11 (2024) Nr. 1

# TRACTATENBLAD

VAN HET

KONINKRIJK DER NEDERLANDEN

**JAARGANG 2024 Nr. 85**

A. TITEL

*Verdrag tussen het Koninkrijk der Nederlanden en de Slowaakse Republiek inzake de uitwisseling en wederzijdse beveiliging van gerubriceerde gegevens (met Bijlage); Bratislava, 2 juli 2024*

**Voor een overzicht van de verdragsgegevens, zie verdragsnummer 012026 in de Verdragenbank.**

B. TEKST[1)]

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

Het Koninkrijk der Nederlanden

en

de Slowaakse Republiek,

Hierna gezamenlijk te noemen „partijen" en elk afzonderlijk „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 opdrachtnemers 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. De partijen nemen alle passende maatregelen krachtens hun nationale wet- en regelgeving om de beveiliging van gerubriceerde gegevens in overeenstemming met dit Verdrag te waarborgen.

3. 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. **„Verdrag",** dit document met inbegrip van de Bijlagen daarbij.
b. **„Bijlage",** een bijlage bij dit document.
c. **„Gerubriceerd contract",** elke wettelijk afdwingbare overeenkomst voor het leveren van goederen of diensten die een van de partijen of een opdrachtnemer onder haar rechtsmacht aangaat met een opdrachtnemer

[1)] De Slowaakse tekst is niet opgenomen.

onder de rechtsmacht van de andere partij, die gerubriceerde gegevens bevat of waarbij voor de uitvoering toegang of mogelijk toegang vereist is tot het genereren, gebruiken of overdragen van gerubriceerde gegevens.
d. **„Gerubriceerde gegevens",** gegevens, materiaal of voorwerpen, ongeacht de vorm of aard daarvan, of delen daarvan, die door een van de partijen als gerubriceerd worden aangemerkt, waarvan de ongeoorloofde bekendmaking, verandering, compromittering of elk verlies de belangen van een of beide partijen in meer of mindere mate zou kunnen schaden.
e. **„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.
f. **„Opdrachtnemer",** elke persoon (anders dan degenen die door een partij in dienst zijn genomen op grond van een contract of arbeidsovereenkomst), rechtspersoon of andere vorm van organisatie onder de rechtsmacht van een partij, die een gerubriceerd contract aangaat of er door gebonden is.
g. **„Veiligheidsmachtiging bedrijfslocatie",** de vaststelling door de bevoegde beveiligingsautoriteit dat een bedrijfslocatie passende veiligheidsmaatregelen 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.
h. **„Need to know",** het vereiste voor een natuurlijke persoon, rechtspersoon of andere organisatievorm, voor toegang tot, kennis van of bezit van gerubriceerde gegevens voor het uitvoeren van hun officiële taken of diensten.
i. **„Partij van herkomst",** de partij onder wier gezag gerubriceerde gegevens zijn gecreëerd.
j. **„Veiligheidsmachtiging personeel",** de vaststelling door de bevoegde beveiligingsautoriteit dat een natuurlijke persoon toestemming heeft gekregen voor de toegang tot en omgang met gerubriceerde gegevens, met inbegrip van een gespecificeerd rubriceringsniveau, in overeenstemming met de nationale wet- en regelgeving.
k. **„Verstrekkende partij",** de partij of opdrachtnemer onder haar rechtsmacht die de gerubriceerde gegevens uit hoofde van dit Verdrag verstrekt aan de ontvangende partij.
l. **„Ontvangende partij",** de partij of opdrachtnemer onder haar rechtsmacht die de gerubriceerde gegevens uit hoofde van dit Verdrag ontvangt van de verstrekkende partij.
m. **„Rubriceringsgids",** een document dat hoort bij een gerubriceerd contract waarin de van toepassing zijnde rubriceringsniveaus voor elk onderdeel van dat gerubriceerde contract worden gespecificeerd.
n. **„Beveiligingsincident",** elke ongeoorloofde bekendmaking, verandering, compromittering, elk verlies, elke toegang, omgang met, elke opslag of vernietiging van gerubriceerde gegevens, in strijd met de nationale wet- en regelgeving van de ontvangende partij en/of dit Verdrag.
o. **„Derde",** elke internationale organisatie, regering of staat, met inbegrip van natuurlijke personen, rechtspersonen of andere organisatievormen 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.

