No. 55230*

Georgia
and
Germany

Agreement between the Government of Georgia and the Government of the Federal Republic of Germany on the exchange and mutual protection of classified information. Tbilisi, 16 November 2017

Entry into force: *14 May 2018 by notification, in accordance with article 16*

Authentic texts: *English, Georgian and German*

Registration with the Secretariat of the United Nations: *Georgia, 29 June 2018*

*No UNTS volume number has yet been determined for this record. The Text(s) reproduced below, if attached, are the authentic texts of the agreement /action attachment as submitted for registration and publication to the Secretariat. For ease of reference they were sequentially paginated. Translations, if attached, are not final and are provided for information only.

Géorgie
et
Allemagne

Accord entre le Gouvernement de la Géorgie et le Gouvernement de la République fédérale d'Allemagne sur l'échange et la protection mutuelle des informations classifiées. Tbilissi, 16 novembre 2017

Entrée en vigueur : *14 mai 2018 par notification, conformément à l'article 16*

Textes authentiques : *anglais, géorgien et allemand*

Enregistrement auprès du Secrétariat de l'Organisation des Nations Unies : *Géorgie, 29 juin 2018*

*Aucun numéro de volume n'a encore été attribué à ce dossier. Les textes disponibles qui sont reproduits ci-dessous sont les textes originaux de l'accord ou de l'action tels que soumis pour enregistrement. Par souci de clarté, leurs pages ont été numérotées. Les traductions qui accompagnent ces textes ne sont pas définitives et sont fournies uniquement à titre d'information.

[ENGLISH TEXT – TEXTE ANGLAIS]

Agreement

between

the Government of Georgia

and

the Government of the Federal Republic of Germany

on the

Exchange and Mutual Protection of Classified Information

The Government of Georgia

and

the Government of the Federal Republic of Germany,

(Hereinafter collectively referred to as „Contracting Parties" and each as „Contracting Party"),

Intending to ensure the protection of classified information that is exchanged between the competent authorities of Georgia and the Federal Republic of Germany as well as with contractors in the territory of the state of the other Contracting Party or between contractors of the two Contracting Parties,

Desirous of laying down an arrangement on the mutual protection of classified information that shall apply to all agreements on cooperation to be concluded between the Contracting Parties and to contracts involving an exchange of classified information,

Have agreed as follows:

Article 1
Definitions

(1) For the purposes of this Agreement

1. „classified information" is

a) in the Federal Republic of Germany

facts, items or knowledge which, regardless of how they are presented, are to be kept secret in the public interest. They shall be classified by, or at the instance of, an official agency in accordance with their need for protection;

b) in Georgia
data/information or a material item (regardless of its form or nature), that has been processed or is in the process of processing, which requires protection against unauthorized handling, includes data/information containing state secrets in the fields of defence, economy, foreign relations, intelligence, state security and protection of law and order of the state and which constitutes state secrets according to the legislation of Georgia.

2. a „classified contract" is

a contract/subcontract between an authority or an enterprise from the state of one Contracting Party (contracting officer) and an authority or enterprise from the state of the other Contracting Party (contractor); under such contract, classified information from the state of the contracting officer is to be released to the contractor, is to be developed by the contractor or is to be made accessible to members of the contractor's staff who are to perform tasks in facilities of the contracting officer.

(2) The levels of security classification are defined as follows:

1. In the Federal Republic of Germany, classified information is

a) STRENG GEHEIM - if knowledge of it by unauthorized persons may pose a threat to the existence or vital interests of the Federal Republic of Germany or one of its federal states *(Länder)*;

b) GEHEIM - if knowledge of it by unauthorized persons may pose a threat to the security of the Federal Republic of Germany or one of its federal states *(Länder)*, or may cause severe damage to their interests;

c) VS-VERTRAULICH - if knowledge of it by unauthorized persons may be damaging to the interests of the Federal Republic of Germany or one of its federal states *(Länder)*;

d) VS-NUR FÜR DEN DIENSTGEBRAUCH - if knowledge of it by unauthorized persons may be disadvantageous to the interests of the Federal Republic of Germany or one of its federal states *(Länder)*.

2. In Georgia, classified information is

a) „განსაკუთრებული მნიშვნელობის" (equivalent to TOP SECRET) - data the dissemination or loss of which may substantially affect the state interests of Georgia in the fields of defence, economy, state security, protection of law and order, and politics of the state, and/or cause the most severe consequences to a state or an organization being a party to an international treaty of Georgia;

b) „სრულიად საიდუმლო" (equivalent to SECRET) - data the dissemination or loss of which may cause severe consequences to the defence, state security, protection of law and order, political and economic interests of Georgia, and to the interests of those persons who cooperate or have cooperated confidentially in the fields of intelligence, state security and protection of law and order, with respective authorities of Georgia exercising relevant activities, and/or data the disclosure of which may cause severe consequences to a state or an organization being a party to an international treaty of Georgia;

c) „საიდუმლო" (equivalent to CONFIDENTIAL) - data the dissemination of which may damage the defence, state security, protection of law and order, political and economic interests of Georgia, and the interests of those persons who are included in a special protection program for a participant in criminal procedures, and/or data the disclosure of which may damage the interests of a state or an organization being a party to an international treaty of Georgia;

d) „შეზღუდული სარგებლობისათვის" (equivalent to RESTRICTED) - data the dissemination of which may negatively affect the defence, state security, protection of law and order, political and economic interests of Georgia, and/or the interests and activities of a state or an organization being a party to an international treaty of Georgia.

Article 2

Comparability

The Contracting Parties stipulate that the following levels of security classification shall be comparable:

Georgia	Federal Republic of Germany	English equivalent
განსაკუთრებული მნიშვნელობის	STRENG GEHEIM	TOP SECRET
სრულიად საიდუმლო	GEHEIM	SECRET
საიდუმლო	VS-VERTRAULICH	CONFIDENTIAL
შეზღუდული სარგებლობისათვის	VS-NUR FÜR DEN DIENSTGEBRAUCH	RESTRICTED

Article 3

Marking

(1) Transmitted classified information shall be marked with the comparable level of national security classification as provided under Article 2 by, or at the instance of, the competent authority of the receiving Contracting Party.

(2) Classified information which is generated by the receiving Contracting Party in connection with classified contracts as well as copies made by the receiving Contracting Party shall also be marked.

(3) Levels of security classification shall, at the request of the competent authority of the originating Contracting Party, be amended or revoked by, or at the instance of, the competent authority of the receiving Contracting Party of the given classified information. The competent authority of the originating Contracting Party shall, without delay, inform the competent authority of the other Contracting Party of its intention to amend or revoke a level of security classification.

(4) Translation, reproduction and destruction of classified information shall be carried out in accordance with the requirements set in the national laws and regulations of the Contracting Parties.

Article 4

Measures at the National Level

(1) Within the scope of their national laws and regulations, the Contracting Parties shall take all appropriate measures to guarantee the protection of classified information generated, exchanged or held under the terms of this Agreement. They shall afford, within the limits of the respective national laws and regulations of the Contracting Parties, such

classified information a degree of protection at least equal to that required by the receiving Contracting Party for its own classified information of the comparable level of security classification.

(2) The period of classification is defined by the respective national laws and regulations of the originating Contracting Party.

(3) The classified information shall be used solely for the designated purpose. The receiving Contracting Party shall not disclose or use, or permit the disclosure or use of, any classified information except for the purposes and within any limitations stated by or at the instance of the originating Contracting Party. The originating Contracting Party must have given its written consent to any arrangement to the contrary.

(4) Access to classified information may be granted according to the respective national laws and regulations of the Contracting Parties. Security clearance shall be granted only after completion of security screening under standards no less stringent than those applied for access to national classified information of the comparable level of security classification.

(5) Access to classified information at the VS-VERTRAULICH / საიდუმლო level or higher by a person holding the nationality of the state of a Contracting Party shall be granted without prior authorization of the originating Contracting Party.

(6) Personal Security Clearances for nationals from the state of the Contracting Party residing, and requiring access to classified information, in their own state shall be undertaken by their competent authorities.

(7) However, Personal Security Clearances for nationals from the state of one Contracting Party who have been legally resident in the state of the other Contracting Party for at least five years and apply for a security-sensitive job in that state, shall be undertaken by the

competent authority of that Contracting Party in accordance with its national laws and regulations; it shall request the competent authority of the other Contracting Party to conduct security checks as appropriate.

(8) The Contracting Parties shall, each within the territory of its state, ensure that the necessary security inspections are carried out and that this Agreement is complied with.

Article 5

Destruction and Return of Classified Information

(1) Classified information shall be destroyed if:

a) it cannot be protected or used in accordance with this Agreement or

b) the originating Contracting Party requires its destruction.

(2) Classified documents shall be destroyed in a way excluding the possibility to reconstruct the classified information contained therein.

(3) Destruction of classified documents is conducted in accordance with national laws and regulations of the Contracting Parties.

(4) Classified material shall be destroyed so that recognition will be impossible, or modified so as to preclude reconstruction of the classified information in whole or in part.

(5) The originating Contracting Party shall be informed about the destruction without delay.

(6) On request of the originating Contracting Party, classified information will be returned.

Article 6

Award of Classified Contracts

(1) Prior to the award of a classified contract, the contracting officer shall, through his competent authority, obtain a Facility Security Clearance from the competent authority of the contractor in order to obtain assurance as to whether the prospective contractor is subject to security oversight by the competent authority of this Contracting Party and whether he has taken the security precautions required for discharging the performance of the classified contract. Where a contractor is not yet subject to security oversight, a request may be made to that end.

