15 (2021) Nr. 1

# TRACTATENBLAD

VAN HET

KONINKRIJK DER NEDERLANDEN

**JAARGANG 2021 Nr. 123**

A. TITEL

*Verdrag tussen het Koninkrijk der Nederlanden en het Koninkrijk Spanje inzake de uitwisseling en wederzijdse beveiliging van gerubriceerde gegevens (met Bijlage); Madrid, 23 september 2021*

**Voor een overzicht van de verdragsgegevens, zie verdragsnummer 012027 in de Verdragenbank.**

B. TEKST

## Agreement between the Kingdom of the Netherlands and the Kingdom of Spain concerning the exchange and mutual protection of classified information

The Kingdom of the Netherlands

and

the Kingdom of Spain,

Hereinafter referred to as "the Parties",

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

Article 1

*purpose*

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

Article 2

*definitions*

For the purpose of this Agreement:

a) **"Classified Contract"** means a contract, including any pre-contractual negotiations, to be entered into by one of the Parties with a Contractor for the supply of goods, execution of works or provision of services, the performance of which requires or involves access or potential access to or the creation of Classified Information.
b) **"Classified Information"** means any information or material designated by a security classification by one of the Parties the unauthorised disclosure or loss of which could cause varying degrees of prejudice to the interests of one or both of the Parties.
c) **"Competent Security Authority"** means the government authority in a Party responsible for the implementation and supervision of this Agreement.
d) **"Contractor"** means any individual or legal entity with the capacity to enter into contracts.

e) **"Facility Security Clearance"** means the positive determination by the Competent Security Authority that a facility has in place appropriate security measures to access and handle Classified Information up to and including a specified security classification level, in accordance with national laws and regulations.
f) **"Need to know"** means the requirement for an individual or a legal entity for access to, knowledge of or possession of Classified Information to perform official tasks or services.
g) **"Originating Party"** means the Party under whose authority Classified Information has been created under this Agreement.
h) **"Personnel Security Clearance"** means the positive determination by the Competent Security Authority that an individual has been security cleared to access and handle Classified Information up to and including a specified classification level, in accordance with its national laws and regulations.
i) **"Providing Party"** means the Party or Contractor under its jurisdiction, which provides Classified Information to the Receiving Party under this Agreement.
j) **"Receiving Party"** means the Party or Contractor under its jurisdiction, which receives Classified Information from the Providing Party under this Agreement.
k) **"Security Classification Guide"** means a document associated with a Classified Contract that identifies each part of that Classified Contract which contains Classified Information, specifying the applicable security classification levels.
l) **"Security Incident"** means an act or an omission, contrary to national laws and regulations, which results in the unauthorised access, disclosure, loss or compromise of Classified Information.
m) **"Third Party"** means any international organisation or state, including legal entities or individuals under its jurisdiction, which is not a Party to this Agreement.

Article 3

*competent security authorities*

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

2. The Competent Security Authorities shall provide each other with official contact details.

Article 4

*security classification levels*

1. The following security classifications of the Parties are equivalent and correspond to the security classification levels specified in their national legislation.

| **For the Kingdom of Spain** | **For the Kingdom of the Netherlands** |
|---|---|
| SECRETO | Stg ZEER GEHEIM |
| RESERVADO | Stg GEHEIM |
| CONFIDENCIAL | Stg CONFIDENTIEEL |
| DIFUSIÓN LIMITADA | DEPARTEMENTAAL VERTROUWELIJK |

2. The Receiving Party shall mark all the Classified Information under this Agreement that it has received from the Providing Party with the security classification that corresponds to the security classification given by the Originating Party in accordance with the scheme contained in paragraph 1 of this Article.

3. The Receiving Party may modify or cancel the security classification of received Classified Information under this Agreement only upon the written approval of the Originating Party.

Article 5

*access to classified information*

1. Access to Classified Information at the Security Classification Levels equivalent to CONFIDENCIAL / Stg CONFIDENTIEEL and above, as mentioned in Article 4 of this Agreement, shall be granted only to those individuals who have a Need to know, hold a Personnel Security Clearance at the corresponding level, are briefed on their responsibilities and have signed a statement of confidentiality in accordance with national laws and regulations.

2. Access to Classified Information at the Security Classification Level equivalent to DIFUSIÓN LIMITADA / DEPARTEMENTAAL VERTROUWELIJK as mentioned in Article 4 of this Agreement, shall be granted only to those individuals who have a Need to know, are briefed on their responsibilities and have signed a statement of confidentiality in accordance with national laws and regulations.

Article 6

*security measures*

1. The Parties shall take all appropriate measures applicable under their national laws and regulations to protect Classified Information generated and/or provided under this Agreement.

2. The Providing Party shall take all appropriate measures to ensure that:
a) Classified Information is marked with the appropriate classification marking in accordance with its national laws and regulations;
b) the Receiving Party is informed of any conditions of release or limitations on the use of the Classified Information provided;
c) the Receiving Party is informed of any subsequent change in the security classification level of the Classified Information provided.

3. The Receiving Party shall take all appropriate measures to ensure that:
a) Classified Information received from the Originating Party is afforded the same level of protection as that given to its national Classified Information of an equivalent security classification level;
b) Classified Information is marked with its own corresponding security classification level;
c) the Security Classification Levels assigned to Classified Information are not altered or revoked without the prior written consent of the Originating Party;
d) that Classified Information is not disclosed or released to a Third Party without the prior written consent of the Originating Party;
e) Classified Information is used solely for the purpose it has been released for and in accordance with handling requirements of the Originating Party.

Article 7

*security co-operation*

1. In order to maintain comparable standards of security, the Competent Security Authorities shall, on request, inform each other about their security regulations, policies and practices for protecting Classified Information.

2. On request of the Competent Security Authority of one Party, the Competent Security Authority of the other Party shall issue a written confirmation that a valid Personnel Security Clearance or Facility Security Clearance has been issued.

3. 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 national laws and regulations.

4. 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.

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

Article 8

*classified contracts*

1. If a Party or a Contractor under its jurisdiction proposes to grant a Classified Contract at the Security Classification Levels equivalent to CONFIDENCIAL / Stg CONFIDENTIEEL or above as mentioned in Article 4 of this Agreement, with a (Sub-)Contractor under the jurisdiction of the other Party, it shall first obtain written confirmation from the other Party that the Contractor has been granted a Facility Security Clearance and/or Personnel Security Clearance(s) at the appropriate security classification level.

