2 (2023) Nr. 1

TRACTATENBLAD

VAN HET

KONINKRIJK DER NEDERLANDEN

JAARGANG 2023 Nr. 18

A. TITEL

Verdrag tussen het Koninkrijk der Nederlanden en de Republiek Polen inzake de uitwisseling en wederzijdse beveiliging van gerubriceerde gegevens (met Bijlage); Warschau, 10 februari 2023

Voor een overzicht van de verdragsgegevens, zie verdragsnummer 012024 in de Verdragenbank.

B. TEKST[1)]

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

The Kingdom of the Netherlands

and

the Republic of Poland,

Hereinafter referred to as "the Parties",

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

Article 1

Purpose and scope

The purpose of this Agreement is to ensure the protection of Classified Information exchanged between the Parties or between legal entities, individuals or other forms of organisation 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, the following definitions mean:
1) **"Breach of security"** – an act or an omission, contrary to national laws and regulations, which results in the unauthorized access, disclosure, loss or compromise of Classified Information;
2) **"Classified Contract"** – a contract, including any pre-contractual negotiations, to be entered into by one of the Parties or a Contractor under its jurisdiction, with a Contractor under the jurisdiction of the other Party, the performance of which requires or involves access or potential access to or the creation of Classified Information;
3) **"Classified Information"** – any information, regardless of its form or objects or any parts thereof, designated by a security classification by one of the Parties, the unauthorised disclosure or loss of which could cause varying degrees of harm to the interests of one or both of the Parties;
4) **"Competent Security Authority"** – the government authority in a Party responsible for the implementa-

[1)] De Poolse tekst is niet opgenomen.

tion and supervision of this Agreement. The Competent Security Authority may delegate part of its responsibilities to a delegated competent security authority;
5) **"Contractor"** – any individual, legal entity or other form of organisation with the capacity to enter into Classified Contracts;
6) **"Facility Security Clearance"** – the determination by either Party confirming that the Contractor, and when applicable the Contractor's facility, fulfills the criteria necessary to protect Classified Information issued in accordance with its national laws and regulations;
7) **"Need-to-know"** – the requirement for an individual for access to, knowledge of or possession of Classified Information to perform official tasks or services;
8) **"Originating Party"** – the Party or Contractor, if applicable under national laws and regulations, under whose authority Classified Information has been created;
9) **"Personnel Security Clearance"** – the determination by either Party confirming that the individual has been appropriately cleared to have access to Classified Information up to and including a specified classification level, issued in accordance with its national laws and regulations;
10) **"Providing Party"** – the Party or Contractor under its jurisdiction, which provides Classified Information to the Receiving Party;
11) **"Receiving Party"** – the Party or Contractor under its jurisdiction, which receives Classified Information from the Providing Party;
12) **"Third Party"** – any international organisation or state, including legal entities, individuals or other forms of organisation 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.

3. The Parties shall inform each other via diplomatic channels about changes in the contact details of the Competent Security Authorities referred to in Paragraph 1.

Article 4

Security Classification Levels

1. The following security classifications levels of the Parties are equivalent, the equivalent in English being an informal translation not part of the national laws and regulations of the Parties:

For the Republic of Poland	For the Kingdom of the Netherlands	Equivalent in English
ŚCIŚLE TAJNE	Stg. ZEER GEHEIM	TOP SECRET
TAJNE	Stg. GEHEIM	SECRET
POUFNE	Stg. CONFIDENTIEEL	CONFIDENTIAL
ZASTRZEŻONE	DEPARTEMENTAAL VERTROUWELIJK	RESTRICTED

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

3. The Receiving Party may modify or revoke the security classification of received Classified Information under this Agreement only upon the written consent of the Party under whose authority the Classified Information has been created.

Article 5

Principles for protection of Classified Information

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

2. Access to Classified Information at the security classification level of ZASTRZEŻONE / DEPARTEMENTAAL VERTROUWELIJK / RESTRICTED as mentioned in Article 4 of this Agreement, shall be granted only to those individuals who have a Need-to-know, are authorized and briefed on their responsibilities in accordance with national laws and regulations.

