2 (2024) Nr. 1

TRACTATENBLAD

VAN HET

KONINKRIJK DER NEDERLANDEN

JAARGANG 2024 Nr. 25

A. TITEL

Verdrag tussen het Koninkrijk der Nederlanden en het Koninkrijk Zweden inzake de uitwisseling en wederzijdse beveiliging van gerubriceerde gegevens (met Bijlage); Stockholm, 18 januari 2024

Voor een overzicht van de verdragsgegevens, zie verdragsnummer 012029 in de Verdragenbank.

B. TEKST

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

The Kingdom of the Netherlands

and

The Kingdom of Sweden,

Hereinafter jointly referred to as "the Parties", and 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 and scope

1. 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.

2. 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:
a) "Classified Contract" means any legally enforceable agreement, including any pre-contractual negotiations, to be entered into by one of the Parties with a Contractor for the supply of goods, execution of works or provision of services, the performance of which requires or involves access or potential access to or the creation of Classified Information.
b) "Classified Information" means any information or material marked by a security classification by one of the Parties, the unauthorised disclosure or loss of which could cause varying degrees of damage or harm to the interests of one or both of the Parties.
c) "Competent Security Authority" means the Party's government authority/authorities 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 or individual with the capacity to enter into contracts.
e) "Facility Security Clearance" means the positive determination by a 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 services or official tasks.
g) "Originating Party" means the Party, under whose authority or supervision Classified Information has been created under this Agreement, in accordance with its national laws and regulations.
h) "Personnel Security Clearance" means the positive determination 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 a Contractor under its jurisdiction, which provides Classified Information to the Receiving Party under this Agreement.
j) "Receiving Party" means the Party or a Contractor under its jurisdiction, which receives Classified Information from the Providing Party under this Agreement.
k) "Security Incident" means an act or an omission, contrary to national laws and regulations, which results in the unauthorised access, disclosure, loss or compromise of Classified Information.
l) "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 changes thereof.

3. The Parties shall inform each other via diplomatic channels about changes in the Competent Security Authorities which require an amendment in the Annex.

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 Sweden
Stg. ZEER GEHEIM	KVALIFICERAT HEMLIG
Stg. GEHEIM	HEMLIG
Stg. CONFIDENTIEEL	KONFIDENTIELL
DEPARTEMENTAAL VERTROUWELIJK	BEGRÄNSAT HEMLIG

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 approval of the Originating Party.

Article 5

Access to Classified Information

1. Access to Classified Information at the security classification levels Stg. CONFIDENTIEEL/KONFIDENTIELL and above shall be granted only to those individuals who have a Need to know, have a Personnel Security Clearance at the corresponding level or who are otherwise duly authorized by virtue of their functions in accordance with national laws and regulations, are briefed on their responsibilities and have signed a statement of confidentiality or are bound by law to confidentiality.

2. Access to Classified Information at the security classification level DEPARTEMENTAAL VERTROUWELIJK/ BEGRÄNSAT HEMLIG 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 or are bound by law to confidentiality.

Article 6

Security measures

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

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

3. The Parties shall take all appropriate measures to ensure that the Receiving Party:
a) affords the same level of protection to Classified Information as afforded to its national Classified Information of an equivalent security classification level;
b) shall take all lawful steps to ensure that Classified Information is not disclosed or released to a Third Party without the prior written consent of the Originating Party;
c) ensures that Classified Information is marked with its own corresponding security classification level;
d) ensures that Classified Information is used solely for the purpose it has been released for and in accordance with handling requirements of the Originating Party.

4. Classified Information jointly originated by the Parties shall be assigned a security classification that is mutually determined by the Parties.

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 the purpose of protecting Classified Information.

2. On request by 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 of the Parties shall recognize Personnel Security Clearances and Facility Security Clearances issued in accordance with the national laws and regulations of the other Party.

4. 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.

5. 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.

6. In case the national laws and regulations of the Parties regarding public access to documents or access to information of public character have an impact on the information exchanged within the framework of this Agreement, the Competent Security Authorities shall inform each other.

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

Article 8

Classified Contracts

1. If a Party or a Contractor under its jurisdiction proposes to grant a Classified Contract at the security classification levels equivalent to "Stg. CONFIDENTIEEL/KONFIDENTIELL" or above as mentioned in article 4 of this Agreement, with a (sub-)Contractor under the jurisdiction of the other Party, it shall first obtain written

confirmation from the other Party that the Contractor has been granted a Facility Security Clearance and/or Personnel Security Clearance(s) at the appropriate security classification level. For Classified Contracts at the security classification level equivalent to "DEPARTEMENTAAL VERTROUWELIJK/BEGRÄNSAT HEMLIG" as mentioned in article 4 of this Agreement, a Facility Security Clearance may be required, if mandated by national laws and regulations of the Contractor.

2. Prior to the award of a Classified Contract, the Competent Security Authority shall ensure that the Contractor:
a) holds a Facility Security Clearance at the appropriate security classification level in order to protect the Classified Information and that the individuals requiring access to Classified Information hold a Personnel Security Clearance at the appropriate security classification level;
b) 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;
c) monitors the security conduct within its facilities;
d) promptly notifies its Competent Security Authority of any Security Incident relating to the Classified Contract.

3. A Classified Contract between legal entities of the Parties shall contain provisions on the security requirements and on the classification of each aspect or element of the Classified Contract. A copy of these provisions shall be submitted to the Competent Security Authorities of the Parties to enable security supervision. The Classified Contract should furthermore include the obligation to notify any Security Incidents, a reference to this Agreement as well as the obligation to impose all stipulations concerning Contractors in this Agreement to the sub-contractor.

4. Each Competent Security Authority may request that a security check is carried out at a facility under the jurisdiction of and by the other Party's Competent Security Authority to ensure continuing compliance with security standards according to this Agreement.

