating Party	**Classification Receiving Entity**
'Stg. ZEER GEHEIM"	"ULTRASSECRETO"
"Stg. GEHEIM"	"SECRETO"
"Stg. CONFIDENTIEEL"	"SECRETO"
"DEPARTEMENTAAL VERTROUWELIJK"	"RESERVADO"
"ULTRASSECRETO"	"Stg. ZEER GEHEIM"
"SECRETO"	"Stg. GEHEIM"
"RESERVADO"	"Stg. CONFIDENTIEEL"

2. Any Classified Information produced pursuant to this Agreement shall be marked with the Originating Party's equivalent Security Classification Level in accordance with paragraph 1 of this article.

3. The Receiving Entity shall mark all the Classified Information under this Agreement that it has received from the Providing Entity with the equivalent Security Classification Level of the Receiving Entity in accordance with paragraph 1 of this article. The Security Classification Level of the Originating Party shall be indicated first, in order to determine the proper equivalent Security Classification Level.

4. The Parties shall notify each other of any change and subsequent amendment to the Security Classification Level of Classified Information.

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

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

7. Classified Information jointly originated by the Parties shall be assigned a Security Classification Level that is mutually determined by the Parties.

Article V

Protection of Classified Information

1. 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. They 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.

2. The treatment of any Classified Information exchanged between the Parties shall respect the provisions of this Agreement.

3. Each Party shall ensure that the necessary measures are implemented for the protection of Classified Information processed, stored or transmitted by communication and information systems, in accordance with the Security Classification Level, this Agreement, and with national laws and regulations.

4. Each Party shall ensure confidentiality, integrity, availability and, where applicable, authenticity, accountability and traceability of Classified Information.

5. The Parties shall not disclose any Classified Information without the Originating Party's written consent.

Article VI

Use of Classified Information

1. Each Party shall ensure that the Providing Entity:
a. marks Classified Information with the appropriate security classification in accordance with its national laws and regulations and
b. informs the Receiving Entity of any conditions of release or limitations on the use of the Classified Information provided, as determined by the Originating Party.

2. Each Party shall ensure that the Receiving Entity:
a. affords the same level of protection to the Classified Information as afforded to its national Classified Information of an equivalent Security Classification Level as determined in article IV, paragraph 1;
b. shall not declassify or downgrade Classified Information without the prior written consent of the Originating Party;
c. shall not disclose Classified Information to a Third Party without prior written consent of the Originating Party; and
d. shall use Classified Information only for the purposes that it has been released for and in accordance with any handling requirements of the Originating Party.

3. Each Party, in accordance with its constitutional requirements, national laws and regulations, shall respect the principle of consent of origin.

Article VII

Access to Classified Information

1. Each Party shall ensure that access to Classified Information is granted on a Need to Know basis.

2. Each Party shall ensure that any individual who has been granted access to Classified Information is informed on its responsibilities to protect such information and has signed a statement of confidentiality in accordance with national laws and regulations of the Receiving Entity.

3. The Parties shall ensure that access to Classified Information is granted only to individuals who hold a Personnel Security Clearance at the corresponding level or who are duly authorized to access Classified Information by virtue of their duties pursuant to national laws and regulations of the Receiving Entity.

Article VIII

Translation, Reproduction and Destruction of Classified Information

1. All translations and reproductions of Classified Information must be protected and controlled in the same manner as the original Classified Information. It shall receive the same Security Classification Level as the original Classified Information.

2. Translations of Classified Information shall contain a suitable annotation in the language of translation, indicating that they contain Classified Information of the Originating Party.

3. The number of reproductions of Classified Information shall be limited to the amount required for its official purpose.

4. Classified Information with Security Classification Level equivalent to ULTRASSECRETO / Stg. ZEER GEHEIM, shall not be reproduced or translated without the prior written consent of the Originating Party.

5. Classified Information with Security Classification Level equivalent to ULTRASSECRETO / Stg. ZEER GEHEIM shall not be destroyed without the prior written consent of the Originating Party. It shall be returned to the Originating Party after it is no longer considered necessary by the Receiving Entity.

6. Classified Information with Security Classification Level equivalent to SECRETO / Stg. GEHEIM shall be destroyed in accordance with national laws and regulations after it is no longer considered necessary by the Receiving Entity.

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

Article IX

Transmission of Classified Information

1. Classified Information with Security Classification Level ULTRASSECRETO / Stg. ZEER GEHEIM and SECRETO / Stg. GEHEIM shall be transmitted between the Parties, through diplomatic channels, or as agreed in writing by the respective Competent Security Authorities.

2. Security Classification Levels that are not included in paragraph 1 shall be transmitted in accordance with national laws and regulations of the Originating Party.

3. Classified Information transmitted through communication systems, networks or other electromagnetic means must use encrypted means mutually accepted by the respective Competent Security Authorities.

4. In the event of transmission of Classified Information that requires special procedures for its transport, a logistical plan must be previously agreed, in writing, by both Competent Security Authorities.

Article X

Visits

1. Visits to facilities where Classified Information will be accessed, processed or recorded are subject to the prior written approval of the Competent Security Authority of the host Party, unless otherwise agreed by the Competent Security Authorities. Such approval will only be granted to individuals who meet the requirements set forth in article VII of this Agreement.

2. The visit request must be submitted to the Competent Security Authority of the host Party, including the following data that will be used only for the purpose of the visit:
a. the visitor's first and last name, date and place of birth, nationality, other citizenships and identification card number/passport number;
b. the visitor's title and function, as well as the name and address of the organization by whom the visitor is employed or that the visitor represents;
c. the specification of the project in which the visitor is participating;
d. the confirmation of the visitor's Personnel Security Clearance and its level and validity;
e. the name of the facility to be visited;
f. the purpose of the visit;
g. the anticipated highest Security Classification Level of the Classified Information to be accessed, processed or stored;
h. the name, address, phone number, e-mail address and point of contact of the facility to be visited;
i. the date and duration of the visit;
j. the total period when visits are recurring; and
k. the date and signature of a representative of the visitor's Competent Security Authority.

3. The visit request must be submitted at least 10 (ten) calendar days in advance of the proposed visit date, unless the Competent Security Authorities agree on a different period.

4. The Competent Security Authorities may agree on a list of visitors entitled to recurring visits for a period not exceeding 12 (twelve) months. The Competent Security Authorities shall agree on the further details of these 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 requests have been approved. Once approval has been given, visiting arrangements for individuals who have been given approval for recurring visits may be made directly with the agency, facility or organization concerned.

6. Any Classified Information transmitted to the visitor shall be deemed Classified Information under this Agreement and shall be handled in accordance with the provisions of this Agreement. In addition, the visitor must comply with the host Party's security regulations.

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

8. When authorized, the Competent Security Authority of the host Party shall notify the requesting Party, as soon as possible, of the visit and also notify the facility to be visited.

Article XI

Security Breach

1. When a Security Breach related to Classified Information under this Agreement is suspected or ascertained by the Receiving Entity, the Competent Security Authority of the Party where the Security Breach occurred shall immediately inform the Competent Security Authority of the other Party. The notice must contain sufficient details for the Originating Party to assess the consequences and circumstances of the suspected or ascertained Security Breach.

2. The Competent Security Authority of the Party where the Security Breach occurred shall immediately take all necessary steps, in accordance with its national laws and regulations, to investigate any suspected or ascertained Security Breach. The Competent Security Authority of the Originating Party may, if agreed, cooperate in the investigation. The Originating Party shall always be informed about the outcome of the investigation and the measures taken, if any.

3. The Competent Security Authority of the Party where the Security Breach occurred shall take all steps, including but not limited to legal steps, in accordance with its national laws and regulations, to mitigate the consequences of a Security Breach and to prevent any recurrence.

4. When a Security Breach has occurred in a Third Party, the Competent Security Authority of the Party that transmitted the information to the Third Party shall immediately inform the Competent Security Authority of the Originating Party about the Security Breach, make sure the Security Breach is investigated properly and communicate the outcome of the investigation and any measures taken.