Article 6

Security measures

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

2. The Parties shall take all appropriate measures to ensure that the Providing Party:
1) marks Classified Information with the appropriate classification marking in accordance with its national laws and regulations;
2) informs the Receiving Party of any conditions of release or limitations on the use of the Classified Information provided;
3) 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:
1) affords the same level of protection to Classified Information as afforded to its national Classified Information of an equivalent security classification level;
2) ensures that Classified Information is marked with its own corresponding security classification level;
3) ensures that the security classification levels assigned to Classified Information are not modified or revoked without the prior written consent of the Party under whose authority the Classified Information has been created;
4) ensures that Classified Information is not disclosed or released to a Third Party without the prior written consent of the Party under whose authority the Classified Information has been created;
5) uses Classified Information solely for the purpose it has been released for and in accordance with handling requirements of the Party under whose authority the Classified Information has been created.

Article 7

Security co-operation

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

2. 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 and in the scope of this Agreement.

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

4. The Competent Security Authorities of the Parties 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 of the Parties shall promptly notify each other in writing about changes in recognized Personnel Security Clearances and Facility Security Clearances for whom or for which a confirmation has been provided.

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 of POUFNE / Stg. CONFIDENTIEEL / CONFIDENTIAL or above as mentioned in Article 4 of this Agreement with a Contractor or a Sub-Contractor under the jurisdiction of the other Party, it shall first obtain written confirmation from the other Party that the Contractor or a Sub-Contractor has been granted a Facility Security Clearance and/or a Personnel Security Clearance at the appropriate security classification level. For ZASTRZEŻONE / DEPARTEMENTAAL VERTROUWELIJK / RESTRICTED security classification level contracts a Facility Security Clearance may be required if mandated by national laws and regulations of the Contractor.

2. The Competent Security Authority shall ensure that the Contractor:
1) 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;
2) monitors the security conduct within its facilities;
3) notifies promptly its Competent Security Authority of any Breach of security relating to the Classified Contract;
4) in addition to the subparagraphs 1, 2 and 3, for Classified Contracts at the security classification levels of POUFNE / Stg. CONFIDENTIEEL / CONFIDENTIAL and above as mentioned in Article 4 of this Agreement, the Competent Security Authority shall ensure that the Contractor holds a Facility Security Clearance at the appropriate security classification level in order to protect the Classified Information and that the individuals requiring access to Classified Information hold a Personnel Security Clearance at the appropriate security classification level.

3. Every Classified Contract concluded in accordance with this Agreement shall include security requirements, in particular:
1) a security classification guide specifying the applicable security classification levels of each part of that Classified Contract;
2) a procedure for communication of changes in the security classification level, taking into account Article 4, Paragraph 3 of this Agreement;
3) the channels and procedures to be used for the transport and/or transmission of Classified Information;
4) instructions for the handling and storage of Classified Information;
5) contact details of the Competent Security Authorities responsible for overseeing the protection of Classified Information related to the Classified Contract;
6) obligation to notify any Breach of security.

4. The Originating Party shall forward a copy of the security requirements, to the Receiving Party, to facilitate the security oversight of the Classified Contract.

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

6. The Parties shall ensure that every Sub-Contractor shall comply with the same conditions for the protection of Classified Information as those laid down for the Contractor.

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 of the Parties.

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

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

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

4. Classified Information at the security classification level of ŚCIŚLE TAJNE / Stg. ZEER GEHEIM / TOP SECRET shall not be translated or reproduced without the prior written consent of the Party under whose authority the Classified Information has been created.

5. Classified Information at the security classification level of ŚCIŚLE TAJNE / Stg. ZEER GEHEIM / TOP SECRET shall not be destroyed without the prior written consent of the Party under whose authority the Classified Information has been created. It shall be returned to that Party after it is no longer considered necessary by the Providing and Receiving Parties.

