2 (2022) Nr. 1

TRACTATENBLAD

VAN HET

KONINKRIJK DER NEDERLANDEN

JAARGANG 2022 Nr. 20

A. TITEL

Verdrag tussen het Koninkrijk der Nederlanden en de Republiek Finland inzake de uitwisseling en wederzijdse beveiliging van gerubriceerde gegevens (met Bijlage); 's-Gravenhage, 22 februari 2022

Voor een overzicht van de verdragsgegevens, zie verdragsnummer 012022 in de Verdragenbank.

B. TEKST

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

The Kingdom of the Netherlands

and

the Republic of Finland,

Hereinafter referred to as "the Parties",

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

Article 2

Definitions

For the purpose of this Agreement:
a) **"Classified Contract"** means any contract or subcontract, which requires or involves Classified Information.
b) **"Classified Information"** means any information or material designated by a security classification by one of the Parties the unauthorised disclosure or loss of which could cause varying degrees of prejudice to the interests of one or both of the Parties.
c) **"Competent Security Authority"** means a National Security Authority or any other competent body authorised in accordance with the national laws and regulations of the Parties which is responsible for the implementation of and compliance with this Agreement.
d) **"Contractor"** means any individual or legal entity with the capacity to enter into contracts.
e) **"Facility Security Clearance"** means the positive determination by the Competent Security Authority that

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

Article 3

Competent Security Authorities

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

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

Article 4

Security classification levels

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

For the Republic of Finland	**For the Kingdom of the Netherlands**	**Equivalent in English[1)]**
ERITTÄIN SALAINEN or YTTERST HEMLIG	Stg ZEER GEHEIM	TOP SECRET
SALAINEN or HEMLIG	Stg GEHEIM	SECRET
LUOTTAMUKSELLINEN or KONFIDENTIELL	Stg CONFIDENTIEEL	CONFIDENTIAL
KÄYTTÖ RAJOITETTU or BEGRÄNSAD TILLGÅNG	DEPARTEMENTAAL VERTROUWELIJK	RESTRICTED

1) For the purpose of this agreement, this English equivalent for classification is used. The official classifications to be used for the marking of classified information are in Finnish/Swedish and Dutch.

2. The Parties shall take all appropriate measures to ensure that 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 Parties shall take all appropriate measures to ensure that the Receiving Party shall not modify or revoke the security classification of received Classified Information under this Agreement without the written approval of the Originating Party.

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

Article 5

Protection of Classified Information

1. The Parties shall take all appropriate measures in accordance with their national laws and regulations so as to protect Classified Information referred to in this Agreement. They shall afford such information at least the same protection as they afford to their own information at the corresponding security classification level. Electronic transmission of Classified Information in an unprotected network by the Receiving Party shall take place using cryptographic tools.

2. The Parties shall not provide access to Classified Information to Third Parties without the prior written consent of the Originating Party.

3. Access to Classified Information shall be limited to individuals who have a "Need-to-know", are briefed on their responsibilities for the protection of Classified Information, have signed a statement of confidentiality and/or are legally bound to confidentiality and who hold a Personnel Security Clearance at the corresponding level or are authorised to have access to such information by virtue of their function, all in accordance with national laws and regulations.

4. A Personnel Security Clearance is not required for access to Classified Information at the security classification level equivalent to "RESTRICTED" as mentioned in Article 4 of this Agreement.

5. Classified Information shall be used solely for the purpose for which it has been provided.

Article 6

Security co-operation

1. In order to maintain comparable standards of security, the Competent Security Authorities shall, on request, inform each other about their national laws and 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 7

Classified Contracts

1. Upon request, the Competent Security Authority of the Receiving Party shall inform the Competent Security Authority of the Originating Party whether a proposed Contractor participating in precontract negotiations of a Classified Contract has been issued an appropriate Facility Security Clearance corresponding to the required security classification level.

2. If a Party or a Contractor under its jurisdiction grants a Classified Contract at the Security Classification Levels equivalent to "CONFIDENTIAL" or above as mentioned in Article 4 of this Agreement, with a (Sub-)Contractor under the jurisdiction of the other Party, it shall first obtain written confirmation from the other Party that the Contractor has been granted a Facility Security Clearance.