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

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

Article 9

Transmission of Classified Information

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

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

Article 10

Reproduction, translation and destruction of Classified Information

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

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

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

4. Classified Information marked at the security classification level Stg. ZEER GEHEIM/KVALIFICERAT HEMLIG shall not be translated or reproduced without the prior written consent of the Originating Party.

5. Classified Information marked at the security classification level Stg. ZEER GEHEIM/KVALIFICERAT HEMLIG shall not be destroyed without the prior written consent of the Originating Party. It shall be returned to the Originating Party after it is no longer considered necessary by the Receiving Party.

6. Classified Information marked up to and including the security classification levels Stg. GEHEIM/HEMLIG 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 Originating Party about the destruction of this Classified Information.

Article 11

Visits

1. Visits requiring access to Classified Information at a security classification level equivalent to Stg. CONFIDENTIEEL/KONFIDENTIELL or above as mentioned in article 4 of this Agreement 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 persons who have a Need to Know, have a Personal 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. If mandated by national laws and regulations of the host Party, DEPARTEMENTAAL VERTROUWELIJK/BEGRÄNSAT HEMLIG level visits may be subject to the prior written consent of the Competent Security Authority of the host Party.

2. The visitor shall submit the request for visit at least ten 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 number, e-mail address and point of contact of the facility to be visited;
g) date and 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 prior to 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. 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.

Article 15

Implementing arrangements

The Competent Security Authorities 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. On the date of entry into force of this Agreement, the Agreement between the Kingdom of the Netherlands and the Kingdom of Sweden on the Reciprocal Protection of Classified Military Information, concluded at The Hague on 29 October 1984 shall cease to be in force.

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. Each Party shall promptly notify the other Party of any changes to its laws and regulations that would affect the protection of Classified Information under this Agreement. In such case, the Parties shall consult to consider possible changes to this Agreement. In the meantime, Classified Information shall continue to be protected as described herein, unless requested otherwise by the Originating Party.

5. 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 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.

6. 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.

7. 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 Stockholm on 18 January 2024 in two original copies, each in the English, Dutch and Swedish language. In case of divergence of interpretation, the English text shall prevail.

For the Kingdom of the Netherlands,

BENGT VAN LOOSDRECHT

For the Kingdom of Sweden,

PÅL JONSON

Annex

1. The Competent Security Authority for the Kingdom of the Netherlands is:
   General Intelligence and Security Service
   Ministry of the Interior and Kingdom Relations
2. 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
3. The Competent Security Authorities for the Kingdom of Sweden are:
   a) The Swedish Armed Forces, Military Intelligence and Security Service (in respect of military matters)
   b) The Swedish Security Police (in respect of civilian matters)
   c) The Swedish Defence Materiel Administration (in respect of industrial security matters)

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

Het Koninkrijk der Nederlanden

en

het Koninkrijk Zweden,

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

Komen, teneinde de wederzijdse beveiliging van gerubriceerde gegevens te waarborgen, in het belang van de nationale veiligheid, 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 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 beveiligingsprocedures en regelingen voor deze beveiliging vastgelegd.

2. 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. „Gerubriceerd contract", elke wettelijk afdwingbare overeenkomst, met inbegrip van eventuele voorafgaande contractonderhandelingen, die een van de partijen aangaat met een opdrachtnemer voor de levering van goederen, uitvoering van werkzaamheden of levering van diensten, waarbij voor de uitvoering toegang of mogelijk toegang tot gerubriceerde gegevens vereist is of waarbij deze gecreëerd worden.
b. „Gerubriceerde gegevens", gegevens die of materiaal dat door een van de partijen als gerubriceerd worden of wordt aangemerkt, waarvan de ongeoorloofde bekendmaking of het verlies de belangen van een of beide partijen in meer of mindere mate zou kunnen schaden.
c. „Bevoegde beveiligingsautoriteit", de overheidsautoriteit/autoriteiten van een partij die verantwoordelijk

is/zijn voor de implementatie van en het toezicht op dit Verdrag. De bevoegde beveiligingsautoriteit kan een deel van zijn verantwoordelijkheden delegeren aan een gemachtigde bevoegde beveiligingsautoriteit.
d. „Opdrachtnemer" , elke rechtspersoon of elke natuurlijke persoon 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 diensten of officiële taken.
g. „Partij van herkomst", de partij onder wier gezag of toezicht gerubriceerde gegevens zijn gecreëerd uit hoofde van dit Verdrag, in overeenstemming met haar nationale wet- en regelgeving.
h. „Veiligheidsmachtiging personeel", de vaststelling 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 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. „Beveiligingsincident", 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.
l. „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 veranderingen daarvan.

3. De partijen informeren elkaar langs diplomatieke weg over veranderingen van de bevoegde beveiligingsautoriteiten die een wijziging van de Bijlage noodzakelijk maken.

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 Zweden
Stg. ZEER GEHEIM	KVALIFICERAT HEMLIG
Stg. GEHEIM	HEMLIG
Stg. CONFIDENTIEEL	KONFIDENTIELL
DEPARTEMENTAAL VERTROUWELIJK	BEGRÄNSAT HEMLIG

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 goedkeuring van de partij van herkomst.

Artikel 5

Toegang tot gerubriceerde gegevens

1. Toegang tot gerubriceerde gegevens op het rubriceringsniveaus Stg. CONFIDENTIEEL/KONFIDENTIELL en hoger wordt uitsluitend verleend aan de natuurlijke personen die van de gegevens op de hoogte moeten zijn (need to know), een veiligheidsmachtiging personeel hebben op het overeenkomstige niveau of die anderszins gemachtigd zijn om toegang te krijgen tot dergelijke gegevens in overeenstemming met de nationale wet- en regelgeving, zijn ingelicht over hun verantwoordelijkheden en een geheimhoudingsverklaring hebben ondertekend of wettelijk tot geheimhouding verplicht zijn.