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

Artikel 4

*Rubriceringsniveaus*

De volgende rubriceringsniveaus van de partijen komen overeen en corresponderen met de rubriceringsniveaus die in de nationale wet- en regelgeving van de partijen staan. 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 het Koninkrijk der Nederlanden | Voor de Slowaakse Republiek | Equivalent in het Engels |
|---|---|---|
| Stg. ZEER GEHEIM | PRÍSNE TAJNÉ | TOP SECRET |
| Stg. GEHEIM | TAJNÉ | SECRET |
| Stg. CONFIDENTIEEL | DÔVERNÉ | CONFIDENTIAL |

| Voor het Koninkrijk der Nederlanden | Voor de Slowaakse Republiek | Equivalent in het Engels |
|---|---|---|
| DEPARTEMENTAAL VERTROUWELIJK | VYHRADENÉ | RESTRICTED |

Artikel 5

*Beveiligingsmaatregelen*

1. De ontvangende partij voorziet alle gerubriceerde gegevens die zij ontvangen heeft van de verstrekkende partij of heeft gegenereerd uit hoofde van dit Verdrag van het rubriceringsniveau dat overeenkomt met de door de partij van herkomst gegeven rubriceringsniveau in overeenstemming met de tabel in artikel 4 en, indien van toepassing, in overeenstemming met het vierde lid van dit artikel.

2. De ontvangende partij zal het rubriceringsniveau van uit hoofde van dit Verdrag ontvangen of gegenereerde gerubriceerde gegevens niet veranderen of intrekken zonder de schriftelijke goedkeuring van de partij van herkomst.

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

4. De partij van herkomst kan de gerubriceerde gegevens tevens voorzien van vereisten voor de omgang ermee, om eventuele beperkingen te stellen aan het gebruik, de bekendmaking, vrijgave en toegang door de ontvangende partij.

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

6. De partijen kennen aan gerubriceerde gegevens die uit hoofde van dit Verdrag worden uitgewisseld of gegenereerd ten minste dezelfde beveiliging toe als aan hun eigen gerubriceerde gegevens met een vergelijkbaar rubriceringsniveau.

7. Overeenkomstig het tweede lid van artikel 1 van dit Verdrag, nemen de partijen alle passende maatregelen om te waarborgen dat de verstrekkende partij:
a. de gerubriceerde gegevens voorziet van de juiste rubriceringsmarkering in overeenstemming met haar 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.

8. Overeenkomstig het tweede lid van artikel 1 van dit Verdrag, nemen de partijen 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. waarborgt dat gerubriceerde gegevens niet bekend worden gemaakt of vrijgegeven aan een derde zonder de voorafgaande schriftelijke toestemming van de partij van herkomst, indien dit noodzakelijk wordt geacht, over de voorwaarden;
c. de gerubriceerde gegevens uitsluitend gebruikt voor het doel waarvoor zij zijn vrijgegeven en in overeenstemming met de eisen voor gebruik van de partij van herkomst.

Artikel 6

*Toegang tot gerubriceerde gegevens*

1. Toegang tot gerubriceerde gegevens wordt uitsluitend verleend aan de natuurlijke personen die van de gegevens op de hoogte moeten zijn (need to know), zijn ingelicht over hun verantwoordelijkheden voor de beveiliging van gerubriceerde gegevens en een geheimhoudingsverklaring hebben ondertekend in overeenstemming met de nationale wet- en regelgeving van de ontvangende partij.

2. In aanvulling van de vereisten in het eerste lid van dit artikel, wordt toegang tot gerubriceerde gegevens met een rubriceringsniveau dat overeenkomt met „CONFIDENTIAL” of hoger zoals vermeld in artikel 4 van dit Verdrag, uitsluitend verleend aan de natuurlijke personen die ook een veiligheidsmachtiging personeel hebben op het overeenkomstige niveau of die anderszins gemachtigd zijn om toegang te krijgen tot gerubriceerde gegevens uit hoofde van hun functie, in overeenstemming met de nationale wet- en regelgeving van de ontvangende partij.

