6 (2026) Nr. 1

# TRACTATENBLAD

VAN HET

KONINKRIJK DER NEDERLANDEN

**JAARGANG 2026 Nr. 47**

A. TITEL

*Verdrag tussen het Koninkrijk der Nederlanden en het Groothertogdom Luxemburg inzake de uitwisseling en wederzijdse beveiliging van gerubriceerde gegevens (met Bijlage); Luxemburg, 21 april 2026*

**Voor een overzicht van de verdragsgegevens, zie verdragsnummer 012023 in de Verdragenbank.**

B. TEKST

## Agreement between the Kingdom of the Netherlands and the Grand Duchy of Luxembourg concerning the exchange and mutual protection of classified information

The Kingdom of the Netherlands

and

the Grand Duchy of Luxembourg,

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

Desiring to establish a system regulating the mutual protection of Classified Information generated or exchanged in the course of the cooperation between the Parties or between public and private entities under their jurisdiction,

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

### Article 1

*Purpose and scope*

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

2. The Parties shall take all appropriate measures under their national laws and regulations to ensure the protection of Classified Information in accordance with this Agreement.

3. This Agreement shall apply to any activities, contracts or agreements involving Classified Information that will be conducted or concluded between the Parties following the entering into force of this Agreement.

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

### Article 2

*Definitions*

For the purpose of this Agreement, the following definitions mean:

a) **"Agreement"** means this document including its Annex.
b) **"Classified Contract"** means any legally enforceable agreement to provide goods or services to be entered into by one of the Parties or a Contractor under its jurisdiction with a Contractor under the jurisdiction of the other Party, which contains Classified Information or the performance of which requires access to Classified Information. This term includes a sub-contract or any pre-contractual activity.
c) **"Classified Information"** means any information, material or object, regardless of its form or nature, or any parts thereof, marked with a security classification by one of the Parties, the unauthorised disclosure, alteration, compromise or loss of which could cause varying degrees of damage or harm to the interests of one or both of the Parties.
d) **"Competent Security Authority"** means the government authority in a Party, or any delegated competent security authority in a military domain, responsible for supervising the implementation of this Agreement in accordance with the national laws and regulations.
e) **"Contractor"** means any individual other than those engaged by a Party under a contract of employment or any legal entity under the jurisdiction of a Party, entering into or bound by a Classified Contract, including a Sub-contractor.
f) **"Facility Security Clearance"** means a positive determination, confirmed 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 its national laws and regulations.
g) **"Need to Know"** means the requirement for an individual or legal entity to access, have knowledge of or possess Classified Information in order to be able to perform their official tasks or services.
h) **"Originating Party"** means the Party under whose authority Classified Information has been created.
i) **"Personnel Security Clearance"** means a positive determination, confirmed 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.
j) **"Providing Entity"** means the Party or Contractor, under its jurisdiction, which releases Classified Information to the Receiving Entity under this Agreement.
k) **"Receiving Entity"** means the Party or Contractor under its jurisdiction, which receives Classified Information from the Providing Entity under this Agreement.
l) **"Security Classification Guide"** means a document associated with a Classified Contract specifying the applicable security classification levels of each part of that Classified Contract.
m) **"Security Incident"** means any unauthorised disclosure, alteration, compromise, loss, access, handling, storage or destruction of Classified Information, contrary to national laws and regulations of the Receiving Entity or this Agreement.
n) **"Sub-contractor**" means a Contractor to whom a prime Contractor grants a sub-contract.
o) **"Third Party"** means any State, including any public or private entity under its jurisdiction, or any international organisation, which is not a Party to this Agreement.

Article 3

*Competent Security Authorities*

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

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

Article 4

*Security classification levels*

1. The Parties undertake to protect Classified Information exchanged between them and agree that the following security classification levels shall be equivalent. The informal translation in English of the Parties' respective security classification levels, is not part of the national laws and regulations of the Parties and shall not be used to mark Classified Information.

| For the Kingdom of the Netherlands | For the Grand Duchy of Luxembourg | In the English language |
|---|---|---|
| Stg. ZEER GEHEIM | TRES SECRET LUX | TOP SECRET |
| Stg. GEHEIM | SECRET LUX | SECRET |
| Stg. CONFIDENTIEEL | CONFIDENTIEL LUX | CONFIDENTIAL |
| DEPARTEMENTAAL VERTROUWELIJK | RESTREINT LUX | RESTRICTED |

Article 5

*Security measures*

1. In accordance with their national laws and regulations, the Parties shall ensure the implementation of appropriate measures to protect Classified Information, which is generated or exchanged under this Agreement. Each Party shall afford to such Classified Information at least the same level of protection as afforded to their own Classified Information of the equivalent security classification levels as set forth in Article 4 of this Agreement.

2. When such Classified Information is processed, stored or transmitted via communication and information systems, these measures shall guarantee the confidentiality, integrity, availability, non-repudiation, authenticity and traceability of access to Classified Information. The Parties shall ensure that such Classified Information is stored and handled in accordance with their national laws and regulations.

3. Any Classified Information released under this Agreement shall be marked with the appropriate security classification level in accordance with the national laws and regulations of the Originating Party.

4. The Receiving Entity shall apply its own security classification to all Classified Information received from the Providing Entity under this Agreement, at the equivalent security classification level in accordance with the scheme contained in article 4, in such a way that it is always clear who the Originating Party is.

5. Where the form or nature of the Classified Information does not allow such marking by the Receiving Entity to apply its own corresponding security classification level, the Competent Security Authorities shall decide whether the marking by the Originating Party suffices.

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

7. The Originating Party shall ensure that the Receiving Entity will be informed of any change in the security classification level of the Classified Information provided, in order to apply the appropriate protection measures.

8. The Originating Party may add handling requirements, in English, on the Classified Information, to specify any limitations on its use, disclosure, release and access by the Receiving Entity.

9. The Parties shall take all appropriate measures to ensure that the Receiving Entity:
a) ensures that Classified Information is not disclosed or released to a Third Party without the prior written consent of the Originating Party;
b) uses Classified Information solely for the purpose it has been released for and within the limitations stated by the Originating Party.

Article 6

*Access to Classified Information*

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

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

Article 7

*Classified contracts*

1. Upon request of the Originating Party, the Competent Security Authority of the Receiving Entity shall inform the Competent Security Authority of the Originating Party whether a Contractor, under its jurisdiction and participating in a Classified Contract or precontractual negotiations regarding a Classified Contract and requiring access to Classified Information, has been issued a Facility Security Clearance at the required secur-

ity classification level. If the Contractor does not, at that point, hold a Facility Security Clearance, or the Facility Security Clearance is at a lower level than that required, the requesting Competent Security Authority shall be informed thereof.

2. If a Party or a Contractor under its jurisdiction proposes to award a Classified Contract involving access to Classified Information marked as CONFIDENTIEL LUX/Stg. CONFIDENTIEEL or above, to a Contractor under the jurisdiction of the other Party, it shall first obtain written confirmation from the Competent Security Authority of the other Party that the Contractor has been granted a Facility Security Clearance at the appropriate security classification level. For Classified Contracts at the security classification level equivalent to RESTREINT LUX/DEPARTEMENTAAL VERTROUWELIJK, a Facility Security Clearance may be required, in accordance with national laws and regulations of the Party under whose jurisdiction the Contractor operates.

3. The Competent Security Authority of the Party having jurisdiction over the Contractor 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 their national laws and regulations as well as with this Agreement;
b) monitors the security conduct within its facilities;
c) notifies promptly its Competent Security Authority of any Security Incident relating to the Classified Contract.

4. In addition to the requirements in paragraph 3 of this article, for Classified Contracts involving access to Classified Information marked as CONFIDENTIEL LUX/Stg. CONFIDENTIEEL or above, the Competent Security Authority shall ensure that the Contractor holds a Facility Security Clearance at the corresponding security classification level in order to protect the Classified Information and that the individuals requiring access to Classified Information hold a Personnel Security Clearance at the corresponding security classification level.