2. Toegang tot gerubriceerde gegevens op het niveau DEPARTEMENTAAL VERTROUWELIJK/BEGRÄNSAT HEMLIG 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 of wettelijk tot geheimhouding verplicht zijn.

Artikel 6

Beveiligingsmaatregelen

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

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

3. De partijen nemen alle passende maatregelen om te waarborgen dat de ontvangende partij:
a. hetzelfde beveiligingsniveau aan gerubriceerde gegevens toekent als aan haar nationale gerubriceerde gegevens met een vergelijkbaar rubriceringsniveau;
b. alle wettige stappen neemt om te waarborgen dat gerubriceerde gegevens niet bekend worden gemaakt of vrijgegeven aan een derde zonder de voorafgaande schriftelijke toestemming van de partij van herkomst;
c. waarborgt dat gerubriceerde gegevens worden voorzien van haar eigen dienovereenkomstige rubriceringsniveau;
d. waarborgt dat gerubriceerde gegevens uitsluitend worden gebruikt voor het doel waarvoor zij zijn verstrekt en in overeenstemming met de eisen voor gebruik van de partij van herkomst.

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

Artikel 7

Beveiligingssamenwerking

1. Teneinde vergelijkbare beveiligingsnormen te handhaven, verstrekken de bevoegde beveiligingsautoriteiten elkaar op verzoek informatie over hun beveiligingsvoorschriften, -beleid en -praktijken met het oog op het beveiligen 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 van de partijen erkennen de veiligheidsmachtigingen personeel en veiligheidsmachtigingen bedrijfslocatie die overeenkomstig de nationale wet- en regelgeving van de andere partij zijn afgegeven.

4. 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.

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

6. In het geval dat de nationale wet- en regelgeving van de partijen inzake publieke toegang tot documenten of toegang tot informatie met een openbaar karakter van invloed zijn op de gegevens die worden uitgewisseld in het kader van dit Verdrag, stellen de bevoegde beveiligingsautoriteiten elkaar in kennis.

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

Artikel 8

Gerubriceerde contracten

1. Indien een partij of een opdrachtnemer onder haar rechtsmacht voorstelt een gerubriceerd contract met een rubriceringsniveau dat overeenkomt met „Stg. CONFIDENTIEEL/ KONFIDENTIELL" of hoger, zoals vermeld in artikel 4 van dit Verdrag toe te kennen aan een (onder-)opdrachtnemer onder de rechtsmacht van de andere partij, dient zij eerst de schriftelijke bevestiging te verkrijgen van de andere partij dat aan deze opdrachtnemer een veiligheidsmachtiging bedrijfslocatie en/of veiligheidsmachtiging personeel is/zijn toegekend op het vereiste rubriceringsniveau. Voor gerubriceerde contracten met het rubriceringsniveau dat overeenkomt met DEPARTEMENTAAL VERTROUWELIJK / BEGRÄNSAT HEMLIG" zoals vermeld in artikel 4 van dit Verdrag, kan een veiligheidsmachtiging bedrijfslocatie vereist zijn indien dit verplicht wordt gesteld in de nationale wet- en regelgeving van de opdrachtnemer.

2. Voorafgaand aan de toekenning van een gerubriceerd contract waarborgt de bevoegde beveiligingsautoriteit dat de opdrachtnemer:
a. een veiligheidsmachtiging bedrijfslocatie bezit met het juiste rubriceringsniveau teneinde de gerubriceerde gegevens te beveiligen en dat de natuurlijke personen die toegang dienen te krijgen tot gerubriceerde gegevens, een veiligheidsmachtiging personeel met het juiste rubriceringsniveau hebben;
b. 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;
c. de beveiligingsuitvoering op zijn locaties in het oog houdt;
d. zijn bevoegde beveiligingsautoriteit onverwijld in kennis stelt van elk beveiligingsincident dat betrekking heeft op het gerubriceerd contract.

3. Een gerubriceerd contract tussen rechtspersonen van de partijen bevat bepalingen inzake beveiligingsvereisten en inzake de rubricering van elk aspect of onderdeel van het gerubriceerd contract. Een kopie van deze bepalingen wordt aan de bevoegde beveiligingsautoriteiten van de partijen gezonden om toezicht op de beveiliging mogelijk te maken. In het gerubriceerd contract dienen verder de verplichting beveiligingsincidenten te melden, een verwijzing naar dit Verdrag en de verplichting om alle bepalingen in dit Verdrag die betrekking hebben op opdrachtnemers ook op onderaannemers toe te passen te zijn opgenomen.

4. Elke bevoegde beveiligingsautoriteit kan verzoeken dat er een beveiligingscontrole wordt uitgevoerd op een faciliteit onder de rechtsmacht van de andere partij door de bevoegde beveiligingsautoriteit van die partij om de blijvende naleving van de beveiligingsvereisten in overeenkomst met dit Verdrag te waarborgen.

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

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

Artikel 9

Overbrenging van Gerubriceerde Gegevens

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

2. De partijen kunnen gerubriceerde gegevens die door encryptie beveiligd zijn langs elektronische weg overbrengen in overeenstemming met procedures die door de 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 de nationale wet- en regelgeving 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 partij van herkomst.

4. Gerubriceerde gegevens op rubriceringsniveau Stg. ZEER GEHEIM/ KVALIFICERAT HEMLIG worden niet vertaald of gereproduceerd zonder de voorafgaande schriftelijke toestemming van de partij van herkomst.