5. Any Party may request information regarding the Security Breach investigation process.

Article XII

Classified Contracts

1. If a Party or a Contractor proposes to grant a Classified Contract, with a Contractor under the jurisdiction of the other Party, it must first obtain written confirmation from the Competent Security Authority of the other Party that the Contractor has received a Facility Security Clearance at the appropriate Security Classification Level.

2. The Competent Security Authority of the Party where the Classified Contract is performed shall ensure that the Contractor and if applicable its sub-contractor:
a) ensures that all individuals granted access to Classified Information are informed of their responsibilities to protect Classified Information in accordance with the conditions defined in this Agreement and with national laws and regulations;
b) monitors the security conduct within its facilities in accordance with national laws and regulations;
c) notifies promptly its Competent Security Authority of any Security Incident relating to the Classified Contract; and
d) holds an appropriate Facility Security Clearance in order to protect the Classified Information and that the individuals requiring access to Classified Information hold an appropriate Personnel Security Clearance.

3. Every Classified Contract including classified sub-contracts concluded in accordance with this Agreement shall include security requirements which identify the following aspects:
a) a security classification guide, which shall always include the table of article IV, paragraph 1 specifying the applicable Security Classification Levels of each part of the Classified Contract;
b) a procedure for communication 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 and storage of Classified Information;
e) contact details of the Competent Security Authorities responsible for overseeing the protection of Classified Information related to the Classified Contract; and
f) obligation to notify any Security Breaches.

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

Article XIII

Costs

Each Party shall bear the costs of its own expenses resulting from the implementation and supervision of all aspects of this Agreement, unless otherwise mutually determined by the Parties.

Article XIV

Dispute settlement

1. Any dispute that may arise between the Parties regarding the interpretation or application of this Agreement, or any related matter, shall be resolved exclusively through consultations and negotiations between the Parties and shall not be referred to any international court or Third Party for settlement.

2. During the dispute settlement period, both Parties will continue to fulfil their obligations under this Agreement.

3. Dispute settlement procedures between both Parties shall be conducted based on the principle of confidentiality.

Article XV

Communication

All formal communications between the Parties relating to the implementation of this Agreement shall be in writing, in the English language.

Article XVI

Entry into force

This Agreement shall enter into force on the first day of the second month following the receipt of the last notification by which the Parties shall inform each other, through diplomatic channels, that their domestic legal requirements necessary for its entry into force have been fulfilled.

Article XVII

Territorial application

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).

Article XVIII

Amendments

1. This Agreement, including its Annex, may be amended at any time, in writing, by means of amendments and with the mutual consent between the Parties. Amendments shall be proposed through diplomatic channels.

2. The amendments shall enter into force under the terms set out in article XVI of this Agreement, with the exception of amendments of the Annex, which shall enter into force on a date to be agreed upon by the Parties.

Article XIX

Validity and Termination

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

2. Either Party may, at any time, terminate this Agreement by giving written notice, through diplomatic channels, to the other Party.

3. Termination shall take effect 6 (six) months after the date on which the other Party receives notice of termination.

4. Upon termination, any Classified Information exchanged, released or generated under this Agreement shall continue to be protected in accordance with the terms of this Agreement before it was terminated, for as long as the Classified Information remains classified.

Article XX

Final Dispositions

The Competent Security Authorities shall inform each other about their respective national laws and regulations and shall promptly notify each other about modifications that affect the protection of Classified Information provided under this Agreement and have an impact on this Agreement. In the event of such changes, the Parties shall discuss the necessity of reviewing this Agreement.

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

DONE in Brasilia on 9 October 2023 in two original copies, each in the Dutch, Portuguese 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,

A.M.A. DRIESSEN

For the Federative Republic of Brazil,

MARCOS ANTONIO AMARO DOS SANTOS

Annex

The Competent Security Authorities, responsible for the implementation and supervision of this Agreement, are:

On behalf of the Federative Republic of Brazil:
The Institutional Security Cabinet of the Presidency of the Federative Republic of Brazil

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

The delegated competent security authority in the military domain is:
Defence Security Authority
Directorate-General of Policy
Ministry of Defence

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

Het Koninkrijk der Nederlanden

en

de Federatieve Republiek Brazilië,

Hierna gezamenlijk te noemen „partijen“ of afzonderlijk „partij“,

In het belang van de nationale veiligheid en om de beveiliging te waarborgen van gerubriceerde gegevens die binnen de reikwijdte van samenwerkingsinstrumenten, contracten en overige overeenkomsten tussen de partijen, hun geaccrediteerde natuurlijke personen, lichamen alsmede publieke en private entiteiten worden uitgewisseld,

Geleid door de wens een kader voor regels en procedures inzake gerubriceerde gegevens vast te stellen in overeenstemming met de nationale wet- en regelgeving van de partijen,

Bevestigend dat dit Verdrag de verplichtingen van beide partijen die voortvloeien uit andere internationale overeenkomsten onverlet laat en niet gebruikt wordt om in te gaan tegen de belangen, veiligheid en territoriale integriteit van andere staten,

Zijn het volgende overeengekomen:

Artikel I

Doel

1. In dit Verdrag worden de regels en procedures vastgesteld voor de beveiliging van gerubriceerde gegevens die worden uitgewisseld tussen bovengenoemde partijen, hun geaccrediteerde natuurlijke personen, lichamen alsmede publieke of private entiteiten onder hun rechtsmacht.

2. Dit Verdrag vormt geen basis om de partijen ertoe te verplichten gerubriceerde gegevens te verstrekken of uit te wisselen.

Artikel II

Begripsomschrijvingen

Voor de toepassing van dit Verdrag wordt verstaan onder:
a. Verdrag, dit verdrag met inbegrip van de Bijlagen daarbij;
b. Bijlage, een bijlage bij dit Verdrag;
c. Gerubriceerd contract, een contract, met inbegrip van eventuele voorafgaande contractonderhandelingen, waarbij voor de uitvoering toegang of mogelijk toegang tot gerubriceerde gegevens vereist is of waarbij deze gecreëerd worden;
d. Gerubriceerde gegevens, gegevens, materiaal of voorwerpen, ongeacht de vorm of aard daarvan, of delen daarvan, met een bepaald rubriceringsniveau, die ongeacht de wijze waarop ze worden aangeboden, beveiligd dienen te worden tegen ongeoorloofde toegang, bekendmaking of andere vorm van compromittering van het doel waarvoor ze bestemd waren, om schade of aantasting van de belangen van een of beide partijen te voorkomen, in overeenstemming met de respectieve wet- en regelgeving van elke partij en dit Verdrag;
e. Bevoegde beveiligingsautoriteit, de autoriteit van elke partij die verantwoordelijk is voor de beveiliging van gerubriceerde gegevens uit hoofde van dit Verdrag;
f. Compromittering, elke vorm van misbruik, schade of ongeoorloofde toegang, verandering, bekendmaking of vernietiging met betrekking tot gerubriceerde gegevens, alsook elk ander handelen of nalaten te handelen dat resulteert in het verlies van de vertrouwelijkheid, integriteit, beschikbaarheid of authenticiteit ervan;
g. Opdrachtnemer, elke rechtspersoon onder de rechtsmacht van een partij die een gerubriceerd contract aangaat of er anderszins door gebonden is;
h. Veiligheidsmachtiging bedrijfslocatie, de vaststelling door de bevoegde beveiligingsautoriteit dat een publieke of private entiteit passende beveiligingsmaatregelen heeft genomen en derhalve geaccrediteerd is voor de omgang met gerubriceerde gegevens in overeenstemming met de nationale wet- en regelgeving van elke partij;
i. Omgang met gerubriceerde gegevens, een reeks handelingen die verband houden met de/het productie, ontvangst, rubricering, gebruik, toegang, reproductie, vervoer, overbrenging, distributie, archivering, opslag, verwijdering, bestemming of controle van gerubriceerde gegevens met een bepaald rubriceringsniveau;
j. Need to Know, het vereiste voor een natuurlijke persoon voor toegang tot, kennis van of bezit van gerubriceerde gegevens in verband met het uitoefenen van officiële werkzaamheden en taken;
k. Partij van herkomst, de partij onder wier gezag gerubriceerde gegevens zijn gecreëerd;
l. Veiligheidsmachtiging personeel, de vaststelling door de bevoegde beveiligingsautoriteit dat een natuurlijke persoon toestemming heeft gekregen voor de toegang tot en omgang met gerubriceerde gegevens op een gespecificeerd rubriceringsniveau, in overeenstemming met de nationale wet- en regelgeving;
m. Verstrekkende entiteit, de partij, of een opdrachtnemer, die de gerubriceerde gegevens uit hoofde van dit Verdrag verstrekt aan de ontvangende entiteit;
n. Ontvangende entiteit, de partij, of een opdrachtnemer, die de gerubriceerde gegevens uit hoofde van dit Verdrag ontvangt;
o. Inbreuk op de beveiliging, elk opzettelijk of onbedoeld handelen of nalaten te handelen dat resulteert in een feitelijke of mogelijke compromittering van gerubriceerde gegevens die uit hoofde van dit Verdrag zijn verstrekt of gegenereerd;
p. Rubriceringsniveau, de mate van beveiliging die wordt toegekend aan gerubriceerde gegevens, in overeenstemming met de nationale wet- en regelgeving van elke partij en zoals opgenomen in artikel IV, eerste lid, van dit Verdrag; en
q. Derde, elke organisatie, staat, regering of natuurlijke persoon die geen partij is bij dit Verdrag.