(2) A Facility Security Clearance shall also be obtained if an enterprise has been requested to submit a bid and if classified information will have to be released prior to the award of a classified contract under the bid procedure.

(3) In the cases referred to in paragraphs (1) and (2) above, the following procedure shall be applied:

1. Requests for the issuance of a Facility Security Clearance for contractors from the state of the other Contracting Party shall contain information on the project as well as the nature, the scope and the level of security classification of the classified information expected to be released to the contractor or to be generated by him.

2. In addition to the full name of the enterprise, its postal address, the name of its security official, its telephone and fax numbers and, if applicable, its e-mail address, Facility Security Clearances must include information in particular on the extent to which, and the level of security classification up to which, security measures have been taken by the respective enterprise on the basis of national laws and regulations.

3. The competent authorities of the Contracting Parties shall inform each other of any changes in the facts covered by issued Facility Security Clearances.

4. The exchange of such information between the competent authorities of the Contracting Parties shall be effected either in the national language of the authority to be informed or in English.

5. Facility Security Clearances and requests addressed to the respective competent authorities of the Contracting Parties for the issuance of Facility Security Clearances shall be transmitted in writing.

Article 7

Performance of Classified Contracts

(1) Classified contracts must contain a security requirement clause under which the contractor is under an obligation to make the arrangements required for the protection of classified information pursuant to the national laws and regulations of his state.

(2) In addition, the security requirement clause shall contain the following provisions:

1. the definition of the term „classified information" and of the comparable levels of security classification of the two Contracting Parties in accordance with the provisions of this Agreement;

2. the name of the competent authority of each of the two Contracting Parties empowered to authorize the release and to coordinate the safeguarding of classified information related to the classified contract;

3. the channels to be used for the transfer of classified information between the competent authorities and contractors involved;

4. the procedures and mechanisms for communicating changes that may arise in respect of classified information either because of changes in its level of security classification or because classification is no longer necessary;

5. the procedures for the approval of visits, or access, by personnel of the contractors;

6. the procedures for transmitting classified information to contractors where such information is to be used or held;

7. the requirement that the contractor shall grant access to classified information only to a person who has a need-to-know and has been charged with, or contributes to, the performance of the classified contract and – except in the case of classified information at the VS-NUR FÜR DEN DIENSTGEBRAUCH / შეზღუდული სარგებლობისათვის level - has been security-cleared to the appropriate level in advance;

8. the requirement that classified information shall only be disclosed, or the disclosure of classified information shall only be permitted, to a third party if this has been approved by the originating Contracting Party;

9. the requirement that the contractor shall immediately notify his competent authority of any actual or suspected loss, leak or unauthorized disclosure of the classified information covered by the classified contract.

(3) The competent authority of the contracting officer shall provide the contractor with a separate list (classification guide) of all documentary records requiring security

classification, shall determine the required level of security classification and shall arrange for this list to be enclosed as an appendix to the classified contract. The competent authority of the contracting officer shall also transmit, or arrange for the transmission of, the list to the competent authority of the contractor.

(4) The competent authority of the contracting officer shall ensure that the contractor will be given access to classified information only after the pertinent Facility Security Clearance has been received from the competent authority of the contractor.

Article 8

Transmission of Classified Information

(1) Classified Information at the STRENG GEHEIM / განსაკუთრებული მნიშვნელობის level shall only be transmitted between the Contracting Parties through Government-to-Government diplomatic channels.

(2) As a matter of principle, classified information at the VS-VERTRAULICH / საიდუმლო and GEHEIM / სრულიად საიდუმლო levels shall be transmitted from one state to another by official courier. The competent authorities of the Contracting Parties may agree on alternative channels of transmission. Receipt of classified information shall be confirmed by, or at the instance of, the competent authority and the classified information shall be forwarded to the recipient in accordance with national laws and regulations.

(3) For a specifically designated project, the competent authorities may agree - generally or subject to restrictions - that classified information at the VS-VERTRAULICH / საიდუმლო and GEHEIM / სრულიად საიდუმლო levels may be transmitted through channels other than official courier, if reliance on the official courier service would cause

undue difficulties for such transportation or for the execution of a classified contract. In such cases:

1. the bearer must be authorized to have access to classified information of the comparable level of security classification;

2. a list of the items of classified information transmitted must be retained by the dispatching competent authority; a copy of this list shall be handed over to the recipient for forwarding to the competent authority;

3. items of classified information must be packed in accordance with the national laws and regulations governing transportation within national boundaries;

4. items of classified information must be delivered against receipt and

5. the bearer must carry a courier certificate issued by the competent authority of the state of the dispatching or the receiving authority.

(4) Where large volumes of classified information are to be transmitted, the means of transportation, the route, and the escort shall be determined on a case-by-case basis and on the basis of a detailed transport plan by the competent authorities.

(5) The electronic transmission of classified information at the VS-VERTRAULICH / საიდუმლო level and higher must not take place in an unencrypted form. Classified information of these levels of security classification may only be encrypted by encryption means approved by mutual agreement by the competent authorities of the Contracting Parties.

(6) Classified information at the VS-NUR FÜR DEN DIENSTGEBRAUCH / შეზღუდული სარგებლობისათვის level may be transmitted by post or other delivery

services to recipients within the territory of the state of the other Contracting Party, taking into account national laws and regulations and provided that the sender and the recipient have reached agreement on the proposed transmission in advance.

(7) Classified information at the VS-NUR FÜR DEN DIENSTGEBRAUCH / შეზღუდული სარგებლობისათვის level may be electronically transmitted or made available by means of devices approved by competent authorities of the Contracting Parties. Classified information of this level of security classification may only be transmitted in an unencrypted form, provided that this is not in contradiction with national laws and regulations, that no approved encryption means are available, transmission is effected within fixed networks only, and the sender and the recipient have reached agreement on the proposed transmission in advance.

Article 9

Visits

(1) As a matter of principle, it is only with the prior permission of the competent authority of the Contracting Party the state of which is to be visited, that visitors from the territory of the state of one Contracting Party will, on the territory of the state of the other Contracting Party, be granted access to classified information and to facilities in which classified information is being handled. Such permission shall be given only to persons having an established need-to-know and having been authorized to have access to classified information in accordance with the respective national laws and regulations of the Contracting Parties.

(2) Requests for visits shall be submitted, on a timely basis and in accordance with the national laws and regulations of the state of the Contracting Party whose territory such visitors wish to enter, to the competent authority of that Contracting Party. The competent

authorities shall inform each other of the details regarding such requests and shall ensure that personal data are protected.

(3) Requests for visits shall be submitted in the language of the state to be visited or in English and shall contain the following information:

1. the visitor's first name and surname, date and place of birth, and his or her passport or identity card number;

2. the visitor's nationality;

3. the visitor's service designation, and the name of his or her parent authority or agency;

4. the level of the visitor's security clearance for access to classified information;

5. the purpose of the visit, and the proposed date of the visit and

6. the designation of the agencies, the contact persons and the installations to be visited.

Article 10

Consultations

(1) The competent authorities of the Contracting Parties shall take note of the provisions governing the protection of classified information that apply within the territory of the state of the other Contracting Party.

(2) To ensure close cooperation in the implementation of this Agreement, the competent authorities shall consult each other at the request of one of these authorities.

(3) Each Contracting Party shall, in addition, allow the competent authority of the other Contracting Party to visit the territory of its state in order to discuss, with its competent authorities, its procedures and facilities for the protection of classified information received from the other Contracting Party. Each Contracting Party shall assist that competent authority in ascertaining whether such classified information which has been made available by the other Contracting Party is adequately protected. The details of the visits shall be laid down by the competent authorities.

Article 11
Dispute Settlement

Any dispute between the Contracting Parties regarding the interpretation or application of this Agreement shall be resolved by consultations or negotiations between the Contracting Parties and shall not be referred to any national or international tribunal or third party for settlement.

Article 12
Violations of Provisions Governing the Mutual Protection of Classified Information

(1) Whenever unauthorized disclosure of classified information cannot be ruled out or if such disclosure is suspected or ascertained, the other Contracting Party shall immediately be informed.

(2) Violations of provisions governing the protection of classified information shall be investigated, and pertinent legal action shall be taken, by the competent authorities and courts of the Contracting Party having jurisdiction, according to that Contracting Party's

national laws and regulations. The other Contracting Party should, if so requested, support such investigations and shall be informed of the outcome.

Article 13

Costs

Each Contracting Party shall pay the expenses incurred by it in implementing the provisions of this Agreement.

Article 14

Competent Authorities

(1) For the purposes of this Agreement, the competent authorities responsible for the implementation of this Agreement shall be:

1. for the Federal Republic of Germany:
   Federal Ministry of the Interior (National Security Authority),
   Federal Ministry of Economic Affairs and Energy (Designated Security Authority),
   Federal Ministry of Defence (Military Security Authority);

2. for Georgia:
   State Security Service of Georgia.

(2) Upon entry into force of this Agreement, the competent authorities shall directly inform each other of their contact details, and any changes thereto.

(3) The Contracting Parties shall inform each other through diplomatic channels of any changes in the competent authorities and their contact details.

(4) In case of changes in the competent authorities, this shall not result in the initiation of amendment to this Agreement.

Article 15

Relationship with Other Agreements, Arrangements and Memoranda of Understanding

Any existing Agreements, Arrangements and Memoranda of Understanding between the Contracting Parties or the competent authorities on the protection of classified information shall be unaffected by this Agreement in so far as they do not conflict with its provisions.