5. Gerubriceerde gegevens op rubriceringsniveau Stg. ZEER GEHEIM/ KVALIFICERAT HEMLIG worden niet vernietigd zonder de voorafgaande schriftelijke toestemming van de partij van herkomst. Zij worden geretourneerd aan de partij van herkomst nadat de ontvangende partij ze niet meer nodig acht.

6. Gerubriceerde gegevens tot en met rubriceringsniveau Stg. GEHEIM/HEMLIG 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 beveiligingsautoriteit van de partij van herkomst onverwijld in kennis van de vernietiging van deze gerubriceerde gegevens.

Artikel 11

Bezoeken

1. Bezoeken waarbij toegang tot gerubriceerde gegevens op het niveau Stg. CONFIDENTIEEL/ KONFIDENTIELL of hoger zoals vermeld in artikel 4 van dit Verdrag 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. Deze goedkeuring wordt uitsluitend verleend aan de natuurlijke personen die van de gegevens op de hoogte moeten zijn (need to know), die 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. Indien dit verplicht is volgens de nationale wet- en regelgeving van de als gastheer optredende partij kunnen bezoeken op het niveau DEPARTEMENTAAL VERTROUWELIJK/ BEGRÄNSAT HEMLIG onderworpen zijn aan voorafgaande schriftelijke toestemming van de bevoegde beveiligingsautoriteit van de als gastheer optredende partij.

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 kan de aanvraag van een verzoek binnen een kortere termijn worden ingediend, mits hierover voorafgaande afstemming 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. datum en 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 autoriteit 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 herhalingen 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 interpretatie of toepassing van dit Verdrag wordt uitsluitend opgelost door middel van onderhandelingen tussen de partijen.

Artikel 15

Uitvoeringsregelingen

De bevoegde beveiligingsautoriteiten 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. Op de datum waarop dit Verdrag in werking treedt, houdt de Overeenkomst tussen het Koninkrijk der Nederlanden en het Koninkrijk Zweden inzake de wederzijdse bescherming van geclassificeerde militaire gegevens, gesloten te Den Haag op 29 oktober 1984, op van kracht te zijn.

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. Elke partij stelt de andere partij onverwijld in kennis van wijzigingen van haar wet- en regelgeving die van invloed zouden zijn op de beveiliging van gerubriceerde gegevens uit hoofde van dit Verdrag. In dat geval bespreken de partijen mogelijke wijzigingen van dit Verdrag. In de tussentijd blijven gerubriceerde gegevens beveiligd zoals hierin beschreven, tenzij de partij van herkomst anderszins verzoekt.

5. 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 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, en de wijziging treedt in werking op een door de partijen overeen te komen datum.

6. 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.

7. 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 Stockholm op 18 januari 2024 in twee oorspronkelijke exemplaren, elk in de Engelse, de Nederlandse en de Zweedse taal. In geval van verschil in interpretatie is de Engelse tekst doorslaggevend.

Voor het Koninkrijk der Nederlanden,

BENGT VAN LOOSDRECHT

Voor het Koninkrijk Zweden,

PÅL JONSON

Bijlage

1. De bevoegde beveiligingsautoriteit van het Koninkrijk der Nederlanden is:
   De Algemene Inlichtingen- en Veiligheidsdienst (AIVD)
   Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
2. De gemachtigde bevoegde beveiligingsautoriteit van het Koninkrijk der Nederlanden voor het militaire domein is:
   De Beveiligingsautoriteit
   Directoraat-Generaal Beleid
   Ministerie van Defensie
3. De bevoegde beveiligingsautoriteiten van het Koninkrijk Zweden zijn:
   a. De Militaire Inlichtingen- en Veiligheidsdienst van de Zweedse strijdkrachten (wat betreft militaire zaken)
   b. De Zweedse Veiligheidspolitie (wat betreft civiele zaken)
   c. De Zweedse Administratie Defensiematerieel (wat betreft industriële beveiliging)

Avtal mellan Konungariket Nederländerna och Konungariket Sverige om utbyte och ömsesidigt skydd av säkerhetsskyddsklassificerade uppgifter

Konungariket Nederländerna

och

Konungariket Sverige,

Nedan tillsammans kallade *parterna* och var för sig *part*,

har, i syfte att säkerställa ömsesidigt skydd av säkerhetsskyddsklassificerade uppgifter och med hänsyn till nationell säkerhet, kommit överens om följande:

Artikel 1

Syfte och tillämpningsområde

1. Syftet med detta avtal är att säkerställa skydd av säkerhetsskyddsklassificerade uppgifter som utbyts mellan parterna och mellan juridiska eller fysiska personer under deras respektive jurisdiktion eller som genereras inom ramen för ett bilateralt samarbete enligt detta avtal. I avtalet fastställs säkerhetsrutiner och säkerhetsarrangemang för sådant skydd.

2. Detta avtal utgör ingen grund för att tvinga parterna att tillhandahålla eller utbyta säkerhetsskyddsklassificerade uppgifter.

