5 (2024) Nr. 1

TRACTATENBLAD

VAN HET

KONINKRIJK DER NEDERLANDEN

JAARGANG 2024 Nr. 30

A. TITEL

Verdrag tussen het Koninkrijk der Nederlanden en Oekraïne inzake de uitwisseling en wederzijdse beveiliging van gerubriceerde gegevens (met Bijlage);
Kyiv, 5 februari 2024

Voor een overzicht van de verdragsgegevens, zie verdragsnummer 013511 in de Verdragenbank.

B. TEKST[1)]

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

The Kingdom of the Netherlands

and

Ukraine,

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

Wishing to ensure the mutual protection of Classified Information, in the interests of national security,

Have agreed as follows:

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) „Breach of Security" 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.
b) „Classified Contract" means a contract, 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.
c) "Classified Information" means any information or material designated by a security classification by one

[1)] De Oekraïense tekst is niet opgenomen.

of the Parties the unauthorised disclosure or loss of which could cause varying degrees of prejudice to the interests of one or both of the Parties.
d) "Competent Security Authority" means the State authority in a Party responsible for the implementation and supervision of this Agreement. The Competent Security Authority may delegate part of its responsibilities to a delegated competent security authority.
e) "Contractor" means any individual or legal entity with the capacity to enter into contracts.
f) "Facility Security Clearance" means a written decision based on a vetting procedure by the Competent Security Authority that a facility has in place appropriate security measures to access and handle Classified Information up to and including a specified security classification level, in accordance with national laws and regulations.
g) "Need to know" means the requirement for an individual or a legal entity for access to, knowledge of or possession of Classified Information to perform official tasks or services.
h) "Originating Party" means the Party under whose authority Classified Information has been created.
i) „Personnel Security Clearance" means the written decision based on a vetting procedure by the Competent Security Authority of one of the Parties that an individual has been security cleared to access and handle Classified Information up to and including a specified classification level, in accordance with its national laws and regulations.
j) "Providing Party" means the Party or Contractor under its jurisdiction, which provides Classified Information to the Receiving Party under this Agreement.
k) "Receiving Party" means the Party or Contractor under its jurisdiction, which receives Classified Information from the Providing Party under this Agreement.
l) "Security Classification Guide" means a document associated with a Classified Contract that identifies each part of that Classified Contract which contains Classified Information, specifying the applicable security classification levels.
m) "Third Party" means any international organisation or state, including legal entities or individuals under its jurisdiction, which is not a Party to this Agreement.

Article 3

Competent Security Authorities

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

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

Article 4

Security classification markings

1. The following security classification markings of the Parties are equivalent and correspond to the security classification levels specified in their national legislation. The English equivalent is an informal translation, not part of the national laws and regulations of the Parties and should not be used to mark Classified Information.

For Ukraine	**For the Kingdom of the Netherlands**	**Equivalent in English**
Особливої важливості	Stg. ZEER GEHEIM	TOP SECRET
ЦілКом таємно	Stg. GEHEIM	SECRET
Таємно	Stg. CONFIDENTIEEL	CONFIDENTIAL
Для службового Користування	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 marking in accordance with the table contained in paragraph 1 of this article.

3. The Receiving Party may modify or cancel the security classification marking of received Classified Information under this Agreement only upon the written approval by the Providing Party.

Article 5

Access to Classified Information

Access to Classified Information shall be granted only to those individuals who have Need to know and who have been authorised for access to such information according to the legislation of the State of the Receiving Party.

Article 6

Security measures

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

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

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

Article 7

Security co-operation

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

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

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

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

5. The communication in relation to co-operation under this Agreement shall be effected in the English language.

Article 8

Classified Contracts

1. If a Party or a Contractor under its jurisdiction proposes to designate a Classified Contract at the security classification levels equivalent to "CONFIDENTIAL" and/or "SECRET" 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 "RESTRICTED" as mentioned in Article 4 of this Agreement, a Facility Security Clearance may be required, if mandated by national laws and regulations of the State of the Contractor.