Artikel III

Bevoegde beveiligingsautoriteiten

1. De bevoegde beveiligingsautoriteiten die verantwoordelijk zijn voor de implementatie van en het toezicht op dit Verdrag, staan vermeld in de Bijlage bij dit Verdrag.

2. De bevoegde beveiligingsautoriteit kan delen van zijn verantwoordelijkheden delegeren aan een gemachtigde bevoegde beveiligingsautoriteit.

3. Elke partij stelt de andere partij schriftelijk in kennis van de contactgegevens van hun respectieve beveiligingsautoriteiten. De bevoegde beveiligingsautoriteiten van de partijen informeren elkaar schriftelijk over veranderingen in hun contactgegevens.

4. Om nauwe samenwerking bij de implementatie van dit Verdrag te waarborgen, kunnen de bevoegde beveiligingsautoriteiten elkaar wanneer nodig raadplegen.

5. Vertegenwoordigers van beide bevoegde beveiligingsautoriteiten kunnen elkaars bedrijfslocaties bezoeken om kennis op te doen over de beveiligingsprocedures en -maatregelen die van toepassing zijn op gerubriceerde gegevens, op voorwaarde dat de bevoegde beveiligingsautoriteit die als gastheer optreedt hiervoor toestemming geeft.

6. De bevoegde beveiligingsautoriteiten verlenen elkaar, op verzoek en in overeenstemming met hun nationale wet- en regelgeving, bijstand bij het uitvoeren van de procedures in verband met de afgifte van veiligheidsmachtigingen bedrijfslocatie of veiligheidsmachtigingen personeel.

7. 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.

8. De bevoegde beveiligingsautoriteiten van de partijen erkennen wederzijds hun veiligheidsmachtigingen personeel en veiligheidsmachtigingen bedrijfslocatie die overeenkomstig hun respectieve wet- en regelgeving en binnen de reikwijdte van dit Verdrag zijn afgegeven.

9. De bevoegde beveiligingsautoriteiten stellen elkaar onverwijld schriftelijk in kennis van veranderingen in erkende veiligheidsmachtigingen bedrijfslocatie of veiligheidsmachtigingen personeel waarvoor een bevestiging is verstrekt overeenkomstig het achtste lid van dit artikel.

Artikel IV

Rubriceringsniveaus

1. De partijen komen overeen dat, in overeenstemming met hun respectieve wet- en regelgeving, de rubriceringsniveaus als volgt met elkaar corresponderen:

Rubricering partij van herkomst	**Rubricering ontvangende entiteit**
„Stg. ZEER GEHEIM”	„ULTRASSECRETO”
„Stg. GEHEIM”	„SECRETO”
„Stg. CONFIDENTIEEL”	„SECRETO”
„DEPARTEMENTAAL VERTROUWELIJK”	„RESERVADO”
„ULTRASSECRETO”	„Stg. ZEER GEHEIM”
„SECRETO”	„Stg. GEHEIM”
„RESERVADO”	„Stg. CONFIDENTIEEL”

2. Alle gerubriceerde gegevens die uit hoofde van dit Verdrag worden geproduceerd worden voorzien van het overeenkomstige rubriceringsniveau van de partij van herkomst in overeenstemming met de tabel in het eerste lid van dit artikel.

3. De ontvangende entiteit voorziet alle gerubriceerde gegevens uit hoofde van dit Verdrag die zij ontvangen heeft van de verstrekkende entiteit van het overeenkomstige rubriceringsniveau van de ontvangende entiteit in overeenstemming met de tabel in het eerste lid van dit artikel. Het rubriceringsniveau van de partij van herkomst wordt als eerste weergegeven om het juiste overeenkomstige rubriceringsniveau te bepalen.

4. De partijen stellen elkaar wederzijds op de hoogte van elke verandering en daaropvolgende aanpassing van het rubriceringsniveau van gerubriceerde gegevens.

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

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

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

Artikel V

Beveiliging van gerubriceerde gegevens

1. 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. Zij 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.

2. Bij de behandeling van gerubriceerde gegevens die zijn uitgewisseld tussen de partijen worden de bepalingen van dit Verdrag gerespecteerd.

3. Elke partij waarborgt dat de noodzakelijke maatregelen worden genomen voor de beveiliging van de gerubriceerde gegevens die worden verwerkt, opgeslagen of overgebracht door communicatie- en informatiesystemen, in overeenstemming met het rubriceringsniveau, dit Verdrag en andere nationale wet- en regelgeving.

4. Elke partij waarborgt de vertrouwelijkheid, integriteit, beschikbaarheid en, waar van toepassing, authenticiteit, verantwoording en traceerbaarheid van gerubriceerde gegevens.

5. De partijen maken geen gerubriceerde gegevens bekend zonder de voorafgaande schriftelijke toestemming van de partij van herkomst.

Artikel VI

Gebruik van gerubriceerde gegevens

1. Elke partij waarborgt dat de verstrekkende entiteit:
a. de gerubriceerde gegevens voorziet van de juiste rubriceringsmarkering in overeenstemming met haar nationale wet- en regelgeving en
b. de ontvangende entiteit in kennis stelt van mogelijke voorwaarden voor vrijgave of beperkingen gesteld aan het gebruik van de verstrekte gerubriceerde gegevens, zoals bepaald door de partij van herkomst.

2. Elke partij waarborgt dat de ontvangende entiteit:
a. hetzelfde beveiligingsniveau aan gerubriceerde gegevens toekent als aan haar nationale gerubriceerde gegevens met een vergelijkbaar rubriceringsniveau als bepaald in artikel IV, eerste lid;
b. het rubriceringniveau van gegevens niet opheft of naar beneden bijstelt zonder de voorafgaande schriftelijke toestemming van de partij van herkomst;
c. gerubriceerde gegevens niet aan een derde bekendmaakt zonder de voorafgaande schriftelijke toestemming van de partij van herkomst; en
d. de gerubriceerde gegevens uitsluitend gebruikt voor het doel waarvoor zij zijn vrijgegeven en in overeenstemming met de eisen voor de omgang ermee van de partij van herkomst.

3. Elke partij respecteert, in overeenkomst met haar constitutionele vereisten en nationale wet- en regelgeving, het beginsel van toestemming van de bron.

Artikel VII

Toegang tot gerubriceerde gegevens

1. Elke partij waarborgt dat toegang tot gerubriceerde gegevens wordt verleend op een need-to-know-basis.

2. Elke partij waarborgt dat elke natuurlijke persoon die toegang is verleend tot gerubriceerde gegevens is ingelicht over zijn verantwoordelijkheden inzake de beveiliging van dergelijke gegevens en een geheimhoudingsverklaring heeft ondertekend in overeenstemming met de nationale wet- en regelgeving van de ontvangende entiteit.