5. Every Classified Contract shall include security requirements which identify the following aspects:
a) a Security Classification Guide;
b) a procedure for notification of changes in the security classification level, taking into account article 5, paragraph 7 of this Agreement;
c) the channels and procedures to be used for the transport and/or transmission of Classified Information;
d) instructions for the handling, storage, destruction and returning of Classified Information;
e) contact details of the Competent Security Authorities responsible for overseeing the protection of Classified Information related to the Classified Contract;
f) the obligation to notify any Security Incidents to the Competent Security Authority of the Contractor and the obligation for Contractors to take all reasonable steps to assist in mitigating the effect of such a security violation, in consultation with the Competent Security Authority;
g) in case a Classified Contract is sub-contracted, in whole or in part, to a sub-Contractor, the obligation to impose all the stipulations concerning Contractors in this Agreement to the sub-Contractor;
h) a reference to this Agreement;
i) a statement that Classified Information exchanged or generated pursuant to the Classified Contract shall be protected by the Contractor in accordance with the applicable national laws and regulations as well as with this Agreement.

6. If a Classified Contract is awarded, the Party or a Contractor under its jurisdiction shall, via its Competent Security Authority, forward a copy of the security requirements referred to in paragraph 5 of this Article to the Competent Security Authority of the Receiving Entity, to facilitate the security oversight of the Classified Contract.

7. 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 8 of this Agreement.

Article 8

*Visits*

1. Visits requiring access to Classified Information marked as CONFIDENTIEL LUX/Stg. CONFIDENTIEEL or above are subject to the prior written consent of the Competent Security Authority of the host Party, unless otherwise agreed between the Competent Security Authorities. Such consent shall be given only to individuals referred to in article 6 of this Agreement. With respect to visits requiring access to Classified Information marked as RESTREINT LUX/DEPARTEMENTAAL VERTROUWELIJK, the prior written consent of the Competent Security Authority of the host Party may be required, in accordance with the national laws and regulations of the Party under whose jurisdiction the visit occurs.

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

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

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

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

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

Article 9

*Transfer of classified information*

1. Classified Information marked as CONFIDENTIEL LUX/Stg. CONFIDENTIEEL or above shall be transferred by means of diplomatic, government or military couriers, or by any other means agreed upon in advance by the Competent Security Authorities, in accordance with their national laws and regulations.

2. Classified Information marked as RESTREINT LUX/DEPARTEMENTAAL VERTROUWELIJK may be transferred by postal services in accordance with the national laws and regulations.

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

4. Classified Information marked as CONFIDENTIEL LUX/Stg. CONFIDENTIEEL or above shall be registered.

Article 10

*Reproduction and translation of classified information*

1. Classified Information marked as TRES SECRET LUX/Stg. ZEER GEHEIM, both the original and the translation, shall not be reproduced or translated without the prior written consent of the Originating Party.

2. Reproductions and translations of Classified Information shall be marked with the original markings and protected in the same way as the original Classified Information.

3. Reproductions and translations shall be limited to the minimum amount required for use under this Agreement.

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

Article 11

*Destruction of classified information*

1. Classified Information marked as TRES SECRET LUX/Stg. ZEER GEHEIM shall be destroyed only with the prior written consent of the Originating Party. By default, it shall be returned to the Originating Party after it is no longer considered necessary by the Receiving Entity.

2. Classified Information marked as SECRET LUX/Stg. GEHEIM or below, shall be destroyed after it is no longer considered necessary by the Receiving Entity, insofar as to prevent its reconstruction in whole or in part.

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

Article 12

*Security cooperation*

1. The Competent Security Authorities shall, on request, inform each other about changes in their national laws and regulations, policies and practices for the protection of 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 an individual has been issued a Personnel Security Clearance or a legal entity has been issued a Facility Security Clearance.

3. Within the scope of this Agreement, each Party shall recognize the Personnel Security Clearances and Facility Security Clearances issued by the other Party.

4. The Competent Security Authorities shall assist each other in carrying out Personnel Security Clearance and Facility Security Clearance investigations on request and in accordance with their national laws and regulations.

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

6. Within the scope of this Agreement and notwithstanding Article 9, each Party shall recognise a formal act of approval issued by the other Party referring to equipment and mechanisms related to and including communication and information systems which are used to process the other Party's Classified Information. When necessary, the updated list of approved equipment and mechanisms shall be exchanged between the Competent Security Authorities.

7. The cooperation under this Agreement is conducted in English.

Article 13

*Security Incident*

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

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

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

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

Article 14

*Costs*

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

Article 15

*Dispute resolution*

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

Article 16

*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 the exchange and mutual protection of Classified Information.

Article 17

*Implementing arrangements*

The Competent Security Authorities of the Parties or any other competent security authorities of the Parties may consult each other on detailed technical aspects relating to the application of this Agreement and may conclude, on a case-by-case basis, appropriate implementing arrangements pursuant to this Agreement.

Article 18

*Final provisions*

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

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

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

4. This Agreement including its Annex may be amended 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 2 of this article, with the exception of an amendment of the Competent Security Authorities listed in the Annex, which amendment shall enter into force on a date to be agreed upon by the Parties.

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

6. In case of termination of this Agreement, all Classified Information exchanged, released or generated under this Agreement shall remain protected in accordance with the terms of this Agreement before it was terminated, for as long as the Classified Information remains classified.

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

DONE in Luxembourg on the 21st day of April 2026, in two original copies, in Dutch, French and English languages, the three texts being equally authentic.

In case of divergence of interpretation, the English text shall prevail.

*For the Kingdom of the Netherlands,*

T.B.W. BERENDSEN

*For the Grand Duchy of Luxembourg,*

X. BETTEL

**Annex**

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

Civil National Security Authority
General Intelligence and Security Service
Ministry of the Interior and Kingdom Relations

The delegated competent security authority:
Military National Security Authority
Defence Security Authority
Directorate-General of Policy
Ministry of Defence.

The Competent Security Authority for the Grand Duchy of Luxembourg is:
Ministère d'Etat
Service de renseignement de l'Etat
Autorité nationale de sécurité.

---

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

Het Koninkrijk der Nederlanden

en

het Groothertogdom Luxemburg,

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

Geleid door de wens een systeem vast te stellen voor het regelen van de wederzijdse beveiliging van gerubriceerde gegevens die zijn gegenereerd of uitgewisseld in het kader van de samenwerking tussen de partijen of tussen publieke of private entiteiten onder hun rechtsmacht,

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

Artikel 1

*Doel en reikwijdte*

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

2. 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.

3. Dit Verdrag is van toepassing op alle activiteiten, contracten of overeenkomsten waarbij gerubriceerde gegevens betrokken zijn die na de inwerkingtreding van dit Verdrag tussen de partijen worden uitgevoerd of gesloten.

