

Agreement

between

the Government of the Republic of Bulgaria

and

the Swiss Federal Council

**on mutual protection and exchange of Classified
Information**

The Government of the Republic of Bulgaria and the Swiss Federal Council (hereinafter referred to as the “Parties”),

Having agreed to hold talks on political and security-related issues and to broaden and tighten their political, military and economic co-operation,

Being aware of the changes in the political situation in the world and recognising the important role of their mutual co-operation for the stabilisation of peace, international security and mutual confidence,

Realising that good co-operation may require the exchange of Classified Information between the Parties,

Desiring to create a set of rules regulating the mutual protection of Classified Information applicable to any future co-operation agreements and Classified Contracts, which will be implemented between the Parties, containing or involving Classified Information,

Have agreed as follows:

Article 1

Objective and Scope

The objective of this Agreement is to ensure the protection of Classified Information that is commonly generated or exchanged either directly or indirectly between the Parties.

This Agreement sets out the procedures, under the laws and regulations of each Party, regarding the application of security principles for the protection of Classified Information exchanged between the Parties.

Article 2

Definitions

For the purpose of this Agreement:

- (1) **“Classified Information”** means information and material of whatever form, nature or method of transmission either manufactured or in the process of manufacture to which a Security Classification Level has been attributed and which, in the interests of national security and in accordance with national laws and regulations, require protection against Unauthorised Access or disclosure.
- (2) **“Security Classification Level”** means the category which, in accordance with the national laws and regulations, characterises the importance of Classified Information, the level of restriction which access to it is subject and the degree of protection which it must meet by the Parties, as well as the category on the basis of which the information is identified.
- (3) **“Competent Security Authority”** means the authority which in compliance with the national laws and regulations of the respective Party performs the State policy for the protection of Classified Information, exercises overall control in this sphere as well as on the implementation of this Agreement. Such authorities are listed in Article 4 of this Agreement.
- (4) **“Originating Party”** means the Party that creates Classified Information.
- (5) **“Receiving Party”** means the Party to which Classified Information is transmitted.
- (6) **“Third Party”** means any person, state or national or international organisation, public or private entity which is not a Party to this Agreement.
- 7) **“Need-to-know” principle** means the necessity to have access to Classified Information in connection with official duties and/or for the performance of a Classified Contract”.
- (8) **“Personnel Security Clearance”** means a positive determination stemming from a vetting procedure that ascertains the loyalty and trustworthiness of an individual entity as well as other security aspects in accordance with national laws and regulations. Such determination enables the individual to be granted access and allows them to handle Classified Information at a certain level without security risk.

(9) **“Facility Security Clearance”** means a determination issued by the competent authority as a result of a vetting procedure which ascertains that, on matters of security, a certain legal entity meets the physical and organisational requirements for the creation, processing and storing of Classified Information in accordance with the national laws and regulations.

(10) **“Contractor”** means an individual or a legal entity possessing the legal capacity to conclude Classified Contracts.

(11) **“Classified Contract”** means a contract which contains or the implementation of which requires access to Classified Information.

(12) **“Declassification of Information”** means the removal of the Security Classification Level.

(13) **“Unauthorised Access to Classified Information”** means any form of disclosure of Classified Information, including misuse, damage, and incorrect classification thereof as well as any other actions, resulting in breach of protection or loss of such information, as well as any actions or inactions that have resulted in making the information known to an unauthorised person.

(14) **“Breach of security”** means an act or an omission contrary to the national laws and regulations which results or may result in an Unauthorised Access or destruction of Classified Information.

Article 3

Security Classification Levels

The Parties agree that the following Security Classification Levels are equivalent and correspond to the Security Classification Levels specified in the national laws and regulations of the respective Party:

For the Republic of Bulgaria	Equivalent in English	For the Swiss Confederation
СЕКРЕТНО	SECRET	GEHEIM/ SECRET/ SEGRETO
ПОВЕРЛИВО	CONFIDENTIAL	VERTRAULICH/ CONFIDENTIEL/ CONFIDENZIALE
ЗА СЛУЖЕБНО ПОЛЗВАНЕ	RESTRICTED	INTERN/ INTERNE/ Ad USO INTERNO

Article 4

Competent Security Authorities

(1) The Competent Security Authorities of the Parties are:

For the Republic of Bulgaria:

State Commission on Information Security

For the Swiss Federal Council:

Federal Department of Defence, Civil Protection and Sport (DDPS)
State Secretariat for Security Policy
Federal Unit for Information Security

(2) The Competent Security Authorities shall inform each other of the national laws and regulations in force regulating the protection of Classified Information.

(3) In order to ensure close co-operation in the implementation of the present Agreement, the Competent Security Authorities may hold consultations in response to a request made by either of them.