Artikel 2

Definitioner

I detta avtal gäller följande definitioner:
a) *säkerhetsskyddsklassificerat kontrakt:* juridiskt bindande avtal, inklusive förhandlingar inför det, som en av parterna ingår med en uppdragstagare för leverans av varor, utförande av byggentreprenad eller tillhandahållande av tjänster som kräver eller innebär tillgång eller möjlig tillgång till eller generering av säkerhetsskyddsklassificerade uppgifter.
b) *säkerhetsskyddsklassificerade uppgifter:* uppgifter eller material som endera parten försett med en säkerhetsskyddsklassificering och vars obehöriga röjande eller förlust i olika utsträckning skulle kunna medföra skada för den ena eller båda parternas intressen.
c) *behörig säkerhetsmyndighet:* den eller de av partens statliga myndigheter som ansvarar för genomförande av och tillsyn över detta avtal. Den behöriga säkerhetsmyndigheten får delegera en del av sitt ansvar till en delegerad behörig säkerhetsmyndighet.
d) *uppdragstagare:* juridisk eller fysisk person som har rättslig förmåga att ingå avtal.
e) *säkerhetsgodkännande av verksamhetsställe:* positivt beslut av en behörig säkerhetsmyndighet om att ett verksamhetsställe har vidtagit tillräckliga säkerhetsskyddsåtgärder för att få tillgång till och hantera säkerhetsskyddsklassificerade uppgifter upp till och med en viss säkerhetsskyddsklass, i enlighet med nationella lagar och andra författningar.
f) *behovsenlig behörighet:* det som krävs för att en fysisk eller juridisk person ska få tillgång till, få kännedom om eller få inneha säkerhetsskyddsklassificerade uppgifter för att tillhandahålla tjänster eller utföra tjänsteuppgifter.
g) *ursprungspart:* den part under vars ansvar eller tillsyn säkerhetsskyddsklassificerade uppgifter har genererats inom ramen för detta avtal i enlighet med partens nationella lagar och andra författningar.
h) *personalsäkerhetsgodkännande:* positivt beslut om att en fysisk person har blivit godkänd från säkerhetssynpunkt att få tillgång till och hantera säkerhetsskyddsklassificerade uppgifter upp till och med en viss säkerhetsskyddsklass, i enlighet med nationella lagar och andra författningar.
i) *tillhandahållande part:* den part, eller en uppdragstagare under dess jurisdiktion, som tillhandahåller den mottagande parten säkerhetsskyddsklassificerade uppgifter inom ramen för detta avtal,
j) *mottagande part:* den part, eller en uppdragstagare under dess jurisdiktion, som tar emot säkerhetsskyddsklassificerade uppgifter från den tillhandahållande parten inom ramen för detta avtal.
k) *säkerhetsskyddsincident:* handling eller underlåtenhet som strider mot nationella lagar eller andra författningar och som leder till obehörig tillgång till eller röjande, förlust eller kompromettering av säkerhetsskyddsklassificerade uppgifter.
l) *tredje part:* internationell organisation eller stat, inklusive juridiska eller fysiska personer under dess jurisdiktion, som inte är part i detta avtal.

Artikel 3

Behöriga säkerhetsmyndigheter

1. Parternas behöriga säkerhetsmyndigheter anges i bilagan till detta avtal.

2. De behöriga säkerhetsmyndigheterna ska meddela varandra sina officiella kontaktuppgifter och ändringar av dessa.

3. Parterna ska på diplomatisk väg underrätta varandra om sådana ändringar av de behöriga säkerhetsmyndigheterna som kräver en ändring i bilagan.

Artikel 4

Säkerhetsskyddsklasser

1. Parternas följande säkerhetsskyddsklasser motsvarar varandra och är de säkerhetsskyddsklasser som anges i deras respektive nationella lagstiftning:

För Konungariket Nederländerna	För Konungariket Sverige
Stg. ZEER GEHEIM	KVALIFICERAT HEMLIG
Stg. GEHEIM	HEMLIG
Stg. CONFIDENTIEEL	KONFIDENTIELL
DEPARTEMENTAAL VERTROUWELIJK	BEGRÄNSAT HEMLIG

2. Den mottagande parten ska förse alla säkerhetsskyddsklassificerade uppgifter som omfattas av detta avtal och som den mottagit från den tillhandahållande parten med en anteckning om den säkerhetsskyddsklass som enligt tabellen i punkt 1 i denna artikel motsvarar den säkerhetsskyddsklass som angetts av ursprungsparten.

3. Den mottagande parten får inte utan skriftligt godkännande från urspungsparten ändra eller häva säkerhetsskyddsklassificeringen av säkerhetsskyddsklassificerade uppgifter som den mottagit inom ramen för detta avtal.

Artikel 5

Tillgång till säkerhetsskyddsklassificerade uppgifter

1. Tillgång till säkerhetsskyddsklassificerade uppgifter i säkerhetsskyddsklass Stg. CONFIDENTIEEL/ KONFIDENTIELL och högre får endast ges till enskilda personer som har behovsenlig behörighet eller ett personalsäkerhetsgodkännande på motsvarande nivå eller som på annat sätt i kraft av sina arbetsuppgifter är vederbörligen bemyndigade i enlighet med nationella lagar och andra författningar, har informerats om sina skyldigheter och har undertecknat en försäkran om tystnadsplikt eller enligt lag har tystnadsplikt.

2. Tillgång till säkerhetsskyddsklassificerade uppgifter i säkerhetsskyddsklass DEPARTEMENTAAL VERTROUWELIJK/ BEGRÄNSAT HEMLIG får endast ges till enskilda personer som har behovsenlig behörighet, har informerats om sina skyldigheter och har undertecknat en försäkran om tystnadsplikt eller enligt lag har tystnadsplikt.

Artikel 6

Säkerhetsskyddsåtgärder

1. Parterna ska vidta alla lämpliga åtgärder som är tillämpliga enligt deras respektive nationella lagar och andra författningar för att skydda säkerhetsskyddsklassificerade uppgifter som genereras och/eller tillhandahålls inom ramen för detta avtal.

2. Parterna ska vidta alla lämpliga åtgärder för att säkerställa att den tillhandahållande parten
a) förser de säkerhetsskyddsklassificerade uppgifterna med lämplig anteckning om säkerhetsskyddsklass i enlighet med sina nationella lagar och andra författningar,
b) informerar den mottagande parten om eventuella villkor för utlämnande eller begränsningar av användningen av de tillhandahållna säkerhetsskyddsklassificerade uppgifterna,
c) informerar den mottagande parten om eventuella senare ändringar av säkerhetsskyddsklassen på de tillhandahållna säkerhetsskyddsklassificerade uppgifterna.