Artikel 7

*Gerubriceerde contracten*

1. Op verzoek van de partij van herkomst deelt de bevoegde beveiligingsautoriteit van de ontvangende partij de bevoegde beveiligingsautoriteit van de partij van herkomst mee of een opdrachtnemer, die valt onder de rechtsmacht van de ontvangende partij en die deelneemt aan een gerubriceerd contract of precontractuele onderhandelingen over een gerubriceerd contract, een passende veiligheidsmachtiging bedrijfslocatie heeft gekregen die overeenstemt met het vereiste rubriceringsniveau. Indien de opdrachtnemer op dat moment niet over een veiligheidsmachtiging bedrijfslocatie beschikt, of indien de veiligheidsmachtiging bedrijfslocatie van een lager niveau is dan vereist, zal de bevoegde beveiligingsautoriteit die het verzoek ontvangt de verzoekende bevoegde beveiligingsautoriteit hiervan op de hoogte brengen.

2. Indien een partij of een opdrachtnemer onder haar rechtsmacht voorstelt een gerubriceerd contract met een rubriceringsniveau dat overeenkomt met „CONFIDENTIAL" 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 bevoegde beveiligingsautoriteit van de andere partij dat aan de opdrachtnemer een veiligheidsmachtiging bedrijfslocatie is 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.

3. Overeenkomstig het tweede lid van artikel 1 van dit Verdrag, waarborgt de partij in wiens rechtsgebied het gerubriceerde contract wordt uitgevoerd dat de opdrachtnemer:
a. 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 in overeenstemming met hun nationale wet- en regelgeving;
b. de beveiligingsuitvoering op zijn locaties in het oog houdt;
c. zijn bevoegde beveiligingsautoriteit onverwijld in kennis stelt van elk beveiligingsincident dat betrekking heeft op het gerubriceerd contract.

4. In aanvulling op de onderdelen a, b en c, van het derde lid van artikel 7 van dit Verdrag, met betrekking tot gerubriceerde contracten met rubriceringsniveaus die overeenkomen met „CONFIDENTIAL" of hoger, zoals vermeld in artikel 4 van dit Verdrag, waarborgt de bevoegde beveiligingsautoriteit 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.

5. Elk gerubriceerd contract dient beveiligingsvereisten te bevatten waarin de volgende aspecten vermeld staan:
a. een rubriceringsgids;
b. een procedure voor het doorgeven van wijzigingen van het rubriceringsniveau, rekening houdend met artikel 5, 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, opslag, vernietiging en retourneren van gerubriceerde gegevens;
e. contactgegevens van de bevoegde beveiligingsautoriteiten die verantwoordelijk zijn voor het toezicht op de beveiliging van gerubriceerde gegevens die betrekking hebben op het gerubriceerde contract;
f. de verplichting elk beveiligingsincident te melden bij de bevoegde beveiligingsautoriteit van de opdrachtnemer en de verplichting voor opdrachtnemers om alle redelijke maatregelen te nemen om het gevolg van een dergelijke inbreuk op de beveiliging te verminderen, in overleg met de bevoegde beveiligingsautoriteit;
g. wanneer een gerubriceerd contract geheel of gedeeltelijk wordt uitbesteed aan een onderaannemer, de verplichting om alle bepalingen betreffende onderaannemers in dit Verdrag op te leggen aan de onderaannemer;
h. een verwijzing naar dit Verdrag;
i. een verklaring dat gerubriceerde gegevens die in het kader van het gerubriceerde contract worden uitgewisseld of gegenereerd, door de opdrachtnemer worden beschermd in overeenstemming met dit Verdrag en de toepasselijke wet- en regelgeving.

6. De bevoegde beveiligingsautoriteit van de partij of een opdrachtnemer onder haar rechtsmacht die de toekenning van het gerubriceerde contract goedkeurt, stuurt een kopie van de beveiligingsvereisten naar de bevoegde beveiligingsautoriteit van de ontvangende partij, om het beveiligingstoezicht op het gerubriceerde contract te vergemakkelijken.

7. 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 8 van dit Verdrag te zijn.

Artikel 8

*Bezoeken*

1. Bezoeken waarbij toegang tot gerubriceerde gegevens op een rubriceringsniveau dat overeenkomt met „CONFIDENTIAL" of hoger zoals vermeld in artikel 4 van dit Verdrag vereist is, dienen vooraf schriftelijk te worden goedgekeurd door de respectieve bevoegde beveiligingsautoriteit van de ontvangende 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) en 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 „RESTRICTED" 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 kunnen de bevoegde beveiligingsautoriteiten een kortere termijn overeenkomen.