3. De partijen waarborgen dat toegang tot gerubriceerde gegevens uitsluitend wordt verleend aan de natuurlijke personen die een veiligheidsmachtiging personeel hebben op het overeenkomstige niveau of die 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 entiteit.

Artikel VIII

Vertaling, reproductie en vernietiging van gerubriceerde gegevens

1. Alle vertalingen en reproducties van gerubriceerde gegevens dienen op dezelfde wijze beveiligd en gecontroleerd te worden als de oorspronkelijke gerubriceerde gegevens. Ze krijgen hetzelfde rubriceringsniveau als de oorspronkelijke gerubriceerde gegevens.

2. Vertalingen van gerubriceerde gegevens 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.

3. Het aantal reproducties van gerubriceerde gegevens blijft beperkt tot het aantal dat nodig is voor officiële doeleinden.

4. Gerubriceerde gegevens met het rubriceringsniveau dat overeenkomt met ULTRASSECRETO / Stg. ZEER GEHEIM, worden niet gereproduceerd of vertaald zonder de voorafgaande schriftelijke toestemming van de partij van herkomst.

5. Gerubriceerde gegevens met het rubriceringsniveau dat overeenkomt met ULTRASSECRETO / Stg. ZEER GEHEIM worden niet vernietigd zonder de voorafgaande schriftelijke toestemming van de partij van herkomst. Zij worden geretourneerd aan de partij van herkomst nadat de ontvangende entiteit ze niet meer nodig acht.

6. Gerubriceerde gegevens met het rubriceringsniveau dat overeenkomt met SECRETO / Stg. GEHEIM worden vernietigd in overeenstemming met de nationale wet- en regelgeving nadat de ontvangende entiteit ze niet meer nodig acht.

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

Artikel IX

Overbrenging van gerubriceerde gegevens

1. Gerubriceerde gegevens met het rubriceringsniveau ULTRASSECRETO / Stg. ZEER GEHEIM en SECRETO / Stg. GEHEIM worden tussen de partijen overgebracht langs diplomatieke weg of zoals schriftelijk overeengekomen door hun respectieve bevoegde beveiligingsautoriteiten.

2. Rubriceringsniveaus die niet in het eerste lid zijn opgenomen worden overgebracht in overeenstemming met de nationale wet- en regelgeving van de partij van herkomst.

3. Indien gerubriceerde gegevens via communicatiesystemen, netwerken of andere elektromagnetische middelen worden overgebracht, dient gebruik te worden gemaakt van encryptiemiddelen die door beide bevoegde beveiligingsautoriteiten wederzijds worden geaccepteerd.

4. In het geval van overbrenging van gerubriceerde gegevens waarbij een speciale vervoersprocedure nodig is, dienen beide bevoegde beveiligingsautoriteiten vooraf schriftelijk een logistiek plan overeen te komen.

Artikel X

Bezoeken

1. Bezoeken aan faciliteiten waar toegang tot gerubriceerde gegevens wordt verkregen of waar deze worden verwerkt of vastgelegd, dienen vooraf schriftelijk te worden goedgekeurd door de bevoegde beveiligingsau-

toriteit van de partij die als gastheer optreedt, tenzij anderszins overeengekomen door de bevoegde beveiligingsautoriteiten. Deze goedkeuring wordt alleen gegeven aan natuurlijke personen die voldoen aan de vereisten van artikel VII van dit Verdrag.

2. De aanvraag voor het bezoek dient te worden ingediend bij de bevoegde beveiligingsautoriteit van de partij die als gastheer optreedt, voorzien van de volgende gegevens die uitsluitend voor het bezoek worden gebruikt:
a. volledige naam, geboortedatum en -plaats, nationaliteit, andere staatsburgerschappen en nummer identiteitskaart/paspoort van de bezoeker;
b. titel en functiebenaming van de bezoeker en de naam en het adres van de organisatie waar de bezoeker werkzaam is of die de bezoeker vertegenwoordigt;
c. de specificatie van het project waaraan de bezoeker deelneemt;
d. de bevestiging van de veiligheidsmachtiging personeel van de bezoeker en het niveau en de geldigheid ervan;
e. de naam van de locatie die bezocht gaat worden;
f. het doel van het bezoek;
g. het verwachte hoogste rubriceringsniveau van de gerubriceerde gegevens waartoe toegang wordt verkregen of die worden verwerkt of opgeslagen;
h. naam, adres, telefoonnummer, e-mailadres en contactpunt van de te bezoeken locatie;
i. datum en duur van het bezoek;
j. volledige periode waarin de herhalingsbezoeken plaatsvinden; en
k. datum en handtekening van een vertegenwoordiger van de bevoegde beveiligingsautoriteit van de bezoeker.

3. De aanvraag voor het bezoek dient ten minste 10 (tien) kalenderdagen vóór de beoogde datum van het bezoek te worden ingediend, tenzij de bevoegde beveiligingsautoriteiten een andere termijn afspreken.

4. De bevoegde beveiligingsautoriteiten kunnen een lijst overeenkomen van bezoekers die herhalingsbezoeken mogen afleggen gedurende een periode van niet langer dan 12 (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 het bezoek is goedgekeurd.

6. Alle gerubriceerde gegevens die aan de bezoeker worden overgedragen worden beschouwd als gerubriceerde gegevens uit hoofde van dit Verdrag en worden behandeld in overeenstemming met de bepalingen van dit Verdrag. Daarnaast dient de bezoeker te voldoen aan de beveiligingsregelingen van de partij die als gastheer optreedt.

7. De partijen waarborgen, in overeenstemming met hun nationale wet- en regelgeving, de beveiliging van de persoonsgegevens van de personen die een bezoek willen brengen. De persoonsgegevens worden niet gebruikt voor enig ander doel dan het besluit over de aanvraag voor een bezoek.

8. Wanneer toestemming wordt verleend stelt de bevoegde beveiligingsautoriteit van de partij die als gastheer optreedt de verzoekende partij zo spoedig mogelijk in kennis van het bezoek en stelt ook de te bezoeken locatie op de hoogte.

Artikel XI

Inbreuk op de beveiliging

1. Wanneer er een inbreuk op de beveiliging met betrekking tot gerubriceerde gegevens uit hoofde van dit Verdrag wordt vermoed of vastgesteld door de ontvangende entiteit, stelt de bevoegde beveiligingsautoriteit van de partij waar de inbreuk op de beveiliging zich heeft voorgedaan de bevoegde beveiligingsautoriteit van de andere partij onverwijld 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 op de beveiliging te beoordelen.

2. De bevoegde beveiligingsautoriteit van de partij waar de inbreuk op de beveiliging zich heeft voorgedaan neemt onmiddellijk alle noodzakelijke stappen, in overeenstemming met haar nationale wet- en regelgeving, om een vermoede of vastgestelde inbreuk op de beveiliging te onderzoeken. De bevoegde beveiligingsautoriteit van de partij van herkomst kan, indien overeengekomen, meewerken aan het onderzoek. De partij van herkomst wordt altijd op de hoogte gesteld van de resultaten van het onderzoek en van de eventueel genomen maatregelen.

3. De bevoegde beveiligingsautoriteit van de partij waar de inbreuk op de beveiliging zich heeft voorgedaan neemt alle stappen, met inbegrip van maar niet beperkt tot juridische stappen, in overeenstemming met haar nationale wet- en regelgeving, om de gevolgen van een inbreuk op de beveiliging te beperken en een herhaling daarvan te voorkomen.

4. Wanneer een inbreuk op de beveiliging zich bij een derde heeft voorgedaan stelt de bevoegde beveiligingsautoriteit van de partij die de gegevens naar de derde heeft overgebracht, onmiddellijk de bevoegde beveiligingsautoriteit van de partij van herkomst in kennis van de inbreuk op de beveiliging, waarborgt dat de inbreuk op de beveiliging goed wordt onderzocht en communiceert de resultaten van het onderzoek en eventueel genomen maatregelen.