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

Artikel 2

*Begripsomschrijvingen*

Voor de toepassing van dit Verdrag wordt verstaan onder:
a. **„Verdrag"**, dit document met inbegrip van de Bijlage daarbij.
b. **„Gerubriceerd contract"**, elke wettelijk afdwingbare overeenkomst voor het leveren van goederen of diensten die een van de partijen of een opdrachtnemer onder haar rechtsmacht aangaat met een opdrachtnemer onder de rechtsmacht van de andere partij, die gerubriceerde gegevens bevat of waarbij

voor de uitvoering toegang vereist is tot gerubriceerde gegevens. Dit begrip omvat een onderaannemingscontract of eventuele voorafgaande contractactiviteiten.

c. **„Gerubriceerde gegevens"**, gegevens, materiaal of voorwerpen, ongeacht de vorm of aard daarvan, of delen daarvan die of dat door een van de partijen is voorzien van een rubriceringsniveau, waarvan de ongeoorloofde bekendmaking, verandering, compromittering of het verlies de belangen van een of beide partijen in meer of mindere mate zou kunnen schaden.

d. **„Bevoegde beveiligingsautoriteit"**, de overheidsautoriteit in een partij, of een gemachtigde bevoegde beveiligingsautoriteit voor het militaire domein, die verantwoordelijk is voor toezicht op de implementatie van dit Verdrag in overeenstemming met de nationale wet- en regelgeving.

e. **„Opdrachtnemer",** elke persoon, anders dan degenen die door een partij in dienst zijn genomen op grond van een arbeidsovereenkomst of een rechtspersoon onder de rechtsmacht van een partij, die een gerubriceerd contract aangaat of er door gebonden is, met inbegrip van een onderaannemer.

f. **„Veiligheidsmachtiging bedrijfslocatie"**, de vaststelling, bevestigd door de bevoegde beveiligingsautoriteit, dat een bedrijfslocatie passende beveiligingsmaatregelen heeft genomen voor de toegang tot en omgang met gerubriceerde gegevens, tot en met een gespecificeerd rubriceringsniveau, in overeenstemming met de nationale wet- en regelgeving.

g. **„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 hun officiële taken of diensten.

h. **„Partij van herkomst"**, de partij onder wier gezag gerubriceerde gegevens zijn gecreëerd.

i. **„Veiligheidsmachtiging personeel"**, de vaststelling, bevestigd door de bevoegde beveiligingsautoriteit, dat een natuurlijke persoon toestemming heeft gekregen voor de toegang tot en omgang met gerubriceerde gegevens tot en met een gespecificeerd rubriceringsniveau, in overeenstemming met de nationale wet- en regelgeving.

j. **„Verstrekkende entiteit"**, de partij of opdrachtnemer onder haar rechtsmacht die de gerubriceerde gegevens uit hoofde van dit Verdrag vrijgeeft aan de ontvangende entiteit.

k. **„Ontvangende entiteit"**, de partij of opdrachtnemer onder haar rechtsmacht die de gerubriceerde gegevens uit hoofde van dit Verdrag ontvangt van de verstrekkende entiteit.

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

m. **„Beveiligingsincident"**, elk(e) ongeoorloofd(e) bekendmaking, verandering, compromittering, verlies, toegang, omgang, opslag of vernietiging van gerubriceerde gegevens in strijd met de nationale wet- en regelgeving van de ontvangende entiteit of dit Verdrag.

n. **„Onderaannemer"**, een opdrachtnemer aan wie een hoofdopdrachtnemer een onderaannemingsovereenkomst verleent.

o. **„Derde"** elke staat, met inbegrip van elke publieke of private entiteit onder zijn rechtsmacht, of elke internationale organisatie die geen partij is bij dit Verdrag.

Artikel 3

*Bevoegde beveiligingsautoriteiten*

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

2. De bevoegde beveiligingsautoriteiten voorzien elkaar van de officiële contactgegevens en veranderingen daarvan.

Artikel 4

*Rubriceringsniveaus*

1. De partijen verbinden zich ertoe de gerubriceerde gegevens die tussen hen worden uitgewisseld te beveiligen en komen overeen dat de volgende rubriceringsniveaus met elkaar overeenkomen. De niet-officiële vertaling in het Engels van de respectieve rubriceringsniveaus van de partijen, maakt geen deel uit van de nationale wet- en regelgeving van de partijen en dient niet gebruikt te worden om gerubriceerde gegevens aan te duiden.

| **Voor het Koninkrijk der Nederlanden** | **Voor het Groothertogdom Luxemburg** | **In de Engelse taal** |
|---|---|---|
| Stg. ZEER GEHEIM | TRES SECRET LUX | TOP SECRET |
| Stg. GEHEIM | SECRET LUX | SECRET |
| Stg. CONFIDENTIEEL | CONFIDENTIEL LUX | CONFIDENTIAL |
| DEPARTEMENTAAL VERTROUWELIJK | RESTREINT LUX | RESTRICTED |

Artikel 5

*Beveiligingsmaatregelen*

1. In overeenstemming met hun nationale wet- en regelgeving waarborgen de partijen de implementatie van passende maatregelen om gerubriceerde gegevens die uit hoofde van dit Verdrag worden gegenereerd of uitgewisseld, te beveiligen. Elke partij kent aan deze gerubriceerde gegevens ten minste dezelfde beveiliging toe als aan haar eigen gerubriceerde gegevens met een vergelijkbaar rubriceringsniveau zoals vervat in artikel 4 van dit Verdrag.

2. Wanneer dergelijke gerubriceerde gegevens worden verwerkt, opgeslagen of overgebracht door communicatie- en informatiesystemen, waarborgen deze maatregelen de vertrouwelijkheid, integriteit, beschikbaarheid, onweerlegbaarheid, authenticiteit en traceerbaarheid van de toegang tot gerubriceerde gegevens. De partijen waarborgen dat deze gerubriceerde gegevens worden opgeslagen en behandeld in overeenstemming met hun nationale wet- en regelgeving.

3. Alle gerubriceerde gegevens die uit hoofde van dit Verdrag worden vrijgegeven worden voorzien van het juiste rubriceringsniveau in overeenstemming met de nationale wet- en regelgeving van de partij van herkomst.

4. De ontvangende entiteit past zijn eigen rubriceringsniveau toe op alle gerubriceerde gegevens die uit hoofde van dit Verdrag van de verstrekkende entiteit zijn ontvangen, op het vergelijkbare rubriceringsniveau in overeenstemming met de tabel vervat in artikel 4, zodanig dat het altijd duidelijk is wie de partij van herkomst is.

5. Wanneer de vorm of de aard van de gerubriceerde gegevens het de ontvangende entiteit niet mogelijk maakt een dergelijke markering toe te passen op haar eigen overeenkomstige rubriceringsniveau, beslissen de bevoegde beveiligingsautoriteiten of de markering door de partij van oorsprong volstaat.

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

7. De partij van herkomst waarborgt dat de ontvangende entiteit op de hoogte wordt gebracht van elke verandering van het rubriceringsniveau van de verstrekte gerubriceerde gegevens, teneinde de relevante beveiligingsmaatregelen toe te passen.

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

9. De partijen nemen alle passende maatregelen om te waarborgen dat de ontvangende entiteit:
a. waarborgt dat gerubriceerde gegevens niet bekend worden gemaakt of vrijgegeven aan een derde zonder de voorafgaande schriftelijke toestemming van de partij van herkomst;
b. de gerubriceerde gegevens uitsluitend gebruikt voor het doel waarvoor zij zijn vrijgegeven en binnen de door de partij van herkomst gestelde beperkingen.

Artikel 6

*Toegang tot gerubriceerde gegevens*

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

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

Artikel 7

*Gerubriceerde contracten*

1. Op verzoek van de partij van herkomst deelt de bevoegde beveiligingsautoriteit van de ontvangende entiteit aan de bevoegde beveiligingsautoriteit van de partij van herkomst mee of een opdrachtnemer die onder haar rechtsmacht valt en deelneemt aan een gerubriceerd contract of precontractuele onderhandelingen inzake een gerubriceerd contract en waarvoor toegang tot gerubriceerde gegevens vereist is, een veiligheidsmachtiging bedrijfslocatie heeft gekregen op het vereiste rubriceringsniveau. Indien de opdrachtnemer niet, op dat moment, over een veiligheidsmachtiging bedrijfslocatie beschikt, of de veiligheidsmachtiging bedrijfslocatie van een lager niveau is dan vereist, wordt de verzoekende bevoegde beveiligingsautoriteit daarvan op de hoogte gesteld.