3. Een aanvraag voor een bezoek dient het volgende te bevatten:
a. volledige naam van de bezoeker, geboortedatum en -plaats, nationaliteit en nummer paspoort/identiteitskaart;
b. officiële titel en huidige functie van de bezoeker en naam van de organisatie die de bezoeker vertegenwoordigt of waar de bezoeker toe behoort;
c. bevestiging van de veiligheidsmachtiging personeel van de bezoeker en het niveau 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 hoogste rubriceringsniveau van de gerubriceerde gegevens die besproken worden of waartoe toegang wordt verkregen;
f. naam, adres, telefoonnummer, e-mailadres en contactpunt van de te bezoeken locatie;
g. van een datum en stempel voorziene handtekening van een vertegenwoordiger van de bevoegde beveiligingsautoriteit van de bezoeker.

4. De bevoegde beveiligingsautoriteiten kunnen een lijst overeenkomen van bezoekers die herhalingsbezoeken mogen afleggen gedurende een periode van niet langer dan twaalf maanden. De bevoegde beveiligingsautoriteiten komen nadere details van de herhalingsbezoeken overeen.

5. De bevoegde beveiligingsautoriteit van de partij die als gastheer optreedt stelt de beveiligingsbeambten van de te bezoeken organisatie in kennis van de gegevens van de natuurlijke personen van wie de bezoekaanvraag is goedgekeurd. Wanneer de goedkeuring eenmaal is verleend, kunnen de praktische aspecten van het bezoek van natuurlijke personen die herhalingsbezoeken mogen afleggen rechtstreeks geregeld worden met het betrokken agentschap of de betrokken locatie of organisatie.

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

7. De partijen waarborgen, in overeenstemming met hun nationale wet- en regelgeving, de beveiliging van de persoonsgegevens van de natuurlijke personen die een bezoek aanvragen waarbij toegang tot gerubriceerde gegevens nodig is. Deze persoonsgegevens worden niet gebruikt voor enig ander doel dan het besluit over de aanvraag voor (herhalings)bezoeken.

Artikel 9

*Overbrenging van gerubriceerde gegevens*

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

2. Elektronische overbrenging van gerubriceerde gegevens mag uitsluitend plaatsvinden met gebruikmaking van encryptie 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. Reproducties en vertalingen worden beperkt tot het minimumaantal dat nodig is voor gebruik uit hoofde van dit Verdrag.

3. Vertalingen 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 met het rubriceringsniveau dat overeenkomt met „TOP SECRET" zoals vermeld in artikel 4 van dit Verdrag worden niet gereproduceerd of vertaald zonder voorafgaande schriftelijke toestemming van de partij van herkomst.

5. Gerubriceerde gegevens met het rubriceringsniveau dat overeenkomt met „TOP SECRET" zoals vermeld in artikel 4 van dit Verdrag worden niet vernietigd zonder voorafgaande schriftelijke toestemming van de partij van herkomst. Zij worden geretourneerd aan de partij van herkomst nadat de 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.

7. Indien een crisissituatie het de ontvangende partij 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

*Beveiligingssamenwerking*

1. De bevoegde beveiligingsautoriteiten verstrekken elkaar op verzoek informatie over wijzigingen in hun nationale wet- en regelgeving, 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 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.

4. De bevoegde beveiligingsautoriteiten verlenen elkaar, op verzoek en in overeenstemming met hun 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. Bij de samenwerking uit hoofde van dit Verdrag wordt gebruikgemaakt van de Engelse taal.

Artikel 12

*Beveiligingsincident*

1. Indien een beveiligingsincident voor de gerubriceerde gegevens van de partij van herkomst wordt vermoed of is vastgesteld door de ontvangende partij, stelt deze haar bevoegde beveiligingsautoriteit hiervan

zo snel mogelijk schriftelijk in kennis. De kennisgeving dient voldoende gedetailleerde informatie te bevatten om de partij van herkomst in staat te stellen de consequenties en omstandigheden van de vermoede of feitelijke inbreuk te beoordelen.