2. The Competent Security Authority shall ensure that the Contractor:
a) ensures that all individuals granted access to Classified Information are informed of their responsibilities to protect Classified Information in accordance with the conditions defined in this Agreement and with national laws and regulations;
b) monitors the security conduct within its facilities;
c) notifies promptly its Competent Security Authority of any Security Incident relating to the Classified Contract.
d) In addition to the subparagraphs a, b and c, for Classified Contracts at the Security Classification Levels equivalent to CONFIDENCIAL / Stg CONFIDENTIEEL 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.

3. Every Classified Contract concluded in accordance with this Agreement shall include a security requirements chapter which identifies the following aspects:
a) A Security Classification Guide;
b) A procedure for communication of changes in the security classification level, taking into account Article 4, paragraph 3 of this Agreement;
c) The channels and procedures to be used for the transport and/or transmission of Classified Information;
d) Instructions for the handling 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;
f) Obligation to notify any Security Incidents.

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

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

6. If a Contractor sub-contracts parts of a Classified Contract, the Contractor and the Sub-contractor shall ensure the observance of this Article.

Article 9

*transmission of classified information*

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

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

Article 10

*reproduction, translation and destruction of classified information*

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

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

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

4. Classified Information marked at the Security Classification Level equivalent to SECRETO / Stg ZEER GEHEIM as mentioned in Article 4 of this Agreement, shall not be translated or reproduced without the prior written consent of the Originating Party.

5. Classified Information marked at the Security Classification Level equivalent to SECRETO / Stg ZEER GEHEIM as mentioned in Article 4 of this Agreement 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 Providing and Receiving Parties.

6. Classified Information marked up to and including the Security Classification Levels equivalent to RESERVADO / Stg GEHEIM as mentioned in Article 4 of this Agreement, shall be destroyed after it is no longer considered necessary by the Receiving Party, in accordance with its national laws and regulations.

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

Article 11

*visits*

1. Visits requiring access to Classified Information are subject to the prior written consent of the respective Competent Security Authority, unless otherwise agreed between the Competent Security Authorities.

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

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

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

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

6. Government officials of either Party shall be permitted to participate in classified meetings by providing proof of their Personnel Security Clearance to the meeting organiser or secretariat ahead of the meeting.

Article 12

*security incident*

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

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

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

Article 13

*costs*

In the case of any cost, each Party shall bear its own costs incurred in the course of implementing its obligations under this Agreement.

Article 14

*dispute resolution*

Any dispute on the interpretation or application of this Agreement shall be settled exclusively through negotiation between the Parties.

Article 15

*relation to other agreements*

This Agreement does not prevail over any international agreement that has already been or may be entered into and that specifically governs a transaction otherwise governed by this Agreement.

Article 16

*implementing arrangements*

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

Article 17

*final provisions*

1. This Agreement is concluded for an indefinite period of time. Each Party shall notify the other Party through diplomatic channels once the national procedures necessary for entry into force of this Agreement have been completed. This Agreement shall enter into force on the first day of the second month following the receipt of the latter notification.

2. With regard to the Kingdom of the Netherlands, this Agreement shall apply to the European part of the Netherlands and the Caribbean part of the Netherlands (the islands of Bonaire, Sint Eustatius and Saba).

3. This Agreement may be amended with the mutual consent of the Parties. Either Party may propose amendments to this Agreement at any time through diplomatic channels. Such amendments shall enter into force under the conditions laid down in paragraph 1 of this Article, with the exception of an amendment to Annex I, which amendment shall enter into force on a date to be agreed upon by the Parties.

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

5. Regardless of the termination of this Agreement, all Classified Information released or generated under this Agreement shall be protected in accordance with this Agreement for as long as it remains classified.

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

DONE in Madrid on 23 September 2021 in two original copies, in the Dutch, Spanish and English languages, all texts being equally authentic. In case of any divergence of interpretation, the English text shall prevail.

*For the Kingdom of the Netherlands,*

JAN TH. VERSTEEG

*For the Kingdom of Spain,*

PAZ ESTEBAN LÓPEZ

---

**Annex I**

The Competent Security Authority for the Kingdom of Spain is:

Secretary of State
Director of the National Intelligence Centre
National Office of Security

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

National Security Authority (NSA)
General Intelligence and Security Service
Ministry of the Interior and Kingdom Relations

---

**Verdrag tussen het Koninkrijk der Nederlanden en het Koninkrijk Spanje inzake de uitwisseling en wederzijdse beveiliging van gerubriceerde gegevens**

Het Koninkrijk der Nederlanden

en

het Koninkrijk Spanje,

Hierna te noemen „de partijen",

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

Artikel 1

*doel*

Dit Verdrag heeft ten doel de beveiliging te waarborgen van gerubriceerde gegevens die worden uitgewisseld tussen de partijen of tussen rechtspersonen of natuurlijke personen onder hun rechtsmacht, of die worden gegenereerd in het kader van een bilateraal programma uit hoofde van dit Verdrag. In het Verdrag worden de veiligheidsprocedures en regelingen voor deze beveiliging vastgelegd.

Artikel 2

*begripsomschrijvingen*

Voor de toepassing van dit Verdrag wordt verstaan onder:

a. **„Gerubriceerd contract"**, een contract, met inbegrip van eventuele voorafgaande contractonderhandelingen, dat een van de partijen aangaat met een opdrachtnemer voor de levering van goederen, uitvoering van werkzaamheden of levering van diensten, waarbij voor de uitvoering toegang of mogelijk toegang tot gerubriceerde gegevens vereist is of waarbij deze gecreëerd worden.
b. **„Gerubriceerde gegevens"**, gegevens die, of materiaal dat, door een van de partijen als gerubriceerd worden of wordt aangemerkt, waarvan de ongeoorloofde bekendmaking of het verlies de belangen van een of beide partijen in meer of mindere mate zou kunnen schaden.
c. **„Bevoegde veiligheidsautoriteit"**, de overheidsautoriteit in een partij die verantwoordelijk is voor de implementatie van en het toezicht op dit Verdrag.
d. **„Opdrachtnemer"**, elke natuurlijke persoon of rechtspersoon die bevoegd is contracten aan te gaan.
e. **„Veiligheidsmachtiging bedrijfslocatie"**, de vaststelling door de bevoegde veiligheidsautoriteit dat een bedrijfslocatie passende veiligheidsmaatregelen heeft genomen voor de toegang tot en de omgang met gerubriceerde gegevens tot en met een gespecificeerd rubriceringsniveau, in overeenstemming met de nationale wet- en regelgeving.
f. **„Need to know"**, het vereiste voor een natuurlijke persoon of rechtspersoon voor toegang tot, kennis van of bezit van gerubriceerde gegevens voor het uitvoeren van officiële taken of diensten.
g. **„Partij van herkomst"**, de partij onder wier gezag gerubriceerde gegevens zijn gecreëerd ingevolge dit Verdrag.
h. **„Veiligheidsmachtiging personeel"**, de vaststelling door de bevoegde veiligheidsautoriteit dat een natuurlijke persoon toestemming heeft gekregen voor de toegang tot en de omgang met gerubriceerde gegevens tot en met een gespecificeerd rubriceringsniveau, in overeenstemming met de nationale wet- en regelgeving.
i. **„Verstrekkende partij"**, de partij of opdrachtnemer onder haar rechtsmacht die de gerubriceerde gegevens uit hoofde van dit Verdrag verstrekt aan de ontvangende partij.
j. **„Ontvangende partij"**, de partij of opdrachtnemer onder haar rechtsmacht die de gerubriceerde gegevens krachtens dit Verdrag ontvangt van de verstrekkende partij.
k. **„Rubriceringsgids"**, een document dat hoort bij een gerubriceerd contract waarin elk onderdeel van het gerubriceerd contract dat gerubriceerde gegevens bevat wordt genoemd, met inbegrip van de rubriceringsniveaus die erop van toepassing zijn.
l. **„Veiligheidsincident",** elk handelen of nalaten te handelen, in strijd met de nationale wet- en regelgeving, dat resulteert in ongeoorloofde toegang tot of bekendmaking, verlies of compromittering van gerubriceerde gegevens.
m. **„Derde",** elke internationale organisatie of staat, met inbegrip van rechtspersonen of natuurlijke personen onder zijn rechtsmacht, die geen partij is bij dit Verdrag.

Artikel 3

*bevoegde veiligheidsautoriteiten*

1. De bevoegde veiligheidsautoriteiten van de partijen staan vermeld in Bijlage 1 bij dit Verdrag.

2. De bevoegde veiligheidsautoriteiten voorzien elkaar van de officiële contactgegevens.

Artikel 4

*rubriceringsniveaus*

1. De volgende rubriceringsniveaus van de partijen komen overeen en corresponderen met de rubriceringsniveaus die in hun nationale wetgeving staan vermeld.

| **Voor het Koninkrijk Spanje** | **Voor het Koninkrijk der Nederlanden** |
|---|---|
| SECRETO | Stg ZEER GEHEIM |
| RESERVADO | Stg GEHEIM |
| CONFIDENCIAL | Stg CONFIDENTIEEL |
| DIFUSIÓN LIMITADA | DEPARTEMENTAAL VERTROUWELIJK |

2. De ontvangende partij voorziet alle gerubriceerde gegevens uit hoofde van dit Verdrag die zij ontvangen heeft van de verstrekkende partij van het rubriceringsniveau dat overeenkomt met het door de partij van herkomst gegeven rubriceringsniveau in overeenstemming met de tabel in het eerste lid van dit artikel.

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

Artikel 5

*toegang tot gerubriceerde gegevens*

1. Toegang tot gerubriceerde gegevens op een rubriceringsniveau dat overeenkomt met CONFIDENCIAL / Stg CONFIDENTIEEL en hoger, zoals vermeld in artikel 4 van dit Verdrag, wordt uitsluitend verleend aan de natuurlijke personen die van de gegevens op de hoogte moeten zijn (need to know), een veiligheidsmachtiging personeel hebben op het overeenkomstige niveau, zijn ingelicht over hun verantwoordelijkheden en een geheimhoudingsverklaring hebben ondertekend in overeenstemming met de nationale wet- en regelgeving.

2. Toegang tot gerubriceerde gegevens op een rubriceringsniveau dat overeenkomt met DIFUSIÓN LIMITADA / DEPARTEMENTAAL VERTROUWELIJK, zoals vermeld in artikel 4 van dit Verdrag, wordt uitsluitend verleend aan de natuurlijke personen die van de gegevens op de hoogte moeten zijn (need to know), zijn ingelicht over hun verantwoordelijkheden en een geheimhoudingsverklaring hebben ondertekend in overeenstemming met de nationale wet- en regelgeving.

Artikel 6

*veiligheidsmaatregelen*

1. De partijen nemen alle passende maatregelen die krachtens hun nationale wet- en regelgeving van toepassing zijn op de uit hoofde van dit Verdrag gegenereerde en/of verstrekte gerubriceerde gegevens.

2. De verstrekkende partij neemt alle passende maatregelen om te waarborgen dat:
a. gerubriceerde gegevens worden voorzien van de juiste rubriceringsmarkering in overeenstemming met haar nationale wet- en regelgeving;
b. de ontvangende partij in kennis wordt gesteld van mogelijke voorwaarden voor vrijgave of beperkingen gesteld aan het gebruik van de verstrekte gerubriceerde gegevens;
c. de ontvangende partij in kennis wordt gesteld van eventuele navolgende veranderingen van het rubriceringsniveau van de verstrekte gerubriceerde gegevens.

3. De ontvangende partij neemt alle passende maatregelen om te waarborgen dat:
a. aan gerubriceerde gegevens die worden ontvangen van de partij van herkomst hetzelfde beveiligingsniveau wordt toegekend als aan haar nationale gerubriceerde gegevens met een overeenkomstig rubriceringsniveau;
b. gerubriceerde gegevens worden voorzien van haar eigen dienovereenkomstige rubriceringsniveau;

c. de aan de gerubriceerde gegevens toegekende rubriceringsniveaus niet worden veranderd of ingetrokken zonder de voorafgaande schriftelijke toestemming van de partij van herkomst;
d. gerubriceerde gegevens niet bekend worden gemaakt of vrijgegeven aan een derde zonder de voorafgaande schriftelijke toestemming van de partij van herkomst;
e. gerubriceerde gegevens uitsluitend worden gebruikt voor het doel waarvoor zij zijn vrijgegeven en in overeenstemming met de eisen voor gebruik van de partij van herkomst.