2. Indien een partij of een opdrachtnemer onder haar rechtsmacht voorstelt een gerubriceerd contract waarvoor toegang tot gerubriceerde gegevens vereist is op het niveau CONFIDENTIEL LUX/Stg. CONFIDENTIEEL of hoger te gunnen aan een opdrachtnemer onder de rechtsmacht van de andere partij, dient zij eerst de schriftelijke bevestiging te verkrijgen van de bevoegde beveiligingsautoriteit van de andere partij dat aan deze opdrachtnemer een veiligheidsmachtiging bedrijfslocatie is toegekend met het vereiste rubriceringsniveau. Voor gerubriceerde contracten met het rubriceringsniveau dat overeenkomt met RESTREINT LUX/ DEPARTEMENTAAL VERTROUWELIJK kan een veiligheidsmachtiging bedrijfslocatie vereist zijn indien dit verplicht wordt gesteld in de nationale wet- en regelgeving van de partij onder wier rechtsmacht de opdrachtnemer zijn activiteiten uitvoert.

3. De bevoegde beveiligingsautoriteit van de partij onder wier rechtsmacht de opdrachtnemer valt, 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 hun nationale wet- en regelgeving en met dit Verdrag;
b. de beveiligingsuitvoering op zijn locaties in het oog houdt;
c. zijn bevoegde beveiligingsautoriteit onverwijld in kennis stelt van elk beveiligingsincident dat betrekking heeft op het gerubriceerd contract.

4. In aanvulling op de vereisten van het derde lid van dit artikel, met betrekking tot gerubriceerde contracten waarbij toegang vereist is tot gerubriceerde gegevens op het niveau CONFIDENTIEL LUX/Stg. CONFIDENTIEEL of hoger, waarborgt de bevoegde beveiligingsautoriteit dat de opdrachtnemer een veiligheidsmachtiging bedrijfslocatie bezit met het vergelijkbaar rubriceringsniveau teneinde de gerubriceerde gegevens te beveiligen en dat de natuurlijke personen die toegang dienen te krijgen tot gerubriceerde gegevens, een veiligheidsmachtiging personeel met het vergelijkbaar rubriceringsniveau hebben.

5. Elk gerubriceerd contract dient beveiligingsvereisten te bevatten waarin de volgende aspecten vermeld staan:
a. een rubriceringsgids;
b. een procedure voor het melden van wijzigingen van het rubriceringsniveau, rekening houdend met artikel 5, zevende 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, opslag, vernietiging en retourneren van gerubriceerde gegevens;
e. contactgegevens van de bevoegde beveiligingsautoriteiten die verantwoordelijk zijn voor het toezicht op de beveiliging van gerubriceerde gegevens die betrekking hebben op het gerubriceerde contract;
f. de verplichting om de bevoegde beveiligingsautoriteit van de opdrachtnemer in kennis te stellen van elk beveiligingsincident en de verplichting voor opdrachtnemers om alle redelijke stappen te nemen om de gevolgen van een dergelijke beveiligingsinbreuk te beperken in samenspraak met de bevoegde beveiligingsautoriteit;
g. wanneer een gerubriceerd contract geheel of gedeeltelijk wordt onderuitbesteed, de verplichting om alle bepalingen betreffende opdrachtnemers in dit Verdrag op te leggen aan de onderaannemer;
h. een verwijzing naar dit Verdrag;
i. een verklaring dat gerubriceerde gegevens die in het kader van het gerubriceerde contract worden uitgewisseld of gegenereerd, door de opdrachtnemer worden beschermd in overeenstemming met de van toepassing zijnde nationale wet- en regelgeving en dit Verdrag.

6. Indien een gerubriceerd contract wordt toegekend, zal de partij of een opdrachtnemer onder haar rechtsmacht, via haar bevoegde beveiligingsautoriteit een kopie sturen van de beveiligingsvereisten zoals bedoeld in het vijfde lid van dit artikel, naar de bevoegde beveiligingsautoriteit van de ontvangende entiteit, om het beveiligingstoezicht op het gerubriceerde contract te vergemakkelijken.

7. 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 8 van dit Verdrag te zijn.

Artikel 8

*Bezoeken*

1. Bezoeken waarbij toegang tot gerubriceerde gegevens op het niveau CONFIDENTIEL LUX/Stg. CONFIDENTIEEL of hoger vereist is, dienen vooraf schriftelijk te worden goedgekeurd door de bevoegde beveiligingsautoriteit van de als gastheer optredende partij, tenzij anderszins overeengekomen door de bevoegde beveiligingsautoriteiten. Dergelijke goedkeuring wordt uitsluitend gegeven aan natuurlijke personen zoals bedoeld in artikel 6 van dit Verdrag. Met betrekking tot bezoeken die toegang vereisen tot gerubriceerde gegevens op het niveau RESTREINT LUX/DEPARTEMENTAAL VERTROUWELIJK, kan de voorafgaande schriftelijke toestemming van de bevoegde beveiligingsautoriteit van de ontvangende partij vereist zijn, in overeenstemming met de nationale wet- en regelgeving van de partij onder wier rechtsmacht het bezoek plaatsvindt.

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

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

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

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

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

Artikel 9

*Overbrenging van gerubriceerde gegevens*

1. Gerubriceerde gegevens op het niveau CONFIDENTIEL LUX/Stg. CONFIDENTIEEL of hoger worden overgebracht door middel van diplomatieke, regerings- of militaire koeriers, of op enige andere wijze die vooraf door de bevoegde beveiligingsautoriteiten is overeengekomen, in overeenstemming met hun nationale wet- en regelgeving.

2. Gerubriceerde gegevens op het niveau RESTREINT LUX/DEPARTEMENTAAL VERTROUWELIJK kunnen worden overgedragen door postdiensten in overeenstemming met de nationale wet- en regelgeving.

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

4. Gerubriceerde gegevens op het niveau CONFIDENTIEL LUX/Stg. CONFIDENTIEEL of hoger worden geregistreerd.

Artikel 10

*Reproductie en vertaling van gerubriceerde gegevens*

1. Gerubriceerde gegevens op het niveau TRES SECRET LUX/Stg. ZEER GEHEIM, zowel het origineel als de vertaling, worden niet gereproduceerd of vertaald zonder de voorafgaande schriftelijke toestemming van de partij van herkomst.

2. Reproducties en vertalingen van gerubriceerde gegevens worden voorzien van de oorspronkelijke rubriceringsmarkeringen en krijgen dezelfde beveiliging als de oorspronkelijke gerubriceerde gegevens.

3. Reproducties en vertalingen worden beperkt tot het minimumaantal dat nodig is voor gebruik uit hoofde van dit Verdrag.

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

Artikel 11

*Vernietiging van gerubriceerde gegevens*

1. Gerubriceerde gegevens op het niveau TRES SECRET LUX/Stg. ZEER GEHEIM worden alleen vernietigd met voorafgaande schriftelijke toestemming van de partij van herkomst. Zij worden standaard geretourneerd aan de partij van herkomst nadat de ontvangende entiteit ze niet meer nodig acht.

2. Gerubriceerde gegevens op het niveau SECRET LUX/Stg. GEHEIM of lager worden vernietigd nadat zij door de ontvangende partij als niet langer nodig worden geacht zodat zij niet geheel of gedeeltelijk kunnen worden gereconstrueerd.

3. Indien een crisissituatie het een 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 partij stelt, via haar bevoegde beveiligingsautoriteit, de bevoegde beveiligingsautoriteit van de verstrekkende partij zo spoedig mogelijk schriftelijk in kennis van de vernietiging van deze gerubriceerde gegevens.

Artikel 12

*Beveiligingssamenwerking*

1. De bevoegde beveiligingsautoriteiten stellen elkaar, op verzoek, in kennis van veranderingen in hun nationale wet- en regelgeving, beleid en praktijken met betrekking tot de beveiliging van gerubriceerde gegevens.

2. Op verzoek van de bevoegde beveiligingsautoriteit van de ene partij bevestigt de bevoegde beveiligingsautoriteit van de andere partij schriftelijk dat er een geldige veiligheidsmachtiging personeel is afgegeven aan een natuurlijke persoon of een veiligheidsmachtiging bedrijfslocatie is afgegeven aan een rechtspersoon.

