15 (2023) Nr. 1

TRACTATENBLAD

VAN HET

KONINKRIJK DER NEDERLANDEN

JAARGANG 2023 Nr. 132

A. TITEL

Beveiligingsverdrag tussen het Koninkrijk der Nederlanden en het Koninkrijk Noorwegen inzake de uitwisseling en wederzijdse beveiliging van gerubriceerde gegevens (met Bijlage); Oslo, 7 november 2023

Voor een overzicht van de verdragsgegevens, zie verdragsnummer 012704 in de Verdragenbank.

B. TEKST[1)]

Security agreement between the Kingdom of the Netherlands and the Kingdom of Norway concerning the exchange and mutual protection of classified information

The Kingdom of the Netherlands

and

the Kingdom of Norway,

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

In order 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 either exchanged or generated under this Agreement between the Parties or between Contractors or other legal entities under their jurisdiction. This Agreement sets out the security procedures and arrangements for such protection.

Article 2

Definitions

For the purpose of this Agreement:
a) "Classified Contract" means an agreement, including any pre-contractual negotiations, the performance of which requires or involves access or potential access to or the creation of Classified Information.
b) "Classified Information" means any information or material designated by a security classification by one of the Parties the unauthorised disclosure, alteration, compromise or loss of which could cause damage or harm 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. The Competent Security Authority may delegate part of its responsibilities to a delegated competent security authority.
d) "Contractor" means any legal entity with the capacity to enter into contracts.
e) "Facility Security Clearance" means the positive determination by the Competent Security Authority that

[1)] De Noorse tekst is niet opgenomen.

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.
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 including any Contractor or other legal entity under its jurisdiction, which provides Classified Information to the Receiving Party under this Agreement.
j) "Receiving Party" means the Party including any Contractor or other legal entity 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 specifying the applicable security classification levels of each part of the Contract.
l) "Security Incident" means any disclosure, alteration, compromise or loss of Classified Information contrary to national laws and regulations of the Receiving Party and/or this Agreement.
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 the Annex of this Agreement.

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

Article 4

Security classification levels

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

For the Kingdom of the Netherlands	For the Kingdom of Norway	Equivalent in English
Stg. ZEER GEHEIM	STRENGT HEMMELIG	TOP SECRET
Stg. GEHEIM	HEMMELIG	SECRET
Stg. CONFIDENTIEEL	KONFIDENSIELT	CONFIDENTIAL
DEPARTEMENTAAL VERTROUWELIJK	BEGRENSET	RESTRICTED

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 shall not modify or revoke the security classification of received Classified Information under this Agreement without the written consent of the Originating Party.

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

Article 5

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 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 "CONFIDENTIAL" or above, shall be granted only to those individuals who additionally hold a Personnel Security Clearance at the corresponding level or who are otherwise duly authorised to access Classified Information by virtue of their function in accordance with the national laws and regulations of the Receiving Party.

Article 6

Security measures

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

2. The Providing Party shall:
a) mark Classified Information with the appropriate security classification in accordance with its national laws and regulations;
b) inform the Receiving Party of any conditions of release or limitations on the use of the Classified Information provided;

3. The Receiving Party shall:
a) afford the same level of protection to Classified Information as afforded to its national Classified Information of an equivalent security classification level;
b) ensure that Classified Information is not disclosed or released to a Third Party without the prior written consent of the Originating Party;
c) use Classified Information solely for the purpose it has been provided 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 or other legal entity under its jurisdiction proposes to grant a Classified Contract at the security classification level equivalent to "CONFIDENTIAL" or above, with a Contractor under the jurisdiction of the other Party, it shall first obtain written confirmation from the Competent Security Authority of the other Party that the Contractor has been granted a Facility Security Clearance at the appropriate security classification level. For Classified Contracts at the security classification level equivalent to "RESTRICTED" a Facility Security Clearance may be required if mandated by national laws and regulations.

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

3. Every Classified Contract including classified sub-contracts concluded in accordance with this Agreement shall include security requirements which identify the following aspects:

a) a Security Classification Guide;
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.

Article 9

Transmission of Classified Information

1. Classified Information at the classification level equivalent to "TOP SECRET" shall be transmitted through diplomatic channels. Classified Information at the classification level equivalent to "SECRET" or below shall be transmitted as agreed between the Competent Security Authorities.