Article 16

Final Provisions

(1) This Agreement shall enter into force on the date on which the Government of Georgia has notified the Government of the Federal Republic of Germany that the national requirements for such entry into force have been fulfilled. The relevant date shall be the date of receipt of the notification.

(2) This Agreement is concluded for an indefinite period of time.

(3) This Agreement may be amended in writing by mutual agreement between the Contracting Parties. Either Contracting Party may at any time submit a written request for the amendment of this Agreement. If such a request is submitted by one of the Contracting Parties, the Contracting Parties shall conduct negotiations on the amendment of this Agreement. Such amendments shall enter into force according to paragraph 1 of this Article.

(4) Either Contracting Party may, through diplomatic channels, denounce this Agreement by giving six months' written notice. In the event of denunciation, classified information transmitted, or generated by the contractor, on the basis of this Agreement shall continue to be treated in accordance with the provisions of Article 4 of this Agreement for as long as is justified by the existence of the security classification.

(5) Registration of this Agreement with the Secretariat of the United Nations, in accordance with Article 102 of the United Nations Charter, shall be initiated by the Contracting Party on the territory of whose state this Agreement is concluded immediately following its entry into force. The other Contracting Party shall be informed of registration, and of the UN registration number, as soon as this has been confirmed by the Secretariat.

Done at Tbilisi on November 16th 2017 in duplicate in the Georgian, German and English languages, all three texts being authentic. In case of divergent interpretations of the Georgian and German texts, the English text shall prevail.

For the Government of Georgia

For the Government of the Federal Republic of Germany

[GEORGIAN TEXT – TEXTE GÉORGIEN]

შეთანხმება

საქართველოს მთავრობასა

და

გერმანიის ფედერაციული რესპუბლიკის მთავრობას

შორის

საიდუმლო ინფორმაციის გაცვლისა და ორმხრივად დაცვის შესახებ

საქართველოს მთავრობას

და

გერმანიის ფედერაციული რესპუბლიკის მთავრობას

(შემდგომში ერთობლივად წოდებულნი, როგორც „ხელშემკვრელი მხარეები“ და თითოეული წოდებული, როგორც „ხელშემკვრელი მხარე“),

განზრახული აქვთ რა, უზრუნველყონ საქართველოსა და გერმანიის ფედერაციული რესპუბლიკის კომპეტენტურ ორგანოებს შორის გაცვლილი, ასევე, მეორე ხელშემკვრელი მხარის სახელმწიფოს ტერიტორიაზე არსებულ კონტრაქტორებთან, ან ორი ხელშემკვრელი მხარის კონტრაქტორებს შორის გაცვლილი, საიდუმლო ინფორმაციის დაცვა,

სურთ რა, შექმნან საიდუმლო ინფორმაციის ორმხრივად დაცვის მარეგულირებელი წესები, რომლებიც გავრცელდება ხელშემკვრელ მხარეებს შორის გასაფორმებელი თანამშრომლობის ყველა შეთანხმებაზე და გავრცელდება კონტრაქტებზე, რომლებიც ითვალისწინებს საიდუმლო ინფორმაციის გაცვლას,

შეთანხმდნენ შემდეგზე:

მუხლი 1

ტერმინთა განმარტება

(1) წინამდებარე შეთანხმების მიზნებისათვის:

1. „საიდუმლო ინფორმაცია“ არის

a) გერმანიის ფედერაციულ რესპუბლიკაში

ფაქტები, საგნები ან ცოდნა, რომელიც, მიუხედავად იმისა, თუ როგორ არის წარმოდგენილი, საიდუმლოდ უნდა იქნას შენახული საჯარო ინტერესიდან გამომდინარე. მათი დასაიდუმლოება, მათი დაცვის საჭიროებიდან გამომდინარე, უნდა განხორციელდეს ოფიციალური უწყების მიერ ან მისი მოთხოვნით;

b) საქართველოში

დამუშავებული ან დამუშავების პროცესში მყოფი ცნობა/ინფორმაცია ან მატერიალური საგანი (მიუხედავად მისი ფორმისა ან ბუნებისა), რომელიც საჭიროებს უნებართვო მოპყრობისაგან დაცვას, შეიცავს სახელმწიფო საიდუმლოების შემცველ მონაცემებს/ინფორმაციას ქვეყნის თავდაცვის, ეკონომიკის, საგარეო ურთიერთობათა, დაზვერვის, სახელმწიფო უსაფრთხოებისა და მართლწესრიგის დაცვის სფეროებში და, საქართველოს კანონმდებლობის შესაბამისად, სახელმწიფო საიდუმლოებას მიეკუთვნება.

2. „საიდუმლო კონტრაქტი“ არის

ერთი ხელშემკვრელი მხარის (კონტრაქტორი ოფიცრის) სახელმწიფოდან ორგანოს ან საწარმოს და მეორე ხელშემკვრელი მხარის (კონტრაქტორის) სახელმწიფოდან ორგანოს ან საწარმოს შორის არსებული კონტრაქტი/ქვეკონტრაქტი; ამგვარი კონტრაქტის ფარგლებში, საიდუმლო ინფორმაცია კონტრაქტორი ოფიცრის სახელმწიფოდან უნდა გადაეცეს კონტრაქტორს, უნდა დამუშავდეს კონტრაქტორის მიერ, ან

ხელმისაწვდომი გახდეს კონტრაქტორის პერსონალის იმ წევრებისთვის, რომლებმაც დავალებები უნდა შეასრულონ კონტრაქტორი ოფიცრის ობიექტებში.

(2) საიდუმლოობის ხარისხები განისაზღვრება შემდეგნაირად:

1. გერმანიის ფედერაციულ რესპუბლიკაში საიდუმლო ინფორმაცია არის

a) STRENG GEHEIM - თუ არაუფლებამოსილი პირების მიერ მისმა ცოდნამ შესაძლოა საფრთხე შეუქმნას გერმანიის ფედერაციული რესპუბლიკის ან მისი ერთ-ერთი ფედერალური მიწის (*Länder*) არსებობას ან არსებით ინტერესებს;

b) GEHEIM – თუ არაუფლებამოსილი პირების მიერ მისმა ცოდნამ შესაძლოა საფრთხე შეუქმნას გერმანიის ფედერაციული რესპუბლიკის ან მისი ერთ-ერთი ფედერალური მიწის (*Länder*) უსაფრთხოებას, ან შესაძლოა მნიშვნელოვანი ზიანი მიაყენოს მათ ინტერესებს;

c) VS-VERTRAULICH - თუ არაუფლებამოსილი პირების მიერ მისი ცოდნა შესაძლოა ზიანის მომტანი იყოს გერმანიის ფედერაციული რესპუბლიკის ან მისი ერთ-ერთი ფედერალური მიწის (*Länder*) ინტერესებისათვის;

d) VS-NUR FÜR DEN DIENSTGEBRAUCH - თუ არაუფლებამოსილი პირების მიერ მისი ცოდნა შესაძლოა არახელსაყრელი იყოს გერმანიის ფედერაციული რესპუბლიკის ან მისი ერთ-ერთი ფედერალური მიწის (*Länder*) ინტერესებისათვის.

2. საქართველოში საიდუმლო ინფორმაცია არის

a) „განსაკუთრებული მნიშვნელობის“ (მასთან გათანაბრებულია TOP SECRET) - მონაცემი, რომლის გავრცელებამ ან დაკარგვამ შეიძლება არსებითად იმოქმედოს საქართველოს სახელმწიფო ინტერესებზე ქვეყნის თავდაცვის, ეკონომიკის, სახელმწიფო უსაფრთხოების, მართლწესრიგის დაცვის და პოლიტიკის სფეროებში, ან/და გამოიწვიოს განსაკუთრებით მძიმე შედეგები საქართველოს საერთაშორისო ხელშეკრულების მონაწილე ქვეყნისათვის თუ ორგანიზაციისათვის;

b) „სრულიად საიდუმლო“ (მასთან გათანაბრებულია SECRET) - მონაცემი, რომლის გავრცელებამ ან დაკარგვამ შეიძლება გამოიწვიოს მძიმე შედეგები საქართველოს თავდაცვის, სახელმწიფო უსაფრთხოების, მართლწესრიგის დაცვის, პოლიტიკური და ეკონომიკური ინტერესებისათვის და იმ პირთა ინტერესებისათვის, რომლებიც დაზვერვის, სახელმწიფო უსაფრთხოებისა და მართლწესრიგის დაცვის სფეროებში კონფიდენციალურად თანამშრომლობენ ან თანამშრომლობდნენ სათანადო საქმიანობის განმახორციელებელ საქართველოს შესაბამის ორგანოებთან, ან/და მონაცემი, რომლის გამჟღავნებამ შეიძლება გამოიწვიოს მძიმე შედეგები საქართველოს საერთაშორისო ხელშეკრულების მონაწილე ქვეყნისათვის თუ ორგანიზაციისათვის;

c) „საიდუმლო“ (მასთან გათანაბრებულია CONFIDENTIAL) - მონაცემი, რომლის გავრცელებამ შეიძლება ზიანი მიაყენოს საქართველოს თავდაცვის, სახელმწიფო უსაფრთხოების, მართლწესრიგის დაცვის, პოლიტიკურ და ეკონომიკურ ინტერესებს და იმ პირთა ინტერესებს, რომლებიც ჩართული არიან სისხლის სამართლის პროცესის მონაწილის

დაცვის სპეციალურ პროგრამაში, ან/და მონაცემი, რომლის გამჟღავნებამ შეიძლება ზიანი მიაყენოს საქართველოს საერთაშორისო ხელშეკრულების მონაწილე ქვეყნისა თუ ორგანიზაციის ინტერესებს;

d) „შეზღუდული სარგებლობისათვის“ (მასთან გათანაბრებულია RESTRICTED) - მონაცემი, რომლის გავრცელებამ შეიძლება უარყოფითი გავლენა მოახდინოს საქართველოს თავდაცვის, სახელმწიფო უსაფრთხოების, მართლწესრიგის დაცვის, პოლიტიკურ და ეკონომიკურ ინტერესებზე, ან/და საქართველოს საერთაშორისო ხელშეკრულების მონაწილე ქვეყნისა თუ ორგანიზაციის ინტერესებსა და საქმიანობაზე.

