

TRACTATENBLAD

VAN HET

KONINKRIJK DER NEDERLANDEN

JAARGANG 2026 Nr. 89

A. TITEL

*Verdrag tussen het Koninkrijk der Nederlanden en de Republiek Malta inzake de wederzijdse beveiliging en uitwisseling van gerubriceerde gegevens (met Bijlage);
Floriana, 28 juli 2026*

Voor een overzicht van de verdragsgegevens, zie verdragsnummer 014021 in de Verdragenbank.

B. TEKST

Agreement between the Kingdom of the Netherlands and the Republic of Malta on mutual protection and exchange of classified information

The Kingdom of the Netherlands

and

the Republic of Malta,

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

Objective and Scope

1. The objective of this Agreement is to ensure protection of Classified Information that is commonly generated or exchanged between the Parties or between Contractors under their jurisdiction.
2. This Agreement shall apply to any contract or agreement as well as any other cooperation between the Parties or between Contractors under their jurisdiction involving Classified Information.
3. This Agreement shall apply to any activities, contracts or agreements involving Classified Information that will be conducted or concluded between the Parties following the entry into force of this Agreement.
4. The provisions of this Agreement shall also apply to the Classified Information already exchanged or generated in the process of cooperation between the Parties before the entry into force of this Agreement.
5. This Agreement does not constitute a basis to compel the provision or exchange of Classified Information by the Parties.
6. This Agreement may not be invoked by either Party to obtain Classified Information that the other Party has received from a Third Party.

Article 2

Definitions

For the purposes of this Agreement:

- a) "Breach of Security" means an omission, or act, contrary to the national laws and regulations and/or this Agreement, the result of which leads, or may lead, to disclosure, loss, destruction, misappropriation or any type of compromise of Classified Information;
- b) "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;
- c) "Classified Information" means any information, document or material, irrespective of its form or nature, generated by or exchanged between the Parties, requiring protection against unauthorised disclosure, loss, destruction, misappropriation or any type of compromise and having been classified by one of the Parties;
- d) "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;
- e) "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;
- f) "Facility Security Clearance" means the determination by the Competent Security Authority confirming, that the facility has in place the appropriate security measures to use and store Classified Information in accordance with its national laws and regulations;
- g) "Host Party" means the Party to whose territory a visit takes place;
- h) "Need-to-know" means the necessity to have access to Classified Information in the scope of a given official position and/or for the performance of a specific task;
- i) "Originating Party" means the Party under whose authority Classified Information has been created;
- j) "Personnel Security Clearance" means the determination by the Competent Security Authority confirming, in accordance with national laws and regulations, as to whether an individual is eligible to have access to Classified Information and up to which security classification level such individual shall be eligible to have access to;
- k) "Receiving Party" means the Party, including any entity under its jurisdiction, to which Classified Information of the Originating Party is transmitted;
- l) "Sub-contractor" means a Contractor to whom a prime Contractor grants a sub-contract;
- m) "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

Security Classification Levels

1. The Parties agree that the following security classification levels are equivalent and correspond to the security classification levels specified in their national laws and regulations. For the Republic of Malta, the Maltese and English markings can be used interchangeably.

FOR THE REPUBLIC OF MALTA	FOR THE KINGDOM OF THE NETHERLANDS
L-OGHĦLA SEGRETEZZA TOP SECRET	Stg. ZEER GEHEIM
SIGRIET SECRET	Stg. GEHEIM
KUNFIDENZJALI CONFIDENTIAL	Stg. CONFIDENTIEEL
RISTRETT RESTRICTED	DEPARTEMENTAAL VERTROUWELIJK

2. Military Classified Information of the Kingdom of the Netherlands marked as DEPARTEMENTAAL VERTROUWELIJK may be subject to additional security measures provided by the Competent Security Authority of the Kingdom of the Netherlands.

3. 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.