3. Binnen de reikwijdte van dit Verdrag erkent elke partij de veiligheidsmachtigingen personeel en veiligheidsmachtigingen bedrijfslocatie die door de andere partij zijn afgegeven.

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

5. De bevoegde beveiligingsautoriteiten stellen elkaar onverwijld schriftelijk in kennis van veranderingen in erkende veiligheidsmachtigingen personeel of veiligheidsmachtigingen bedrijfslocatie waarvoor een bevestiging is verstrekt.

6. Binnen de reikwijdte van dit Verdrag en niettegenstaande artikel 9, erkent elke partij een door de andere partij afgegeven formele goedkeuringshandeling die betrekking heeft op apparatuur en mechanismen in verband met en met inbegrip van communicatie- en informatiesystemen die worden gebruikt om de gerubriceerde gegevens van de andere partij te verwerken. Indien nodig wordt de bijgewerkte lijst van goedgekeurde apparatuur en mechanismen uitgewisseld tussen de bevoegde beveiligingsautoriteiten.

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

Artikel 13

*Beveiligingsincident*

1. Indien een beveiligingsincident met betrekking tot de gerubriceerde gegevens van de partij van herkomst wordt vermoed of vastgesteld door de ontvangende entiteit, stelt zij haar bevoegde beveiligingsautoriteit daarvan zo spoedig mogelijk schriftelijk in kennis. De kennisgeving dient voldoende gedetailleerde informatie te bevatten om de partij van herkomst in staat te stellen de consequenties en omstandigheden van de vermoede of vastgestelde inbreuk te beoordelen.

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

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

4. De bevoegde beveiligingsautoriteit van de ontvangende entiteit neemt passende maatregelen in overeenstemming met haar nationale wet- en regelgeving om de gevolgen van het beveiligingsincident te beperken en om herhaling ervan te voorkomen. De bevoegde beveiligingsautoriteit van de partij van herkomst wordt in kennis gesteld van de uitkomsten van het onderzoek en de eventuele getroffen maatregelen.

Artikel 14

*Kosten*

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

Artikel 15

*Oplossing van geschillen*

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

Artikel 16

*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 de uitwisseling en wederzijdse beveiliging van gerubriceerde gegevens.

Artikel 17

*Uitvoeringsregelingen*

De bevoegde beveiligingsautoriteiten van de partijen of andere bevoegde autoriteiten op het gebied van beveiliging van de partijen kunnen elkaar raadplegen over gedetailleerde technische aspecten in verband met de toepassing van dit Verdrag en kunnen per geval passende uitvoeringsregelingen uit hoofde van dit Verdrag sluiten.

Artikel 18

*Slotbepalingen*

1. Dit Verdrag wordt gesloten voor onbepaalde tijd.

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

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

4. Dit Verdrag, met inbegrip van de Bijlage daarbij, kan met wederzijdse instemming van de partijen worden gewijzigd. Elke partij kan op elk moment langs diplomatieke weg wijzigingen van dit Verdrag voorstellen. Dergelijke wijzigingen treden in werking onder de voorwaarden vervat in het tweede lid van dit artikel, met uitzondering van een wijziging van de bevoegde beveiligingsautoriteiten die staan vermeld in de Bijlage, welke wijziging in werking treedt op een door de partijen overeen te komen datum.

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

6. In geval van beëindiging van dit Verdrag blijven alle uit hoofde van dit Verdrag uitgewisselde, vrijgegeven of gegenereerde gerubriceerde gegevens beveiligd in overeenstemming met de bepalingen van dit Verdrag voor de beëindiging ervan, zolang deze gerubriceerde gegevens gerubriceerd blijven.

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

GEDAAN te Luxemburg op 21 april 2026, in twee oorspronkelijke exemplaren, in de Nederlandse, de Franse en de Engelse taal, waarbij de drie teksten gelijkelijk authentiek zijn.

In geval van verschil in interpretatie is de Engelse tekst doorslaggevend.

*Voor het Koninkrijk der Nederlanden,*

T.B.W. BERENDSEN

*Voor het Groothertogdom Luxemburg,*

X. BETTEL

---

**Bijlage**

De bevoegde beveiligingsautoriteit van het Koninkrijk der Nederlanden is:

De civiele Nationale Beveiligingsautoriteit:
De Algemene Inlichtingen- en Veiligheidsdienst (AIVD)
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

De gemachtigde bevoegde beveiligingsautoriteit:
De militaire Nationale Beveiligingsautoriteit
De Beveiligingsautoriteit
Directoraat-Generaal Beleid
Ministerie van Defensie.

De bevoegde beveiligingsautoriteit van het Groothertogdom Luxemburg is:
Ministère d'Etat
Service de renseignement de l'Etat
Autorité nationale de sécurité.

---

**Accord entre le Royaume des Pays-Bas et le Grand-Duché de Luxembourg relatif à l'échange et la protection mutuelle des informations classifiées**

Le Royaume des Pays-Bas

et

le Grand-Duché de Luxembourg,

Ci-après dénommés conjointement les « Parties » et individuellement une « Partie »,

Désirant mettre en place un système régissant la protection des Informations classifiées produites ou échangées dans le cadre de la coopération entre les Parties ou entre des entités publiques et privées relevant de leur juridiction,

Souhaitant assurer la protection mutuelle des Informations classifiées, ont convenu, dans l'intérêt de la sécurité nationale, de ce qui suit :

Article 1er

*Objet et champ d'application*

1. Le présent Accord a pour objet d'assurer la protection des Informations classifiées échangées entre les Parties, entre une Partie et un Contractant relevant de la juridiction de l'autre Partie ou entre des Contractants relevant des juridictions respectives des Parties, ou produites dans le cadre du présent Accord. Le présent Accord définit les procédures et les mesures de sécurité permettant d'assurer cette protection.

2. Les Parties s'engagent à prendre toutes les mesures appropriées dans le respect de leurs lois et réglementations nationales afin de garantir la protection des Informations classifiées conformément au présent Accord.

3. Le présent Accord s'applique à l'ensemble des activités, contrats ou accords impliquant des Informations classifiées, qui seront menés ou conclus entre les Parties après l'entrée en vigueur du présent Accord.

4. Le présent Accord ne constitue pas un fondement permettant de contraindre les Parties à fournir ou à échanger des Informations classifiées.