2. The Parties may electronically transmit Classified Information only when protected by cryptographic means in accordance with procedures to be approved by both 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 article 5 of this Agreement 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 "TOP SECRET" 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 "TOP SECRET" 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 "SECRET" 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. After Classified Information with security classification level "SECRET" has been destroyed according to this paragraph, a notification will be sent to the Originating Party.

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.

8. Classified information shall be destroyed in such a way that it is impossible to restore it in whole or in part.

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 and is 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 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 handled in accordance with the provisions of this Agreement.

6. Official representatives of the Parties are 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 immediately investigate 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 of the Receiving Party shall take appropriate measures in accordance with its national laws and regulations to limit the consequences of the Security Incident and to prevent a recurrence of any actual or suspected Security Incident. 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

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 and will not be referred to any national or international tribunal or third party for settlement.

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 of the annex, 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 Oslo on this 7th day of November 2023 in two original copies, each in the English, Dutch and Norwegian language. In case of divergence of interpretation of this Agreement, the English text shall prevail.

For the Kingdom of the Netherlands,

J.C.M. GROFFEN

For the Kingdom of Norway,

EMILIE ENGER MEHL

Annex

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

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

The Competent Security Authority for the Kingdom of Norway is:
Norwegian National Security Authority

The delegated Competent Security Authority for Request for Visits is:
Defence Security Agency

Beveiligingsverdrag tussen het Koninkrijk der Nederlanden en het Koninkrijk Noorwegen inzake de uitwisseling en wederzijdse beveiliging van gerubriceerde gegevens

Het Koninkrijk der Nederlanden

en

het Koninkrijk Noorwegen,

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

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

Dit Verdrag heeft ten doel de beveiliging te waarborgen van gerubriceerde gegevens die uit hoofde van dit Verdrag worden uitgewisseld tussen of gegenereerd door de partijen of tussen of door opdrachtnemers of andere rechtspersonen onder hun rechtsmacht. In het Verdrag worden de beveiligingsprocedures 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, 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, verandering, compromitering of het verlies de belangen van een of beide partijen zou kunnen schaden.
c. „Bevoegde beveiligingsautoriteit", de overheidsautoriteit in een partij die verantwoordelijk is voor de implementatie van en toezicht op dit Verdrag. De bevoegde beveiligingsautoriteit kan een deel van zijn verantwoordelijkheden delegeren aan een gemachtigde bevoegde beveiligingsautoriteit.
d. „Opdrachtnemer", elke rechtspersoon die bevoegd is contracten aan te gaan.
e. „Veiligheidsmachtiging bedrijfslocatie", de vaststelling 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.
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 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.
i. „Verstrekkende partij", de partij, met inbegrip van elke opdrachtnemer of andere rechtspersoon onder haar rechtsmacht, die de gerubriceerde gegevens uit hoofde van dit Verdrag verstrekt aan de ontvangende partij.
j. „Ontvangende partij", de partij, met inbegrip van elke opdrachtnemer of andere rechtspersoon onder haar rechtsmacht, die de gerubriceerde gegevens uit hoofde van dit Verdrag ontvangt van de verstrekkende partij.
k. „Rubriceringsgids", een document dat hoort bij een gerubriceerd contract waarin de van toepassing zijnde rubriceringsniveaus voor elk onderdeel van het contract worden gespecificeerd.
l. „Beveiligingsincident", elke bekendmaking, verandering, compromitering of elk verlies van gerubriceerde gegevens in strijd met de nationale wet- en regelgeving en/of dit Verdrag.
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 beveiligingsautoriteiten

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

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

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 der Nederlanden	**Voor het Koninkrijk Noorwegen**	**Equivalent in het Engels**
Stg. ZEER GEHEIM	STRENGT HEMMELIG	TOP SECRET
Stg. GEHEIM	HEMMELIG	SECRET
Stg. CONFIDENTIEEL	KONFIDENSIELT	CONFIDENTIAL
DEPARTEMENTAAL VERTROUWELIJK	BEGRENSET	RESTRICTED

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 zal het rubriceringsniveau van uit hoofde van dit Verdrag ontvangen gerubriceerde gegevens niet veranderen of intrekken zonder de schriftelijke instemming van de partij van herkomst.

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

Artikel 5

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 en een geheimhoudingsverklaring hebben ondertekend in overeenstemming met de nationale wet- en regelgeving.