6. Classified Information up to and including the security classification level of TAJNE / Stg. GEHEIM / 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. In case of exceptional circumstances which make it impossible to protect Classified Information provided under this Agreement, the Classified Information shall be destroyed immediately. The Receiving Party shall notify promptly in writing the Competent Security Authority of the Providing Party about the destruction of this Classified Information.

Article 11

Visits

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

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

3. Request for visit shall include:
1) full name of the visitor, date and place of birth, nationality and passport / ID card number;
2) official title of the visitor and name of the organisation the visitor represents;
3) confirmation of the visitor's Personnel Security Clearance and its validity;
4) date and duration of the visit. In the case of recurring visits the total period covered by the visits shall be stated;
5) purpose of the visit and the anticipated security classification level of Classified Information to be discussed or accessed;
6) name and contact details of the facility to be visited;
7) dated and stamped signature of a representative of the visitor's Competent Security Authority.

4. The Competent Security Authorities of the Parties may agree on a list of visitors entitled to recurring visits valid for a period of 12 months. The Competent Security Authorities of the Parties shall agree on the further details of the recurring visits.

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

6. Visits involving access to Classified Information at the security classification level of ZASTRZEŻONE / DEPARTEMENTAAL VERTROUWELIJK / RESTRICTED shall be arranged directly between authorised sending and hosting entities.

7. The Parties shall ensure, pursuant to their national laws and regulations, the protection of the personal data of the persons arriving on a visit involving access to Classified Information.

Article 12

Breach of security

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

2. The Receiving Party shall investigate immediately any actual or suspected Breach of security. 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 Breach of security 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

Languages

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

Article 15

Dispute resolution

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

Article 16

Implementing arrangements

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

Article 17

Final provisions

1. 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 date of receipt of the latter notification.

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

3. This Agreement may be amended with the 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.

4. This Agreement is concluded for an indefinite period of time. A Party may terminate this Agreement in writing at any time through diplomatic channels. In this case, the Agreement shall expire six months after the date of receipt of such notification.

5. Regardless of the termination of this Agreement, all Classified Information exchanged 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 authorized thereto, have signed this Agreement.

DONE in Warsaw on 10 February 2023 in two original copies, each in the Dutch, Polish and English languages, all texts being equally authentic. In case of divergences of interpretation, the English text shall prevail.

For the Kingdom of the Netherlands,

DAPHNE BERGSMA

For the Republic of Poland,

LECH WOJCIECHOWSKI

Annex 1

1. The Competent Security Authority for the Republic of Poland is:
   Head of the Internal Security Agency
2. The Competent Security Authority for the Kingdom of the Netherlands is:
   General Intelligence and Security Service
   Ministry of the Interior and Kingdom Relations
3. 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