3. Parterna ska vidta alla lämpliga åtgärder för att säkerställa att den mottagande parten
a) ger de säkerhetsskyddsklassificerade uppgifterna samma skydd som den ger sina nationella säkerhetsskyddsklassificerade uppgifter i motsvarande säkerhetsskyddsklass,
b) vidtar alla lagliga åtgärder för att säkerställa att de säkerhetsskyddsklassificerade uppgifterna inte röjs eller lämnas ut till en tredje part utan föregående skriftligt medgivande från ursprungsparten,
c) säkerställer att de säkerhetsskyddsklassificerade uppgifterna förses med en anteckning om den mottagande partens motsvarande säkerhetsskyddsklass,
d) säkerställer att de säkerhetsskyddsklassificerade uppgifterna endast används för det ändamål som de lämnats ut för och i enlighet med ursprungspartens villkor för hantering.

4. Säkerhetsskyddsklassificerade uppgifter som har sitt ursprung hos båda parterna ska delas in i en säkerhetsskyddsklass som parterna gemensamt kommer överens om.

Artikel 7

Säkerhetssamarbete

1. I syfte att upprätthålla ett jämförbart säkerhetsskydd ska de behöriga säkerhetsmyndigheterna på begäran informera varandra om sina säkerhetsbestämmelser, säkerhetsföreskrifter och säkerhetsförfaranden för skydd av säkerhetsskyddsklassificerade uppgifter.

2. På begäran av endera partens behöriga säkerhetsmyndighet ska den andra partens behöriga säkerhetsmyndighet skriftligen bekräfta att ett giltigt personalsäkerhetsgodkännande eller säkerhetsgodkännande av verksamhetsställe har utfärdats.

3. Parternas behöriga säkerhetsmyndigheter ska erkänna personalsäkerhetsgodkännanden och säkerhetsgodkännanden av verksamhetsställen som utfärdats i enlighet med den andra partens nationella lagar och andra författningar.

4. De behöriga säkerhetsmyndigheterna ska på begäran och i enlighet med nationella lagar och andra författningar hjälpa varandra att göra prövningar för säkerhetsgodkännanden av verksamhetsställen och personalsäkerhetsgodkännanden.

5. De behöriga säkerhetsmyndigheterna ska utan dröjsmål skriftligen underrätta varandra om ändringar av erkända personalsäkerhetsgodkännanden och säkerhetsgodkännanden av verksamhetsställen för vilka en bekräftelse har lämnats.

6. Om parternas nationella lagar och andra författningar som rör allmänhetens rätt att ta del av handlingar eller offentliga uppgifter påverkar de uppgifter som utbyts inom ramen för detta avtal ska de behöriga säkerhetsmyndigheterna informera varandra om detta.

7. Samarbetet inom ramen för detta avtal ska bedrivas på engelska.

Artikel 8

Säkerhetsskyddsklassificerade kontrakt

1. Om en part eller en uppdragstagare under dess jurisdiktion avser att tilldela en uppdragstagare (eller underleverantör) under den andra partens jurisdiktion ett säkerhetsskyddsklassificerat kontrakt i en säkerhetsskyddsklass som motsvarar Stg. CONFIDENTIEEL/ KONFIDENTIELL eller högre i enlighet med vad som anges i artikel 4 i detta avtal, ska den först inhämta en skriftlig bekräftelse från den andra parten om att uppdragstagaren (eller underleverantören) har fått ett säkerhetsgodkännande av verksamhetsställe och/eller ett eller flera personalsäkerhetsgodkännanden för lämplig säkerhetsskyddsklass. För säkerhetsskyddsklassificerade kontrakt i den säkerhetsskyddsklass som motsvarar DEPARTEMENTAAL VERTROUWELIJK/ BEGRÄNSAT HEMLIG i enlighet med vad som anges i artikel 4 i detta avtal kan ett säkerhetsgodkännande av verksamhetsställe begäras om det krävs enligt uppdragstagarens nationella lagar och andra författningar.

2. Före tilldelningen av ett säkerhetsskyddsklassificerat kontrakt ska den behöriga säkerhetsmyndigheten säkerställa att uppdragstagaren
a) innehar ett säkerhetsgodkännande av verksamhetsställe för lämplig säkerhetsskyddsklass för att skydda de säkerhetsskyddsklassificerade uppgifterna och att de enskilda personer som behöver tillgång till säkerhetsskyddsklassificerade uppgifter innehar ett personalsäkerhetsgodkännande för lämplig säkerhetsskyddsklass,
b) säkerställer att alla enskilda personer som ges tillgång till säkerhetsskyddsklassificerade uppgifter informeras om sin skyldighet att skydda de säkerhetsskyddsklassificerade uppgifterna i enlighet med de villkor som anges i detta avtal och med nationella lagar och andra författningar,
c) övervakar säkerheten på sina verksamhetsställen,
d) utan dröjsmål underrättar sin behöriga säkerhetsmyndighet om alla eventuella säkerhetsskyddsincidenter som rör det säkerhetsskyddsklassificerade kontraktet.

3. Ett säkerhetsskyddsklassificerat kontrakt mellan juridiska personer under parternas jurisdiktion ska innehålla bestämmelser om säkerhetsskyddskraven för och säkerhetsskyddsklassificeringen av varje aspekt eller beståndsdel av det säkerhetsskyddsklassificerade kontraktet. En kopia av dessa bestämmelser ska lämnas in till parternas behöriga säkerhetsmyndigheter så att tillsyn kan utövas över säkerhetsskyddet. Det säkerhetsskyddsklassificerade kontraktet bör också inkludera skyldigheten att rapportera eventuella säkerhetsskyddsincidenter, en hänvisning till detta avtal och skyldigheten att tillämpa alla bestämmelser i detta avtal som avser uppdragstagaren även på underleverantören.