2. Toegang tot gerubriceerde gegevens met een rubriceringsniveau dat overeenkomt met „CONFIDENTIAL" of hoger wordt uitsluitend verleend aan de natuurlijke personen die ook een veiligheidsmachtiging personeel hebben op het overeenkomstige niveau of die anderszins gemachtigd zijn om toegang te krijgen tot gerubriceerde gegevens uit hoofde van hun functie in overeenstemming met de nationale wet- en regelgeving van de ontvangende partij.

Artikel 6

Beveiligingsmaatregelen

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

2. De verstrekkende partij:
a. voorziet de gerubriceerde gegevens van de juiste rubriceringsmarkering in overeenstemming met haar nationale wet- en regelgeving;
b. stelt de ontvangende partij in kennis van mogelijke voorwaarden voor vrijgave of beperkingen gesteld aan het gebruik van de verstrekte gerubriceerde gegevens;

3. De ontvangende partij:
a. kent hetzelfde beveiligingsniveau toe aan gerubriceerde gegevens als aan hun nationale gerubriceerde gegevens met een vergelijkbaar rubriceringsniveau;
b. waarborgt dat gerubriceerde gegevens niet bekend worden gemaakt of vrijgegeven aan een derde zonder de voorafgaande schriftelijke toestemming van de partij van herkomst;
c. gebruikt de gerubriceerde gegevens uitsluitend voor het doel waarvoor zij zijn verstrekt en in overeenstemming met de eisen voor gebruik van de partij van herkomst.

Artikel 7

Beveiligingssamenwerking

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

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

3. De bevoegde beveiligingsautoriteiten 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 of veiligheidsmachtiging personeel.

4. De bevoegde beveiligingsautoriteiten stellen elkaar onverwijld schriftelijk in kennis van veranderingen in erkende veiligheidsmachtigingen bedrijfslocatie of 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 of andere rechtspersoon onder haar rechtsmacht voorstelt een gerubriceerd contract met een rubriceringsniveau dat overeenkomt met „CONFIDENTIAL" of hoger, toe te kennen aan een opdrachtnemer onder de rechtsmacht van de andere partij, dient zij eerst de schriftelijke bevestiging te verkrijgen van de bevoegde beveiligingsautoriteit van de andere partij dat aan deze opdrachtnemer een veiligheidsmachtiging bedrijfslocatie is toegekend op het vereiste rubriceringsniveau. Een veiligheidsmachtiging bedrijfslocatie op het niveau „RESTRICTED" kan vereist zijn indien dit verplicht wordt gesteld in de nationale wet- en regelgeving.

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

3. Elk gerubriceerd contract, met inbegrip van gerubriceerde onderaannemingscontracten, dat in overeenstemming met dit Verdrag wordt gesloten dient beveiligingsvereisten te bevatten waarin de volgende aspecten vermeld staan:
a. een rubriceringsgids;
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 overdracht van gerubriceerde gegevens;
d. instructies voor de omgang met en opslag van gerubriceerde gegevens;
e. contactgegevens van de bevoegde beveiligingsautoriteiten die verantwoordelijk zijn voor het toezicht op de beveiliging van gerubriceerde gegevens die betrekking hebben op het gerubriceerde contract;
f. de verplichting elk beveiligingsincident te melden.

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

Artikel 9

Overbrenging van gerubriceerde gegevens

1. Gerubriceerde gegevens met het rubriceringsniveau dat overeenkomt met „TOP SECRET" worden langs diplomatieke weg verzonden. Gerubriceerde gegevens met het rubriceringsniveau dat overeenkomt met „SECRET" of lager wordt verzonden zoals overeengekomen door de bevoegde beveiligingsautoriteiten.

2. De partijen kunnen gerubriceerde gegevens die door encryptie beveiligd zijn uitsluitend langs elektronische weg verzenden in overeenstemming met procedures die door beide bevoegde beveiligingsautoriteiten dienen te worden goedgekeurd.

Artikel 10

Reproductie, vertaling en vernietiging van gerubriceerde gegevens

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

2. 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 artikel 5 van dit Verdrag gemachtigd zijn om toegang te krijgen 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 het rubriceringsniveau dat overeenkomt met „TOP SECRET" zoals vermeld in artikel 4 van dit Verdrag worden niet vertaald of gereproduceerd zonder voorafgaande schriftelijke toestemming van de partij van herkomst.