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

Het Koninkrijk der Nederlanden

en

de Republiek Polen,

Hierna te noemen „de partijen",

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

Artikel 1

Doel en reikwijdte

Dit Verdrag heeft ten doel de beveiliging te waarborgen van gerubriceerde gegevens die worden uitgewisseld tussen de partijen of tussen rechtspersonen, natuurlijke personen of andere organisatievormen 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:
1. **„Inbreuk op de veiligheid"**, 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.
2. **„Gerubriceerd contract"**, een contract, met inbegrip van eventuele voorafgaande contractonderhandelingen, dat een van de partijen of een opdrachtnemer onder haar rechtsmacht aangaat met een opdrachtnemer onder de rechtsmacht van de andere partij waarbij voor de uitvoering toegang of mogelijk toegang tot gerubriceerde gegevens vereist is of waarbij deze gecreëerd worden.
3. **„Gerubriceerde gegevens"**, gegevens, ongeacht de vorm daarvan, voorwerpen of delen daarvan, die door een van de partijen als gerubriceerd worden aangemerkt, waarvan de ongeoorloofde bekendmaking of het verlies de belangen van een of beide partijen in meer of mindere mate zou kunnen schaden.
4. **„Bevoegde veiligheidsautoriteit"**, de overheidsautoriteit in een partij die verantwoordelijk is voor de implementatie van en toezicht op dit Verdrag. De bevoegde veiligheidsautoriteit kan een deel van zijn verantwoordelijkheden delegeren aan een gemachtigde bevoegde veiligheidsautoriteit.
5. **„Opdrachtnemer"**, elke natuurlijke persoon, rechtspersoon of andere organisatievorm die bevoegd is gerubriceerde contracten aan te gaan.
6. **„Veiligheidsmachtiging bedrijfslocatie"**, de vaststelling door een van de partijen dat de opdrachtnemer, en wanneer van toepassing de bedrijfslocatie van de opdrachtnemer, voldoet aan de criteria die nodig zijn om gerubriceerde gegevens te beveiligen die zijn afgegeven in overeenstemming met de nationale wet- en regelgeving.
7. **„Need to know"**, het vereiste voor een natuurlijke persoon voor toegang tot, kennis van of bezit van gerubriceerde gegevens voor het uitvoeren van officiële taken of diensten.
8. **„Partij van herkomst"**, de partij of opdrachtnemer, indien van toepassing ingevolge nationale wet- en regelgeving, onder wier of wiens gezag gerubriceerde gegevens zijn gecreëerd.
9. **„Veiligheidsmachtiging personeel**", de vaststelling door een van de partijen dat de natuurlijke persoon de

juiste toestemming heeft gekregen voor de toegang tot gerubriceerde gegevens, met inbegrip van een gespecificeerd rubriceringsniveau, afgegeven in overeenstemming met de nationale wet- en regelgeving.
10. **„Verstrekkende partij"**, de partij of opdrachtnemer onder haar rechtsmacht die de gerubriceerde gegevens verstrekt aan de ontvangende partij.
11. **„Ontvangende partij"**, de partij of opdrachtnemer onder haar rechtsmacht die de gerubriceerde gegevens ontvangt van de verstrekkende partij.
12. **„Derde",** elke internationale organisatie of staat, met inbegrip van rechtspersonen, natuurlijke personen of andere organisatievormen 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.

3. De partijen informeren elkaar langs diplomatieke weg over veranderingen in de contactgegevens van de bevoegde veiligheidsautoriteiten bedoeld in het eerste lid.

Artikel 4

Rubriceringsniveaus

1. De volgende rubriceringsniveaus van de partijen komen overeen, waarbij het Engelse equivalent een niet-officiële vertaling betreft die geen deel uitmaakt van de nationale wet- en regelgeving van de partijen:

Voor de Republiek Polen	**Voor het Koninkrijk der Nederlanden**	**Equivalent in het Engels**
ŚCIŚLE TAJNE	Stg. ZEER GEHEIM	TOP SECRET
TAJNE	Stg. GEHEIM	SECRET
POUFNE	Stg. CONFIDENTIEEL	CONFIDENTIAL
ZASTRZEŻONE	DEPARTEMENTAAL VERTROUWELIJK	RESTRICTED

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

3. De ontvangende partij mag het rubriceringsniveau van uit hoofde van dit Verdrag ontvangen gerubriceerde gegevens uitsluitend veranderen of intrekken na schriftelijke goedkeuring van de partij onder wier gezag de gerubriceerde gegevens zijn gecreëerd.

Artikel 5

Beginselen voor de beveiliging van gerubriceerde gegevens

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

2. Toegang tot gerubriceerde gegevens op het rubriceringsniveau ZASTRZEŻONE / DEPARTEMENTAAL VERTROUWELIJK / RESTRICTED, zoals vermeld in artikel 4 van dit Verdrag, wordt uitsluitend verleend aan de natuurlijke personen die van de gegevens op de hoogte moeten zijn (need to know), gemachtigd zijn en zijn ingelicht over hun verantwoordelijkheden in overeenstemming met de nationale wet- en regelgeving.