5. Elke partij kan om informatie verzoeken over de onderzoeksprocedure inzake de inbreuk op de beveiliging.

Artikel XII

Gerubriceerde contracten

1. Indien een partij of een opdrachtnemer voorstelt een gerubriceerd contract toe te kennen 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 is toegekend op het vereiste rubriceringsniveau.

2. De bevoegde beveiligingsautoriteit van de partij waar het gerubriceerde contract wordt uitgevoerd waarborgt dat de opdrachtnemer, en indien van toepassing zijn onderaannemer:
a. waarborgt dat alle natuurlijke personen die toegang krijgen tot gerubriceerde gegevens in kennis worden gesteld van hun verantwoordelijkheid de gerubriceerde gegevens te beveiligen in overeenstemming met de voorwaarden omschreven in dit Verdrag en de nationale wet- en regelgeving;
b. de beveiligingsuitvoering op zijn locaties in het oog houdt in overeenstemming met de nationale wet- en regelgeving;
c. zijn bevoegde beveiligingsautoriteit onverwijld in kennis stelt van elk beveiligingsincident dat betrekking heeft op het gerubriceerd contract; en
d. een juiste veiligheidsmachtiging bedrijfslocatie bezit teneinde de gerubriceerde gegevens te beveiligen en dat de natuurlijke personen die toegang dienen te krijgen tot gerubriceerde gegevens, een juiste veiligheidsmachtiging personeel hebben.

3. Elk gerubriceerd contract, met inbegrip van gerubriceerde onderaannemingscontracten, dat in overeenstemming met dit Verdrag wordt gesloten dient beveiligingsvereisten te bevatten waarin de volgende aspecten vermeld staan:
a. een rubriceringsgids, waarin in ieder geval de tabel van artikel IV, eerste lid, is opgenomen met een specificatie van de toepasselijke rubriceringsniveaus van elk deel van het gerubriceerde contract;
b. een procedure voor het doorgeven van wijzigingen van het rubriceringsniveau;
c. de kanalen en procedures die gebruikt dienen te worden voor het vervoer en/of de overdracht van gerubriceerde gegevens;
d. instructies voor de omgang met en opslag 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; en
f. de verplichting elke inbreuk op de beveiliging te melden.

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

Artikel XIII

Kosten

Elke partij draagt haar eigen kosten die ontstaan in verband met de uitvoering van en het toezicht op alle aspecten van dit Verdrag, tenzij de partijen anderszins overeenkomen.

Artikel XIV

Beslechting van geschillen

1. Elk geschil dat tussen de partijen kan ontstaan omtrent de uitlegging of toepassing van dit Verdrag, of omtrent daarmee samenhangende kwesties, wordt uitsluitend door middel van overleg en onderhandelingen tussen de partijen opgelost en niet ter beslechting voorgelegd aan een internationaal scheidsgerecht of een andere derde.

2. Tijdens het proces van geschillenbeslechting blijven beide partijen hun verplichtingen uit hoofde van dit Verdrag nakomen.

3. De procedure voor geschillenbeslechting tussen beide partijen wordt uitgevoerd met inachtneming van het beginsel van vertrouwelijkheid.

Artikel XV

Communicatie

Alle formele communicatie tussen de partijen over de uitvoering van dit Verdrag geschiedt schriftelijk in de Engelse taal.

Artikel XVI

Inwerkingtreding

Dit Verdrag treedt in werking op de eerste dag van de tweede maand die volgt op de ontvangst van de laatste kennisgeving waarin de partijen elkaar langs diplomatieke weg ervan in kennis hebben gesteld dat aan de interne wettelijke vereisten voor de inwerkingtreding van dit Verdrag is voldaan.

Artikel XVII

Territoriale toepassing

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).

Artikel XVIII

Wijzigingen

1. Dit Verdrag, met inbegrip van de Bijlage erbij, kan te allen tijde schriftelijk worden aangepast door middel van wijzigingen en met wederzijdse instemming van de partijen. Voorstellen voor wijzigingen geschieden langs diplomatieke weg.

2. De wijzigingen treden in werking onder de voorwaarden vervat in artikel XVI van dit Verdrag, met uitzondering van wijzigingen van de Bijlage, welke in werking treden op een door de partijen overeen te komen datum.

Artikel XIX

Geldigheid en beëindiging

1. Dit Verdrag wordt gesloten voor onbepaalde tijd.

2. Elke partij kan dit Verdrag te allen tijde beëindigen door de andere partij daarvan langs diplomatieke weg kennis te geven.

3. De beëindiging wordt van kracht 6 (zes) maanden na de datum waarop de andere partij de kennisgeving van beëindiging ontvangt.

4. Na de beëindiging 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.

Artikel XX

Slotbepalingen

De bevoegde beveiligingsautoriteiten brengen elkaar op de hoogte van hun respectieve nationale wet- en regelgeving en stellen elkaar onverwijld in kennis van wijzigingen die van invloed zijn op de beveiliging van gerubriceerde gegevens uit hoofde van dit Verdrag en die gevolgen hebben voor dit Verdrag. In het geval van dergelijke wijzigingen, bespreken de partijen of het noodzakelijk is dit Verdrag te herzien.

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

GEDAAN te Brasilia op 9 oktober 2023 in twee oorspronkelijke exemplaren, elk in de Nederlandse, de Portugese 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,

A.M.A. Driessen

Voor de Federatieve Republiek Brazilië,

MARCOS ANTONIO AMARO DOS SANTOS

Bijlage

De bevoegde beveiligingsautoriteiten die verantwoordelijk zijn voor de implementatie van en het toezicht op dit Verdrag zijn:

Namens de Federatieve Republiek Brazilië:
Het Kabinet voor Institutionele Veiligheid van het Presidentschap van de Federatieve Republiek Brazilië (Gabinete de Segurança Institucional da Presidência da República)

Namens het Koninkrijk der Nederlanden:
De bevoegde beveiligingsautoriteit is:
De Algemene Inlichtingen- en Veiligheidsdienst (AIVD)
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

De gemachtigde bevoegde beveiligingsautoriteit voor het militaire domein is:
De Beveiligingsautoriteit
Directoraat-Generaal Beleid
Ministerie van Defensie

Acordo entre o Reino dos Países Baixos e a República Federative do Brasil sobre Troca e Proteção Mútua de Informações classificadas

O Reino dos Países Baixos

e

a República Federativa do Brasil,

Doravante denominados em conjunto como «Partes», ou separadamente, como «Parte».

No interesse da segurança nacional e para garantir a proteção de Informações Classificadas trocadas no âmbito de instrumentos de cooperação, contratos e outros acordos firmados entre as Partes, seus indivíduos credenciados, órgãos, bem como entidades públicas e privadas.

Desejando estabelecer uma estrutura de regras e procedimentos relacionados às Informações Classificadas de acordo com as leis e regulamentos nacionais das Partes.

Confirmando que este Acordo não afetará os compromissos de ambas as Partes que derivam de outros acordos internacionais e que não será usado contra os interesses, a segurança e a integridade territorial de outros Estados,

Acordaram o seguinte:

Artigo I

Finalidade

1. Este Acordo estabelece regras e procedimentos para a proteção de Informações Classificadas trocadas entre as referidas Partes, seus indivíduos credenciados, órgãos, bem como entidades públicas ou privadas sob sua jurisdição.