Artikel 7

*veiligheidssamenwerking*

1. Teneinde vergelijkbare veiligheidsnormen te handhaven, verstrekken de bevoegde veiligheidsautoriteiten elkaar op verzoek informatie over hun veiligheidsvoorschriften, -beleid en -praktijken met betrekking tot de beveiliging van gerubriceerde gegevens.

2. Op verzoek van de bevoegde veiligheidsautoriteit van de ene partij bevestigt de bevoegde veiligheidsautoriteit van de andere partij schriftelijk dat er een geldige veiligheidsmachtiging personeel of veiligheidsmachtiging bedrijfslocatie is afgegeven.

3. De bevoegde veiligheidsautoriteiten verlenen elkaar, op verzoek en in overeenstemming met de nationale wet- en regelgeving, bijstand bij het uitvoeren van onderzoeken in verband met de afgifte van een veiligheidsmachtiging bedrijfslocatie en veiligheidsmachtiging personeel.

4. De bevoegde veiligheidsautoriteiten stellen elkaar onverwijld schriftelijk in kennis van veranderingen in erkende veiligheidsmachtigingen bedrijfslocatie en veiligheidsmachtigingen personeel waarvoor een bevestiging is verstrekt.

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

Artikel 8

*gerubriceerde contracten*

1. Indien een partij of een opdrachtnemer onder haar rechtsmacht voorstelt een gerubriceerd contract met een rubriceringsniveau dat overeenkomt met CONFIDENCIAL / Stg CONFIDENTIEEL of hoger, zoals vermeld in artikel 4 van dit Verdrag, te gunnen aan een (onder)opdrachtnemer onder de rechtsmacht van de andere partij, dient zij eerst de schriftelijke bevestiging te verkrijgen van de andere partij dat aan deze opdrachtnemer een veiligheidsmachtiging bedrijfslocatie en/of veiligheidsmachtiging(en) personeel is/zijn toegekend op het juiste rubriceringsniveau.

2. De bevoegde veiligheidsautoriteit waarborgt dat de opdrachtnemer:
a. waarborgt dat alle natuurlijke personen die toegang krijgen tot gerubriceerde gegevens in kennis worden gesteld van hun verantwoordelijkheid de gerubriceerde gegevens te beveiligen in overeenstemming met de voorwaarden omschreven in dit Verdrag en de nationale wet- en regelgeving;
b. de beveiligingsuitvoering op zijn locaties in het oog houdt;
c. zijn bevoegde veiligheidsautoriteit onverwijld in kennis stelt van elk veiligheidsincident dat betrekking heeft op het gerubriceerde contract.
d. In aanvulling op de onderdelen a, b en c, van dit lid, met betrekking tot gerubriceerde contracten met een rubriceringsniveau dat overeenkomt met CONFIDENCIAL / Stg CONFIDENTIEEL of hoger, zoals vermeld in artikel 4 van dit Verdrag, waarborgt de bevoegde veiligheidsautoriteit dat de opdrachtnemer een veiligheidsmachtiging bedrijfslocatie bezit op 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 op het juiste rubriceringsniveau hebben.

3. Elk gerubriceerd contract dat in overeenstemming met dit Verdrag wordt gesloten dient een hoofdstuk met veiligheidsvereisten te bevatten waarin de volgende aspecten vermeld staan:
a. een rubriceringsgids;
b. een procedure voor het doorgeven van wijzigingen van het rubriceringsniveau, rekening houdend met artikel 4, derde lid, van dit Verdrag;
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 en opslag van gerubriceerde gegevens;
e. contactgegevens van de bevoegde veiligheidsautoriteiten die verantwoordelijk zijn voor het toezicht op de beveiliging van gerubriceerde gegevens die betrekking hebben op het gerubriceerde contract;
f. de verplichting van elk veiligheidsincident kennis te geven.

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

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

6. Indien een opdrachtnemer delen van een gerubriceerd contract uitbesteedt aan een onderopdrachtnemer, waarborgen de opdrachtnemer en de onderopdrachtnemer de naleving van dit artikel.

Artikel 9

*overbrenging van gerubriceerde gegevens*

1. Gerubriceerde gegevens worden overgebracht in overeenstemming met de nationale wet- en regelgeving van de verstrekkende partij of zoals anderszins overeengekomen tussen de bevoegde veiligheidsautoriteiten.

2. De partijen kunnen gerubriceerde gegevens die door encryptie beveiligd zijn langs elektronische weg overbrengen in overeenstemming met procedures die door de bevoegde veiligheidsautoriteiten dienen te worden goedgekeurd.

Artikel 10

*reproductie, vertaling en vernietiging van gerubriceerde gegevens*

1. Reproducties en vertalingen van gerubriceerde gegevens krijgen dezelfde markering en beveiliging als de oorspronkelijke gerubriceerde gegevens.

2. Vertalingen of reproducties worden beperkt tot het minimumaantal dat nodig is voor gebruik uit hoofde van dit Verdrag en worden uitsluitend gemaakt door natuurlijke personen die in overeenstemming met de nationale wet- en regelgeving gemachtigd zijn toegang te hebben tot gerubriceerde gegevens met het rubriceringsniveau van de gerubriceerde gegevens die vertaald of gereproduceerd worden.

3. Vertalingen dienen te worden voorzien van een passende annotatie in de taal waarin zij zijn gesteld met de aanduiding dat zij gerubriceerde gegevens bevatten van de verstrekkende partij.

4. Gerubriceerde gegevens met een markering op het rubriceringsniveau dat overeenkomt met SECRETO / Stg ZEER GEHEIM zoals vermeld in artikel 4 van dit Verdrag, worden niet vertaald of gereproduceerd zonder de voorafgaande schriftelijke toestemming van de partij van herkomst.

5. Gerubriceerde gegevens met een markering op het rubriceringsniveau dat overeenkomt met SECRETO / Stg ZEER GEHEIM zoals vermeld in artikel 4 van dit Verdrag, worden niet vernietigd zonder de voorafgaande schriftelijke toestemming van de partij van herkomst. Zij worden geretourneerd aan de partij van herkomst nadat de verstrekkende en de ontvangende partij ze niet meer nodig achten.