4. The Competent Security Authorities shall inform one another of any new or further security classification concerning any information, which could be exchanged or produced under this Agreement.

Article 4

Competent Security Authorities

1. The Competent Security Authorities of the Parties are listed in the Annex of this Agreement.
2. The Competent Security Authorities shall provide one another with official contact details and changes thereof.
3. The Parties shall inform one another through diplomatic channels about changes in the Competent Security Authorities.
4. The Competent Security Authorities shall inform one another, on request, of the laws and regulations in force in their Parties, as well as any changes regarding the protection of Classified Information generated or exchanged in accordance with this Agreement.
5. In order to achieve and maintain equivalent standards of security, the Competent Security Authorities may provide one another with information about the security standards, procedures and practises for the protection of Classified Information employed by the respective Party.

Article 5

Security Cooperation

1. Within the scope of this Agreement, each Party shall mutually recognise the Personnel and Facility Security Clearances granted in accordance with the national laws and regulations of the other Party. The security clearances shall be equivalent in accordance with article 3 of this Agreement.
2. The Competent Security Authorities shall assist one another in carrying out Facility Security Clearance and Personnel Security Clearance investigations on request and in accordance with their national laws and regulations.
3. Upon request of the Competent Security Authority of the Originating Party, the Competent Security Authority of the Receiving Party shall issue a written confirmation that an individual has been issued a Personnel Security Clearance or a legal entity has been issued a Facility Security Clearance.
4. If the Competent Security Authorities of one of the Parties considers that a company registered on its national territory is owned or controlled by a Third Party whose aims are not compatible with its interests, that company shall not be issued a Facility Security Clearance. The Competent Security Authorities of the Parties that applied for a Facility Security Clearance shall be notified accordingly as quickly as possible.
5. The Competent Security Authorities shall promptly notify one another in writing about changes in recognised Personnel Security Clearances and Facility Security Clearances for whom or for which a confirmation or a rejection has been provided.
6. The cooperation under this Agreement shall be effected in English.

Article 6

Protection of Classified Information

1. In accordance with their national laws and regulations, the Parties shall take all appropriate measures for the protection of Classified Information, which is exchanged or generated under this Agreement. As a minimum, the same level of protection shall be assigned to such Classified Information as is provided for the national Classified Information of the equivalent security classification level in accordance with article 3 of this Agreement.
2. Regarding the security of agencies, offices and facilities under their jurisdiction, the Parties shall ensure that any requirements arising from the national security laws and regulations are complied with, in particular via inspections.
3. The Originating Party shall inform the Receiving Party in writing about any change of the security classification level of the provided Classified Information, in order to apply the appropriate protection measures.

4. 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.
5. In addition to the requirements in paragraph 4 of this article, access to Classified Information at the security classification levels equivalent to KUNFIDENZJALI / CONFIDENTIAL / Stg. CONFIDENTIEEL and above as mentioned in article 3 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.
6. Classified Information jointly originated by the Parties shall be assigned a security classification level that is mutually determined by the Parties.
7. The Receiving Party shall:
 - a) submit Classified Information to any Third Party only upon prior written consent of the Originating Party;
 - b) mark the received Classified Information in accordance with article 3 of this Agreement;
 - c) not downgrade or declassify the provided Classified Information without the prior written consent of the Originating Party; and
 - d) use Classified Information solely for the purposes it has been provided for.

Article 7

Transmission of Classified Information

1. Classified Information shall be transmitted in accordance with the national laws and regulations of the Originating Party through diplomatic channels unless otherwise agreed upon by the Competent Security Authorities.
2. The Competent Security Authorities of both Parties may, by mutual agreement, agree that Classified Information may be transferred by a means other than through diplomatic channels when this method of transfer proves to be unsuitable or difficult.
3. Electronic transmission of Classified Information shall only be carried out through certified cryptographic means agreed upon by the Parties.
4. If transferred Classified Information is marked KUNFIDENZJALI / CONFIDENTIAL / Stg. CONFIDENTIEEL and above, the Receiving Party shall confirm the receipt in writing. The receipt of other Classified Information shall be confirmed upon request.
5. The transfer of an important quantity of Classified Information shall be organised between the respective Competent Security Authorities on a case-by-case basis.