2. Este Acordo não constitui fundamento para obrigar o fornecimento ou troca de Informações Classificadas pelas Partes.

Artigo II

Definições

Para os fins deste Acordo, o termo:
a. Acordo significa este acordo incluindo seus Anexos;
b. Anexo significa um anexo a este Acordo;
c. Contrato Classificado significa um acordo, incluindo quaisquer negociações pré-contratuais, cuja execução requeira ou implique o acesso ou potencial acesso ou a criação de Informação Classificada;
d. Informação Classificada significa a informação, material ou objeto, independentemente da sua forma ou natureza ou qualquer parte do mesmo, com um determinado Nível de Classificação de Segurança, que independentemente da forma como é apresentado deve ser protegido contra o acesso não autorizado, divulgação ou outro tipo de Comprometimento da Informação para o qual foi designado, para evitar danos ou prejuízos no interesse de uma ou ambas as Partes, de acordo com as respectivas leis e regulamentos de cada Parte e deste Acordo;
e. Autoridade de Segurança Competente (ASC) significa a autoridade de cada Parte responsável pela segurança de Informações Classificadas sob este Acordo;
f. Comprometimento da Informação significa qualquer forma de uso indevido, dano ou acesso não autorizado, alteração, divulgação ou destruição de Informações Classificadas, bem como qualquer outra ação ou omissão que resulte na perda de sua confidencialidade, integridade, disponibilidade ou autenticidade;
g. Contratante significa qualquer pessoa jurídica sob a jurisdição de uma Parte, celebrando ou de outra forma vinculada a um Contrato Classificado;
h. Autorização de Segurança de Instalação significa a certificação pela Autoridade de Segurança Competente de que uma entidade pública ou privada possui medidas de segurança apropriadas e, portanto, foi credenciada para o Tratamento de Informações Classificadas, de acordo com as leis e regulamentos nacionais de cada Parte;
i. Tratamento de Informações Classificadas significa um conjunto de ações relacionadas com a produção, recepção, classificação, utilização, acesso, reprodução, transporte, transmissão, distribuição, arquivamento, armazenamento, eliminação, destino ou controle de Informações Classificadas num determinado Nível de Classificação de Segurança;
j. "Necessidade de Conhecer" significa a exigência de um indivíduo acessar, ter conhecimento ou possuir Informações Classificadas para o desempenho de funções e tarefas oficiais;
k. Parte Originária significa a Parte sob cuja autoridade as Informações Classificadas foram criadas;
l. Credencial de Segurança Pessoal significa a certificação de que um determinado indivíduo foi aprovado em segurança e, portanto, credenciado para o Tratamento de Informações Classificadas, em um determinado Nível de Classificação de Segurança, de acordo com as leis e regulamentos nacionais de cada Parte;
m. Entidade Provedora significa a Parte, ou Contratante, que fornece Informações Classificadas à Entidade Receptora nos termos deste Acordo;
n. Entidade Receptora significa a Parte, ou Contratante, que recebe Informações Classificadas nos termos deste Acordo;
o. Violação de Segurança significa qualquer ação ou omissão, intencional ou acidental, que resulte em um Comprometimento da Informação real ou possível de Informações Classificadas fornecidas ou geradas sob este Acordo;
p. Nível de Classificação de Segurança significa o nível de proteção atribuído às Informações Classificadas, de acordo com as leis e regulamentos nacionais de cada Parte e conforme incorporado no artigo IV, parágrafo 1 deste Acordo; e
q. Terceiro significa qualquer organização, estado, governo ou indivíduo que não seja Parte deste Acordo.

Artigo III

Autoridades de Segurança Competentes

1. As Autoridades de Segurança Competentes, responsáveis pela implementação e supervisão deste Acordo, estão listadas no Anexo a este Acordo.

2. A Autoridade de Segurança Competente pode delegar partes de suas responsabilidades a uma Autoridade de Segurança Competente delegada.

3. Cada Parte fornecerá à outra os dados de contato de sua respectiva Autoridade de Segurança Competente, por escrito. As Autoridades de Segurança Competentes das Partes deverão informar-se por escrito sobre alterações em seus dados de contato.

4. A fim de garantir uma cooperação estreita na implementação deste Acordo, as Autoridades de Segurança Competentes poderão consultar-se sempre que necessário.

5. Representantes de ambas as Autoridades de Segurança Competentes poderão visitar mutuamente as suas instalações com a intenção de adquirir conhecimento de procedimentos e medidas de segurança aplicáveis à Informação Classificada, sujeito à aprovação da Autoridade de Segurança Competente anfitriã.

6. Mediante solicitação, as Autoridades de Segurança Competentes poderão auxiliar-se mutuamente à realização dos procedimentos para a concessão de Autorizações de Segurança de Instalações e Credenciais de Segurança Pessoal, por meio de solicitação e de acordo com suas leis e regulamentos nacionais.

7. Mediante solicitação da Autoridade de Segurança Competente de uma Parte, a Autoridade de Segurança Competente da outra Parte emitirá uma confirmação por escrito de que foi emitida uma Credencial de Segurança Pessoal e/ou Autorização de Segurança de Instalação válida.

8. As Autoridades de Segurança Competentes das Partes deverão reconhecer mutuamente suas Credenciais de Segurança Pessoal e, Autorizações de Segurança de Instalações emitidas de acordo com suas respectivas leis e regulamentos e dentro do escopo deste Acordo.

9. As Autoridades de Segurança Competentes notificarão imediatamente umas às outras, por escrito, sobre alterações nas Credenciais de Segurança Pessoal e Autorizações de Segurança de Instalações reconhecidas para quem ou para as quais uma confirmação foi fornecida de acordo com o parágrafo 8 deste artigo.

Artigo IV

Níveis de Classificação de Segurança

1. As Partes concordam que os Níveis de Classificação de Segurança, de acordo com suas respectivas leis e regulamentos nacionais, deverão corresponder entre si na seguinte forma de equivalência:

Classificação Parte Originária	**Classificação Entidade Receptora**
«Stg. ZEER GEHEIM»	«ULTRASSECRETO»
«Stg. GEHEIM»	«SECRETO»
«Stg. CONFIDENTIEEL»	«SECRETO»
«DEPARTEMENTAAL VERTROUWELIJK»	«RESERVADO»
«ULTRASSECRETO»	«Stg. ZEER GEHEIM»
«SECRETO»	«Stg. GEHEIM»
«RESERVADO»	«Stg. CONFIDENTIEEL»

2. Quaisquer Informações Classificadas, produzidas nos termos deste Acordo, deverão ser marcadas com o Nível de Classificação de Segurança equivalente da Parte Originária, de acordo com o parágrafo 1 deste artigo.

3. A Entidade Receptora deverá marcar todas as Informações Classificadas sob este Acordo que tenha recebido da Entidade Provedora com o Nível de Classificação de Segurança equivalente à Entidade Receptora de acordo com o parágrafo 1 deste artigo. O Nível de Classificação de Segurança da Parte Originária deverá ser indicado primeiro, a fim de determinar o Nível de Classificação de Segurança equivalente apropriado.

4. As Partes notificarão uma à outra sobre qualquer alteração e posterior alteração no Nível de Classificação de Segurança de Informações Classificadas.

5. A Parte Originária poderá marcar a Informação Classificada com requisitos de tratamento, para especificar qualquer limitação ao seu uso, divulgação, liberação e acesso pela Entidade Receptora.

6. A Entidade Receptora não modificará ou revogará a classificação de segurança das Informações Classificadas recebidas ou geradas no âmbito deste Acordo sem a aprovação prévia por escrito da Parte Originária.

7. As Informações Classificadas originadas em conjunto pelas Partes será atribuído um Nível de Classificação de Segurança mutuamente determinado pelas Partes.

Artigo V

Proteção de Informações Classificadas

1. As Partes deverão tomar todas as medidas apropriadas de acordo com suas leis e regulamentos nacionais para garantir a proteção de Informações Classificadas em conformidade com este Acordo. Deverão proporcionar às Informações Classificadas trocadas ou geradas sob este Acordo, pelo menos, a mesma proteção que concedem às suas próprias Informações Classificadas ao Nível de Classificação de Segurança correspondente.

2. O tratamento de qualquer Informação Classificada trocada entre as Partes deverá respeitar as disposições deste Acordo.

3. Cada Parte garantirá que sejam implementadas as medidas necessárias para a proteção de Informações Classificadas processadas, armazenadas ou transmitidas por sistemas de comunicação e informação, de acordo com o Nível de Classificação de Segurança, este Acordo, e com as leis e regulamentos nacionais.

4. Cada Parte garantirá a confidencialidade, integridade, disponibilidade e, quando aplicável, autenticidade, responsabilidade e rastreabilidade de Informações Classificadas.