(4) In order to achieve and maintain comparable standards of security, the respective Competent Security Authorities shall, on request, provide each other with information about the security standards, procedures and practices for protection of Classified Information employed by the respective Party.

(5) The Intelligence and Counterintelligence Services of the Parties may exchange and return operative information directly with each other in accordance with national laws and regulations.

(6) The Parties shall notify each other through diplomatic channels of any subsequent changes to their Competent Security Authorities.

Article 5

Access to Classified Information

(1) In compliance with their national laws and regulations, the Parties shall implement all appropriate measures for the protection of Classified Information which is commonly generated or exchanged either directly or indirectly under

this Agreement. The same level of protection shall be ensured for such Classified Information as is provided for national Classified Information, with the corresponding Security Classification Level.

(2) The Parties shall in due time inform each other about any changes in the national laws and regulations affecting the protection of Classified Information. In such cases, the Parties shall inform each other in compliance with Paragraphs 3 and 4 of Article 4 in order to discuss possible amendments to this Agreement. Meanwhile, the Classified Information shall be protected according to the provisions of the Agreement, unless otherwise agreed in writing.

(3) No individual shall be entitled to access Classified Information solely by virtue of his or her rank, official position or security clearance. Access to Classified Information at the level of ПОВЕРЛИВО/ CONFIDENTIAL/ VERTRAULICH/ CONFIDENTIEL/ CONFIDENZIALE and above shall be granted only to those individuals who have been issued a security clearance and in accordance with the "Need-to-know" principle.

(4) The Receiving Party shall:

- a) not disclose Classified Information to a Third Party without the prior written consent of the Competent Security Authority of the Originating Party;
- b) grant Classified Information a Security Classification Level equivalent to that provided by the Originating Party;
- c) not use Classified Information for other purposes than those it has been provided for;
- d) guarantee private rights, such as patent rights, copyrights or trade secrets that are attached to Classified Information.

(5) If any other Agreement concluded between the Parties contains stricter regulations regarding the exchange or protection of Classified Information, those regulations shall apply.

Article 6

Transfer of Classified Information

(1) As a rule, Classified Information shall be transferred by means of diplomatic or military couriers or by other means satisfying the requirements of the national laws and regulations of the Parties. The Receiving Party shall confirm in writing the receipt of Classified Information.

(2) Classified Information may be transmitted via protected telecommunication systems, networks or other electromagnetic means approved by the Competent Security Authorities and holding a certificate duly issued pursuant to the national laws and regulations of either Party.

(3) Other approved means of transfer of Classified Information may only be used if agreed upon between the Competent Security Authorities.

(4) In the case of transferring a large consignment containing Classified Information, the Competent Security Authorities shall mutually agree on and approve the means of transportation, the route and the other security measures.

Article 7

Translation, reproduction, destruction

(1) All translations of Classified Information shall be made by individuals who have appropriate Personnel Security Clearance. Such translation shall bear the same security classification marking in accordance with Article 3 as the original document.

(2) When Classified Information is reproduced, all original security markings thereon shall also be reproduced or marked on each copy. Such reproduced information shall be placed under the same control as the original information. The number of copies shall be limited to that required for official purposes.

(3) Classified Information shall be destroyed or modified insofar as required to prevent its reconstruction in whole or in part.

(4) The Originating Party may expressly prohibit the reproduction, alteration or destruction of Classified Information by marking the relevant carrier of Classified Information or by sending subsequent written notice. If destruction of Classified Information is prohibited, it shall be returned to the Competent Security Authority of the Originating Party.

(5) In the case of a crisis situation which makes it impossible to protect and return Classified Information generated or transferred according to this Agreement, the Classified Information shall be destroyed immediately. The Receiving Party shall notify the Competent Security Authority of the Originating Party of the destruction of the Classified Information as soon as possible.

Article 8

Classified Contracts

(1) Classified Contracts shall be concluded and implemented in accordance with national laws and regulations of each Party. Upon request, the Competent Security Authority of each Party shall furnish information as to whether a proposed Contractor has been issued with a Facility Security Clearance corresponding to the required Security Classification Level. If the proposed Contractor does not hold a Facility Security Clearance, the Competent Security Authority of each Party may request that the Contractor be security cleared.

(2) A security annex will be an integral part of each Classified Contract or sub-contract. In this annex the contract awarding authority shall specify which Classified Information will be released to or generated by the Receiving Party. The security annex shall contain provisions on the security requirements. A copy of the security annex shall be submitted to the Competent Security Authorities of the Parties.