6. Gerubriceerde gegevens met een markering tot en met het rubriceringsniveau dat overeenkomt met RESERVADO / Stg GEHEIM zoals vermeld in artikel 4 van dit Verdrag, worden vernietigd nadat de ontvangende partij ze niet meer nodig acht, in overeenstemming met haar nationale wet- en regelgeving.

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

Artikel 11

*bezoeken*

1. Bezoeken waarbij toegang tot gerubriceerde gegevens vereist is, dienen vooraf schriftelijk te worden goedgekeurd door de respectieve bevoegde veiligheidsautoriteit, tenzij anderszins overeengekomen door de bevoegde veiligheidsautoriteiten.

2. De bezoeker dient de aanvraag voor het bezoek ten minste twintig dagen vóór de beoogde datum van het bezoek in bij zijn bevoegde veiligheidsautoriteit, die de aanvraag doorstuurt naar de bevoegde veiligheids-

autoriteit van de andere partij. In dringende gevallen kan de aanvraag van een verzoek binnen een kortere termijn worden ingediend, mits hierover voorafgaande coördinatie tussen de bevoegde veiligheidsautoriteiten plaatsvindt.

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

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

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

6. Het is overheidsfunctionarissen van elke partij toegestaan deel te nemen aan gerubriceerde vergaderingen indien zij vooraf bij de organisator van de vergadering of het secretariaat aantonen dat zij beschikken over een veiligheidsmachtiging personeel.

Artikel 12

*veiligheidsincident*

1. De bevoegde veiligheidsautoriteiten stellen elkaar onverwijld schriftelijk in kennis van een feitelijk of vermoedelijk veiligheidsincident waarbij gerubriceerde gegevens van de andere partij betrokken zijn.

2. De ontvangende partij onderzoekt feitelijke of vermoedelijke veiligheidsincidenten onmiddellijk. De bevoegde autoriteit van de partij van herkomst verleent, indien nodig, medewerking aan het onderzoek.

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

Artikel 13

*kosten*

Indien er sprake is van kosten, draagt elke partij haar eigen kosten die ontstaan in verband met de uitvoering van haar verplichtingen ingevolge dit Verdrag.

Artikel 14

*oplossing van geschillen*

Elk geschil omtrent de interpretatie of toepassing van dit Verdrag wordt uitsluitend beslecht door middel van onderhandelingen tussen de partijen.

Artikel 15

*relatie met andere verdragen*

Dit Verdrag heeft geen voorrang boven elk internationaal verdrag dat reeds is gesloten of nog kan worden gesloten en dat specifiek betrekking heeft op een verrichting waarop dit Verdrag anderszins van toepassing is.

Artikel 16

*uitvoeringsregelingen*

De bevoegde veiligheidsautoriteiten kunnen uitvoeringsregelingen sluiten ingevolge dit Verdrag.

Artikel 17

*slotbepalingen*

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

2. Ten aanzien van het Koninkrijk der Nederlanden is dit Verdrag van toepassing op het Europese deel van Nederland en op het Caribische deel van Nederland (de eilanden Bonaire, Sint Eustatius en Saba).

3. Dit Verdrag kan met wederzijdse instemming van de partijen worden gewijzigd. Elke partij kan te allen tijde langs diplomatieke weg wijzigingen van dit Verdrag voorstellen. Dergelijke wijzigingen treden in werking onder de voorwaarden vervat in het eerste lid van dit artikel, met uitzondering van een wijziging van Bijlage 1, welke wijziging in werking treedt op een door de partijen overeen te komen datum.

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

5. Ongeacht de beëindiging van dit Verdrag blijven alle uit hoofde van dit Verdrag vrijgegeven of gegenereerde gerubriceerde gegevens beveiligd in overeenstemming met dit Verdrag zolang deze gegevens gerubriceerd blijven.

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

GEDAAN te Madrid op 23 september 2021 in twee oorspronkelijke exemplaren, elk in de Nederlandse, de Spaanse 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,*

JAN TH. VERSTEEG

*Voor het Koninkrijk Spanje,*

PAZ ESTEBAN LÓPEZ

---

**Bijlage I**

De bevoegde veiligheidsautoriteit van het Koninkrijk Spanje is:

Staatssecretaris
Directeur van het Nationaal Inlichtingencentrum
Nationaal Veiligheidsbureau

De bevoegde veiligheidsautoriteit van het Koninkrijk der Nederlanden is:

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

---

**Acuerdo entre el Reino de los Países Bajos y el Reino de España para el intercambio y la protección mutua de la información clasificada**

El Reino de los Países Bajos

Y

el Reino de España,

En lo sucesivo denominados las «Partes»

Deseando garantizar la protección mutua de la Información Clasificada generada, en interés de la seguridad nacional, han convenido en lo siguiente;

Artículo 1

*objeto*

El objeto del presente Acuerdo es garantizar la protección de la Información Clasificada intercambiada entre las Partes, o por personas físicas o jurídicas bajo su jurisdicción, o generada en el marco de un programa bilateral en virtud del presente Acuerdo. El Acuerdo establece los procedimientos y medidas de seguridad para dicha protección.

Artículo 2

*definiciones*

A los efectos del presente Acuerdo:

a) Por **«Contrato Clasificado»** se entenderá un contrato, incluida cualquier negociación precontractual, que vaya a ser celebrado por una de las Partes con un Contratista para el suministro de mercancías, la ejecución de un trabajo o la prestación de un servicio cuya realización implique acceder a Información Clasificada o generarla;
b) Por **«Información Clasificada»** se entenderá cualquier información o material al que una de las Partes haya asignado una clasificación de seguridad, cuya pérdida o divulgación no autorizada podría provocar distintos grados de perjuicio a los intereses de una o ambas Partes.
c) Por **«Autoridad de Seguridad Competente»** se entenderá la autoridad del Gobierno de una Parte que es responsable de la aplicación y supervisión del presente Acuerdo.
d) Por **«Contratista»** se entenderá toda persona física o entidad con capacidad jurídica para celebrar contratos.
e) Por **«Habilitación de Seguridad de Establecimiento»** se entenderá la certificación, por parte de una Autoridad de Seguridad Competente, de que se han implantado en un establecimiento concreto las medidas oportunas de seguridad para el acceso a la Información Clasificada y su gestión hasta un Grado de Clasificación de Seguridad específico, de conformidad con las leyes y reglamentos nacionales.
f) Por **«Necesidad de Conocer»** se entenderá la necesidad de que una persona o entidad jurídica tenga acceso a Información Clasificada, conocimiento o posesión de la misma a efectos del desempeño de sus funciones o servicios oficiales.
g) Por **«Parte de Origen»** se entenderá la Parte bajo cuya autoridad se haya creado Información Clasificada con arreglo al presente Acuerdo;
h) Por **«Habilitación Personal de Seguridad»** se entenderá la certificación, por parte de una Autoridad de Seguridad Competente, de que una persona ha obtenido la habilitación de seguridad para el acceso a Información Clasificada y la gestión de la misma, hasta un Grado de Clasificación de Seguridad específico, este incluido, de conformidad con las leyes y reglamentos nacionales.
i) Por **«Parte Proveedora»** se entenderá la Parte, o un Contratista bajo su jurisdicción, que proporcione Información Clasificada a la Parte Receptora con arreglo al presente Acuerdo.
j) Por **«Parte Receptora»** se entenderá la Parte, o un Contratista bajo su jurisdicción, que reciba Información Clasificada de la Parte Proveedora con arreglo al presente Acuerdo.
k) Por **«Guía de Clasificación de Seguridad»** se entenderá un documento asociado al Contrato Clasificado que identifique las partes del Contrato Clasificado que contienen Información Clasificada, especificando los Grados de Clasificación de Seguridad aplicables.
l) Por **«Incidente de Seguridad»** se entenderá una acción u omisión contraria a las leyes y reglamentos nacionales que resulta en el acceso no autorizado, la divulgación, la pérdida o el comprometimiento de la Información Clasificada.
m) Por **«Tercero»** se entenderá toda organización internacional o Estado, incluidas las personas físicas y jurídicas bajo su jurisdicción, que no sea Parte en el presente Acuerdo.

Artículo 3

*autoridades de seguridad competentes*

1. Las Autoridades de Seguridad Competentes de las Partes figuran en el Anexo 1 al presente Acuerdo.

2. Las Autoridades de Seguridad Competentes deberán facilitarse mutuamente datos de contacto oficiales.

Artículo 4

*grados de clasificación de seguridad*

1. Los siguientes Grados de Clasificaciones de Seguridad de las Partes son equivalentes y corresponden a los Grados de Clasificación de Seguridad detallados en su legislación nacional.

| **Para el Reino de España** | **Para el Reino de los Países Bajos** |
|---|---|
| SECRETO | Stg ZEER GEHEIM |
| RESERVADO | Stg GEHEIM |
| CONFIDENCIAL | Stg CONFIDENTIEEL |
| DIFUSIÓN LIMITADA | DEPARTEMENTAAL VERTROUWELIJK |

2. La Parte Receptora marcará toda la Información Clasificada facilitada por la Parte Proveedora con los Grados de Clasificación de Seguridad que se corresponden con la Clasificación de Seguridad otorgada por la Parte de Origen, de conformidad con la tabla de equivalencias del apartado 1 del presente Artículo.

3. La Parte Receptora podrá modificar o cancelar la Clasificación de Seguridad de la Información Clasificada recibida en virtud del presente Acuerdo únicamente previa autorización por escrito de la Parte de Origen.

Artículo 5

*acceso a la información clasificada*

1. El acceso a la Información Clasificada con un Grado de Seguridad CONFIDENCIAL / Stg CONFIDENTIEEL o con un grado de seguridad superior, según se menciona en el artículo 4 del presente Acuerdo, se limitará a las personas que tengan Necesidad de Conocer, que hayan recibido la Habilitación Personal de Seguridad pertinente, a quienes se haya informado de sus responsabilidades y que hayan firmado una declaración de confidencialidad de conformidad con las leyes y reglamentos nacionales.

2. El acceso a la Información Clasificada con un Grado de Seguridad DIFUSIÓN LIMITADA / DEPARTEMENTAAL VERTROUWELIJK, según se menciona en el artículo 4 del presente Acuerdo, se limitará a las personas que tengan Necesidad de Conocer, a quienes se haya informado de sus responsabilidades y que hayan firmado una declaración de confidencialidad de conformidad con las leyes y reglamentos nacionales.

Artículo 6

*medidas de seguridad*

1. Las Partes deberán adoptar todas las medidas oportunas aplicables con arreglo a sus leyes y reglamentos nacionales para proteger la Información Clasificada generada y/o facilitada en virtud del presente Acuerdo.

2. La Parte Proveedora adoptará todas las medidas oportunas para garantizar:
a) Que se otorga a la Información Clasificada la clasificación adecuada de conformidad con sus leyes y reglamentos nacionales;
b) Que se informa a la Parte Receptora de las condiciones de divulgación o limitaciones al uso de la Información Clasificada recibida;
c) Que se informa a la Parte Receptora de cualquier cambio posterior en el Grado de Clasificación de Seguridad de la Información Clasificada facilitada.

3. La Parte Receptora adoptará todas las medidas oportunas para garantizar:
a) Que se otorga a la Información Clasificada facilitada por la Parte de Origen el mismo nivel de protección que se da a su Información Clasificada nacional con un Grado de Clasificación de Seguridad equivalente;
b) Que la Información Clasificada se marca con su Grado de Clasificación de Seguridad propio correspondiente;
c) Que los Grados de Clasificación de Seguridad asignados a la Información Clasificada no se modifican o cancelan sin el consentimiento previo por escrito de la Parte de Origen;

d) Que la Información Clasificada no sea divulgada o cedida a ningún Tercero sin el previo consentimiento por escrito de la Parte de Origen;
e) Que la Información Clasificada se utiliza solo para el fin para el que ha sido cedida y de conformidad con los requisitos de gestión de la Parte de Origen.

Artículo 7

*cooperación en materia de seguridad*

1. Con el propósito de mantener niveles de seguridad equiparables, las Autoridades de Seguridad Competentes deberán, previa solicitud, informarse mutuamente de sus reglamentos, normas y prácticas de seguridad para la protección de la Información Clasificada.

2. A petición de la Autoridad de Seguridad Competente de una Parte, la Autoridad de Seguridad Competente de la otra Parte deberá confirmar por escrito que se ha expedido una Habilitación Personal de Seguridad o Habilitación de Seguridad de Establecimiento válida.