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

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

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

Artikel 13

*Kosten*

Elke partij draagt haar eigen kosten die ontstaan in verband met de implementatie en tenuitvoerlegging van haar verplichtingen ingevolge dit Verdrag, tenzij de partijen gezamenlijk anders bepalen.

Artikel 14

*Oplossing van geschillen*

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

Artikel 15

*Uitvoeringsregelingen*

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

Artikel 16

*Slotbepalingen*

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

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

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

4. Een partij kan dit Verdrag te allen tijde schriftelijk langs diplomatieke weg beëindigen. In dat geval eindigt het Verdrag zes maanden na ontvangst van deze kennisgeving.

5. In het geval van beëindiging van dit Verdrag blijven alle uit hoofde van dit Verdrag uitgewisselde, vrijgegeven of gegenereerde gerubriceerde gegevens beveiligd in overeenstemming met de bepalingen van dit Verdrag voor de beëindiging ervan, zolang deze gerubriceerde gegevens gerubriceerd blijven.

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

GEDAAN te Bratislava op 2 juli 2024, in twee oorspronkelijke exemplaren, elk in de Nederlandse, de Slowaakse en de Engelse taal.

In geval van verschil in interpretatie is de Engelse tekst doorslaggevend.

*Voor het Koninkrijk der Nederlanden,*

GABRIELLA SANCISI

*Voor de Slowaakse Republiek,*

ROMAN KONEČNÝ

**Bijlage 1**

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 beveiligingsautoriteit van de Slowaakse Republiek is:**
   De Nationale Beveiligingsautoriteit van de Slowaakse Republiek

---

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

The Kingdom of the Netherlands

and

the Slovak Republic,

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 either exchanged between the Parties or between Contractors under their jurisdiction, or generated (in the framework of a bilateral program) under this Agreement. This Agreement sets out the security procedures and arrangements for such protection.

2. The Parties shall take all appropriate measures under their national laws and regulations to ensure the protection of Classified Information in accordance with this Agreement.

3. 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, the following definitions mean:
a) **"Agreement"** means this document including its Annexes.
b) **"Annex"** means an attachment to this document.
c) **"Classified Contract"** means any legally enforceable agreement to provide goods or services 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, which contains Classified Information or the performance of which requires access or potential access to the generation, use or transfer of Classified Information.
d) **"Classified Information"** means any information, material or object, regardless its form or nature, or any

parts thereof, marked with a security classification by one of the Parties, the unauthorised disclosure, alteration, compromise or loss of which could cause varying degrees of damage or harm to the interests of one or both of the Parties.
e) **"Competent Security Authority"** means the government authority in a Party responsible for the implementation and supervision of this Agreement. The Competent Security Authority may delegate part of its responsibilities to a delegated competent security authority.
f) **"Contractor"** means any individual (other than those engaged by a Party under a contract or employment), legal entity or other forms of organisation under the jurisdiction of a Party, entering into or bound by a Classified Contract.
g) **"Facility Security Clearance"** means the positive determination by the Competent Security Authority that a facility has in place appropriate security measures to access and handle Classified Information up to and including a specified security classification level, in accordance with its national laws and regulations.
h) **"Need to Know"** means the requirement for an individual, legal entity or other form of organisation, to access, have knowledge of, or possess Classified Information in order to be able to perform their official tasks or services.
i) **"Originating Party"** means the Party under whose authority Classified Information has been created.
j) **"Personnel Security Clearance"** means the positive determination by the Competent Security Authority that an individual has been security cleared to access and handle Classified Information up to and including a specified classification level, in accordance with its national laws and regulations.
k) **"Providing Party"** means the Party or Contractor under its jurisdiction, which provides Classified Information to the Receiving Party under this Agreement.
l) **"Receiving Party"** means the Party or Contractor under its jurisdiction, which receives Classified Information from the Providing Party under this Agreement.
m) **"Security Classification Guide"** means a document associated with a Classified Contract specifying the applicable security classification levels of each part of that Classified Contract.
n) **"Security Incident"** means any unauthorised disclosure, alteration, compromise, loss, access, handling, storage or destruction of Classified Information, contrary to national laws and regulations of the Receiving Party and/or this Agreement.
o) **"Third Party"** means any international organisation, government or state, including individuals, legal entities 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*