Artikel 6

Veiligheidsmaatregelen

1. De partijen nemen alle passende maatregelen die krachtens hun nationale wet- en regelgeving van toepassing zijn op de bescherming van 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:
1. gerubriceerde gegevens voorziet van de juiste rubriceringsmarkering in overeenstemming met hun nationale wet- en regelgeving;
2. de ontvangende partij in kennis stelt van mogelijke voorwaarden voor vrijgave of beperkingen gesteld aan het gebruik van de verstrekte gerubriceerde gegevens;
3. 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:
1. hetzelfde beveiligingsniveau aan gerubriceerde gegevens toekent als aan haar nationale gerubriceerde gegevens met een vergelijkbaar rubriceringsniveau;
2. waarborgt dat gerubriceerde gegevens worden voorzien van haar eigen dienovereenkomstige rubriceringsniveau;
3. waarborgt dat de aan de gerubriceerde gegevens toegekende rubriceringsniveaus niet worden gewijzigd of ingetrokken zonder de voorafgaande schriftelijke toestemming van de partij onder wier gezag de gerubriceerde gegevens zijn gecreëerd;
4. waarborgt dat gerubriceerde gegevens niet bekend worden gemaakt of vrijgegeven aan een derde zonder de voorafgaande schriftelijke toestemming van de partij onder wier gezag de gerubriceerde gegevens zijn gecreëerd;
5. gerubriceerde gegevens uitsluitend gebruikt voor het doel waarvoor zij zijn vrijgegeven en in overeenstemming met de eisen voor gebruik van de partij onder wier gezag de gerubriceerde gegevens zijn gecreëerd.

Artikel 7

Veiligheidssamenwerking

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

2. De bevoegde veiligheidsautoriteiten van de partijen erkennen de veiligheidsmachtigingen personeel en veiligheidsmachtigingen bedrijfslocatie die overeenkomstig de nationale wet- en regelgeving van de andere partij en binnen de reikwijdte van dit Verdrag zijn afgegeven.

3. Op verzoek van de bevoegde veiligheidsautoriteit van de ene partij verstrekt de bevoegde veiligheidsautoriteit van de andere partij een schriftelijke bevestiging dat er een geldige veiligheidsmachtiging personeel of veiligheidsmachtiging bedrijfslocatie is afgegeven.

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

Artikel 8

Gerubriceerde contracten

1. Indien een partij of een opdrachtnemer onder haar rechtsmacht voorstelt een gerubriceerd contract op het rubriceringsniveau POUFNE / Stg. CONFIDENTIEEL / CONFIDENTIAL of hoger, zoals vermeld in artikel 4 van dit Verdrag te gunnen aan een opdrachtnemer of onderaannemer de rechtsmacht van de andere partij, dient zij eerst de schriftelijke bevestiging te verkrijgen van de andere partij dat aan deze opdrachtnemer of onderaannemer een veiligheidsmachtiging bedrijfslocatie en/of veiligheidsmachtiging personeel is/zijn toegekend op het juiste rubriceringsniveau. Voor het rubriceringsniveau ZASTRZEŻONE / DEPARTEMENTAAL VERTROUWELIJK / RESTRICTED kan een veiligheidsmachtiging bedrijfslocatie nodig zijn indien die verplicht is volgens de nationale wet- en regelgeving van de opdrachtnemer.

2. De bevoegde veiligheidsautoriteit waarborgt dat de opdrachtnemer:
1. 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;
2. de beveiligingsuitvoering op zijn locaties in het oog houdt;
3. zijn bevoegde veiligheidsautoriteit onverwijld in kennis stelt van elke inbreuk op de veiligheid die betrekking heeft op een gerubriceerd contract;

4. In aanvulling op de onderdelen 1, 2 en 3, met betrekking tot gerubriceerde contracten op het rubriceringsniveau POUFNE / Stg. CONFIDENTIEEL / CONFIDENTIAL en hoger, zoals vermeld in artikel 4 van dit Verdrag, waarborgt de bevoegde veiligheidsautoriteit dat de opdrachtnemer 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.