მუხლი 2

შესაბამისობა

ხელშემკვრელი მხარეები ადგენენ, რომ შემდეგი საიდუმლოობის ხარისხები შესაბამისობაშია ერთმანეთთან:

საქართველო	გერმანიის ფედერაციული რესპუბლიკა	ინგლისური ეკვივალენტი
განსაკუთრებული მნიშვნელობის	STRENG GEHEIM	TOP SECRET
სრულიად საიდუმლო	GEHEIM	SECRET
საიდუმლო	VS-VERTRAULICH	CONFIDENTIAL
შეზღუდული სარგებლობისათვის	VS-NUR FÜR DEN DIENSTGEBRAUCH	RESTRICTED

მუხლი 3

გრიფი

(1) გადაცემულ საიდუმლო ინფორმაციას გრიფი უნდა მიენიჭოს ეროვნული საიდუმლოობის შესაბამისი ხარისხის მიხედვით, როგორც ეს დადგენილია მე-2 მუხლით, მიმღები ხელშემკვრელი მხარის კომპეტენტური ორგანოს მიერ ან მისი მოთხოვნით.

(2) ასევე, გრიფი უნდა მიენიჭოს საიდუმლო ინფორმაციას, რომელიც იქმნება მიმღები ხელშემკვრელი მხარის მიერ საიდუმლო კონტრაქტებთან დაკავშირებით, ისევე, როგორც მიმღები ხელშემკვრელი მხარის მიერ შესრულებულ ასლებს.

(3) წარმომშობი ხელშემკვრელი მხარის კომპეტენტური ორგანოს მოთხოვნის შემთხვევაში, საიდუმლოობის ხარისხები უნდა შეიცვალოს ან გაუქმდეს მოცემული საიდუმლო ინფორმაციის მიმღები ხელშემკვრელი მხარის კომპეტენტური ორგანოს მიერ ან მისი დავალებით. წარმომშობი ხელშემკვრელი მხარის კომპეტენტურმა ორგანომ დაუყოვნებლივ უნდა აცნობოს მეორე ხელშემკვრელი მხარის კომპეტენტურ ორგანოს, საიდუმლოობის ხარისხის შეცვლასთან ან გაუქმებასთან დაკავშირებით, საკუთარი განზრახვის შესახებ.

(4) საიდუმლო ინფორმაციის თარგმნა, გამრავლება და განადგურება უნდა განხორციელდეს ხელშემკვრელი მხარეების შიდასახელმწიფოებრივი კანონმდებლობით დადგენილი მოთხოვნების შესაბამისად.

მუხლი 4

ეროვნულ დონეზე გასატარებელი ზომები

(1) ხელშემკვრელი მხარეები, საკუთარი შიდასახელმწიფოებრივი კანონმდებლობის ფარგლებში, მიიღებენ ყველა სათანადო ზომას, რათა უზრუნველყონ წინამდებარე შეთანხმების პირობების შესაბამისად შექმნილი, გაცვლილი ან არსებული საიდუმლო ინფორმაციის დაცვა. ხელშემკვრელ მხარეთა შესაბამისი შიდასახელმწიფოებრივი კანონმდებლობის ფარგლებში, ისინი უზრუნველყოფენ ამგვარი საიდუმლო ინფორმაციის დაცვას ისეთი ხარისხით, რომელიც, სულ მცირე, უთანაბრდება მიმღები ხელშემკვრელი მხარის მიერ, საიდუმლოობის შესაბამისი ხარისხის მქონე, საკუთარი საიდუმლო ინფორმაციისთვის მოთხოვნილ ხარისხს.

(2) დასაიდუმლოების ვადა განისაზღვრება წარმომშობი ხელშემკვრელი მხარის შესაბამისი შიდასახელმწიფოებრივი კანონმდებლობით.

(3) საიდუმლო ინფორმაცია გამოიყენება მხოლოდ განსაზღვრული მიზნისათვის. მიმღები ხელშემკვრელი მხარე არ გაამჟღავნებს ან გამოიყენებს ნებისმიერ საიდუმლო ინფორმაციას და არ დაუშვებს მის გამჟღავნებას ან გამოყენებას, გარდა იმ შემთხვევებისა, თუ ეს ხორციელდება წარმომშობი ხელშემკვრელი მხარის მიერ ან მისი მოთხოვნით დადგენილი მიზნებისთვის და ნებისმიერი შეზღუდვით. ნებისმიერ სხვაგვარ შეთანხმებაზე წარმომშობ ხელშემკვრელ მხარეს გაცემული უნდა ჰქონდეს წერილობითი თანხმობა.

(4) საიდუმლო ინფორმაციის გაცნობის უფლების მინიჭება შეიძლება განხორციელდეს ხელშემკვრელი მხარეების შესაბამისი შიდასახელმწიფოებრივი კანონმდებლობის თანახმად. საიდუმლო ინფორმაციასთან დაშვების მინიჭება ხორციელდება მხოლოდ და მხოლოდ

უსაფრთხოების შემოწმების დასრულების შემდეგ, ისეთი სტანდარტების შესაბამისად, რომლებიც საიდუმლოობის შესაბამისი ხარისხის მქონე ეროვნული საიდუმლო ინფორმაციის გაცნობის მიმართ გამოყენებულ სტანდარტებზე არანაკლებ მკაცრია.

(5) პირს, რომელსაც ხელშემკვრელი მხარის სახელმწიფოს მოქალაქეობა აქვს, ენიჭება VS-VERTRAULICH / „საიდუმლო" ან უფრო მაღალი ხარისხის მქონე საიდუმლო ინფორმაციის გაცნობის უფლება, წარმომშობი ხელშემკვრელი მხარის წინასწარი ნებართვის გარეშე.

(6) საიდუმლო ინფორმაციასთან ინდივიდუალური დაშვება ხელშემკვრელი მხარის სახელმწიფოს იმ მოქალაქეების მიმართ, რომლებიც ცხოვრობენ და საჭიროებენ საიდუმლო ინფორმაციის გაცნობას საკუთარ სახელმწიფოში, ხორციელდება მათი კომპეტენტური ორგანოების მიერ.

(7) თუმცა, საიდუმლო ინფორმაციასთან ინდივიდუალური დაშვება ერთ-ერთი ხელშემკვრელი მხარის სახელმწიფოს იმ მოქალაქეების მიმართ, რომლებიც კანონიერად ცხოვრობდნენ მეორე ხელშემკვრელი მხარის სახელმწიფოში, სულ მცირე, ხუთი წლის მანძილზე და ამ სახელმწიფოში იწყებენ უსაფრთხოებასთან დაკავშირებულ სამსახურს, ხორციელდება ამ ხელშემკვრელი მხარის კომპეტენტური ორგანოს მიერ, მისი შიდასახელმწიფოებრივი კანონმდებლობის შესაბამისად; საჭიროებიდან გამომდინარე, ის მეორე ხელშემკვრელი მხარის კომპეტენტურ ორგანოს მოსთხოვს უსაფრთხოების შემოწმების ჩატარებას.

(8) ხელშემკვრელი მხარეები, თითოეული საკუთარი სახელმწიფოს ტერიტორიაზე, უზრუნველყოფს, რომ ჩატარდეს აუცილებელი უსაფრთხოების შემოწმებები და შესრულდეს წინამდებარე შეთანხმება.

მუხლი 5

საიდუმლო ინფორმაციის განადგურება და უკან დაბრუნება

(1) საიდუმლო ინფორმაცია უნდა განადგურდეს, თუ:

a) შეუძლებელია მისი დაცვა ან გამოყენება წინამდებარე შეთანხმების შესაბამისად, ან

b) წარმომშობი ხელშემკვრელი მხარე მოითხოვს მის განადგურებას.

(2) საიდუმლო დოკუმენტები ისე უნდა განადგურდეს, რომ გამოირიცხოს მათში არსებული საიდუმლო ინფორმაციის აღდგენის შესაძლებლობა.

(3) საიდუმლო დოკუმენტების განადგურება ხორციელდება ხელშემკვრელ მხარეთა შიდასახელმწიფოებრივი კანონმდებლობის შესაბამისად.

(4) საიდუმლო ინფორმაციის შემცველი საგნობრივი მასალა ისე უნდა განადგურდეს, რომ შეუძლებელი იყოს მისი ამოცნობა, ან ისე უნდა შეიცვალოს, რომ გამოირიცხოს საიდუმლო ინფორმაციის მთლიანად ან ნაწილობრივ აღდგენა.

(5) წარმომშობ ხელშემკვრელ მხარეს დაუყოვნებლივ უნდა ეცნობოს განადგურების შესახებ.