The following security classifications of the Parties are equivalent and correspond to the security classification levels specified in the Parties national laws and regulations. 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 the Kingdom of the Netherlands | For the Slovak Republic | Equivalent in English |
|---|---|---|
| Stg. ZEER GEHEIM | PRÍSNE TAJNÉ | TOP SECRET |
| Stg. GEHEIM | TAJNÉ | SECRET |
| Stg. CONFIDENTIEEL | DÔVERNÉ | CONFIDENTIAL |
| DEPARTEMENTAAL VERTROUWELIJK | VYHRADENÉ | RESTRICTED |

Article 5

*Security measures*

1. The Receiving Party shall mark all the Classified Information that it has received from the Providing Party or that it has generated under this Agreement with the Receiving Party's security classification that corresponds to the security classification given by the Originating Party in accordance with the scheme contained in Article 4 and, where applicable, in accordance with paragraph 4 of this Article.

2. The Receiving Party shall not modify or revoke the security classification of received or generated Classified Information under this Agreement without the written approval of the Originating Party.

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

4. The Originating Party may additionally mark the Classified Information with handling requirements, to specify any limitations on its use, disclosure, release and access by the Receiving Party.

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

6. The Parties shall afford Classified Information exchanged or generated under this Agreement at least the same protection as they afford to their own Classified Information at the corresponding security classification level.

7. In accordance with Article 1, paragraph 2, of this Agreement, the Parties shall take all appropriate measures to ensure that the Providing Party:
a) marks Classified Information with the appropriate security classification 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.

8. In accordance with Article 1, paragraph 2, of this Agreement, 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) ensures that Classified Information is not disclosed or released to a Third Party without the prior written consent of the Originating Party, if deemed necessary, on conditions;
c) uses Classified Information solely for the purpose it has been released for and in accordance with handling requirements of the Originating Party.

Article 6

*Access to Classified Information*

1. Access to Classified Information shall be granted only to those individuals who have a Need to Know, are briefed on their responsibilities for the protection of Classified Information, and have signed a statement of confidentiality in accordance with the national laws and regulations of the Receiving Party.

2. In addition to the requirements in paragraph 1 of this Article, access to Classified Information at the security classification levels equivalent to "CONFIDENTIAL" and above as mentioned in Article 4 of this Agreement, shall be granted only to those individuals who hold a Personnel Security Clearance at the corresponding level or who are otherwise duly authorised to access Classified Information by virtue of their function, in accordance with the national laws and regulations of the Receiving Party.

Article 7

*Classified Contracts*

1. Upon request of the Originating Party, the Competent Security Authority of the Receiving Party shall inform the Competent Security Authority of the Originating Party whether a Contractor, under jurisdiction of the Receiving Party and participating in a Classified Contract or precontractual negotiations regarding a Classified Contract, has been issued a Facility Security Clearance at the required security classification level. If the Contractor does not, at that point, holds a Facility Security Clearance, or the Facility Security Clearance is at a lower level than that required, the Competent Security Authority receiving the request shall inform the requesting Competent Security Authority of that fact.

2. If a Party or a Contractor under its jurisdiction proposes to grant a Classified Contract at a security classification level equivalent to "CONFIDENTIAL" or above as mentioned in Article 4 of this Agreement, with a (sub-) Contractor under the jurisdiction of the other Party, it shall first obtain written confirmation from the Competent Security Authority of the other Party that the Contractor has been granted a Facility Security Clearance at the appropriate security classification level. For Classified Contracts at the security classification level equivalent to "RESTRICTED" 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.

3. In accordance with Article 1, paragraph 2, of this Agreement, the Party under whose jurisdiction the Classified Contract is to be performed 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 in accordance with their national laws and regulations;
b) monitors the security conduct within its facilities;
c) notifies promptly its Competent Security Authority of any Security Incident relating to the Classified Contract.

4. In addition to Article 7, paragraph 3, subparagraphs a, b and c of this Agreement, for Classified Contracts at the security classification levels equivalent to "CONFIDENTIAL" or 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.