Article 2

*Définitions*

Aux fins du présent Accord, les définitions suivantes s'appliquent :
a) **« Accord »** désigne le présent document, y compris son annexe.
b) **« Contrat classifié »** désigne tout accord juridiquement contraignant visant à fournir des biens ou des services, conclu par l'une des Parties ou un Contractant relevant de sa juridiction avec un Contractant relevant de la juridiction de l'autre Partie, qui contient des Informations classifiées ou dont l'exécution nécessite l'accès à des Informations classifiées. Ce terme comprend tout contrat de sous-traitance ou toute activité précontractuelle.
c) **« Informations classifiées »** désigne toute information, tout document ou tout objet, quelle que soit sa forme ou sa nature, ou toute partie de ceux-ci, qui a été classifié par l'une des Parties et dont la divulgation, la modification, la compromission ou la perte non autorisées pourraient entraîner des dommages ou des préjudices de gravité variable aux intérêts de l'une ou des deux Parties.
d) **« Autorité compétente en matière de sécurité »** désigne l'autorité publique d'une Partie, ou toute autorité de sécurité compétente déléguée dans un domaine militaire, chargée de superviser la mise en œuvre du présent Accord conformément aux lois et réglementations nationales.
e) **« Contractant »** désigne toute personne physique autre que celles liées par un contrat de travail avec une Partie ou toute personne morale relevant de la juridiction d'une Partie, qui conclut ou est liée par un Contrat classifié, y compris un Sous-traitant.
f) **« Habilitation de sécurité d'établissement »** désigne une décision positive, confirmée par l'Autorité compétente en matière de sécurité, selon laquelle un établissement dispose de mesures de sécurité appropriées pour accéder et traiter des Informations classifiées jusqu'à un niveau de classification de sécurité spécifié, conformément à ses lois et réglementations nationales.
g) **« Besoin d'en connaître »** désigne l'exigence pour une personne physique ou morale d'accéder à des Informations classifiées, d'en avoir connaissance ou d'en détenir pour l'exécution de leurs tâches ou services officiels.
h) **« Partie d'origine »** désigne la Partie sous l'autorité de laquelle les Informations classifiées ont été créées.
i) **« Habilitation de sécurité du personnel »** désigne une décision positive, confirmée par l'Autorité compétente en matière de sécurité, selon laquelle une personne est autorisée à accéder et traiter des Informations classifiées jusqu'à un niveau de classification spécifié, conformément à ses lois et réglementations nationales.
j) **« Entité émettrice »** désigne la Partie ou le Contractant relevant de sa juridiction qui communique des Informations classifiées à l'Entité destinataire en vertu du présent Accord.
k) **« Entité destinataire »** désigne la Partie ou le Contractant relevant de sa juridiction qui reçoit des Informations classifiées de la part de l'Entité émettrice dans le cadre du présent Accord.
l) **« Guide de classification de sécurité »** désigne un document annexé à un Contrat classifié qui précise les niveaux de classification de sécurité applicables à chaque élément dudit Contrat classifié.
m) **« Incident de sécurité »** désigne toute divulgation, modification, compromission, perte, accès, traitement, stockage ou destruction non autorisés d'Informations classifiées, contraires aux lois et réglementations nationales de l'Entité destinataire ou au présent Accord.
n) **« Sous-traitant »** désigne un Contractant auquel un Contractant principal attribue un contrat de sous-traitance.
o) **« Tiers »** désigne tout État, y compris toute entité publique ou privée relevant de sa juridiction, ou toute organisation internationale qui n'est pas l'une des Parties au présent Accord.

Article 3

*Autorités compétentes en matière de sécurité*

1. Les Autorités compétentes en matière de sécurité des Parties sont énumérées à l'annexe du présent Accord.

2. Les Autorités compétentes en matière de sécurité se fournissent mutuellement leurs coordonnées officielles et s'informent de toute modification les concernant.

Article 4

*Niveaux de classification de sécurité*

1. Les Parties s'engagent à protéger les Informations classifiées qu'elles échangent entre elles et conviennent que les niveaux de classification de sécurité suivants sont équivalents. La traduction anglaise des niveaux de classification de sécurité respectifs des Parties est informelle, ne fait pas partie des lois et réglementations nationales des Parties et ne peut pas être utilisée pour marquer les Informations classifiées.

| **Pour le Royaume des Pays-Bas** | **Pour le Grand-Duché de Luxembourg** | **En langue anglaise** |
|---|---|---|
| Stg. ZEER GEHEIM | TRES SECRET LUX | TOP SECRET |
| Stg. GEHEIM | SECRET LUX | SECRET |
| Stg. CONFIDENTIEEL | CONFIDENTIEL LUX | CONFIDENTIAL |
| DEPARTEMENTAAL VERTROUWELIJK | RESTREINT LUX | RESTRICTED |

Article 5

*Mesures de sécurité*

1. Conformément à leurs lois et réglementations nationales, les Parties s'engagent à mettre en œuvre des mesures appropriées pour protéger les Informations classifiées produites ou échangées dans le cadre du présent Accord. Chaque Partie accorde à ces Informations classifiées au moins le même niveau de protection que celui accordé à ses propres Informations classifiées ayant un niveau de classification de sécurité équivalent, tel que défini à l'article 4 du présent Accord.

2. Lorsque ces Informations classifiées sont traitées, stockées ou transmises au moyen de systèmes de communication et d'information, ces mesures garantissent la confidentialité, l'intégrité, la disponibilité, la non-répudiation, l'authenticité et la traçabilité de l'accès aux Informations classifiées. Les Parties veillent à ce que ces Informations classifiées soient stockées et traitées conformément à leurs lois et réglementations nationales.

3. Toute Information classifiée communiquée dans le cadre du présent Accord est marquée du niveau de classification de sécurité approprié, conformément aux lois et réglementations nationales de la Partie d'origine.

4. L'Entité destinataire appose son propre niveau de classification de sécurité à toutes les Informations classifiées reçues de la Partie émettrice dans le cadre du présent Accord, au niveau de classification de sécurité équivalent conformément au tableau figurant à l'article 4, de sorte que l'identité de la Partie d'origine soit toujours clairement identifiable.

5. Lorsque la forme ou la nature des Informations classifiées ne permet pas à l'Entité destinataire d'apposer un tel marquage à son propre niveau de classification de sécurité correspondant, les Autorités compétentes en matière de sécurité déterminent si le marquage réalisé par la Partie d'origine est suffisant.

6. L'Entité destinataire ne peut pas modifier ni supprimer la classification de sécurité des Informations classifiées reçues en vertu du présent Accord sans l'accord écrit de la Partie d'origine.

7. La Partie d'origine s'assure que l'Entité destinataire est informée de toute modification du niveau de classification de sécurité des Informations classifiées fournies, afin d'appliquer les mesures de protection appropriées.

8. La Partie d'origine peut ajouter en anglais sur les Informations classifiées des exigences concernant leur traitement afin de préciser toute restriction relative à leur utilisation, leur divulgation, leur communication et leur accès par l'Entité destinataire.

9. Les Parties prennent toutes les mesures appropriées pour garantir que l'Entité destinataire :
a) veille à ce que les Informations classifiées ne soient pas divulguées ni communiquées à un Tiers sans le consentement écrit préalable de la Partie d'origine ;
b) n'utilise les Informations classifiées qu'aux fins pour lesquelles elles ont été communiquées et dans les limites fixées par la Partie d'origine.

Article 6

*Accès aux informations classifiées*

1. L'accès aux Informations classifiées n'est accordé qu'aux personnes ayant un Besoin d'en connaître, ayant été informées de leurs responsabilités en matière de protection des Informations classifiées et ayant reconnu leurs responsabilités en matière de protection des Informations classifiées en vertu des lois et réglementations nationales de l'Entité destinataire.

2. Outre les exigences énoncées au paragraphe 1 du présent article, l'accès aux Informations classifiées de niveau CONFIDENTIEL LUX/Stg. CONFIDENTIEEL et supérieur n'est accordé qu'aux personnes disposant d'une Habilitation de sécurité du personnel au moins au niveau équivalent ou qui ont été dûment autorisées à accéder à des Informations classifiées en raison de leurs fonctions, conformément aux lois et réglementations nationales de l'Entité destinataire.

Article 7

*Contrats classifiés*

1. À la demande de la Partie d'origine, l'Autorité compétente en matière de sécurité de l'Entité destinataire s'engage à informer l'Autorité compétente en matière de sécurité de la Partie d'origine si un Contractant, relevant de sa juridiction et participant à un Contrat classifié ou à des négociations précontractuelles concernant un Contrat classifié et nécessitant l'accès à des Informations classifiées, a obtenu une Habilitation de sécurité d'établissement au niveau de classification de sécurité requis. Si, à la réception de la demande, le Contractant ne détient pas d'Habilitation de sécurité d'établissement ou si celle-ci est d'un niveau inférieur à celui requis, l'Autorité compétente en matière de sécurité qui a présenté la demande en est informée.