(6) წარმომშობი ხელშემკვრელი მხარის მოთხოვნის შემთხვევაში, საიდუმლო ინფორმაცია ექვემდებარება დაბრუნებას.

მუხლი 6

საიდუმლო კონტრაქტების დადება

(1) საიდუმლო კონტრაქტის დადებამდე კონტრაქტორმა ოფიცერმა, საკუთარი კომპეტენტური ორგანოს მეშვეობით, კონტრაქტორის კომპეტენტური ორგანოსგან უნდა მიიღოს საიდუმლო ინფორმაციასთან იურიდიული პირის დაშვება, რათა გარანტია ჰქონდეს, რომ შესაძლო კონტრაქტორი ექვემდებარება ამ ხელშემკვრელი მხარის კომპეტენტური ორგანოს უსაფრთხოების კონტროლს და რომ მას გატარებული აქვს საიდუმლო კონტრაქტის შესრულებისთვის საჭირო უსაფრთხოების ზომები. თუ კონტრაქტორი ჯერ არ ექვემდებარება უსაფრთხოების კონტროლს, ამ მიზნით შესაძლებელია მოთხოვნის გაკეთება.

(2) ასევე, საიდუმლო ინფორმაციასთან იურიდიული პირის დაშვების მიღება აუცილებელია იმ შემთხვევაშიც, თუ საწარმოს მოეთხოვება სატენდერო შეთავაზების გაკეთება და თუ, სატენდერო პროცედურის ფარგლებში, საიდუმლო ინფორმაციის გაცემა უნდა მოხდეს საიდუმლო კონტრაქტის დადებამდე.

(3) პირველი და მე-2 პუნქტებით გათვალისწინებულ შემთხვევებში გამოიყენება შემდეგი პროცედურები:

1. იმისათვის, რომ მეორე ხელშემკვრელი მხარის სახელმწიფოდან კონტრაქტორს მიენიჭოს საიდუმლო ინფორმაციასთან იურიდიული პირის დაშვება, მოთხოვნა უნდა შეიცავდეს ინფორმაციას პროექტის, ასევე, იმ საიდუმლო ინფორმაციის ბუნების, ფარგლებისა და საიდუმლოობის ხარისხის შესახებ, რომლის მიმართ არსებობს მოლოდინი, რომ გადაეცემა კონტრაქტორს ან შეიქმნება მის მიერ.

2. საწარმოს სრულ დასახელებაზე, მის საფოსტო მისამართზე, მისი უსაფრთხოების თანამდებობის პირის ვინაობაზე, საწარმოს ტელეფონისა და ფაქსის ნომრების და მისი ელექტრონული ფოსტის მისამართზე, ასეთის არსებობის შემთხვევაში, დამატებით, საიდუმლო ინფორმაციასთან იურიდიული პირის დაშვება უნდა შეიცავდეს ინფორმაციას, განსაკუთრებით იმის შესახებ, შესაბამისი საწარმოს მიერ თუ რა ფარგლებში და საიდუმლოობის რომელ ხარისხამდე იქნა გატარებული უსაფრთხოების ზომები, შიდასახელმწიფოებრივი კანონმდებლობის შესაბამისად.

3. ხელშემკვრელი მხარეების კომპეტენტური ორგანოები ერთმანეთს აცნობებენ საიდუმლო ინფორმაციასთან იურიდიული პირის უკვე გაცემული დაშვებით გათვალისწინებული ფაქტების ნებისმიერი ცვლილების შესახებ.

4. ხელშემკვრელი მხარეების კომპეტენტურ ორგანოებს შორის ასეთი ინფორმაციის გაცვლა განხორციელდება იმ ორგანოს სახელმწიფო ენაზე, რომელსაც მიეწოდება ინფორმაცია, ან ინგლისურ ენაზე.

5. საიდუმლო ინფორმაციასთან იურიდიული პირის დაშვება და, საიდუმლო ინფორმაციასთან იურიდიული პირის დაშვების მინიჭების მიზნით, ხელშემკვრელი მხარეების შესაბამისი კომპეტენტური ორგანოებისადმი მიმართული მოთხოვნები გადაიცემა წერილობით.

მუხლი 7

საიდუმლო კონტრაქტების შესრულება

(1) საიდუმლო კონტრაქტები უნდა შეიცავდეს უსაფრთხოების მოთხოვნების შესახებ მუხლს, რომლის თანახმად, კონტრაქტორი ვალდებულია, საკუთარი სახელმწიფოს შიდასახელმწიფოებრივი კანონმდებლობის შესაბამისად, მიიღოს საიდუმლო ინფორმაციის დასაცავად საჭირო ზომები.

(2) უსაფრთხოების მოთხოვნების შესახებ მუხლი, დამატებით, უნდა შეიცავდეს შემდეგ დებულებებს:

1. ტერმინის „საიდუმლო ინფორმაცია“ და ორივე ხელშემკვრელი მხარის შესაბამისი საიდუმლოობის ხარისხების განმარტება, წინამდებარე შეთანხმების დებულებების შესაბამისად;

2. ორივე ხელშემკვრელი მხარის კომპეტენტური ორგანოს დასახელება, რომელიც უფლებამოსილია, ნებართვა გასცეს საიდუმლო კონტრაქტთან დაკავშირებული საიდუმლო ინფორმაციის გაცემაზე და კოორდინაცია გაუწიოს მის დაცვას;

3. არხები, რომლებიც გამოყენებული იქნება კომპეტენტურ ორგანოებსა და შესაბამის კონტრაქტორებს შორის საიდუმლო ინფორმაციის გადასაცემად;

4. საიდუმლო ინფორმაციასთან დაკავშირებით იმ ცვლილებების შეტყობინების პროცედურები და მექანიზმები, რომლებიც შეიძლება გამოწვეულ იქნას საიდუმლო ინფორმაციის საიდუმლოობის ხარისხის

ცვლილების გამო, ან იმის გამო, რომ დასაიდუმლოება აღარ არის საჭირო;

5. თანხმობის პროცედურები კონტრაქტორების პერსონალის ვიზიტებზე ან მათ მიერ წვდომაზე;

6. საიდუმლო ინფორმაციის გადაცემის პროცედურები იმ კონტრაქტორებისთვის, სადაც მოხდება ამგვარი ინფორმაციის გამოყენება ან განთავსება;

7. მოთხოვნა, რომ კონტრაქტორი საიდუმლო ინფორმაციის გაცნობის უფლებას მიანიჭებს მხოლოდ იმ პირს, რომელსაც აქვს ინფორმაციის გაცნობის საჭიროება და დავალებული აქვს ან წვლილი შეაქვს საიდუმლო კონტრაქტის შესრულებაში, და რომელიც - VS-NUR FÜR DEN DIENSTGEBRAUCH / „შეზღუდული სარგებლობისათვის“ ხარისხის მქონე საიდუმლო ინფორმაციის შემთხვევის გარდა - წინასწარ არის შემოწმებული საიდუმლო ინფორმაციის შესაბამის ხარისხზე;

8. მოთხოვნა, რომ საიდუმლო ინფორმაციის მესამე მხარისთვის გამჟღავნება მხოლოდ იმ შემთხვევაში მოხდება, ან საიდუმლო ინფორმაციის მესამე მხარისთვის გამჟღავნება მხოლოდ იმ შემთხვევაში იქნება ნებადართული, თუ ამაზე არსებობს წარმომშობი ხელშემკვრელი მხარის თანხმობა;

9. მოთხოვნა, რომ კონტრაქტორი დაუყოვნებლივ შეატყობინებს საკუთარ კომპეტენტურ ორგანოს საიდუმლო კონტრაქტით გათვალისწინებული საიდუმლო ინფორმაციის ნებისმიერი ფაქტობრივი ან შესაძლო დაკარგვის, გაჟონვის ან უნებართვო გამჟღავნების შესახებ.

(3) კონტრაქტორი ოფიცრის კომპეტენტური ორგანო კონტრაქტორს მიაწვდის ყველა იმ დოკუმენტური ჩანაწერის ცალკე სიას (საიდუმლოობის სახელმძღვანელო), რომელიც საჭიროებს დასაიდუმლოებას, განსაზღვრავს საიდუმლოობის საჭირო ხარისხს და უზრუნველყოფს, რომ ეს სია თან დაერთოს საიდუმლო კონტრაქტს დანართის სახით. კონტრაქტორი ოფიცრის კომპეტენტური ორგანო, ასევე, გადასცემს ან უზრუნველყოფს ამ სიის გადაცემას კონტრაქტორის კომპეტენტური ორგანოსთვის.

(4) კონტრაქტორი ოფიცრის კომპეტენტური ორგანო უზრუნველყოფს, რომ კონტრაქტორს ჰქონდეს საიდუმლო ინფორმაციის გაცნობის უფლება მხოლოდ მას შემდეგ, რაც კონტრაქტორის კომპეტენტური ორგანოსგან მიიღებს საიდუმლო ინფორმაციასთან იურიდიული პირის სათანადო დაშვებას.

მუხლი 8

საიდუმლო ინფორმაციის გადაცემა

(1) STRENG GEHEIM / „განსაკუთრებული მნიშვნელობის“ ხარისხის მქონე საიდუმლო ინფორმაცია ხელშემკვრელ მხარეთა შორის გადაიცემა მხოლოდ მთავრობათაშორისი დიპლომატიური არხებით.