5. Every Classified Contract shall include security requirements which identify the following aspects:
a) a Security Classification Guide;
b) a procedure for communication of changes in the security classification level, taking into account Article 5, 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, storage, destruction and returning 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) the obligation to notify any Security Incidents to the Competent Security Authority of the Contractor and the obligation for Contractors to take all reasonable steps to assist in mitigating the effect of such a security violation, in consultation with the Competent Security Authority;
g) in case a Classified Contract in whole or in part is sub-contracted to a sub-Contractor, the obligation to impose all the stipulations concerning Contractors in this Agreement to the sub-Contractor;
h) a reference to this Agreement;
i) a statement that Classified Information exchanged or generated pursuant to the Classified Contract shall be protected by the Contractor in accordance with this Agreement and applicable laws and regulations.

6. The Competent Security Authority of the Party or a Contractor under its jurisdiction awarding the Classified Contract shall forward a copy of the security requirements to the Competent Security Authority of the Receiving Party, to facilitate the security oversight of the Classified Contract.

7. 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 8 of this Agreement.

## Article 8

*Visits*

1. Visits requiring access to Classified Information at a security classification level equivalent to "CONFIDENTIAL" 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 and who hold a valid Personal Security Clearance to the appropriate 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, "RESTRICTED" 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 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 Competent Security Authorities may agree on a shorter period.

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 and present position of the visitor and name of the organization the visitor represents or to which the visitor belongs;
c) confirmation of the visitor's Personnel Security Clearance and its level and 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 highest security classification level of Classified Information to be discussed or accessed;
f) name, address, phone number, e-mail address and point of contact of the facility to be visited;
g) dated and stamped signature of a representative of the visitor's Competent Security Authority.

4. The Competent Security Authorities may agree on a list of visitors entitled to recurring visits for a period not exceeding twelve months. The Competent Security Authorities shall agree on the further details of the recurring visits.

5. The Competent Security Authority of the host Party shall inform the security officials of the organization to be visited, of the details of those individuals whose visit request has been approved. Once approval has been given, visit arrangements for individuals who have been given approval for recurring visits may be made directly with the agency, facility or organization concerned.

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

7. The Parties shall ensure, pursuant to their national laws and regulations, the protection of the personal data of the individuals requesting for a visit requiring access to Classified Information. This personal data shall not be used for any other purpose than determining on the request for (recurring) visits.

Article 9

*Transmission of Classified Information*

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

2. Electronic transmission of Classified Information may take place only by using cryptographic means 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. 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 of translation, indicating that they contain Classified Information of the Originating Party.

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

5. Classified Information marked at the security classification level equivalent to "TOP SECRET" as mentioned in Article 4 of this Agreement shall be destroyed only with 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 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.

7. If a crisis situation makes it impossible for a Receiving Party 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

*Security co-operation*

1. The Competent Security Authorities shall, on request, inform each other about changes in their national laws and regulations, policies and practices for protecting Classified Information.

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

3. The Competent Security Authorities 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.

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

Article 12

*Security incident*

1. In case a Security Incident of the Classified Information of the Originating Party is suspected or ascertained by the Receiving Party, it shall inform its Competent Security Authority in writing as soon as possible. The notice must contain sufficient details for the Originating Party to assess the consequences and circumstances of the suspected or actual violation.

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

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

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

Article 13

*Costs*

Each Party shall bear its own costs incurred in the course of implementing and executing its obligations under this Agreement, unless otherwise mutually determined by the Parties.

Article 14

*Dispute resolution*

Any dispute arising from the interpretation, implementation or application of this Agreement shall be settled exclusively through consultation or negotiations between the Parties and shall not be referred to any national or international tribunal or Third Party for resolution.

Article 15

*Implementing arrangements*

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

Article 16

*Final provisions*

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

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

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

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

5. In case of termination of this Agreement, all Classified Information exchanged, released or generated under this Agreement shall remain protected in accordance with the terms of this Agreement before it was terminated, for as long as the Classified Information remains classified.

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

DONE in Bratislava on 2 July 2024 in two original copies each in the Dutch, Slovak and the English languages. In case of divergence of interpretation, the English text shall prevail.

*For the Kingdom of the Netherlands,*

GABRIELLA SANCISI

*For the Slovak Republic,*

ROMAN KONEČNÝ

**Annex 1**

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 Authority for the Slovak Republic is:**
   National Security Authority of the Slovak Republic

---

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 *vierentwintigste* juli 2024.

*De Minister van Buitenlandse Zaken,*

C.C.J. VELDKAMP

trb-2024-85
ISSN 0920 - 2218
's-Gravenhage 2024