3. In the case of an open tender the Competent Security Authority of the Receiving Party may provide the Competent Security Authority of the Originating Party with the relevant Facility Security Clearance certificates without a formal request.

4. A Facility Security Clearance is not required for Classified Contracts at the security classification level equivalent to "RESTRICTED" as mentioned in Article 4 of this Agreement.

5. Representatives of the Competent Security Authorities of the Parties may visit each other in order to analyse the efficiency of the measures adopted by a Contractor for the protection of Classified Information involved in a Classified Contract.

6. Every Classified Contract concluded in accordance with this Agreement shall include security requirements which identify the following aspects:
a) a Security Classification Guide;
b) contact details of the Competent Security Authorities responsible for implementing the Classified Contract and for overseeing the protection of Classified Information related to the Classified Contract;
c) laws and regulations concerning the protection of Classified Information;
d) procedure and requirements for access to Classified Information;
e) handling and storing of Classified Information;
f) transportation and electronic transmission of Classified Information;
g) marking of Classified Information;
h) obligation to monitor security conduct and notify its Competent Security Authority in case of any Security Incident;
i) protection of Classified Information after termination of the Classified Contract;
j) destroying or returning of Classified Information;
k) release of information related to the Classified Contract.

7. 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.

8. 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 10 of this Agreement.

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

Article 8

Transmission of Classified Information between the Parties

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

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

Article 9

Reproduction, translation and destruction of Classified Information

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

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

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

4. Classified Information marked at the Security Classification Level equivalent to "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.

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

Article 10

Visits

1. Visits requiring access to Classified Information at the level "CONFIDENTIAL" or above as mentioned in Article 4 of this Agreement 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 fourteen days in advance of the proposed date of the visit to his Competent Security Authority, which shall forward it to the Competent Security Authority of the other Party. In urgent cases, the request for visit may be submitted at a shorter notice, subject to prior coordination between the Competent Security Authorities.

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

4. The Competent Security Authorities may agree on a list of visitors entitled to recurring visits. The Competent Security Authorities shall agree on the further details of the recurring visits. However the validity of authorisations for recurring visits shall not exceed twelve (12) months.

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

Article 11

Security Incident

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

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

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

Article 12

Costs

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

Article 13

Dispute resolution

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

Article 14

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 15

Implementing arrangements

The appropriate authorities of the Parties may conclude implementing arrangements pursuant to this Agreement.

Article 16

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, including its Annex, may be amended with the mutual consent of the Parties. Either Party may propose amendments to this Agreement, including its Annex, 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.

6. After the entry into force of this Agreement, the Kingdom of the Netherlands shall take immediate measures to have the Agreement registered by the Secretariat of the United Nations in accordance with Article 102 of the Charter of the United Nations.

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

DONE in The Hague on the 22nd day of February 2022, in two original copies, in the English language.

For the Kingdom of the Netherlands,

SIMONE SMIT

For the Republic of Finland,

PÄIVI KAUKORANTA

Annex I

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

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

The Competent Security Authority for The Republic of Finland is:

C. VERTALING

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

Het Koninkrijk der Nederlanden

en

de Republiek Finland

Hierna te noemen „de partijen",

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

Artikel 1

Doel

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

Artikel 2

Begripsomschrijvingen

Voor de toepassing van dit Verdrag wordt verstaan onder:
a. **„Gerubriceerd contract"**, elk contract of subcontract waarvoor gerubriceerde gegevens vereist zijn of waarbij deze betrokken zijn.
b. **„Gerubriceerde gegevens"**, gegevens die of materiaal dat door een van de partijen als gerubriceerd worden of wordt aangemerkt, waarvan de ongeoorloofde bekendmaking of het verlies de belangen van een of beide partijen in meer of mindere mate zou kunnen schaden.
c. **„Bevoegde veiligheidsautoriteit"**, een nationale veiligheidsautoriteit of een andere overeenkomstig de nationale wet- en regelgeving van de partijen gemachtigde bevoegde instantie die verantwoordelijk is voor de implementatie van en toezicht op dit Verdrag.
d. **„Opdrachtnemer"**, elke natuurlijke persoon of rechtspersoon die bevoegd is contracten aan te gaan.
e. **„Veiligheidsmachtiging bedrijfslocatie"**, de vaststelling door de bevoegde veiligheidsautoriteit dat een bedrijfslocatie passende veiligheidsmaatregelen heeft genomen voor de toegang tot en verwerking van gerubriceerde gegevens tot en met een bepaald 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.
h. **„Veiligheidsmachtiging personeel**", de vaststelling door de bevoegde veiligheidsautoriteit dat een natuurlijke persoon een veiligheidsmachtiging heeft gekregen voor de toegang tot en verwerking van gerubriceerde gegevens tot en met een bepaald rubriceringsniveau, in overeenstemming met de nationale wet- en regelgeving.
i. **„Verstrekkende partij"**, de partij of opdrachtnemer onder haar rechtsmacht die de gerubriceerde gegevens uit hoofde van dit Verdrag verstrekt aan de ontvangende partij.
j. **„Ontvangende partij"**, de partij of opdrachtnemer onder haar rechtsmacht die de gerubriceerde gegevens uit hoofde van dit Verdrag ontvangt van de verstrekkende partij.
k. **„Rubriceringsgids"**, een document dat hoort bij een gerubriceerd contract waarin elk onderdeel van het gerubriceerd contract dat gerubriceerde gegevens bevat wordt genoemd, met inbegrip van de rubriceringsniveaus die erop van toepassing zijn.
l. **„Veiligheidsincident"**, elk handelen of nalaten te handelen, in strijd met de nationale wet- en regelgeving, dat resulteert in ongeoorloofde toegang tot of bekendmaking, verlies of compromittering van gerubriceerde gegevens van de andere partij.
m. **„Derde",** elke internationale organisatie of staat, met inbegrip van rechtspersonen of natuurlijke personen onder zijn rechtsmacht, die geen partij is bij dit Verdrag.

Artikel 3

Bevoegde veiligheidsautoriteiten

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

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

Artikel 4

Rubriceringsniveaus

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

Voor de Republiek Finland	**Voor het Koninkrijk der Nederlanden**	**Equivalent in het Engels**[1)]
ERITTÄIN SALAINEN of YTTERST HEMLIG	Stg ZEER GEHEIM	TOP SECRET
SALAINEN of HEMLIG	Stg GEHEIM	SECRET
LUOTTAMUKSELLINEN of KONFIDENTIELL	Stg CONFIDENTIEEL	CONFIDENTIAL
KÄYTTÖ RAJOITETTU of BEGRÄNSAD TILLGÅNG	DEPARTEMENTAAL VERTROUWELIJK	RESTRICTED

1) Voor de toepassing van dit Verdrag wordt dit Engelse equivalent voor rubricering gebruikt. De officiële rubriceringen die voor het aanduiden van gerubriceerde gegevens zullen worden gebruikt zijn in het Fins/Zweeds en het Nederlands.

2. De partijen nemen alle passende maatregelen om te waarborgen dat de ontvangende partij alle gerubriceerde gegevens uit hoofde van dit Verdrag die zij ontvangen heeft van de verstrekkende partij, voorziet 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 partijen nemen alle passende maatregelen om te waarborgen dat de ontvangende partij het rubriceringsniveau van de ontvangen gerubriceerde gegevens uit hoofde van dit Verdrag niet wijzigt of intrekt zonder de schriftelijke goedkeuring van de partij van herkomst.

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

Artikel 5

Beveiliging van gerubriceerde gegevens

1. De partijen nemen alle passende maatregelen in overeenstemming met hun nationale wet- en regelgeving om de in dit Verdrag bedoelde gerubriceerde gegevens te beveiligen. Zij kennen aan dergelijke gegevens dezelfde beveiliging toe als aan hun eigen gegevens met een vergelijkbaar rubriceringsniveau. Elektronische overdracht van gerubriceerde gegevens in een onbeveiligd netwerk door de ontvangende partij zal plaatsvinden met gebruikmaking van cryptografische middelen.