(2) პრინციპის დონეზე, VS-VERTRAULICH / „საიდუმლო“ და GEHEIM / „სრულიად საიდუმლო“ ხარისხების მქონე საიდუმლო ინფორმაცია ერთი სახელმწიფოდან მეორეში გადაიცემა ოფიციალური კურიერის მეშვეობით. ხელშემკვრელი მხარეების კომპეტენტური ორგანოები შესაძლოა შეთანხმდნენ გადაცემის ალტერნატიულ არხებზე. საიდუმლო ინფორმაციის მიღება უნდა დამოწმდეს კომპეტენტური ორგანოს მიერ ან მისი მოთხოვნით და საიდუმლო

ინფორმაცია მიმღებთან უნდა გადაიგზავნოს შიდასახელმწიფოებრივი კანონმდებლობის შესაბამისად.

(3) სპეციალურად განსაზღვრული პროექტისთვის კომპეტენტური ორგანოები შესაძლოა შეთანხმდნენ - ზოგადად ან შეზღუდვების გათვალისწინებით - რომ VS-VERTRAULICH / „საიდუმლო“ და GEHEIM / „სრულიად საიდუმლო“ ხარისხების მქონე საიდუმლო ინფორმაცია შესაძლებელია გადაცემულ იქნას, ოფიციალური კურიერის გარდა, სხვა არხებით, თუ ოფიციალური კურიერის მომსახურების გამოყენება გამოიწვევს განსაკუთრებულ სირთულეს ამგვარი ტრანსპორტირებისთვის, ან საიდუმლო კონტრაქტის შესრულებისთვის. ასეთ შემთხვევებში:

1. გადამტანი უნდა იყოს უფლებამოსილი, გაეცნოს შესაბამისი საიდუმლოობის ხარისხის მქონე საიდუმლო ინფორმაციას;

2. გადაცემული საიდუმლო ინფორმაციის შემცველი საგნების სია უნდა დარჩეს გამგზავნ კომპეტენტურ ორგანოსთან; ამ სიის ასლი უნდა გადაეცეს მიმღებს, კომპეტენტური ორგანოსთვის მისი გადაგზავნის მიზნით;

3. საიდუმლო ინფორმაციის შემცველი საგნები უნდა შეიფუთოს ეროვნულ საზღვრებში ტრანსპორტირების მარეგულირებელი შიდასახელმწიფოებრივი კანონმდებლობის შესაბამისად;

4. საიდუმლო ინფორმაციის შემცველი საგნების ჩაბარება უნდა მოხდეს მიღების დამადასტურებელი ჩანაწერით, და

5. გადამტანმა თან უნდა იქონიოს, გამგზავნი ან მიმღები ორგანოს სახელმწიფოს კომპეტენტური ორგანოს მიერ გაცემული, კურიერის სერთიფიკატი.

(4) როდესაც დიდი ოდენობის საიდუმლო ინფორმაციის გადაცემა ხდება, ტრანსპორტირების საშუალებები, მარშრუტი და ესკორტი განისაზღვრება კომპეტენტური ორგანოების მიერ ყოველ კონკრეტულ შემთხვევაში და დეტალური ტრანსპორტირების გეგმის საფუძველზე.

(5) VS-VERTRAULICH / „საიდუმლო“ და უფრო მაღალი ხარისხის მქონე საიდუმლო ინფორმაციის ელექტრონული გადაცემა არ უნდა განხორციელდეს დაუშიფრავი ფორმით. აღნიშნული საიდუმლოობის ხარისხების მქონე საიდუმლო ინფორმაცია შესაძლებელია დაიშიფროს მხოლოდ ხელშემკვრელი მხარეების კომპეტენტური ორგანოების მიერ ურთიერთშეთანხმებით დამტკიცებული დაშიფვრის საშუალებებით.

(6) VS-NUR FÜR DEN DIENSTGEBRAUCH / „შეზღუდული სარგებლობისათვის” ხარისხის მქონე საიდუმლო ინფორმაცია მეორე ხელშემკვრელი მხარის სახელმწიფოს ტერიტორიაზე არსებულ მიმღებებს შესაძლოა გადაეცეთ ფოსტით ან მიწოდების სხვა მომსახურებით, შიდასახელმწიფოებრივი კანონმდებლობისა და იმის გათვალისწინებით, რომ შესაძლო გადაცემის შესახებ მიმღებსა და გამგზავნს შორის წინასწარ იქნა მიღწეული შეთანხმება.

(7) VS-NUR DEN DIENSTGEBRAUCH / „შეზღუდული სარგებლობისათვის” ხარისხის მქონე საიდუმლო ინფორმაცია შესაძლებელია ელექტრონულად გადაიცეს ან ხელმისაწვდომი გახდეს ხელშემკვრელი მხარეების კომპეტენტური ორგანოების მიერ დამტკიცებული მოწყობილობის საშუალებით. საიდუმლოობის აღნიშნული ხარისხის საიდუმლო ინფორმაცია მხოლოდ იმ

შემთხვევაში შეიძლება გადაიცეს დაუშიფრავი ფორმით, თუ ეს არ ეწინააღმდეგება შიდასახელმწიფოებრივ კანონმდებლობას, დამტკიცებული დაშიფვრის საშუალებები არ არის ხელმისაწვდომი, გადაცემა ხორციელდება მხოლოდ ფიქსირებული ქსელით და გამგზავნი და მიმღები წინასწარ შეთანხმდნენ შესაძლო გადაცემაზე.

მუხლი 9

ვიზიტები

(1) პრინციპის დონეზე, ვიზიტორებს ერთი ხელშემკვრელი მხარის სახელმწიფოს ტერიტორიიდან მიენიჭებათ მეორე ხელშემკვრელი მხარის სახელმწიფოს ტერიტორიაზე საიდუმლო ინფორმაციის გაცნობის უფლება და დაშვება იმ ობიექტებზე, სადაც ხორციელდება საიდუმლო ინფორმაციასთან მოპყრობა, მხოლოდ იმ ხელშემკვრელი მხარის კომპეტენტური ორგანოს წინასწარი ნებართვით, რომლის სახელმწიფოშიც უნდა განხორციელდეს ვიზიტი. ამგვარი ნებართვა გაიცემა მხოლოდ იმ პირებზე, რომლებსაც აქვთ ინფორმაციის გაცნობის დადასტურებული საჭიროება და უფლებამოსილნი არიან, გაეცნონ საიდუმლო ინფორმაციას, ხელშემკვრელი მხარეების შესაბამისი შიდასახელმწიფოებრივი კანონმდებლობის თანახმად.

(2) ვიზიტის შესახებ მოთხოვნა ხელშემკვრელი მხარის კომპეტენტურ ორგანოს უნდა წარედგინოს დროულად და ამ ხელშემკვრელი მხარის შიდასახელმწიფოებრივი კანონმდებლობის შესაბამისად, რომლის სახელმწიფოს ტერიტორიაზეც სურთ ამ ვიზიტორებს შესვლა. კომპეტენტური ორგანოები ერთმანეთს შეატყობინებენ ამგვარი მოთხოვნის დეტალების შესახებ და უზრუნველყოფენ პერსონალური მონაცემების დაცვას.

(3) ვიზიტის შესახებ მოთხოვნის წარდგენა უნდა მოხდეს იმ სახელმწიფოს ენაზე, სადაც ხორციელდება ვიზიტი, ან ინგლისურ ენაზე და უნდა მოიცავდეს შემდეგ ინფორმაციას:

1. ვიზიტორის სახელი და გვარი, დაბადების ადგილი და თარიღი, მისი პასპორტის ან პირადობის დამადასტურებელი დოკუმენტის ნომერი;

2. ვიზიტორის მოქალაქეობა;

3. ვიზიტორის სამსახურებრივი თანამდებობა და იმ ორგანოს ან უწყების დასახელება, რომელსაც იგი წარმოადგენს;

4. საიდუმლო ინფორმაციის გაცნობის მიზნებისთვის, საიდუმლო ინფორმაციასთან ვიზიტორის დაშვების ხარისხი;

5. ვიზიტის მიზანი და ვიზიტის სავარაუდო თარიღი, და

6. იმ უწყებების დასახელება, საკონტაქტო პირები და ნაგებობები, სადაც უნდა განხორციელდეს ვიზიტი.

მუხლი 10

კონსულტაციები

(1) ხელშემკვრელი მხარეების კომპეტენტურმა ორგანოებმა უნდა გაითვალისწინონ მეორე ხელშემკვრელი მხარის სახელმწიფოს ტერიტორიაზე მოქმედი დებულებები, რომლებიც არეგულირებს საიდუმლო ინფორმაციის დაცვას.

(2) წინამდებარე შეთანხმების შესრულებისას მჭიდრო თანამშრომლობის უზრუნველსაყოფად, კომპეტენტური ორგანოები ერთმანეთთან გამართავენ კონსულტაციებს, ერთ-ერთი ამ ორგანოს მოთხოვნის საფუძველზე.

(3) თითოეული ხელშემკვრელი მხარე მეორე ხელშემკვრელი მხარის კომპეტენტურ ორგანოს, დამატებით, ნებას დართავს, ვიზიტით ეწვიოს მისი სახელმწიფოს ტერიტორიას, რათა მის კომპეტენტურ ორგანოებთან განიხილოს მისი ობიექტები და პროცედურები, რომლებიც გამოიყენება მეორე ხელშემკვრელი მხარისგან მიღებული საიდუმლო ინფორმაციის დასაცავად. თითოეული ხელშემკვრელი მხარე დაეხმარება აღნიშნულ კომპეტენტურ ორგანოს, დაადგინოს, არის თუ არა ამგვარი საიდუმლო ინფორმაცია, რომელიც ხელმისაწვდომი გახდა მეორე ხელშემკვრელი მხარის მიერ, ადეკვატურად დაცული. ვიზიტის დეტალები განისაზღვრება კომპეტენტური ორგანოების მიერ.