2. The Competent Security Authority under whose jurisdiction the Contractor operates, shall ensure that the Contractor:
a) ensures that all individuals granted access to Classified Information are informed of their responsibilities to protect Classified Information in accordance with the conditions defined in this Agreement and with national laws and regulations;
b) monitors the security conduct within its facilities;

c) notifies promptly its Competent Security Authority of any Breach of Security relating to the Classified Contract;
d) in addition to the subparagraphs a), b) and c) of this paragraph, for Classified Contracts at the security classification levels equivalent to "CONFIDENTIAL" and/or "SECRET" as mentioned in Article 4 of this Agreement holds a Facility Security Clearance at the appropriate security classification level in order to protect the Classified Information;
e) in addition to the subparagraphs a), b) and c) of this paragraph, for Classified Contracts at the security classification levels equivalent to "CONFIDENTIAL" and/or "SECRET" as mentioned in Article 4 of this Agreement, ensures 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 a security requirements chapter which identifies the following aspects:
a) a Security Classification Guide;
b) a procedure for communication between the parties to the Classified Contract of changes in the security classification level, taking into account article 4, paragraph 3 of this Agreement;
c) the channels and procedures to be used for the transport and/or transmission of Classified Information;
d) instructions for the handling and storage of Classified Information;
e) contact details of the Competent Security Authorities responsible for overseeing the protection of Classified Information related to the Classified Contract;
f) obligation to notify any Breach of Security.

4. The Competent Security Authority of the Party authorising the award of the Classified Contract shall forward a copy of the security requirements chapter, to the Competent Security Authority of the Receiving Party, to facilitate the security oversight of the Classified Contract.

5. If a Contractor sub-contracts parts of a Classified Contract, the Contractor and the sub-Contractor shall ensure the observance of this Agreement;

6. 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.

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 means in accordance with procedures to be mutually 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 authorised in accordance with national laws and regulations to access Classified Information at the security classification level of the Classified Information being translated or reproduced.

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

4. Classified Information at the security classification levels equivalent to "TOP SECRET" as mentioned in Article 4 of this Agreement shall not be translated or reproduced without the prior written consent of the Providing Party.

5. Classified Information at the security classification levels equivalent to "TOP SECRET" as mentioned in Article 4 of this Agreement shall not be destroyed without the prior written consent of the Providing Party. It shall be returned to the Providing Party after it is no longer considered necessary by the Receiving Party.

6. Classified Information marked up to and including security classification levels equivalent to "SECRET" as mentioned in Article 4 of this Agreement shall be destroyed after it is no longer considered necessary by the Receiving Party, in accordance with its national laws and regulations.

7. If a crisis situation makes it impossible to ensure the protection of Classified Information provided under this Agreement, the Classified Information shall be destroyed immediately in such a way that this Classified Information is no longer accessible. 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.

2. The visitor shall submit the request for visit at least ten days in advance of the proposed date of the visit to the Competent Security Authority of the Party within
whose jurisdiction the visitor operates. The request shall be forwarded 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) dated and stamped signature of a representative of the visitor's Competent Security Authority of the Party within whose jurisdiction the visitor operates.

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 treated in accordance with the provisions of this Agreement.

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 in accordance with national laws and regulations. The Providing Party shall, if required, cooperate in the investigation.

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

Relation to other agreements

This Agreement does not prevail over any international agreement that has already been or may be entered into and that specifically governs a transaction otherwise governed by this Agreement.

Article 16

Implementing arrangements

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

Article 17

Final provisions

1. This Agreement is concluded for an indefinite period of time. Each Party shall notify the other Party through diplomatic channels once the national measures necessary for entry into force of this Agreement have been completed. This Agreement shall enter into force on the first day of the second month following the receipt of the latter notification.

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

3. This Agreement may be amended with the mutual consent of the Parties. Either Party may propose amendments to this Agreement at any time through diplomatic channels. Such amendments shall enter into force under the conditions laid down in paragraph 1 of this Article, with the exception of an amendment of Annex 1, which amendment shall enter into force on a date to be agreed upon by the Parties.

4. A Party may terminate this Agreement in writing at any time. In this case, the Agreement shall expire six months after receipt of the notification.

5. Regardless of the termination of this Agreement, all Classified Information exchanged 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 there to, have signed this Agreement.

DONE at Kyiv on 5 February 2024 in two original copies, each in the English, Dutch and Ukrainian languages all texts being equally authentic. In case of divergences of interpretation, the English text shall prevail.

For the Kingdom of the Netherlands,

M.J. DE VINK

For Ukraine,

SERHII ANDRUSHCHENKO

Annex I

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

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

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

Het Koninkrijk der Nederlanden

en

Oekraïne,

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

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

Zijn het volgende overeengekomen:

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. „Inbreuk op de beveiliging", 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.
b. „Gerubriceerd contract", een contract, met inbegrip van eventuele voorafgaande contractonderhandelingen, dat 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.
c. „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.
d. „Bevoegde beveiligingsautoriteit", de overheidsautoriteit in een partij die verantwoordelijk is voor de implementatie van en toezicht op dit Verdrag. De bevoegde beveiligingsautoriteit kan een deel van zijn verantwoordelijkheden delegeren aan een gemachtigde bevoegde beveiligingsautoriteit.
e. „Opdrachtnemer", elke natuurlijke persoon of rechtspersoon die bevoegd is contracten aan te gaan.
f. „Veiligheidsmachtiging bedrijfslocatie", een schriftelijk besluit op basis van een antecedentenonderzoek door de bevoegde beveiligingsautoriteit dat een bedrijfslocatie passende beveiligingsmaatregelen heeft genomen voor de toegang tot en omgang met gerubriceerde gegevens, met inbegrip van een gespecificeerd rubriceringsniveau, in overeenstemming met de nationale wet- en regelgeving.
g. „Need to know", het vereiste voor een natuurlijke persoon of rechtspersoon voor toegang tot, kennis van of bezit van gerubriceerde gegevens voor het uitvoeren van officiële taken of diensten.
h. „Partij van herkomst", de partij onder wier gezag gerubriceerde gegevens zijn gecreëerd.
i. „Veiligheidsmachtiging personeel", het schriftelijk besluit op basis van een antecedentenonderzoek door de bevoegde beveiligingsautoriteit van een van de partijen dat een natuurlijke persoon toestemming heeft gekregen voor toegang tot en omgang met gerubriceerde gegevens, met inbegrip van een gespecificeerd rubriceringsniveau, in overeenstemming met de nationale wet- en regelgeving.
j. „Verstrekkende partij", de partij of opdrachtnemer onder haar rechtsmacht die de gerubriceerde gegevens uit hoofde van dit Verdrag verstrekt aan de ontvangende partij.
k. „Ontvangende partij", de partij of opdrachtnemer onder haar rechtsmacht die de gerubriceerde gegevens

uit hoofde van dit Verdrag ontvangt van de verstrekkende partij.
l. „Rubriceringsgids", een document dat hoort bij een gerubriceerd contract waarin de van toepassing zijnde rubriceringsniveaus voor elk onderdeel van het gerubriceerde contract dat gerubriceerde gegevens bevat worden gespecificeerd.
m. „Derde", elke internationale organisatie of staat, met inbegrip van rechtspersonen of natuurlijke personen onder zijn rechtsmacht, die geen partij is bij dit Verdrag.

Artikel 3

Bevoegde beveiligingsautoriteiten

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

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

Artikel 4

Rubriceringsmarkeringen

1. De volgende rubriceringsmarkeringen van de partijen komen overeen en corresponderen met de rubriceringsniveaus die in hun nationale wetgeving staan vermeld. Het Engelse equivalent is een niet-officiële vertaling, die geen deel uitmaakt van de nationale wet- en regelgeving van de partijen en niet gebruikt dient te worden om gerubriceerde gegevens aan te duiden.

Voor Oekraïne	**Voor het Koninkrijk der Nederlanden Nederland**	**Equivalent in het Engels**
Особливої важливості	Stg. ZEER GEHEIM	TOP SECRET
ЦілКом таємно	Stg. GEHEIM	SECRET
Таємно	Stg. CONFIDENTIEEL	CONFIDENTIAL
Для службового Користування	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 de rubriceringsmarkering in overeenstemming met de tabel in het eerste lid van dit artikel.

3. De ontvangende partij mag de rubriceringsmarkering van uit hoofde van dit Verdrag ontvangen gerubriceerde gegevens uitsluitend veranderen of schrappen na schriftelijke goedkeuring van de verstrekkende partij.

Artikel 5

Toegang tot gerubriceerde gegevens

Toegang tot gerubriceerde gegevens wordt uitsluitend verleend aan de natuurlijke personen die van de gegevens op de hoogte moeten zijn (need to know) en die gemachtigd zijn toegang te hebben tot dergelijke gegevens op grond van de wetgeving van de staat van de ontvangende partij.

Artikel 6

Beveiligingsmaatregelen

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

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

3. De ontvangende partij neemt alle passende maatregelen om te waarborgen dat:

a. hetzelfde beveiligingsniveau aan gerubriceerde gegevens wordt toegekend als aan haar nationale gerubriceerde gegevens met een vergelijkbaar rubriceringsniveau;
b. gerubriceerde informatie wordt voorzien van haar eigen dienovereenkomstige rubriceringsmarkering;
c. de aan de gerubriceerde gegevens toegekende rubriceringsmarkeringen niet worden veranderd of ingetrokken zonder de voorafgaande schriftelijke toestemming van de verstrekkende partij;
d. gerubriceerde gegevens niet bekend worden gemaakt of vrijgegeven aan een derde zonder de voorafgaande schriftelijke toestemming van de verstrekkende partij;
e. gerubriceerde gegevens uitsluitend worden gebruikt voor het doel waarvoor zij zijn vrijgegeven en in overeenstemming met de eisen voor gebruik van de partij van herkomst.