2. De partijen verstrekken geen toegang tot gerubriceerde gegevens aan een derde zonder de voorafgaande schriftelijke toestemming van de partij van herkomst.

3. De toegang tot gerubriceerde gegevens wordt beperkt tot personen die van de gegevens op de hoogte moeten zijn (need to know), zijn geïnstrueerd over hun verantwoordelijkheden voor de bescherming van gerubriceerde gegevens, een geheimhoudingsverklaring hebben ondertekend en/of wettelijk tot geheimhouding verplicht zijn en in het bezit zijn van een veiligheidsmachtiging personeel van het overeenkomstige niveau of uit hoofde van hun functie gemachtigd zijn om toegang te hebben tot dergelijke gegevens, een en ander in overeenstemming met de nationale wet- en regelgeving.

4. Een veiligheidsmachtiging personeel is niet vereist voor toegang tot gerubriceerde gegevens met een rubriceringsniveau dat overeenkomt met “RESTRICTED” zoals vermeld in artikel 4 van dit Verdrag.

5. Gerubriceerde gegevens worden uitsluitend gebruikt voor het doel waarvoor zij zijn verstrekt.

Artikel 6

Veiligheidssamenwerking

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

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

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

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

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

Artikel 7

Gerubriceerde contracten

1. Op verzoek deelt de bevoegde veiligheidsautoriteit van de ontvangende partij de bevoegde veiligheidsautoriteit van de partij van herkomst mee of een voorgestelde opdrachtnemer die deelneemt aan precontractuele onderhandelingen over een gerubriceerd contract, een passende veiligheidsmachtiging bedrijfslocatie heeft gekregen die overeenstemt met het vereiste rubriceringsniveau.

2. Indien een partij of een opdrachtnemer onder haar rechtsmacht een gerubriceerd contract met een rubriceringsniveau dat overeenkomt met CONFIDENTIAL of hoger, zoals vermeld in artikel 4 van dit Verdrag, gunt aan een (onder)opdrachtnemer onder de rechtsmacht van de andere partij, dient zij eerst de schriftelijke bevestiging te verkrijgen van de andere partij dat aan deze opdrachtnemer een veiligheidsmachtiging bedrijfslocatie is toegekend.

3. In geval van een openbare aanbesteding kan de bevoegde veiligheidsautoriteit van de ontvangende partij de bevoegde veiligheidsautoriteit van de partij van herkomst de relevante certificaten van veiligheidsmachtiging bedrijfslocatie verstrekken zonder een formeel verzoek daartoe.

4. Een veiligheidsmachtiging bedrijfslocatie is niet vereist voor toegang tot gerubriceerde gegevens op het rubriceringsniveau dat overeenkomt met “RESTRICTED” zoals vermeld in artikel 4 van dit Verdrag.

5. Vertegenwoordigers van de bevoegde veiligheidsautoriteiten van de partijen kunnen elkaar bezoeken om de doeltreffendheid te beoordelen van de maatregelen die een opdrachtnemer heeft genomen ter bescherming van gerubriceerde gegevens die te maken hebben met een gerubriceerd contract.

6. Elk gerubriceerd contract dat in overeenstemming met dit Verdrag wordt gesloten dient veiligheidsvereisten te bevatten waarin de volgende aspecten vermeld staan:
a. een rubriceringsgids;
b. contactgegevens van de bevoegde veiligheidsautoriteiten die verantwoordelijk zijn voor het uitvoeren van het gerubriceerd contract en het toezicht op de beveiliging van gerubriceerde gegevens die betrekking hebben op het gerubriceerd contract;
c. wet- en regelgeving met betrekking tot de bescherming van gerubriceerde gegevens;
d. procedure en vereisten voor toegang tot gerubriceerde gegevens;
e. de omgang met en opslag van gerubriceerde gegevens;
f. vervoer en elektronische overdracht van gerubriceerde gegevens;
g. markeren van gerubriceerde gegevens;
h. verplichting om beveiligingsuitvoering te controleren en zijn bevoegde veiligheidsautoriteit in kennis te stellen van elk veiligheidsincident;
i. beveiliging van gerubriceerde gegevens na beëindiging van het gerubriceerd contract;
j. vernietigen of retourneren van gerubriceerde gegevens;
k. vrijgeven van gerubriceerde gegevens met betrekking tot het gerubriceerd contract.