მუხლი 11

დავის გადაწყვეტა

ხელშემკვრელ მხარეთა შორის წინამდებარე შეთანხმების განმარტებასთან ან გამოყენებასთან დაკავშირებული ნებისმიერი დავა უნდა გადაწყდეს ხელშემკვრელ მხარეებს შორის კონსულტაციების ან მოლაპარაკებების გზით და გადასაწყვეტად არ უნდა გადაეცეს რომელიმე ეროვნულ ან საერთაშორისო სასამართლოს, ან მესამე მხარეს.

მუხლი 12

საიდუმლო ინფორმაციის ორმხრივად დაცვის მარეგულირებელი დებულებების დარღვევა

(1) მეორე ხელშემკვრელ მხარეს დაუყოვნებლივ უნდა ეცნობოს, როდესაც შეუძლებელია საიდუმლო ინფორმაციის უნებართვო გამჟღავნების გამორიცხვა, ან თუ არსებობს ეჭვი ან დადგენილია ამგვარი გამჟღავნება.

(2) კომპეტენტურმა ორგანოებმა და ხელშემკვრელი მხარის სასამართლოებმა, რომლებსაც, ამ ხელშემკვრელი მხარის შიდასახელმწიფოებრივი კანონმდებლობის შესაბამისად, აქვთ იურისდიქცია, უნდა გამოიძიონ საიდუმლო ინფორმაციის დაცვის მარეგულირებელი დებულებების დარღვევები და მიიღონ შესაბამისი სამართლებრივი ზომები. მეორე ხელშემკვრელმა მხარემ ხელი უნდა შეუწყოს ამ გამოძიებას, ასეთი მოთხოვნის არსებობის შემთხვევაში, და ის ინფორმირებული უნდა იყოს შედეგების შესახებ.

მუხლი 13

ხარჯები

თითოეული ხელშემკვრელი მხარე უზრუნველყოფს მის მიერ წინამდებარე შეთანხმების დებულებების შესრულებისას გაწეული ხარჯების დაფარვას.

მუხლი 14

კომპეტენტური ორგანოები

(1) წინამდებარე შეთანხმების მიზნებისათვის, წინამდებარე შეთანხმების შესრულებაზე პასუხისმგებელი კომპეტენტური ორგანოები არიან:

1. გერმანიის ფედერაციული რესპუბლიკისთვის:
   შინაგან საქმეთა ფედერალური სამინისტრო (ეროვნული უსაფრთხოების ორგანო),
   ეკონომიკისა და ენერგეტიკის ფედერალური სამინისტრო (განსაზღვრული უსაფრთხოების ორგანო),
   თავდაცვის ფედერალური სამინისტრო (სამხედრო უსაფრთხოების ორგანო);

2. საქართველოსთვის:
   საქართველოს სახელმწიფო უსაფრთხოების სამსახური.

(2) წინამდებარე შეთანხმების ძალაში შესვლის შემდეგ კომპეტენტური ორგანოები უშუალოდ აცნობებენ ერთმანეთს საკუთარ საკონტაქტო მონაცემებს და მასში ნებისმიერი ცვლილების შესახებ.

(3) ხელშემკვრელი მხარეები დიპლომატიური არხებით აცნობებენ ერთმანეთს კომპეტენტური ორგანოების ნებისმიერი ცვლილების შესახებ და მათ საკონტაქტო მონაცემებს.

(4) კომპეტენტური ორგანოების ცვლილების შემთხვევაში, ეს არ აისახება წინამდებარე შეთანხმებაში ცვლილებების შეტანის ინიცირებაზე.

მუხლი 15

ურთიერთობა სხვა ხელშეკრულებებთან, შეთანხმებებთან და ურთიერთგაგების მემორანდუმებთან

წინამდებარე შეთანხმება გავლენას არ მოახდენს საიდუმლო ინფორმაციის დაცვის შესახებ ხელშემკვრელ მხარეებს ან კომპეტენტურ ორგანოებს შორის არსებულ წებისმიერ ხელშეკრულებაზე, შეთანხმებაზე და ურთიერთგაგების მემორანდუმზე იმდენად, რამდენადაც ისინი წინააღმდეგობაში არ მოდის მის დებულებებთან.

მუხლი 16

დასკვნითი დებულებები

(1) წინამდებარე შეთანხმება ძალაში შედის მისი ძალაში შესვლისთვის აუცილებელი შიდასახელმწიფოებრივი მოთხოვნების დასრულების შესახებ საქართველოს მთავრობის მიერ გერმანიის ფედერაციული რესპუბლიკის მთავრობის შეტყობინების დღეს. შესაბამის თარიღად განისაზღვრება შეტყობინების მიღების თარიღი.

(2) წინამდებარე შეთანხმება იდება განუსაზღვრელი ვადით.

(3) წინამდებარე შეთანხმებაში შესაძლებელია წერილობით ცვლილებების შეტანა, ხელშემკვრელ მხარეთა ურთიერთშეთანხმების საფუძველზე. თითოეულ ხელშემკვრელ მხარეს ნებისმიერ დროს შეუძლია წარადგინოს წერილობითი მოთხოვნა წინამდებარე შეთანხმებაში ცვლილებების შეტანის თაობაზე. თუ ერთ-ერთი ხელშემკვრელი მხარე წარადგენს ამგვარ მოთხოვნას, ხელშემკვრელი მხარეები მოლაპარაკებებს გამართავენ წინამდებარე შეთანხმებაში ცვლილებების შეტანის თაობაზე. აღნიშნული ცვლილებები ძალაში შედის ამ მუხლის პირველი პუნქტის შესაბამისად.

(4) თითოეულ ხელშემკვრელ მხარეს შეუძლია, დიპლომატიური არხების მეშვეობით, განახორციელოს წინამდებარე შეთანხმების დენონსაცია,

ექვსთვიანი წერილობითი შეტყობინების გაგზავნით. დენონსაციის შემთხვევაში, წინამდებარე შეთანხმების საფუძველზე გადაცემულ ან კონტრაქტორის მიერ შექმნილ საიდუმლო ინფორმაციასთან მოპყრობა უნდა გაგრძელდეს წინამდებარე შეთანხმების მე-4 მუხლის დებულებების შესაბამისად მანამდე, სანამ ეს გამართლებული იქნება დასაიდუმლოების არსებობით.

(5) გაერთიანებული ერების ორგანიზაციის წესდების 102-ე მუხლის შესაბამისად, გაერთიანებული ერების ორგანიზაციის სამდივნოში წინამდებარე შეთანხმების დარეგისტრირების ინიცირებას, მისი ძალაში შესვლის შემდეგ, დაუყოვნებლივ მოახდენს ის ხელშემკვრელი მხარე, რომლის სახელმწიფოს ტერიტორიაზეც იდება წინამდებარე შეთანხმება. რეგისტრაციის და გაეროს სარეგისტრაციო ნომრის შესახებ მეორე ხელშემკვრელი მხარე ინფორმირებული უნდა იყოს დაუყოვნებლივ მას შემდეგ, რაც ეს დადასტურდება სამდივნოს მიერ.

შესრულებულია ქ. თბილისი 2017 წლის 16 ნოემბერი ორ დედნად ქართულ, გერმანულ და ინგლისურ ენებზე, სამივე ტექსტი თანაბრად ავთენტურია. ქართულ და გერმანულ ტექსტებს შორის განსხვავებული განმარტების შემთხვევაში, უპირატესობა მიენიჭება ტექსტს ინგლისურ ენაზე.

საქართველოს მთავრობის სახელით	გერმანიის ფედერაციული რესპუბლიკის მთავრობის სახელით

[GERMAN TEXT – TEXTE ALLEMAND]

Abkommen

zwischen

der Regierung von Georgien

und

der Regierung der Bundesrepublik Deutschland

über den Austausch und den gegenseitigen Schutz von Verschlusssachen

Die Regierung von Georgien

und

die Regierung der Bundesrepublik Deutschland –

(im Folgenden gemeinsam als „Vertragsparteien“ und einzeln als „Vertragspartei“ bezeichnet,)

in der Absicht, den Schutz von Verschlusssachen zu gewährleisten, die zwischen den zuständigen Behörden Georgiens und der Bundesrepublik Deutschland sowie mit Auftragnehmern im Hoheitsgebiet des Staates der anderen Vertragspartei oder zwischen Auftragnehmern beider Vertragsparteien ausgetauscht werden,

von dem Wunsch geleitet, eine Regelung über den gegenseitigen Schutz von Verschlusssachen zu schaffen, die auf alle zwischen den Vertragsparteien zu schließenden Abkommen über Zusammenarbeit und auf Verträge, die einen Austausch von Verschlusssachen mit sich bringen, Anwendung findet –

sind wie folgt übereingekommen:

Artikel 1
Begriffsbestimmungen

(1) Im Sinne dieses Abkommens

1. sind „Verschlusssachen“

   a) in der Bundesrepublik Deutschland
   im öffentlichen Interesse geheimhaltungsbedürftige Tatsachen, Gegenstände oder

Erkenntnisse, unabhängig von ihrer Darstellungsform. Sie werden entsprechend ihrer Schutzbedürftigkeit von einer amtlichen Stelle oder auf deren Veranlassung eingestuft;

b) in Georgien
Daten beziehungsweise Informationen oder Gegenstände (unabhängig von ihrer Form oder Beschaffenheit), die verarbeitet wurden oder werden und die vor unbefugtem Gebrauch geschützt werden müssen, Daten beziehungsweise Informationen umfassen, die Staatsgeheimnisse in den Bereichen Verteidigung, Wirtschaft, auswärtige Beziehungen, Geheimdienst, staatliche Sicherheit und Schutz von Recht und Ordnung des Staates enthalten, und die Staatsgeheimnisse im Sinne der Rechtsordnung von Georgien sind;

2. ist ein „Verschlusssachenauftrag"

ein Vertrag beziehungsweise Untervertrag zwischen einer Behörde oder einem Unternehmen aus dem Staat der einen Vertragspartei (Auftraggeber) und einer Behörde oder einem Unternehmen aus dem Staat der anderen Vertragspartei (Auftragnehmer); im Rahmen eines derartigen Vertrags sind Verschlusssachen aus dem Staat des Auftraggebers dem Auftragnehmer zu überlassen, von dem Auftragnehmer zu entwickeln oder Mitarbeitern des Auftragnehmers, die Arbeiten in Einrichtungen des Auftraggebers durchzuführen haben, zugänglich zu machen.