3. Las Autoridades de Seguridad Competentes, previa petición y de conformidad con las leyes y reglamentos nacionales, deberán colaborar entre sí para efectuar las investigaciones relativas a la Habilitación de Seguridad de Establecimiento y la Habilitación Personal de Seguridad.

4. Las Autoridades de Seguridad Competentes se notificarán inmediatamente por escrito cualquier cambio en las Habilitaciones Personales de Seguridad y las Habilitaciones de Seguridad de Establecimiento otorgadas para las que se haya facilitado una confirmación.

5. La cooperación con arreglo al presente Acuerdo se desarrollará en inglés.

Artículo 8

*contratos clasificados*

1. Si una Parte, o un Contratista bajo su jurisdicción, propone celebrar un Contrato Clasificado que suponga el acceso a Información Clasificada marcada como CONFIDENCIAL / Stg CONFIDENTIEEL o con un grado de seguridad superior, según se menciona en el artículo 4 del presente Acuerdo, con un (Sub) Contratista bajo la jurisdicción de la otra Parte, obtendrá previamente confirmación por escrito de esta última de que el Contratista ha obtenido una Habilitación de Seguridad de Establecimiento y/o una Habilitación Personal de Seguridad del Grado de Clasificación oportuno.

2. La Autoridad de Seguridad Competente velará por que el Contratista:
a) Garantice que se informa a todas las personas con acceso a la Información Clasificada de su responsabilidad de protegerla de conformidad con lo dispuesto en el presente Acuerdo y en las leyes y reglamentos nacionales;
b) Supervise el comportamiento relativo a la seguridad en sus instalaciones;
c) Notifique inmediatamente a la Autoridad de Seguridad Competente cualquier Incidente de Seguridad relativo al Contrato Clasificado.
d) Además de lo previsto en las letras a), b) y c), en el caso de Contratos Clasificados con un Grado de Clasificación equivalente a CONFIDENCIAL / Stg CONFIDENTIEEL o con un grado de seguridad superior, según se menciona en el artículo 4 del presente Acuerdo, la Autoridad de Seguridad Competente garantizará que el Contratista cuenta con una Habilitación de Seguridad de Establecimiento con el Grado de Clasificación de Seguridad oportuno para proteger la Información Clasificada y que las personas que precisen acceso a la Información Clasificada tienen una Habilitación Personal de Seguridad con el Grado de Clasificación de Seguridad pertinente.

3. Todo Contrato Clasificado celebrado de conformidad con el presente Acuerdo incluirá una sección de requisitos de seguridad que determine las siguiente cuestiones:
a) Una guía de clasificación de seguridad;
b) Un procedimiento de comunicación de los cambios en los grados de clasificación de seguridad, teniendo en cuenta el apartado 3 del artículo 4 del presente Acuerdo;
c) Los canales y procedimientos que deberán utilizarse para el transporte y/o transmisión de la Información Clasificada;
d) Las instrucciones para la gestión y almacenamiento de la Información Clasificada;
e) Los datos de contacto de las Autoridades de Seguridad Competentes responsables de supervisar la protección de Información Clasificada relativa al Contrato Clasificado;
f) La obligación de informar de cualquier Incidente de Seguridad.

4. La Autoridad de Seguridad Competente de la Parte que autorice la adjudicación del Contrato Clasificado deberá enviar el texto de la sección de requisitos de seguridad a la Autoridad de Seguridad Competente de la Parte Receptora para facilitar la supervisión de la seguridad del contrato.

5. Los procedimientos para la aprobación de las visitas del personal de una Parte a la otra Parte vinculadas a actividades del Contrato Clasificado se seguirán de conformidad con el artículo 11 del presente Acuerdo.

6. Si un Contratista subcontrata partes de un Contrato Clasificado, el Contratista y los Subcontratistas deberán garantizar el cumplimento del presente artículo.

Artículo 9

*transmisión de la información clasificada*

1. La Información Clasificada se transmitirá de conformidad con las leyes y reglamentos nacionales de la Parte Proveedora o de la forma en que lo acuerden las Autoridades de Seguridad Competentes.

2. Las Partes podrán transmitir por vía electrónica Información Clasificada protegida por medios criptográficos, de conformidad con los procedimientos que aprueben las Autoridades de Seguridad Competentes.

Artículo 10

*reproducción, traducción y destrucción de la información clasificada*

1. Toda traducción y reproducción de Información Clasificada mantendrá el Grado de Clasificación de Seguridad original y se protegerá en consecuencia.

2. Las traducciones y reproducciones se limitarán al mínimo requerido para su uso con arreglo al presente Acuerdo y serán realizadas únicamente por personas que hayan sido autorizadas, de conformidad con las leyes y reglamentos nacionales, para acceder a Información Clasificada del Grado de Clasificación de Seguridad que vaya a reproducirse o traducirse.

3. Las traducciones incorporarán la pertinente anotación en el idioma de destino en la que se indicará que contienen Información Clasificada de la otra Parte.

4. La Información Clasificada con un Grado de Clasificación de Seguridad equivalente a SECRETO / Stg ZEER GEHEIM, según se menciona en el artículo 4 del presente Acuerdo, no podrá traducirse ni reproducirse sin el previo consentimiento por escrito de la Parte de Origen.

5. La Información Clasificada con un Grado de Clasificación de Seguridad equivalente a SECRETO / Stg ZEER GEHEIM, según se menciona en el artículo 4 del presente Acuerdo, no podrá destruirse sin el previo consentimiento por escrito de la Parte de Origen. Deberá devolverse a la Parte de Origen cuando las Partes Proveedora y Receptora ya no la consideren necesaria.

6. La Información Clasificada con un Grado de Clasificación de Seguridad equivalente a RESERVADO / Stg GEHEIM, según se menciona en el artículo 4 del presente Acuerdo, deberá destruirse cuando la Parte Receptora ya no la considere necesaria, de conformidad con sus leyes y reglamentos nacionales.

7. En caso de situación de crisis en la que resulte imposible proteger la Información Clasificada facilitada en virtud del presente Acuerdo, esta deberá destruirse de inmediato. La Parte Receptora notificará de inmediato por escrito a la Autoridad de Seguridad Competente de la Parte Proveedora la destrucción de dicha Información Clasificada.