4. Varje behörig säkerhetsmyndighet får begära att den andra partens behöriga säkerhetsmyndighet genomför en säkerhetsskyddskontroll på ett verksamhetsställe under sin jurisdiktion för att säkerställa att säkerhetsskyddskraven i detta avtal kontinuerligt efterlevs.

5. Förfarandena för att godkänna besök som rör verksamhet kopplad till säkerhetsskyddsklassificerade kontrakt och som den ena partens personal gör hos den andra parten ska överensstämma med artikel 11 i detta avtal.

6. Om en uppdragstagare lägger ut delar av ett säkerhetsskyddsklassificerat kontrakt på en underleverantör ska uppdragstagaren och underleverantören säkerställa att denna artikel följs.

Artikel 9

Överföring av säkerhetsskyddsklassificerade uppgifter

1. Säkerhetsskyddsklassificerade uppgifter ska överföras i enlighet med den tillhandahållande partens nationella lagar och andra författningar eller på annat sätt som de behöriga säkerhetsmyndigheterna kommit överens om.

2. Parterna får på elektronisk väg överföra säkerhetsskyddsklassificerade uppgifter som skyddas med kryptering i enlighet med förfaranden som ska godkännas av de behöriga säkerhetsmyndigheterna.

Artikel 10

Återgivning, översättning och förstöring av säkerhetsskyddsklassificerade uppgifter

1. Återgivningar och översättningar av säkerhetsskyddsklassificerade uppgifter ska förses med anteckning och ges samma skydd som de ursprungliga säkerhetsskyddsklassificerade uppgifterna.

2. Översättningar och återgivningar ska begränsas till det minimum som krävs för användning inom ramen för detta avtal och får endast göras av enskilda personer som i enlighet med nationella lagar och andra författningar är behöriga att få tillgång till säkerhetsskyddsklassificerade uppgifter i den säkerhetsskyddsklass som gäller för de säkerhetsskyddsklassificerade uppgifter som översätts eller återges.

3. Översättningar ska innehålla en lämplig förklarande not på det språk som de har översatts till om att de innehåller säkerhetsskyddsklassificerade uppgifter från ursprungsparten.

4. Säkerhetsskyddsklassificerade uppgifter med markeringen Stg. ZEER GEHEIM/ KVALIFICERAT HEMLIG får inte översättas eller återges utan föregående skriftligt medgivande från ursprungsparten.

5. Säkerhetsskyddsklassificerade uppgifter med markeringen Stg. ZEER GEHEIM/ KVALIFICERAT HEMLIG får inte förstöras utan föregående skriftligt medgivande från ursprungsparten. De ska återsändas till ursprungsparten när den mottagande parten inte längre anser sig behöva dem.

6. Säkerhetsskyddsklassificerade uppgifter med markeringen Stg. GEHEIM/ HEMLIG eller lägre ska förstöras i enlighet med den mottagande partens nationella lagar och andra författningar när den mottagande parten inte längre anser sig behöva dem.

7. Om en krissituation gör det omöjligt att skydda säkerhetsskyddsklassificerade uppgifter som tillhandahållits inom ramen för detta avtal ska de säkerhetsskyddsklassificerade uppgifterna omedelbart förstöras. Den mottagande parten ska utan dröjsmål skriftligen meddela ursprungspartens behöriga säkerhetsmyndighet om förstöringen av de säkerhetsskyddsklassificerade uppgifterna.

Artikel 11

Besök

1. För besök som kräver tillgång till säkerhetsskyddsklassificerade uppgifter i säkerhetsskyddsklass Stg. CONFIDENTIEEL/ KONFIDENTIELL eller högre i enlighet med vad som anges i artikel 4 i detta avtal krävs föregående skriftligt medgivande från värdpartens behöriga säkerhetsmyndighet, såvida de behöriga säkerhetsmyndigheterna inte har kommit överens om annat. Sådant medgivande får endast lämnas till personer som har behovsenlig behörighet, innehar ett personalsäkerhetsgodkännande på motsvarande nivå eller som på annat sätt i kraft av sina arbetsuppgifter är vederbörligen bemyndigade, i enlighet med den mottagande partens nationella lagar och andra författningar. Om värdpartens nationella lagar och andra författningar kräver det kan besök på nivån DEPARTEMENTAAL VERTROUWELIJK/ BEGRÄNSAT HEMLIG kräva föregående skriftligt medgivande från värdpartens behöriga säkerhetsmyndighet.

2. Besökaren ska minst tio dagar innan det föreslagna datumet för besöket lämna in framställningen om besök till sin behöriga säkerhetsmyndighet, som ska vidarebefordra den till den andra partens behöriga säkerhetsmyndighet. I brådskande fall får framställan om besök lämnas in med kortare varsel, under förutsättning att samordning först sker mellan de behöriga säkerhetsmyndigheterna.

3. Framställningar om besök ska innehålla
a) besökarens fullständiga namn, födelsedatum och födelseort, medborgarskap och pass- eller id-kortsnummer,
b) besökarens officiella titel och namnet på den organisation som besökaren företräder,
c) bekräftelse på besökarens personalsäkerhetsgodkännande och dess giltighet,

d) besökets tidpunkt och längd; för återkommande besök ska den totala tidsperiod som besöken omfattar anges,
e) ändamålet med besöket och förväntad säkerhetsskyddsklass på de säkerhetsskyddsklassificerade uppgifter som ska diskuteras eller som det ska ges tillgång till,
f) namn, adress, telefonnummer, e-postadress och kontaktpunkt avseende det verksamhetsställe som ska besökas,
g) datum och underskrift från en företrädare för besökarens behöriga säkerhetsmyndighet.