(3) The Contractor's obligation to protect the Classified Information shall, in all cases, refer, at least, to the following:

a) an obligation that the Contractor shall disclose the Classified Information only to a person who has been previously security cleared for access with regard to the relevant contract activities, who has a "need-to-know" and who is employed or engaged in carrying out the contract;

b) the means to be used for the transfer of the Classified Information;

c) the procedures and mechanisms for communicating the changes that may arise in respect of Classified Information either because of changes in its Security Classification Level or because protection is no longer necessary;

d) the procedure for the approval of visits, access or inspection by personnel of one Party to facilities of the other Party which are covered by the contract;

e) an obligation to notify in due time the Contractor's Competent Security Authority of any actual, attempted or suspected Unauthorised Access to Classified Information of the contract;

f) that the Classified Information under the contract may only be used for purposes related to the subject of the contract;

g) strict adherence to the procedures for destruction of the Classified Information;

h) provisions that Classified Information generated under the contract may only be forwarded to any Third Party with the written consent of the Competent Security Authority of the Originating Party.

(4) The measures required for the protection of Classified Information as well as the procedure for the assessment of and the indemnification for possible losses caused to the Contractors by Unauthorised Access to Classified Information shall be specified in more detail in the respective Classified Contract.

(5) Contracts placed with Contractors involving Classified Information at 3A CЛYЖЕБHO ПOЛЗBAHE/ RESTRICTED/ INTERN/ INTERNE/ Ad USO INTERNO levels shall contain an appropriate clause identifying the minimum measures to be applied for the protection of such Classified Information. A Facility Security Clearance as well as Personnel Security Clearances shall not be necessary for this kind of contract.

Article 9

Visits

(1) Security experts of the Competent Security Authorities may hold regular meetings to discuss the procedures for protection of Classified Information.

(2) Visitors shall receive prior authorisation from the Competent Security Authority of the host Party only if they are authorised for access to Classified Information in accordance with their national laws and regulations and if they need access to Classified Information or to premises where Classified Information is originated, handled or stored. The authorisation may be obtained by submitting a request for visit.

(3) Visiting procedures shall be agreed between the Competent Security Authorities.

(4) The request for visit shall contain the following information:

- a) name of the visitor(s), date and place of birth, passport (ID card) number;
- b) citizenships of the visitor(s);
- c) position title of the visitor(s) and name of the organisation she/he/they represent/s;
- d) security clearance of the visitor(s) of appropriate classification level;

e) purpose, proposed working programme and planned date of the visit;

f) names of organisations and facilities requested to be visited.

(5) The Competent Security Authorities of the Parties may agree to establish lists of authorized persons to make recurring visits. Those lists are valid for an initial period of twelve months. Once those lists have been approved by the Competent Security Authorities of the Parties, the terms of the specific visits shall be directly arranged with the appropriate authorities of the organisations to be visited by those persons, in accordance with the terms and conditions agreed upon.

(6) Each Party shall guarantee protection of personal data of the visitors, in accordance with the respective national laws and regulations.

Article 10 Breach of Security

(1) In the event of a Breach of Security, the Competent Security Authority in whose state a Breach of Security has occurred shall inform the Competent Security Authority of the other Party as soon as possible and shall carry out the appropriate investigation. The other Party shall, if required, cooperate in the investigation.

(2) In the event of a Breach of Security occurs in a third country, the Competent Security Authority of the Originating Party shall take the actions under paragraph 1, where possible.

(3) In every case, the other Party shall be informed of the results of the investigation and shall receive the final report on the reasons and extent of damage caused.

Article 11 Expenses

Each Party shall bear its own expenses incurred in the course of implementing its obligations under this Agreement.

Article 12 Final Provisions

(1) This Agreement is concluded for an indefinite period of time and enters into force on the date of receiving the latest notice whereby the Parties inform each

other through diplomatic channels of the fulfilment of all internal legal procedures necessary for its entry into force.

(2) This Agreement may be amended on the basis of mutual written consent by both Parties. Such amendments shall enter into force in accordance with Paragraph 1 of this Article.

(3) Each Party may terminate this Agreement by written notice forwarded to the other Party. The termination shall enter into force six months after the date of receipt of the notification. Notwithstanding the termination of this Agreement, all Classified Information transferred pursuant to this Agreement shall continue to be protected in accordance with the provisions set forth herein, until the Originating Party dispenses the Receiving Party from this obligation.

(4) Any dispute regarding the interpretation or application of this Agreement shall be resolved amicably by consultation between the Parties without recourse to outside jurisdiction.

In witness whereof the undersigned, being duly authorized by their respective Governments, have signed this Agreement in 2 original copies, each in the Bulgarian, German and English languages, all texts being equally authentic. In case of any divergence of interpretation, the English language text shall prevail.

Signed in Sofia

on 26.11.2025

FOR THE GOVERNMENT
OF REPUBLIC OF BULGARIA

Petar GROSHLEV

Chairperson of the State Commission
on Information Security

Signed in Bern

on 20.01.2026

FOR THE SWISS FEDERAL
COUNCIL

Dr. Markus MÄDER

State Secretary
State Secretariat for Security Policy