Artikel 7

Beveiligingssamenwerking

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

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

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

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

5. De communicatie in verband met samenwerking uit hoofde van dit Verdrag vindt plaats in de Engelse taal.

Artikel 8

Gerubriceerde contracten

1. Indien een partij of een opdrachtnemer onder haar rechtsmacht voorstelt een gerubriceerd contract met een veiligheidsmarkering die overeenkomt met „CONFIDENTIAL" en/of „SECRET", zoals vermeld in artikel 4 van dit Verdrag, te sluiten met 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(en) personeel is/zijn toegekend op het juiste rubriceringsniveau. Voor gerubriceerde contracten met het rubriceringsniveau dat overeenkomt met „RESTRICTED" 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. De bevoegde beveiligingsautoriteit onder wier rechtsmacht de opdrachtnemer zijn activiteiten uitvoert, waarborgt dat de opdrachtnemer:
a. waarborgt dat alle natuurlijke personen die toegang krijgen tot gerubriceerde gegevens in kennis worden gesteld van hun verantwoordelijkheid de gerubriceerde gegevens te beveiligen in overeenstemming met de voorwaarden omschreven in dit Verdrag en de nationale wet- en regelgeving;
b. de beveiligingsuitvoering op zijn locaties in het oog houdt;
c. zijn bevoegde beveiligingsautoriteit onverwijld in kennis stelt van elke inbreuk op de beveiliging die betrekking heeft op een gerubriceerd contract;
d. in aanvulling op de onderdelen a, b en c, van dit lid, met betrekking tot gerubriceerde contracten met een rubriceringsniveau dat overeenkomt met „CONFIDENTIAL" en/of „SECRET", zoals vermeld in artikel 4 van dit Verdrag, een veiligheidsmachtiging bedrijfslocatie heeft met het juiste rubriceringsniveau om de gerubriceerde gegevens te beveiligen;
e. in aanvulling op de onderdelen a, b en c, van dit lid, met betrekking tot gerubriceerde contracten met een rubriceringsniveau dat overeenkomt met „CONFIDENTIAL" en/of „SECRET", zoals vermeld in artikel 4 van dit Verdrag, waarborgt 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 een hoofdstuk met beveiligingsvereisten te bevatten waarin de volgende aspecten vermeld staan:
a. een rubriceringsgids;
b. een procedure voor het doorgeven door de partijen bij gerubriceerde contracten van wijzigingen van het rubriceringsniveau, rekening houdend met artikel 4, derde lid, van dit Verdrag;

c. de kanalen en procedures die gebruikt dienen te worden voor het vervoer en/of de overbrenging van gerubriceerde gegevens;
d. instructies voor de omgang met en opslag van gerubriceerde gegevens;
e. contactgegevens van de bevoegde beveiligingsautoriteiten die verantwoordelijk zijn voor het toezicht op de beveiliging van gerubriceerde gegevens die betrekking hebben op het gerubriceerde contract;
f. de verplichting elke inbreuk op de beveiliging te melden.

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

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

6. 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.

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 wederzijds 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 verstrekkende partij.

4. Gerubriceerde gegevens met het rubriceringsniveau dat overeenkomt met „TOP SECRET” zoals vermeld in artikel 4 van dit Verdrag worden niet vertaald of gereproduceerd zonder de voorafgaande schriftelijke toestemming van de verstrekkende partij.

5. Gerubriceerde gegevens met het rubriceringsniveau dat overeenkomt met „TOP SECRET” zoals vermeld in artikel 4 van dit Verdrag worden niet vernietigd zonder de voorafgaande schriftelijke toestemming van de verstrekkende partij. Zij worden geretourneerd aan de verstrekkende partij nadat de ontvangende partij ze niet meer nodig acht.

6. Gerubriceerde gegevens tot en met rubriceringsniveaus die overeenkomen met „SECRET” zoals vermeld in artikel 4 van dit Verdrag worden vernietigd nadat de ontvangende partij ze niet meer nodig acht, in overeenstemming met haar nationale wet- en regelgeving.

7. Indien een crisissituatie het onmogelijk maakt de beveiliging van uit hoofde van dit Verdrag verstrekte gegevens te waarborgen, dienen de gerubriceerde gegevens onmiddellijk op zodanige wijze vernietigd te worden dat deze gerubriceerde gegevens niet langer toegankelijk zijn. De ontvangende partij stelt de bevoegde beveiligingsautoriteit van de verstrekkende partij onverwijld 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 beveiligingsautoriteit, tenzij anderszins overeengekomen door de bevoegde beveiligingsautoriteiten.