Article 8

Reproduction and Translation of Classified Information

1. Translations and reproductions of Classified Information shall be made in accordance with the national laws and regulations of the Receiving Party and the following procedures:
 - a) the translators shall be granted the appropriate Personnel Security Clearance in accordance with their national laws and regulations;
 - b) the translations and the reproductions shall be marked and protected as the original Classified Information;
 - c) the translations and the number of copies shall be limited to that required for official purposes; and
 - d) the translations shall bear an appropriate note in the language of the translation indicating that it contains Classified Information received from the Originating Party.
2. Classified Information marked SIGRIET / SECRET / Stg. GEHEIM or above shall be translated or reproduced only in exceptional cases and upon the prior written consent of the Originating Party.

Article 9

Destruction of Classified Information

1. Classified Information shall be destroyed after having been recognised as no longer necessary by the Receiving Party, so as to prevent its partial or total reconstruction, with the exception of information classi-

fied as L-OGHΛA SEGRETEZZA / TOP SECRET / Stg. ZEER GEHEIM. Classified Information marked L-OGHΛA SEGRETEZZA / TOP SECRET / Stg. ZEER GEHEIM shall be returned to the Originating Party after it is no longer considered necessary by the Receiving Party.

2. Classified Information marked up to SIGRIET/ SECRET / Stg. GEHEIM or below shall be destroyed after having been recognised as no longer necessary by the Receiving Party, insofar as to prevent its reconstruction in whole or in part. Classified Information marked up to SIGRIET/ SECRET / Stg. GEHEIM or below shall be destroyed in such a way that it is impossible to restore it in whole or in part.

3. The Receiving Party shall notify the Originating Party about the destruction of information classified as KUNFIDENZJALI / CONFIDENTIAL / Stg. CONFIDENTIEEL or above.

4. In case of a crisis situation, which makes it impossible to protect or return Classified Information generated or exchanged under this Agreement, Classified Information shall be destroyed immediately. The Competent Security Authority of the Receiving Party shall notify the Competent Security Authority of the Originating Party about the destruction of Classified Information as soon as possible.

Article 10

Classified Contracts

1. The Competent Security Authority of the Originating Party shall notify the Competent Security Authority of the Receiving Party of any Classified Contract prior to any exchange of Classified Information. This notification must specify the highest level of classification of the information involved in the Contract.

2. A Party that intends to enter into or to authorise one of its Contractors to enter into a Classified Contract with a Contractor of the other Party shall check with the Competent Security Authorities of the Receiving Party that the latter has the suitable clearance level required in order to perform the Classified Contract.

3. Upon request of the Originating Party, the Competent Security Authority of the Receiving Party shall confirm that a proposed Contractor has been issued an appropriate Personnel and/or Facility Security Clearance. If the proposed Contractor does not hold an appropriate security clearance, the Competent Security Authority of the Originating Party may request the Competent Security Authority of the Receiving Party to issue the appropriate security clearance.

4. The Competent Security Authority in which jurisdiction the Classified Contract is to be performed, shall assume the responsibility for prescribing and administering security measures for the respective Classified Contract under the same standards and requirements that rule the protection of the Classified Contracts of the respective Parties in accordance with article 3 of this Agreement.

5. A Classified Contract shall include a specific section or security annex identifying the security requirements of the Classified Contract. The security annex shall be an integral part of each Classified Contract, or sub-contract, by which the Originating Party shall specify which Classified Information is to be released to the Receiving Party, which security classification level has been assigned to that information and the Contractor and/or Sub-contractor's obligations to protect the Classified Information. These instructions shall be consistent with those given by the Competent Security Authority of the Originating Party. The Competent Security Authority of the Originating Party shall send a copy of the security annex to the Competent Security Authority of the other Party.