5. As Partes não divulgarão nenhuma Informação Classificada sem o consentimento por escrito da Parte Originária.

Artigo VI

Uso de Informações Classificadas

1. Cada Parte deverá garantir que a Entidade Provedora:
a. marcará as Informações Classificadas com a classificação de segurança apropriada de acordo com suas leis e regulamentos nacionais e
b. informará a Entidade Receptora de quaisquer condições de divulgação ou limitações à utilização de Informação Classificada disponibilizada, conforme determinado pela Parte Originária.

2. Cada Parte deverá garantir que a Entidade Receptora:
a. oferecerá às Informações Classificadas o mesmo nível de proteção concedido às suas Informações Classificadas nacionais de um Nível de Classificação de Segurança equivalente conforme determinado no artigo IV, parágrafo 1;
b. não deverá desclassificar ou rebaixar as Informações Classificadas sem o consentimento prévio por escrito da Parte Originária;
c. não divulgará Informações Classificadas a Terceiros sem o consentimento prévio por escrito da Parte Originária; e
d. deverá usar as Informações Classificadas apenas para os fins para os quais foram divulgadas e de acordo com quaisquer requisitos de manuseio da Parte Originária.

3. Cada Parte, de acordo com seus requisitos constitucionais, leis e regulamentos nacionais, respeitará o princípio do consentimento de origem.

Artigo VII

Acesso às Informações Classificadas

1. Cada Parte garantirá que o acesso às Informações Classificadas seja concedido com base na Necessidade de Conhecer.

2. Cada Parte deverá garantir que qualquer indivíduo que tenha acesso às Informações Classificadas seja informado sobre suas responsabilidades para proteger essas informações e tenha assinado uma declaração de confidencialidade de acordo com as leis e regulamentos nacionais da Entidade Receptora.

3. As Partes garantirão que o acesso às Informações Classificadas seja concedido apenas a indivíduos que possuam uma Credencial de Segurança Pessoal ao nível correspondente ou que estejam devidamente autorizados a acessar à Informação Classificada em virtude de suas funções nos termos das leis e regulamentos nacionais da Entidade Receptora.

Artigo VIII

Tradução, Reprodução e Destruição de Informações Classificadas

1. Todas as traduções e reproduções de Informações Classificadas deverão ser protegidas e controladas da mesma forma que as Informações Classificadas originais. Deverão receber o mesmo Nível de Classificação de Segurança que as Informações Classificadas originais.

2. As traduções de Informações Classificadas deverão conter uma anotação adequada no idioma da tradução, indicando que contêm Informações Classificadas da Parte Originária.

3. O número de reproduções de Informações Classificadas será limitado ao necessário para sua finalidade oficial.

4. Informações Classificadas com Nível de Classificação de Segurança equivalente a ULTRASSECRETO / Stg. ZEER GEHEIM, não deverão ser reproduzidas ou traduzidas sem o consentimento prévio por escrito da Parte Originária.

5. Informações Classificadas com Nível de Classificação de Segurança equivalente a ULTRASSECRETO / Stg. ZEER GEHEIM não deverão ser destruídas sem o consentimento prévio por escrito da Parte Originária. Deverão ser devolvidas à Parte Originária quando não forem mais consideradas necessárias pela Entidade Receptora.

6. Informações Classificadas com Nível de Classificação de Segurança equivalente a SECRETO / Stg. GEHEIM deverão ser destruídas de acordo com as leis e regulamentos nacionais depois que não forem mais consideradas necessárias pela Entidade Receptora.

7. Se uma situação de crise impossibilitar a Entidade Receptora de proteger a Informação Classificada prestada sob este Acordo, a Informação Classificada será imediatamente destruída. A Entidade Receptora notificará prontamente por escrito a Autoridade de Segurança Competente da Parte Originária sobre a destruição desta Informação Classificada.

Artigo IX

Transmissão de Informações Classificadas

1. Informações Classificadas com Nível de Classificação de Segurança ULTRASSECRETO / Stg. ZEER GEHEIM e SECRETO / Stg. GEHEIM serão transmitidas entre as Partes, por via diplomática, ou conforme acordado por escrito pelas respectivas Autoridades de Segurança Competentes.

2. Os Níveis de Classificação de Segurança não incluídos no parágrafo 1 serão transmitidos de acordo com as leis e regulamentos nacionais da Parte Originária.

3. As Informações Classificadas transmitidas através de sistemas de comunicação, redes ou outros meios eletromagnéticos deverão utilizar meios criptografados mutuamente aceitos pelas respectivas Autoridades de Segurança Competentes.

4. No caso de transmissão de Informações Classificadas que requeira procedimentos especiais para o seu transporte, deverá ser previamente acordado, por escrito, um plano logístico por ambas as Autoridades de Segurança Competentes.

Artigo X

Visitas

1. As visitas às instalações onde as Informações Classificadas serão acessadas, processadas ou registradas estarão sujeitas à aprovação prévia por escrito da Autoridade de Segurança Competente da Parte anfitriã, salvo acordo em contrário das Autoridades de Segurança Competentes. Tal aprovação somente será concedida às pessoas físicas que atendam aos requisitos estabelecidos no artigo VII deste Acordo.

2. O pedido de visita deverá ser submetido à Autoridade de Segurança Competente da Parte anfitriã, incluindo os seguintes dados que serão utilizados apenas para efeitos da visita:

a. nome e sobrenome do visitante, data e local de nascimento, nacionalidade, outras cidadanias e número do cartão de identificação/número do passaporte;
b. o título e a função do visitante, bem como o nome e endereço da organização pela qual o visitante é empregado ou que o visitante representa;
c. a especificação do projeto no qual o visitante estará participando;
d. a confirmação da Credencial de Segurança Pessoal do visitante e seu nível e validade;
e. o nome da instalação a ser visitada;
f. o propósito da visita;
g. o Nível de Classificação de Segurança mais alto antecipado das Informações Classificadas a serem acessadas, processadas ou armazenadas;
h. o nome, endereço, número de telefone, endereço de e-mail e ponto de contato da instalação a ser visitada;
i. a data e duração da visita;
j. o período total em que as visitas são recorrentes; e
k. a data e assinatura de um representante da Autoridade de Segurança Competente do visitante.

3. A solicitação de visita deverá ser apresentada com antecedência mínima de 10 (dez) dias corridos da data proposta para a visita, salvo se as Autoridades de Segurança Competentes acordarem prazo diverso.

4. As Autoridades de Segurança Competentes poderão acordar uma lista de visitantes com direito a visitas recorrentes por um período não superior a 12 (doze) meses. As Autoridades de Segurança Competentes deverão concordar com os detalhes adicionais destas visitas recorrentes.

5. A Autoridade de Segurança Competente da Parte anfitriã informará os funcionários de segurança da organização a ser visitada sobre os detalhes daqueles indivíduos cujos pedidos de visita foram aprovados. Uma vez concedida à aprovação, os arranjos de visitas para indivíduos que receberam aprovação para visitas recorrentes podem ser feitos diretamente com a agência, instalação ou organização em questão.

6. Quaisquer Informações Classificadas transmitidas ao visitante serão consideradas Informações Classificadas nos termos deste Acordo e serão tratadas em conformidade com as disposições deste Acordo. Além disso, o visitante deverá cumprir os regulamentos de segurança da Parte anfitriã.

7. As Partes garantirão, de acordo com suas leis e regulamentos nacionais, a proteção dos dados pessoais dos indivíduos que solicitarão uma visita. Os dados pessoais não serão utilizados para outra finalidade que não seja autorizar o pedido de visita.

8. Quando autorizada, a Autoridade de Segurança Competente da Parte anfitriã notificará a Parte requerente, com a maior brevidade possível, da visita e também notificará a instalação a ser visitada.

Artigo XI

Violação de Segurança

1. Sempre que a Entidade Receptora suspeite ou verifique uma Violação de Segurança relacionada com Informação Classificada sob este Acordo, a Autoridade de Segurança Competente da Parte onde ocorreu a Violação de Segurança informará imediatamente a Autoridade de Segurança Competente da outra Parte. A notificação deverá conter detalhes suficientes para que a Parte Originária avalie as consequências e circunstâncias da Violação de Segurança suspeita ou constatada.