Artículo 11

*visitas*

1. Las visitas que requieran acceso a Información Clasificada estarán sujetas al consentimiento previo y por escrito de las respectivas Autoridades de Seguridad Competentes, a menos que dichas Autoridades acuerden otra cosa.

2. El visitante deberá enviar la solicitud de visita al menos veinte días antes de la fecha propuesta para la visita a su Autoridad de Seguridad Competente, que la remitirá a la Autoridad de Seguridad Competente de la otra Parte. En casos urgentes, el plazo de presentación de la solicitud podrá acortarse, previa coordinación entre las respectivas Autoridades de Seguridad Competentes.

3. La solicitud de visita deberá incluir:

a) El nombre completo, la fecha y lugar de nacimiento, la nacionalidad y el número del pasaporte/documento de identidad del visitante;
b) El cargo oficial del visitante y el nombre de la organización a la que representa;
c) La confirmación de la Habilitación Personal de Seguridad y su validez;
d) La fecha y la duración de la visita. Si se trata de visitas recurrentes deberá indicarse el periodo total en el que se producirán;
e) El objetivo de la visita y el Grado de Clasificación de Seguridad previsto de la Información Clasificada que se tratará o la que se tendrá acceso;
f) El nombre, dirección, número de teléfono/fax, dirección de correo electrónico y punto de contacto de los establecimientos que vayan a visitarse;
g) La fecha, firma y sello de un representante de la Autoridad de Seguridad Competente del visitante.

4. Las Autoridades Nacionales de Seguridad podrán acordar una lista de visitantes autorizados para realizar visitas recurrentes. Dichas Autoridades acordarán los ulteriores pormenores de dichas visitas.

5. La Información Clasificada facilitada a un visitante o que se le transmita deberá tratarse de conformidad con las disposiciones del presente Acuerdo.

6. Los funcionarios públicos de cualquiera de las Partes tendrán permiso para participar en reuniones clasificadas entregando, con antelación a la celebración de la reunión, al organizador o secretario de la misma un certificado que acredite que están en posesión de una Habilitación Personal de Seguridad.

Artículo 12

*incidentes de seguridad*

1. Las Autoridades de Seguridad Competentes deberán informarse inmediatamente por escrito de cualquier Incidente de Seguridad real o presunto que afecte a Información Clasificada de la otra Parte.

2. La Parte Receptora investigará de inmediato cualquier Incidente de Seguridad real o supuesto. La Autoridad de Seguridad Competente de la Parte de Origen cooperará, si es necesario, en dicha investigación.

3. La Autoridad de Seguridad Competente adoptará las medidas adecuadas, de conformidad con sus leyes y reglamentos nacionales, para limitar las consecuencias derivadas del incidente y evitar que vuelva a suceder. Se informará a la Autoridad de Seguridad Competente de la Parte de Origen del resultado de la investigación y de las medidas que, en su caso, se hayan adoptado.

Artículo 13

*gastos*

Cada una de las Partes deberá asumir cualesquiera gastos en los que haya podido incurrir durante el cumplimiento de sus obligaciones en virtud del presente Acuerdo.

Artículo 14

*resolución de controversias*

Las Partes resolverán exclusivamente mediante negociación toda controversia en torno a la interpretación o aplicación del presente Acuerdo.

Artículo 15

*relación con otros acuerdos*

El presente Acuerdo no prevalece sobre ningún acuerdo internacional que ya se haya celebrado o que pueda celebrarse y que se aplique a una transacción regida por lo demás por el presente Acuerdo.

Artículo 16

*acuerdos de aplicación*

Las Autoridades de Seguridad Competentes podrán celebrar acuerdos de aplicación en relación con el presente Acuerdo.

Artículo 17

*disposiciones finales*

1. El presente Acuerdo se concluye por un periodo indefinido. Cada Parte informará a la otra Parte, por conducto diplomático, de que se han completado sus trámites internos necesarios para la entrada en vigor del presente Acuerdo, que será efectivo el primer día del segundo mes posterior a la recepción de la última notificación.

2. En lo que respecta al Reino de los Países Bajos, el Presente Acuerdo se aplicará a las zonas europea y caribeña de los Países Bajos (las islas de Bonaire, San Eustaquio y Saba).

3. El presente Acuerdo podrá enmendarse en cualquier momento por mutuo consentimiento de las Partes. Cada Parte podrá proponer enmiendas al presente Acuerdo en cualquier momento por conducto diplomático, las cuales entrarán en vigor según las condiciones establecidas en el apartado 1 del presente artículo, a excepción de las enmiendas al Anexo 1, que entrarán en vigor en la fecha acordada entre las Partes.

4. Una Parte podrá dar por terminado el presente Acuerdo por escrito por conducto diplomático en cualquier momento; en este caso, el Acuerdo expirará seis meses después de la recepción de dicha notificación.

5. Independientemente de la terminación del presente Acuerdo, toda la Información Clasificada cedida o generada en virtud del mismo deberá protegerse de conformidad con él mientras siga estando clasificada.

EN FE de lo cual, los representantes debidamente autorizados de las Partes firman el presente Acuerdo.

HECHO en Madrid el 23 de septiembre 2021 en dos ejemplares originales, en neerlandés, español e inglés, siendo todos los textos igualmente auténticos. En caso de discrepancias en la interpretación, prevalecerá el texto inglés.

*Por el Reino de los Países Bajos,*

JAN TH. VERSTEEG

*Por el Reino de España,*

PAZ ESTEBAN LÓPEZ

---

**Anexo 1**

La Autoridad de Seguridad Competente para el Reino de España es:

Secretario de Estado
Director del Centro Nacional de Inteligencia
Oficina Nacional de Seguridad

La Autoridad de Seguridad Competente para el Reino de los Países Bajos es:
Autoridad Nacional de Seguridad (ANS)
Servicio de Inteligencia y Seguridad General
Ministerio del Interior y de Relaciones del Reino

---

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 17, eerste lid, in werking treden op de eerste dag van de tweede maand die volgt op de ontvangst van de laatste kennisgeving waarbij partijen elkaar langs diplomatieke weg ervan in kennis hebben gesteld dat de nationale procedures die nodig zijn voor de inwerkingtreding van het Verdrag zijn voltooid.

Uitgegeven de *vijfde* oktober 2021.

*De Minister van Buitenlandse Zaken,*

H.P.M. KNAPEN

trb-2021-123
ISSN 0920 - 2218
's-Gravenhage 2021