6. Each Classified Contract concluded in accordance with this Agreement shall include:

- a) obligation of the Contractor to ensure that its premises have necessary conditions for handling and storing Classified Information of appropriate security classification level;
- b) obligation of the Contractor to ensure that persons who perform duties requiring access to Classified Information are granted the appropriate level of Personnel Security Clearance;
- c) obligation of the Contractor to ensure that all persons with access to Classified Information are informed of their responsibility towards the protection of Classified Information in accordance with the national laws and regulations;
- d) obligation of the Contractor to allow periodical security inspections of its premises;
- e) list of Classified Information and list of areas in which Classified Information may arise;
- f) list of communication means and electronic means for transmission;
- g) instructions for the handling, storage, destruction and returning of Classified Information;
- h) procedure for the transportation of Classified Information;
- i) list of appropriate authorised individuals or legal entities responsible for the coordination of the safeguarding of Classified Information related to the Classified Contract;
- j) procedure for reporting any changes in the security classification level of Classified Information;
- k) the obligation of the Contractor to notify any Breach of Security to the Competent Security Authority;

- l) contact details of the Competent Security Authorities responsible for overseeing the protection of Classified Information related to the Classified Contract;
 - m) obligation of the Contractor to forward a copy of the Classified Contract to its own Competent Security Authority;
 - n) 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; and
 - o) 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.
7. Prior to the release to either Party's Contractors or prospective Contractors of any Classified Information received from the other Party, the Receiving Party shall, in accordance with its national laws and regulations, ensure that Contractors or prospective Contractors can afford adequate security protection to Classified Information and:
- a) perform an appropriate Facility Security Clearance procedure of the Contractors and Sub-contractors;
 - b) perform an appropriate Personnel Security Clearance procedure for all personnel whose duties require access to Classified Information;
 - c) ensure that all persons having access to Classified Information are informed of their responsibilities and obligations;
 - d) carry out periodic security inspections of relevant security-cleared facilities.
8. As soon as pre-contractual negotiations begin between a potential Contractor under the jurisdiction of one Party and another possible Contractor under the jurisdiction of the other Party, aiming at the signing of Classified Contracts, the Competent Security Authority shall inform the other Party of the security classification level given to the Classified Information related to those pre-contractual negotiations.
9. Copy of each Classified Contract shall be forwarded to the Competent Security Authority of the Party where the work is to be performed, to allow adequate security supervision and control.
10. If a Classified Contract allows the Contractor that part of the Classified Contract is performed by a Sub-contractor:
- a) Prior to executing a Classified Contract with a Sub-contractor, the Contractor shall, through its Competent Security Authority, obtain the authorisation of the Competent Security Authority falling under the jurisdiction of the Sub-contractor;
 - b) All the articles in this Agreement, concerning the Contractor, shall also apply to and be imposed on the Sub-contractor;
 - c) Whenever a Contractor engages a Sub-contractor outside the jurisdiction of one of the Parties, prior written approval of the Originating Party of the involved Classified Information in the Classified Contract is required.
11. Classified Contracts shall be concluded and implemented in accordance with national laws and regulations.

Article 11

Visits

- 1. Visits requiring access to Classified Information shall be subject to prior written consent given by the Competent Security Authority of the Host Party.
- 2. Visits involving access to Classified Information shall be allowed only if the visitors have been granted the appropriate Personnel Security Clearance and authorised to receive or to have access to Classified Information in accordance with their national laws and regulations.
- 3. Visits involving access to Classified Information by nationals from a Third Party shall only be authorised by a common agreement between the Parties.
- 4. The Competent Security Authority of the Host Party shall receive a request for visit from the other Competent Security Authority at least ten (10) working days in advance. The request for visit shall include:
 - a) The visitor's name and surname, place and date of birth, nationality, passport or identification document number;
 - b) The job and position of the visitor;
 - c) The name of the legal entity represented by the visitor;
 - d) The name, address and point of contact of the legal entity to be visited;
 - e) The confirmation of the visitor's Personnel Security Clearance and its validity;
 - f) The purpose of the visit, as well as a statement of the highest security classification level of the Classified Information to be involved;