2. Si une Partie ou un Contractant relevant de sa juridiction propose un Contrat classifié impliquant l'accès à des Informations classifiées de niveau CONFIDENTIEL LUX/Stg. CONFIDENTIEEL ou supérieur, à un Contractant relevant de la juridiction de l'autre Partie, l'Autorité compétente en matière de sécurité de l'autre Partie doit avoir confirmé au préalable par écrit que le Contractant a obtenu une Habilitation de sécurité d'établissement au niveau approprié. Pour les Contrats classifiés de niveau RESTREINT LUX/DEPARTEMENTAAL VERTROUWELIJK, une Habilitation de sécurité d'établissement peut être requise, conformément aux lois et réglementations nationales de la Partie dont relève le Contractant.

3. L'Autorité compétente en matière de sécurité de la Partie ayant juridiction sur le Contractant veille à ce que le Contractant :
a) S'assure que toutes les personnes ayant accès à des Informations classifiées soient informées de leurs responsabilités en matière de protection des Informations classifiées, conformément à leurs lois et réglementations nationales et au présent Accord ;
b) surveille la mise en œuvre des mesures de sécurité dans ses établissements ;
c) notifie son Autorité compétente en matière de sécurité de tout incident de sécurité lié au Contrat classifié dans les plus brefs délais.

4. Outre les exigences énoncées au paragraphe 3 du présent article, pour les Contrats classifiés impliquant l'accès aux Informations classifiées de niveau CONFIDENTIEL LUX/Stg. CONFIDENTIEEL ou supérieur, l'Autorité compétente en matière de sécurité veille à ce que le contractant détienne une Habilitation de sécurité d'établissement au niveau de classification de sécurité correspondant afin de protéger les Informations classifiées et à ce que les personnes devant avoir accès à des Informations classifiées détiennent une Habilitation de sécurité du personnel au niveau de classification de sécurité correspondant.

5. Tout Contrat classifié inclut des exigences de sécurité précisant les aspects suivants :
a) un Guide de classification de sécurité ;
b) une procédure de notification des modifications du niveau de classification de sécurité, compte tenu de l'article 5 paragraphe 7 du présent Accord ;
c) les canaux et procédures à utiliser pour le transport et/ou la transmission d'Informations classifiées ;

d) les instructions relatives au traitement, au stockage, à la destruction et au renvoi d'Informations classifiées ;
e) les coordonnées des Autorités compétentes en matière de sécurité chargées de superviser la protection des Informations classifiées liées au Contrat classifié ;
f) l'obligation de signaler tout Incident de sécurité à l'Autorité compétente en matière de sécurité du Contractant et l'obligation pour les Contractants de prendre toutes les mesures raisonnables pour atténuer les effets d'une telle faille de sécurité, en consultation avec l'Autorité compétente en matière de sécurité ;
g) dans le cas où un Contrat classifié est sous-traité en tout ou en partie à un Sous-traitant, l'obligation d'imposer au Sous-traitant toutes les stipulations concernant les Contractants figurant dans le présent Accord ;
h) une référence au présent Accord ;
i) une déclaration selon laquelle les Informations classifiées échangées ou produites dans le cadre du Contrat classifié sont protégées par le Contractant conformément aux lois et réglementations nationales applicables ainsi qu'au présent Accord.

6. Si un Contrat classifié est attribué, la Partie ou un Contractant relevant de sa juridiction transmet, par l'intermédiaire de son Autorité compétente en matière de sécurité, une copie des exigences de sécurité visées au paragraphe 5 du présent article à l'Autorité compétente en matière de sécurité de l'Entité destinataire, afin de faciliter la supervision de la sécurité du Contrat classifié.

7. Les procédures d'approbation des visites associées aux activités relevant des Contrats classifiés effectuées par le personnel d'une Partie auprès de l'autre Partie sont conformes à l'article 8 du présent Accord.

Article 8

*Visites*

1. Les visites nécessitant l'accès à des Informations classifiées de niveau CONFIDENTIEL LUX/Stg. CONFIDENTIEEL ou supérieur sont soumises à l'accord écrit préalable de l'Autorité compétente en matière de sécurité de la Partie hôte, sauf convention contraire des Autorités compétentes en matière de sécurité. Cet accord n'est donné qu'aux personnes visées à l'article 6 du présent Accord. En ce qui concerne les visites nécessitant l'accès à des informations classifiées portant la mention RESTREINT LUX/DEPARTEMENTAAL VERTROUWELIJK, l'accord écrit préalable de l'Autorité compétente en matière de sécurité de la Partie hôte peut être requis, conformément aux lois et réglementations nationales de la Partie sous la juridiction de laquelle la visite a lieu.

2. Le visiteur soumet sa demande de visite au moins dix jours calendaires avant la date proposée à son Autorité compétente en matière de sécurité, qui la transmet à l'Autorité compétente en matière de sécurité de l'autre Partie. En cas d'urgence, les Autorités compétentes en matière de sécurité peuvent convenir d'un délai plus court.

3. La demande de visite inclut :
a) le nom complet du visiteur, la date et le lieu de naissance, la nationalité et le numéro de passeport/carte d'identité ;
b) le titre officiel et la fonction actuelle du visiteur, ainsi que le nom de l'organisation qu'il représente ou à laquelle il appartient ;
c) la confirmation de l'Habilitation de sécurité du personnel du visiteur, de son niveau et de sa validité ;
d) la date et la durée de la visite. En cas de visites répétées, la durée totale couverte par les visites est indiquée ;
e) le but de la visite et le niveau de classification de sécurité le plus élevé prévu pour les Informations classifiées qui seront discutées ou consultées ;
f) le nom, l'adresse, le numéro de téléphone, l'adresse de courrier électronique du point de contact de l'établissement à visiter ;
g) la signature datée et tamponnée d'un représentant de l'Autorité compétente en matière de sécurité du visiteur.

4. Les Autorités compétentes en matière de sécurité peuvent convenir d'une liste de visiteurs autorisés à effectuer des visites régulières pendant une période n'excédant pas douze mois. Les Autorités compétentes en matière de sécurité s'accordent sur les modalités supplémentaires concernant les visites régulières.

5. L'Autorité compétente en matière de sécurité de la Partie hôte communique aux responsables de la sécurité de l'établissement qui fera l'objet de la visite les coordonnées des personnes dont la demande de visite a été approuvée. Une fois l'autorisation accordée, les modalités de visite pour les personnes autorisées à effectuer des visites régulières peuvent être convenues directement avec le responsable de l'établissement concerné.

6. Les Informations classifiées fournies à un visiteur ou obtenues par celui-ci doivent être traitées conformément aux dispositions du présent Accord.

Article 9

*Transfert d'informations classifiées*

1. Les Informations classifiées de niveau CONFIDENTIEL LUX/Stg. CONFIDENTIEEL ou supérieur sont transférées par courrier diplomatique, gouvernemental ou militaire, ou par tout autre moyen convenu au préalable par les Autorités compétentes en matière de sécurité, conformément à leurs lois et réglementations nationales.

2. Les Informations classifiées de niveau RESTREINT LUX/DEPARTEMENTAAL VERTROUWELIJK peuvent être transférées par des services postaux conformément aux lois et réglementations nationales.

3. La transmission électronique d'Informations classifiées ne peut avoir lieu qu'en utilisant des moyens cryptographiques conformément aux procédures qui seront convenues par les Autorités compétentes en matière de sécurité.

4. Les Informations classifiées de niveau CONFIDENTIEL LUX/Stg. CONFIDENTIEEL ou supérieur sont enregistrées.

Article 10

*Reproduction et traduction d'informations classifiées*

1. Les originaux et les traductions d'Informations classifiées de niveau TRÈS SECRET LUX/Stg. ZEER GEHEIM ne sont pas reproduites ni traduites sans l'accord écrit préalable de la Partie d'origine.

2. Les reproductions et traductions d'Informations classifiées sont marquées du niveau de classification de sécurité des Informations classifiées originales et sont protégées de la même manière que les Informations classifiées originales.

3. Le nombre de reproductions et de traductions est limité au strict minimum pour l'utilisation prévue dans le cadre du présent Accord.