4. De behöriga säkerhetsmyndigheterna kan komma överens om en förteckning över besökare som får göra återkommande besök. De behöriga säkerhetsmyndigheterna ska komma överens om närmare bestämmelser för återkommande besök.

5. Säkerhetsskyddsklassificerade uppgifter som en besökare tillhandahålls eller får del av ska hanteras i enlighet med bestämmelserna i detta avtal.

6. Parternas officiella företrädare får delta i säkerhetsskyddsklassificerade möten om de uppvisar bevis på sitt personalsäkerhetsgodkännande för mötesarrangören eller sekretariatet innan mötet.

Artikel 12

Säkerhetsskyddsincidenter

1. De behöriga säkerhetsmyndigheterna ska omedelbart skriftligen underrätta varandra om alla faktiska eller misstänkta säkerhetsskyddsincidenter som rör den andra partens säkerhetsskyddsklassificerade uppgifter.

2. Den mottagande parten ska omedelbart utreda alla faktiska eller misstänkta säkerhetsskyddsincidenter. Ursprungspartens behöriga säkerhetsmyndighet ska om så krävs medverka i utredningen.

3. Den mottagande partens behöriga säkerhetsmyndighet ska vidta lämpliga åtgärder i enlighet med sina nationella lagar och andra författningar för att begränsa konsekvenserna av säkerhetsskyddsincidenten och för att förhindra att den inträffar igen. Ursprungspartens behöriga säkerhetsmyndighet ska informeras om resultatet av utredningen och om eventuella åtgärder som vidtagits.

Artikel 13

Kostnader

Vardera parten ska stå för sina egna kostnader som den ådragit sig i samband med fullgörandet av sina skyldigheter enligt detta avtal.

Artikel 14

Tvistlösning

Eventuella tvister i fråga om tolkningen eller tillämpningen av detta avtal ska lösas uteslutande genom förhandling mellan parterna.

Artikel 15

Genomförandebestämmelser

De behöriga säkerhetsmyndigheterna får fastställa genomförandebestämmelser till detta avtal.

Artikel 16

Slutbestämmelser

1. Detta avtal ingås på obestämd tid. Vardera parten ska på diplomatisk väg meddela den andra parten när de nationella förfaranden som krävs för att detta avtal ska träda i kraft är slutförda. Avtalet träder i kraft den första dagen i den andra månaden efter att det sista meddelandet mottogs.

2. Överenskommelsen mellan Konungariket Nederländerna och Konungariket Sverige om ömsesidigt skydd av sekretessbelagd militär information, som ingicks i Haag den 29 oktober 1984, upphör att gälla den dag då det här avtalet träder i kraft.

3. Vad gäller Konungariket Nederländerna är detta avtal tillämpligt på den europeiska delen av Nederländerna och den karibiska delen av Nederländerna (öarna Bonaire, Sint Eustatius och Saba).

4. Vardera parten ska utan dröjsmål underrätta den andra parten om alla eventuella ändringar i sina lagar och andra författningar som skulle påverka skyddet av säkerhetsskyddsklassificerade uppgifter inom ramen för detta avtal. Parterna ska i sådana fall samråda för att överväga eventuella ändringar av detta avtal. De säkerhetsskyddsklassificerade uppgifterna ska under tiden fortsätta att vara skyddade i enlighet med detta avtal såvida inte annat begärs av ursprungsparten.

5. Detta avtal och bilagan till det får ändras med parternas ömsesidiga medgivande. Endera parten får när som helst på diplomatisk väg föreslå ändringar av detta avtal. Sådana ändringar träder i kraft i enlighet med villkoren i punkt 1 i denna artikel, med undantag för ändringar av bilagan, vilka träder i kraft den dag som parterna kommer överens om.

6. Endera parten får när som helst skriftligen säga upp detta avtal på diplomatisk väg. I sådant fall upphör avtalet att gälla sex månader efter att ett meddelande om detta mottagits.

7. Även om detta avtal sägs upp ska alla säkerhetsskyddsklassificerade uppgifter som lämnats ut eller genererats inom ramen för detta avtal skyddas i enlighet med detta avtal så länge de är säkerhetsskyddsklassificerade.

Till bekräftelse härav har parternas företrädare, därtill vederbörligen bemyndigade, undertecknat detta avtal.

Upprättat i Stockholm den 18 januari 2024 i två original på engelska, nederländska och svenska. Vid skiljaktiga tolkningar ska den engelska texten gälla.

För Konungariket Nederländerna,

BENGT VAN LOOSDRECHT

För Konungariket Sverige,

PÅL JONSON

Biliga

1. Konungariket Nederländernas behöriga säkerhetsmyndighet är
   Nederländernas underrättelse- och säkerhetstjänst (Algemene Inlichtingen- en Veiligheidsdienst, AIVD)
   Nederländernas ministerium för inrikes frågor och konungarikets inre förbindelser (Ministerie van Binnenlandse Zaken en Koninkrijksrelaties).
2. Den delegerade behöriga säkerhetsmyndigheten för Konungariket Nederländerna på det militära området är
   Nederländernas försvarssäkerhetsmyndighet (Beveiligingsautoriteit)
   Generaldirektoratet för politik (Directoraat-Generaal Beleid)
   Nederländernas försvarsministerium (Ministerie van Defensie).
3. Konungariket Sveriges behöriga säkerhetsmyndigheter är
   a) Militära underrättelse- och säkerhetstjänsten vid Försvarsmakten (när det gäller militära frågor),
   b) Säkerhetspolisen (när det gäller civila frågor),
   c) Försvarets materielverk (när det gäller industrisäkerhetsfrågor).

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, 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 *veertiende* februari 2024.

De Minister van Buitenlandse Zaken,

H.G.J. BRUINS SLOT

trb-2024-25
ISSN 0920 - 2218
's-Gravenhage 2024