- g) The expected date and duration of the requested visit; and
 - h) The date, signature and stamping of the official seal of the Competent Security Authority of the requesting Party.
5. The validity of visit approval shall not exceed one (1) year. In case of recurring visits, the total period covered by the visits shall be stated in the request for visit. The Parties may draw up lists of individuals authorised to make recurring visits. The lists shall be valid for a maximum of twelve (12) months upon agreement between the Competent Security Authorities of the Parties. The lists shall be drawn up in accordance with the national laws and regulations of the Host Party.
6. The Competent Security Authority of the Host Party shall inform the security officials of the agency, facility and organisation to be visited, including 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 organisation concerned.
7. In urgent cases, the request for visit shall be transmitted in writing at least seven (7) days in advance.
8. All visitors shall comply with the security regulations and instructions of the Host Party.
9. Either Party shall ensure the protection of personal data and, health and safety of the visitors according to its respective national laws and regulations.

Article 12

Breach of Security

1. The Competent Security Authority of the Receiving Party shall immediately notify the Competent Security Authority of the Originating Party in writing of any suspicion or discovery of a Breach of Security. The notice must contain enough details so that the Originating Party may fully assess the consequences.
2. The Competent Security Authority of the Receiving Party shall undertake all possible appropriate measures in accordance with its national laws and regulations so as to limit the consequences of the Breach of Security and to prevent further violations and ensure the appropriate investigation.
3. Upon request, the Competent Security Authority of the Originating Party shall provide investigative assistance.
4. The Competent Security Authority of the Receiving Party shall inform the Competent Security Authority of the Originating Party of the outcome of the proceedings and the corrective measures undertaken due to the violation.
5. If a breach of security occurs during transportation in a Third Party, the Competent Security Authority of the dispatching Party shall take the actions prescribed in paragraph 1 of this article.
6. The Originating Party shall be informed of the results of the investigation and shall receive a report, in English, on the reasons and extent of the damage.

Article 13

Costs

Each Party shall bear its own costs incurred in the course of application and supervision of this Agreement.

Article 14

Settlement of Disputes

Any dispute regarding the interpretation, implementation or application of this Agreement shall be solved exclusively through diplomatic channels between the Parties unless a settlement by the Competent Security Authorities can be achieved. Any dispute shall not be referred to any national or international tribunal or court or to any Third Party for settlement. Meanwhile, the Parties shall continue to fulfil the provisions set forth in this Agreement.

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

4. This Agreement may be terminated by a Party through diplomatic channels. In that case, the termination takes effect six (6) months from the date on which the other Party has received the notice through diplomatic channels.

5. In case of termination of this Agreement, all Classified Information exchanged, released or generated pursuant to this Agreement shall continue to be protected in accordance with the provisions set forth herein and, upon request, returned to the Originating Party.

IN WITNESS WHEREOF, the undersigned representatives, being duly authorised by their respective Governments, have signed this Agreement.

DONE in Floriana on 28-07-2026, in two original copies, in the English language.

For the Kingdom of the Netherlands,

DJOEKE ADIMI-KOEKKOEK

For the Republic of Malta,

JOSEPH BUGEJA

Annex

The Competent Security Authority for the Republic of Malta is:
National Security Authority
Ministry for Home Affairs, Security, Reforms and Equality (MHSR)

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

D. PARLEMENT

Het Verdrag, met Bijlage, heeft 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 *tiende* augustus 2026.

De Minister van Buitenlandse Zaken,

T.B.W. BERENDSEN