4. Les traductions indiquent expressément dans la langue de traduction qu'elles contiennent des Informations classifiées reçues de la Partie d'origine.

Article 11

*Destruction des informations classifiées*

1. Les Informations classifiées de niveau TRÈS SECRET LUX/Stg. ZEER GEHEIM ne peuvent être détruites qu'avec l'accord écrit préalable de la Partie d'origine. Par défaut, elles sont restituées à la Partie émettrice après avoir été reconnues par l'Entité destinataire comme n'étant plus nécessaires.

2. Les Informations classifiées de niveau SECRET LUX/Stg. GEHEIM ou inférieure sont détruites après avoir été reconnues par l'Entité destinataire comme n'étant plus nécessaires, de manière à empêcher leur reconstitution totale ou partielle.

3. Lorsqu'une situation de crise empêche une Entité destinataire de protéger les Informations classifiées fournies en vertu du présent Accord, celles-ci sont détruites immédiatement. L'Entité destinataire informe, par l'intermédiaire de son Autorité compétente en matière de sécurité, par écrit et dans les meilleurs délais l'Autorité compétente en matière de sécurité de la Partie d'origine de la destruction de ces Informations classifiées.

Article 12

*Coopération en matière de sécurité*

1. Les Autorités compétentes en matière de sécurité s'informent mutuellement, sur demande, des modifications apportées à leurs lois et réglementations nationales, à leurs politiques et à leurs pratiques en matière de protection des Informations classifiées.

2. À la demande de l'Autorité compétente en matière de sécurité d'une des Parties, l'Autorité compétente en matière de sécurité de l'autre Partie confirme par écrit la délivrance d'une Habilitation de sécurité du personnel à une personne physique ou d'une Habilitation de sécurité d'établissement à une personne morale.

3. Dans le cadre du présent Accord, chaque Partie reconnaît les Habilitations de sécurité du personnel et les Habilitations de sécurité d'établissement délivrées par l'autre Partie.

4. Sur demande et conformément à leurs lois et réglementations nationales, les Autorités compétentes en matière de sécurité se prêtent mutuellement assistance pour mener à bien les enquêtes relatives aux demandes d'Habilitations de sécurité du personnel et d'Habilitations de sécurité d'établissement.

5. Les Autorités compétentes en matière de sécurité se tiennent mutuellement informées sans délai par écrit des modifications apportées aux Habilitations de sécurité du personnel et aux Habilitations de sécurité d'établissement pour lesquelles une confirmation a été fournie.

6. Dans le cadre du présent Accord et nonobstant l'article 9, chaque Partie reconnaît un acte d'approbation formel délivré par l'autre Partie concernant les équipements et mécanismes liés aux systèmes de communication et d'information utilisés pour traiter les Informations classifiées de l'autre Partie. Si nécessaire, la liste mise à jour des équipements et mécanismes approuvés est échangée entre les Autorités compétentes en matière de sécurité.

7. La coopération dans le cadre du présent Accord est menée en anglais.

Article 13

*Incident de sécurité*

1. Si l'Entité destinataire soupçonne ou constate un Incident de sécurité concernant les Informations classifiées de la Partie d'origine, elle en informe immédiatement par écrit son Autorité compétente en matière de sécurité. La notification contient suffisamment de détails pour que la Partie d'origine puisse évaluer les conséquences et les circonstances de la violation présumée ou avérée.

2. Les Autorités compétentes en matière de sécurité s'informent immédiatement par écrit de tout Incident de sécurité réel ou potentiel impliquant des Informations classifiées.

3. L'Entité destinataire doit immédiatement enquêter sur tout Incident de sécurité réel ou potentiel. L'Autorité compétente en matière de sécurité de la Partie d'origine coopère, si nécessaire, à l'enquête.

4. L'Autorité compétente en matière de sécurité de l'Entité destinataire prend les mesures appropriées, conformément à ses lois et réglementations nationales, afin de limiter les conséquences et d'empêcher que l'Incident de sécurité ne se reproduise. L'Autorité compétente en matière de sécurité de la Partie d'origine est informée du résultat de l'enquête et, le cas échéant, des mesures prises.

Article 14

*Coûts*

Chaque Partie prend en charge ses propres frais encourus dans le cadre de la mise en œuvre et de l'exécution de ses obligations en vertu du présent Accord.

Article 15

*Règlement des litiges*

Tout litige découlant de l'interprétation, de la mise en œuvre ou de l'application du présent Accord sera réglé exclusivement par consultation ou négociation entre les Parties par la voie diplomatique.

Article 16

*Articulation avec d'autres accords*

Le présent Accord ne prévaut sur aucun accord international qui a déjà été conclu ou qui pourrait être conclu et qui régit spécifiquement l'échange et la protection mutuelle des Informations classifiées.

Article 17

*Modalités d'application*

Les Autorités compétentes en matière de sécurité des Parties ou toute autre autorité compétente en matière de sécurité des Parties peuvent se consulter sur les aspects techniques détaillés liés à l'application du présent Accord et peuvent convenir, au cas par cas, de modalités d'application appropriées conformément au présent Accord.

Article 18

*Dispositions finales*

1. Le présent Accord est conclu pour une durée indéterminée.

2. Chaque Partie notifie à l'autre Partie, par voie diplomatique, l'achèvement des procédures nationales nécessaires à l'entrée en vigueur du présent Accord. Le présent Accord entrera en vigueur le premier jour du deuxième mois suivant la réception de cette dernière notification.

3. En ce qui concerne le Royaume des Pays-Bas, le présent Accord s'applique à la partie européenne des Pays-Bas et à la partie caribéenne des Pays-Bas (les îles de Bonaire, Saint-Eustache et Saba).

4. Le présent Accord, y compris son annexe, peut être modifié d'un commun accord des Parties. Chacune des Parties peut proposer à tout moment des amendements au présent Accord par voie diplomatique. Ces amendements entrent en vigueur dans les conditions prévues au paragraphe 2 du présent article, à l'exception d'un amendement concernant les Autorités compétentes en matière de sécurité énumérées à l'annexe, qui entre en vigueur à une date à convenir entre les Parties.

5. Chacune des Parties peut résilier le présent Accord à tout moment par écrit et par voie diplomatique. Dans ce cas, l'Accord prendra fin six mois après réception de cette notification.

6. En cas de résiliation du présent Accord, les Informations classifiées échangées, communiquées ou produites dans le cadre du présent Accord resteront protégées conformément aux dispositions de ce dernier avant sa résiliation, tant que les Informations classifiées resteront classifiées.

EN FOI DE QUOI, les représentants des Parties, dûment mandatés à cet effet, ont signé le présent Accord.

FAIT à Luxembourg le 21 avril 2026, en deux exemplaires originaux, en langues néerlandaise, française et anglaise, les trois textes faisant également foi.

En cas de divergence d'interprétation, le texte anglais prévaut.

*Pour le Royaume des Pays-Bas,*

T.B.W. BERENDSEN

*Pour le Grand-Duché de Luxembourg,*

X. BETTEL

---

**Annexe**

L'Autorité compétente en matière de sécurité pour le Royaume des Pays-Bas est :

Autorité nationale de sécurité civile
Service général de renseignement et de sécurité
Ministère de l'Intérieur et des Relations du Royaume

Autorité déléguée compétente en matière de sécurité :
Autorité nationale de sécurité militaire
Autorité de sécurité en matière de défense
Direction générale de la politique
Ministère de la Défense.

L'autorité compétente en matière de sécurité pour le Grand-Duché de Luxembourg est :
Ministère d'État
Service de renseignement de l'État
Autorité nationale de sécurité.

---

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

Uitgegeven de *dertigste* april 2026.

*De Minister van Buitenlandse Zaken,*

T.B.W. BERENDSEN

trb-2026-47
ISSN 0920 - 2218
's-Gravenhage 2026