3. Elk gerubriceerd contract dat in overeenstemming met dit Verdrag wordt gesloten dient veiligheidsvereisten te bevatten, in het bijzonder:
1. een rubriceringsgids waarin de rubriceringsniveaus die van toepassing zijn op elk onderdeel van het gerubriceerde contract worden gespecificeerd;
2. een procedure voor het doorgeven van wijzigingen van het rubriceringsniveau, rekening houdend met artikel 4, derde lid, van dit Verdrag;
3. de kanalen en procedures die gebruikt dienen te worden voor het vervoer en/of de overbrenging van gerubriceerde gegevens;
4. instructies voor de omgang met en opslag van gerubriceerde gegevens;
5. contactgegevens van de bevoegde veiligheidsautoriteiten die verantwoordelijk zijn voor het toezicht op de beveiliging van gerubriceerde gegevens die betrekking hebben op het gerubriceerde contract;
6. de verplichting elke inbreuk op de veiligheid te melden.

4. De partij van herkomst stuurt een kopie van de veiligheidsvereisten naar de ontvangende partij, om het veiligheidstoezicht op het gerubriceerde contract te vergemakkelijken.

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

6. De partijen waarborgen dat elke onderaannemer voldoet aan dezelfde voorwaarden voor de beveiliging van gerubriceerde gegevens als die voor de opdrachtnemer zijn neergelegd.

Artikel 9

Overbrenging van gerubriceerde gegevens

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

2. De partijen kunnen gerubriceerde gegevens die door encryptie beveiligd zijn langs elektronische weg overbrengen in overeenstemming met procedures die door de bevoegde veiligheidsautoriteiten van de partijen 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. Reproducties en vertalingen worden beperkt tot het minimumaantal dat nodig is voor gebruik uit hoofde van dit Verdrag.

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 partij van herkomst.

4. Gerubriceerde gegevens op rubriceringsniveau ŚCIŚLE TAJNE / Stg. ZEER GEHEIM / TOP SECRET worden niet vertaald of gereproduceerd zonder de voorafgaande schriftelijke toestemming van de partij onder wier gezag de gerubriceerde gegevens zijn gecreëerd.

5. Gerubriceerde gegevens op rubriceringsniveau ŚCIŚLE TAJNE / Stg. ZEER GEHEIM / TOP SECRET worden niet vernietigd zonder de voorafgaande schriftelijke toestemming van de partij onder wier gezag de gerubriceerde gegevens zijn gecreëerd. Zij worden geretourneerd aan die partij nadat de verstrekkende en de ontvangende partij ze niet meer nodig achten.

6. Gerubriceerde gegevens tot en met rubriceringsniveau TAJNE / Stg. GEHEIM / 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. In geval van uitzonderlijke omstandigheden die het onmogelijk maken 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 schriftelijk in kennis van de vernietiging van deze gerubriceerde gegevens.

Artikel 11

Bezoeken

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

2. De bezoeker dient de aanvraag voor het bezoek ten minste tien kalenderdagen vóór de beoogde datum van het bezoek in bij zijn bevoegde veiligheidsautoriteit, die de aanvraag doorstuurt naar de bevoegde veiligheidsautoriteit 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 van de partijen.

3. Een aanvraag voor een bezoek dient de volgende gegevens te bevatten:
1. volledige naam van de bezoeker, geboortedatum en -plaats, nationaliteit en nummer van het paspoort/ de identiteitskaart;
2. officiële functiebenaming van de bezoeker en de naam van de organisatie die de bezoeker vertegenwoordigt;
3. bevestiging van de veiligheidsmachtiging personeel van de bezoeker en de geldigheid ervan;
4. datum en duur van het bezoek. In het geval van herhalingsbezoeken dient de volledige periode waarin de bezoeken plaatsvinden te worden vermeld;
5. doel van het bezoek en het verwachte rubriceringsniveau van de gerubriceerde gegevens die besproken worden of waartoe toegang wordt verkregen;
6. naam en contactgegevens van de te bezoeken locatie;
7. van een datum en stempel voorziene handtekening van een vertegenwoordiger van de bevoegde veiligheidsautoriteit van de bezoeker.