2. De bezoeker dient de aanvraag voor het bezoek ten minste tien dagen vóór de beoogde datum van het bezoek in bij de bevoegde beveiligingsautoriteit van de partij onder wier rechtsmacht de bezoeker opereert. De aanvraag wordt doorgestuurd naar de bevoegde beveiligingsautoriteit van de andere partij. In dringende gevallen kan de aanvraag van een verzoek binnen een kortere termijn worden ingediend, mits hierover voorafgaande coördinatie tussen de bevoegde beveiligingsautoriteiten plaatsvindt.

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

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.

Artikel 12

Inbreuk op de beveiliging

1. De bevoegde beveiligingsautoriteiten stellen elkaar onverwijld schriftelijk in kennis van feitelijke of vermoedelijke inbreuken op de veiligheid waarbij gerubriceerde informatie van de andere partij betrokken is.

2. De ontvangende partij onderzoekt feitelijke of vermoedelijke inbreuken op de beveiliging onmiddellijk in overeenstemming met de nationale wet- en regelgeving. De verstrekkende partij verleent, indien nodig, medewerking aan het onderzoek.

3. De bevoegde beveiligingsautoriteiten nemen passende maatregelen in overeenstemming met hun nationale wet- en regelgeving, met inbegrip van maatregelen om de gevolgen van het incident te beperken en herhaling van de inbreuk op de veiligheid te voorkomen. De bevoegde beveiligingsautoriteit van de verstrekkende partij wordt in kennis gesteld van de uitkomsten van het onderzoek en 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

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

Relatie met andere verdragen

Dit Verdrag heeft geen voorrang boven elk internationaal verdrag dat reeds is gesloten of nog kan worden gesloten en dat specifiek betrekking heeft op een verrichting waarop dit Verdrag anderszins van toepassing is.

Artikel 16

Uitvoeringsregelingen

De bevoegde beveiligingsautoriteiten kunnen uitvoeringsregelingen sluiten ingevolge dit Verdrag.

Artikel 17

Slotbepalingen

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

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

3. Dit Verdrag kan met wederzijdse instemming van de partijen worden gewijzigd. Elke partij kan op elk moment langs diplomatieke weg wijzigingen van dit Verdrag voorstellen. Dergelijke wijzigingen treden in werking onder de voorwaarden vervat in het eerste lid van dit artikel, met uitzondering van een wijziging van Bijlage 1, welke wijziging in werking treedt op een door de partijen overeen te komen datum.

4. Een partij kan dit Verdrag te allen tijde schriftelijk opzeggen. In dat geval eindigt het Verdrag zes maanden na ontvangst van de kennisgeving.

5. Ongeacht de beëindiging van dit Verdrag blijven alle uit hoofde van dit Verdrag uitgewisselde 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 Kyiv op 5 februari 2024 in twee oorspronkelijke exemplaren, elk in de Engelse, de Nederlandse en de Oekraïense taal, waarbij alle teksten gelijkelijk authentiek zijn. In geval van verschil in interpretatie is de Engelse tekst doorslaggevend.

Voor het Koninkrijk der Nederlanden,

M.J. DE VINK

Voor Oekraïne,

SERHII ANDRUSHCHENKO

Bijlage I

1. De bevoegde beveiligingsautoriteit voor Oekraïne is:
   De Veiligheidsdienst van Oekraïne
2. De bevoegde beveiligingsautoriteit van het Koninkrijk der Nederlanden is:
   De Algemene Inlichtingen- en Veiligheidsdienst (AIVD)
   Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
   De gemachtigde bevoegde beveiligingsautoriteit van het Koninkrijk der Nederlanden voor het militaire domein is:
   De Beveiligingsautoriteit
   Directoraat-Generaal Beleid

D. PARLEMENT

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

G. INWERKINGTREDING

De bepalingen van het Verdrag, met Bijlage, zullen ingevolge artikel 17, eerste lid, van het Verdrag in werking treden op de eerste dag van de tweede maand die volgt op de ontvangst van de laatste kennisgeving waarin de partijen elkaar langs diplomatieke weg in kennis hebben gesteld van de voltooiing van de nationale maatregelen die nodig zijn voor de inwerkingtreding van het Verdrag.

Uitgegeven de *negenentwintigste* februari 2024.

De Minister van Buitenlandse Zaken,

H.G.J. BRUINS SLOT

trb-2024-30
ISSN 0920 - 2218
's-Gravenhage 2024