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

8. 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 10 van dit Verdrag te zijn.

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

Artikel 8

Overdracht van gerubriceerde gegevens tussen de partijen

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

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

Artikel 9

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 de nationale wet- en regelgeving gemachtigd zijn toegang te hebben tot gerubriceerde gegevens met het rubriceringsniveau van de gerubriceerde gegevens die vertaald of gereproduceerd worden.

3. Vertalingen dienen te worden voorzien van een passende annotatie in de taal waarin zij zijn vertaald 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 in overeenstemming met haar nationale wet- en regelgeving vernietigd nadat de ontvangende partij ze niet meer nodig acht.

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

Artikel 10

Bezoeken

1. Bezoeken waarbij toegang tot gerubriceerde gegevens op het niveau “CONFIDENTIAL” of hoger zoals vermeld in artikel 4 van dit Verdrag vereist is, dienen vooraf schriftelijk te worden goedgekeurd door de respectieve bevoegde veiligheidsautoriteit, tenzij anderszins overeengekomen door de bevoegde veiligheidsautoriteiten.

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

autoriteit van de andere partij. In dringende gevallen kan de aanvraag voor een bezoek op een kortere termijn worden ingediend, mits hierover voorafgaand afstemming plaatsvindt tussen de bevoegde veiligheidsautoriteiten.

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, telefoon-/faxnummer, e-mailadres en contactpunt van de te bezoeken locatie;
g. van een datum en stempel voorziene handtekening van een vertegenwoordiger van de bevoegde veiligheidsautoriteit van de bezoeker.

4. De bevoegde veiligheidsautoriteiten kunnen een lijst overeenkomen van bezoekers die herhalingsbezoeken mogen afleggen. De bevoegde veiligheidsautoriteiten komen nadere details van de herhalingsbezoeken overeen. De geldigheidsduur van vergunningen voor herhalingsbezoeken mag echter niet meer dan twaalf (12) maanden bedragen.

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

Artikel 11

Veiligheidsincident

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

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

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

Artikel 12

Kosten

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

Artikel 13

Oplossing van geschillen

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

Artikel 14

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 15

Uitvoeringsregelingen

De bevoegde autoriteiten van de partijen kunnen uitvoeringsregelingen sluiten ingevolge dit Verdrag.

Artikel 16

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 en de Bijlage daarbij kunnen met wederzijdse instemming van de partijen worden gewijzigd. Elke partij kan op elk moment langs diplomatieke weg wijzigingen van dit Verdrag en de Bijlage daarbij 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.

6. Na de inwerkingtreding van dit Verdrag neemt het Koninkrijk der Nederlanden onverwijld maatregelen om het Verdrag te doen registreren door het Secretariaat van de Verenigde Naties overeenkomstig artikel 102 van het Handvest van de Verenigde Naties.

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

GEDAAN te 's-Gravenhage op 22 februari 2022 in twee oorspronkelijke exemplaren, in de Engelse taal.

Voor het Koninkrijk der Nederlanden,

SIMONE SMIT

Voor de Republiek Finland,

PÄIVI KAUKORANTA

Bijlage I

De bevoegde veiligheidsautoriteit van het Koninkrijk der Nederlanden is:

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

De bevoegde veiligheidsautoriteit van de Republiek Finland is:

De Nationale Veiligheidsautoriteit
Ministerie van Buitenlandse Zaken van Finland

D. PARLEMENT

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

G. INWERKINGTREDING

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

Uitgegeven de *eerste* maart 2022.

De Minister van Buitenlandse Zaken,

W.B. HOEKSTRA

trb-2022-20
ISSN 0920 - 2218
's-Gravenhage 2022