4. De bevoegde veiligheidsautoriteiten van de partijen kunnen een lijst overeenkomen van bezoekers die herhalingsbezoeken mogen brengen die geldig is voor een periode van 12 maanden. De bevoegde veiligheidsautoriteiten van de partijen 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. Bezoeken waarbij toegang nodig is tot gerubriceerde gegevens op rubriceringsniveau ZASTRZEŻONE / DEPARTEMENTAAL VERTROUWELIJK / RESTRICTED worden rechtstreeks geregeld tussen de bevoegde zendende en ontvangende entiteiten.

7. De partijen waarborgen, in overeenstemming met hun nationale wet- en regelgeving, de beveiliging van de persoonsgegevens van de personen die een bezoek brengen waarbij toegang tot gerubriceerde gegevens nodig is.

Artikel 12

Inbreuk op de veiligheid

1. De bevoegde veiligheidsautoriteiten stellen elkaar onverwijld schriftelijk in kennis van feitelijke of vermoedelijke inbreuken op de veiligheid waarbij gerubriceerde gegevens van de andere partij betrokken zijn.

2. De ontvangende partij onderzoekt feitelijke of vermoedelijke inbreuken op de veiligheid onmiddellijk. De bevoegde veiligheidsautoriteit 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 de inbreuk op de veiligheid te beperken en herhalingen te voorkomen. De bevoegde veiligheidsautoriteit van de partij van herkomst wordt in kennis gesteld van de uitkomst van het onderzoek en, indien van toepassing, de 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

Talen

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

Artikel 15

Oplossing van geschillen

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

Artikel 16

Uitvoeringsregelingen

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

Artikel 17

Slotbepalingen

1. 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 datum van ontvangst van de laatste kennisgeving.

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

3. Dit Verdrag kan met instemming van de partijen worden gewijzigd. Elke partij kan op elk moment langs diplomatieke weg wijzigingen van dit Verdrag voorstellen. Deze wijzigingen treden in werking in overeenstemming met de in het eerste lid van dit artikel vastgelegde voorwaarden.

4. Dit Verdrag wordt gesloten voor onbepaalde tijd. Een partij kan dit Verdrag te allen tijde schriftelijk langs diplomatieke weg beëindigen. In dat geval eindigt het Verdrag zes maanden na de datum van ontvangst van deze kennisgeving.

5. Ongeacht de beëindiging van dit Verdrag blijven alle uit hoofde van dit Verdrag uitgewisselde 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 Warschau op 10 februari 2023 in twee oorspronkelijke exemplaren, elk in de Nederlandse, de Poolse en de Engelse taal, waarbij alle teksten gelijkelijk authentiek zijn. In geval van verschil in interpretatie is de Engelse tekst doorslaggevend.

Voor het Koninkrijk der Nederlanden,

DAPHNE BERGSMA

Voor de Republiek Polen,

LECH WOJCIECHOWSKI

Bijlage I

1. De bevoegde veiligheidsautoriteit van de Republiek Polen is:
   Het Hoofd van het Agentschap Binnenlandse Veiligheid
2. De bevoegde veiligheidsautoriteit van het Koninkrijk der Nederlanden is:
   De Algemene Inlichtingen- en Veiligheidsdienst (AIVD)
   Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
3. De gemachtigde bevoegde veiligheidsautoriteit van het Koninkrijk der Nederlanden in het militaire domein is:
   De Beveiligingsautoriteit
   Directoraat-Generaal Beleid
   Ministerie van Defensie

D. PARLEMENT

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

G. INWERKINGTREDING

De bepalingen van het Verdrag, met Bijlage, zullen ingevolge artikel 17, eerste lid, in werking treden op de eerste dag van de tweede maand die volgt op de ontvangst van de laatste kennisgeving waarbij 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 *achtentwintigste* februari 2023.

De Minister van Buitenlandse Zaken,

W.B. HOEKSTRA

trb-2023-18
ISSN 0920 - 2218
's-Gravenhage 2023