5. Gerubriceerde gegevens met het rubriceringsniveau dat overeenkomt met „TOP SECRET" zoals vermeld in artikel 4 van dit Verdrag worden niet vernietigd zonder 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 tot en met rubriceringsniveaus die overeenkomen met „SECRET" 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. Nadat gerubriceerde gegevens met rubriceringsniveau „SECRET" zijn vernietigd overeenkomstig dit lid, wordt een kennisgeving naar de partij van herkomst gezonden.

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 beveiligingsautoriteit van de verstrekkende partij onverwijld in kennis van de vernietiging van deze gerubriceerde gegevens.

8. Gerubriceerde gegevens worden op zodanige wijze vernietigd dat het onmogelijk is deze geheel of deels te herstellen.

Artikel 11

Bezoeken

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

2. De bezoeker dient de aanvraag voor het bezoek ten minste twintig 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 kan de aanvraag van een verzoek binnen een kortere termijn worden ingediend, mits hierover voorafgaande coördinatie tussen de bevoegde beveiligingsautoriteiten plaatsvindt.

3. Een aanvraag voor een bezoek dient de volgende gegevens te bevatten:
a. volledige naam van de bezoeker, geboortedatum en -plaats, nationaliteit en nummer paspoort/ identiteitskaart;

b. officiële functiebenaming 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, telefoonnummer, e-mailadres en contactpunt van de te bezoeken locatie;
g. van een datum en stempel voorziene handtekening van een vertegenwoordiger van de bevoegde beveiligingsautoriteit van de bezoeker.

4. De bevoegde beveiligingsautoriteiten kunnen een lijst overeenkomen van bezoekers die herhalingsbezoeken mogen afleggen. De bevoegde beveiligingsautoriteiten 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 officiële vertegenwoordigers van de partijen 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

Beveiligingsincident

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

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

3. De bevoegde beveiligingsautoriteit van de ontvangende partij neemt passende maatregelen in overeenstemming met zijn nationale wet- en regelgeving om de gevolgen van het beveiligingsincident te beperken en om herhaling van een feitelijk of vermoedelijk beveiligingsincident te voorkomen. De bevoegde beveiligingsautoriteit van de partij van herkomst wordt in kennis gesteld van de uitkomsten van het onderzoek en de eventuele getroffen maatregelen.

Artikel 13

Kosten

Elke partij draagt haar eigen kosten die ontstaan in verband met de uitvoering van haar verplichtingen ingevolge dit Verdrag.

Artikel 14

Oplossing van geschillen

Elk geschil omtrent de uitlegging of toepassing van dit Verdrag wordt uitsluitend door middel van onderhandelingen tussen de partijen opgelost en niet ter beslechting voorgelegd aan een nationaal of internationaal scheidsgerecht of een andere derde.

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 beveiligingsautoriteiten 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 op elk moment langs diplomatieke weg wijzigingen van dit Verdrag voorstellen. Dergelijke wijzigingen treden in werking onder de voorwaarden vervat in het eerste lid van dit artikel, met uitzondering van een wijziging van de Bijlage, welke 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 Oslo op 7 november 2023 in twee oorspronkelijke exemplaren, elk in de Engelse, de Nederlandse en de Noorse taal. In geval van verschillen in interpretatie van dit Verdrag is de Engelse tekst doorslaggevend.

Voor het Koninkrijk der Nederlanden,

J.C.M. GROFFEN

Voor het Koninkrijk Noorwegen,

EMILIE ENGER MEHL

Bijlage

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

De gemachtigde bevoegde beveiligingsautoriteit van het Koninkrijk der Nederlanden in het militaire domein is:
De Beveiligingsautoriteit
Directoraat-Generaal Beleid
Ministerie van Defensie

De bevoegde beveiligingsautoriteit van het Koninkrijk Noorwegen is:
De Noorse Nationale Beveiligingsautoriteit

De gedelegeerde bevoegde beveiligingsautoriteit voor verzoeken voor bezoeken is:
Het Defensiebeveiligingsagentschap

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, 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 *negenentwintigste* november 2023.

De Minister van Buitenlandse Zaken,

H.G.J. BRUINS SLOT

trb-2023-132
ISSN 0920 - 2218
's-Gravenhage 2023