2. A Autoridade de Segurança Competente da Parte onde ocorreu a Violação de Segurança tomará imediatamente todas as medidas necessárias, de acordo com suas leis e regulamentos nacionais, para investigar qualquer Violação de Segurança suspeita ou comprovada. A Autoridade de Segurança Competente da Parte Originária poderá, se acordado, cooperar na investigação. A Parte Originária será sempre informada sobre o resultado da investigação e as medidas tomadas, se houver.

3. A Autoridade de Segurança Competente da Parte onde ocorreu a Violação de Segurança deverá tomar todas as medidas, incluindo, entre outras, medidas legais, de acordo com suas leis e regulamentos nacionais, para mitigar as consequências de uma Violação de Segurança e evitar qualquer recorrência.

4. Quando ocorrer uma Violação de Segurança em um Terceiro, a Autoridade de Segurança Competente da Parte que transmitiu as informações ao Terceiro, informará imediatamente a Autoridade de Segurança Competente da Parte Originária sobre a Violação de Segurança, certificando-se de que a Violação de Segurança seja investigada adequadamente e comunique o resultado da investigação e quaisquer medidas tomadas.

5. Qualquer Parte poderá solicitar informações sobre o processo de investigação de Violação de Segurança.

Artigo XII

Contratos Classificados

1. Se uma Parte ou um Contratado propuser a concessão de um Contrato Classificado, com um Contratado sob a jurisdição da outra Parte, deverá primeiro obter confirmação por escrito da Autoridade de Segurança Competente da outra Parte de que o Contratado recebeu uma Autorização de Segurança de Instalação no Nível de Classificação de Segurança apropriado.

2. A Autoridade de Segurança Competente da Parte onde o Contrato Classificado será executado deverá garantir que o Contratante e, se aplicável, o seu subcontratante:
a. garante que todos os indivíduos com acesso às Informações Classificadas sejam informados de suas responsabilidades para proteger as Informações Classificadas de acordo com as condições definidas neste Acordo e com as leis e regulamentos nacionais;
b. monitora a conduta de segurança dentro de suas instalações de acordo com as leis e regulamentos nacionais;
c. notifique prontamente a sua Autoridade de Segurança Competente sobre qualquer Violação de Segurança relacionada com o Contrato Classificado; e
d. possua uma Credencial de Segurança de Instalação adequada para proteger as Informações Classificadas e que os indivíduos que precisarem de acesso às Informações Classificadas possuam uma Credencial de Segurança Pessoal adequada.

3. Todo Contrato Classificado, incluindo subcontratos classificados celebrados em conformidade com este Acordo, deverá incluir requisitos de segurança que identifiquem os seguintes aspectos:
a. um guia de classificação de segurança, que incluirá sempre a tabela do artigo IV, parágrafo 1°, especificando os Níveis de Classificação de Segurança aplicáveis a cada parte do Contrato Classificado;
b. um procedimento para comunicação de alterações no Nível de Classificação de Segurança;
c. os canais e procedimentos a utilizar para o transporte e/ou transmissão de Informação Classificada;
d. instruções para o tratamento e armazenamento de Informações Classificadas;
e. detalhes de contato das Autoridades de Segurança Competentes responsáveis por supervisionar a proteção de Informações Classificadas relacionadas ao Contrato Classificado; e
f. obrigação de notificar quaisquer Violações de Segurança.

4. A Autoridade de Segurança Competente da Parte que autoriza a adjudicação do Contrato Classificado deverá remeter cópia do capítulo dos requisitos de segurança à Autoridade de Segurança Competente da Entidade Receptora, para facilitar a fiscalização da segurança do Contrato Classificado.

Artigo XIII

Custos

Cada Parte arcará com os custos de suas próprias despesas resultantes da implementação e supervisão de todos os aspectos deste Acordo, a menos que mutuamente determinado pelas Partes.

Artigo XIV

Solução de Controvérsias

1. Qualquer controvérsia que possa surgir entre as Partes em relação à interpretação ou aplicação deste Acordo, ou qualquer assunto relacionado, será resolvida exclusivamente por meio de consultas e negociações entre as Partes e não deverá ser encaminhada a nenhum tribunal internacional ou Terceiro para resolução.

2. Durante o período de solução de controvérsias, ambas as Partes continuarão cumprindo suas obrigações nos termos deste Acordo.

3. Os procedimentos de solução de controvérsias entre ambas as Partes serão conduzidos com base no princípio da confidencialidade.

Artigo XV

Comunicação

Todas as comunicações formais entre as Partes relacionadas à implementação deste Acordo serão feitas por escrito, no idioma inglês.

Artigo XVI

Entrada em Vigor

Este Acordo entrará em vigor no primeiro dia do segundo mês seguinte ao recebimento da última notificação pela qual as Partes se informarão, por via diplomática, que seus requisitos legais internos necessários para sua entrada em vigor foram cumpridos.

Artigo XVII

Aplicação Territorial

No que diz respeito ao Reino dos Países Baixos, o presente Acordo aplica-se à parte europeia dos Países Baixos e à parte caribenha dos Países Baixos (as ilhas de Bonaire, Sint Eustatius e Saba).

Artigo XVIII

Emendas

1. Este Acordo, incluindo seu Anexo, poderá ser alterado a qualquer momento, por escrito, por meio de emendas e consentimento mútuo entre as Partes. As emendas serão propostas por via diplomática.

2. As emendas entrarão em vigor nos termos do artigo XVI deste Acordo, com exceção das emendas do Anexo, que entrarão em vigor em data a ser acordada pelas Partes.

Artigo XIX

Validade e Rescisão

1. Este Acordo será celebrado por tempo indeterminado.

2. Qualquer das Partes poderá, a qualquer momento, rescindir este Acordo por meio de notificação por escrito, por via diplomática, à outra Parte.

3. A rescisão entrará em vigor 6 (seis) meses após a data em que a outra Parte receber a notificação de rescisão.

4. Após a rescisão, quaisquer Informações Classificadas trocadas, divulgadas ou geradas sob este Acordo continuarão a ser protegidas em conformidade com os termos deste Acordo antes de sua rescisão, enquanto as Informações Classificadas permanecerem classificadas.

Artigo XX

Disposições Finais

Cada Autoridade de Segurança Competente deverá informar-se mutuamente sobre suas respetivas leis e regulamentos nacionais e notificar-se imediatamente sobre as alterações que afetem a proteção de Informações Classificadas fornecidas sob este Acordo e tenham impacto no presente Acordo. No caso de tais alterações, as Partes discutirão a necessidade de revisão deste Acordo.

EM FÉ DO QUE, os representantes devidamente autorizados das Partes assinaram este Acordo.

FEITO EM Brasília em 9 de outubro 2023 em dois exemplares originais, cada um nas línguas holandesa, portuguesa e inglesa, sendo todos os textos igualmente autênticos. Em caso de divergência de interpretação, prevalecerá o texto em inglês.

Pelo Reino dos Países Baixos,

A.M.A. DRIESSEN

Pela República Federativa do Brasil,

MARCOS ANTIONO AMARO DOS SANTOS

Anexo

As Autoridades de Segurança Competentes, responsáveis pela implementação e supervisão deste Acordo, são:

Em nome da República Federativa do Brasil:
Gabinete de Segurança Institucional da Presidência da República Federativa do Brasil

Em nome do Reino dos Países Baixos:
A Autoridade de Segurança Competente é:
Serviço Geral de Inteligência e Segurança
Ministério do Interior e Relações do Reino

A Autoridade de Segurança Competente delegada no domínio militar é:
Autoridade de Segurança de Defesa
Direção-Geral de Política
Ministro da defesa

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 XVI 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 ervan in kennis hebben gesteld dat aan de interne wettelijke vereisten voor de inwerkingtreding van het Verdrag is voldaan.

Uitgegeven de *zestiende* oktober 2023.

De Minister van Buitenlandse Zaken,

H.G.J. BRUINS SLOT

trb-2023-120
ISSN 0920 - 2218
's-Gravenhage 2023