(2) Für die Geheimhaltungsgrade gelten die folgenden Begriffsbestimmungen:

1. In der Bundesrepublik Deutschland sind Verschlusssachen

a) STRENG GEHEIM, wenn die Kenntnisnahme durch Unbefugte den Bestand oder lebenswichtige Interessen der Bundesrepublik Deutschland oder eines ihrer Länder gefährden kann,

b) GEHEIM, wenn die Kenntnisnahme durch Unbefugte die Sicherheit der Bundesrepublik Deutschland oder eines ihrer Länder gefährden oder ihren Interessen schweren Schaden zufügen kann,

c) VS-VERTRAULICH, wenn die Kenntnisnahme durch Unbefugte für die Interessen der Bundesrepublik Deutschland oder eines ihrer Länder schädlich sein kann,

d) VS-NUR FÜR DEN DIENSTGEBRAUCH, wenn die Kenntnisnahme durch Unbefugte für die Interessen der Bundesrepublik Deutschland oder eines ihrer Länder nachteilig sein kann.

2. In Georgien sind Verschlusssachen

a) „განსაკუთრებული მნიშვნელობის" (entspricht TOP SECRET) – Daten, deren Offenlegung oder Verlust die staatlichen Interessen Georgiens in den Bereichen Verteidigung, Wirtschaft, staatliche Sicherheit, Schutz von Recht und Ordnung sowie Politik des Staates grundlegend beeinträchtigen beziehungsweise schwerste Folgen für Staaten oder Organisationen haben kann, die internationale Vertragspartner Georgiens sind,

b) „სრულიად საიდუმლო" (entspricht SECRET) – Daten, deren Offenlegung oder Verlust schwerwiegende Folgen für die Interessen Georgiens in den Bereichen Verteidigung, staatliche Sicherheit, Schutz von Recht und Ordnung, Politik und Wirtschaft und für die Interessen der Personen haben kann, die vertraulich in den Bereichen Nachrichtendienst, staatliche Sicherheit sowie Schutz von Recht und Ordnung mit den entsprechenden georgischen Behörden, welche diesbezügliche Tätigkeiten durchführen, zusammenarbeiten oder zusammengearbeitet haben, beziehungsweise Daten, deren Bekanntgabe

schwerwiegende Folgen für Staaten oder Organisationen haben kann, die internationale Vertragspartner Georgiens sind,

c) „საიდუმლო" (entspricht CONFIDENTIAL) – Daten, deren Offenlegung den Interessen Georgiens in den Bereichen Verteidigung, staatliche Sicherheit, Schutz von Recht und Ordnung, Politik und Wirtschaft und den Interessen von Personen, die in ein Sonderschutzprogramm für Beteiligte an Strafverfahren einbezogen sind, schaden kann, beziehungsweise Daten, deren Bekanntgabe den Interessen von Staaten oder Organisationen schaden kann, die internationale Vertragspartner Georgiens sind,

d) „შეზღუდული სარგებლობისათვის" (entspricht RESTRICTED) – Daten, deren Offenlegung die Interessen Georgiens in den Bereichen Verteidigung, staatliche Sicherheit, Schutz von Recht und Ordnung, Politik und Wirtschaft beziehungsweise die Interessen und Aktivitäten von Staaten oder Organisationen, die internationale Vertragspartner Georgiens sind, beeinträchtigen kann.

Artikel 2
Vergleichbarkeit

Die Vertragsparteien legen fest, dass folgende Geheimhaltungsgrade vergleichbar sind:

Georgien	Bundesrepublik Deutschland	englische Entsprechung
განსაკუთრებული მნიშვნელობის	STRENG GEHEIM	TOP SECRET
სრულიად საიდუმლო	GEHEIM	SECRET
საიდუმლო	VS-VERTRAULICH	CONFIDENTIAL
შეზღუდული სარგებლობისათვის	VS-NUR FÜR DEN DIENSTGEBRAUCH	RESTRICTED

Artikel 3

Kennzeichnung

(1) Die übermittelten Verschlusssachen werden von der zuständigen Behörde der empfangenden Vertragspartei oder auf deren Veranlassung mit dem nach Artikel 2 vergleichbaren innerstaatlichen Geheimhaltungsgrad gekennzeichnet.

(2) Die Kennzeichnungspflicht gilt auch für Verschlusssachen, die bei der empfangenden Vertragspartei im Zusammenhang mit Verschlusssachenaufträgen entstehen, und für von der empfangenden Vertragspartei hergestellte Kopien.

(3) Geheimhaltungsgrade werden auf Ersuchen der zuständigen Behörde der herausgebenden Vertragspartei von der zuständigen Behörde der die betreffende Verschlusssache empfangenden Vertragspartei oder auf deren Veranlassung geändert oder aufgehoben. Die zuständige Behörde der herausgebenden Vertragspartei teilt der zuständigen Behörde der anderen Vertragspartei ihre Absicht, einen Geheimhaltungsgrad zu ändern oder aufzuheben, unverzüglich mit.

(4) Die Übersetzung, Vervielfältigung und Vernichtung von Verschlusssachen erfolgt im Einklang mit den in den innerstaatlichen Gesetzen und sonstigen Vorschriften der Vertragsparteien niedergelegten Anforderungen.

Artikel 4

Innerstaatliche Maßnahmen

(1) Die Vertragsparteien treffen im Rahmen ihrer innerstaatlichen Gesetze und sonstigen Vorschriften alle geeigneten Maßnahmen, um den Schutz von Verschlusssachen zu gewährleisten, die nach diesem Abkommen entstehen, ausgetauscht oder aufbewahrt werden. Sie gewähren diesen Verschlusssachen innerhalb der Grenzen der jeweiligen innerstaatlichen Gesetze und sonstigen Vorschriften der Vertragsparteien mindestens den

gleichen Schutz, wie er von der empfangenden Vertragspartei für eigene Verschlusssachen des vergleichbaren Geheimhaltungsgrads gefordert wird.

(2) Die Dauer des Geheimschutzes bemisst sich nach den jeweiligen innerstaatlichen Gesetzen und sonstigen Vorschriften der herausgebenden Vertragspartei.

(3) Die Verschlusssachen werden ausschließlich für den angegebenen Zweck verwendet. Die empfangende Vertragspartei darf Verschlusssachen weder bekanntgeben oder nutzen noch ihre Bekanntgabe oder Nutzung gestatten, es sei denn, dies geschieht für die Zwecke und mit den etwaigen Beschränkungen, die von oder auf Veranlassung der herausgebenden Vertragspartei festgelegt worden sind. Einer gegenteiligen Regelung muss die herausgebende Vertragspartei schriftlich zugestimmt haben.

(4) Die Verschlusssachen können im Einklang mit den jeweiligen innerstaatlichen Gesetzen und sonstigen Vorschriften der Vertragsparteien zugänglich gemacht werden. Die Ermächtigung zum Zugang setzt eine Sicherheitsüberprüfung voraus, die mindestens so streng sein muss wie diejenige, die für den Zugang zu innerstaatlichen Verschlusssachen des vergleichbaren Geheimhaltungsgrads durchgeführt wird.

(5) Der Zugang zu Verschlusssachen des Geheimhaltungsgrads საიდუმლო / VS-VERTRAULICH und höher durch eine Person mit der Staatsangehörigkeit des Staates einer Vertragspartei wird ohne vorherige Genehmigung der herausgebenden Vertragspartei gewährt.

(6) Sicherheitsüberprüfungen von Staatsangehörigen des Staates der Vertragspartei, die ihren Aufenthalt im eigenen Staat haben und dort Zugang zu Verschlusssachen benötigen, werden von deren zuständigen Behörden vorgenommen.

(7) Sicherheitsüberprüfungen von Staatsangehörigen des Staates einer Vertragspartei, die seit mindestens fünf Jahren ihren rechtmäßigen Aufenthalt im Staat der anderen

Vertragspartei haben und sich dort um eine sicherheitsempfindliche Tätigkeit bewerben, werden hingegen von der zuständigen Behörde dieser Vertragspartei im Einklang mit ihren innerstaatlichen Gesetzen und sonstigen Vorschriften durchgeführt; sie ersucht die zuständige Behörde der anderen Vertragspartei, gegebenenfalls Sicherheitsprüfungen durchzuführen.

(8) Die Vertragsparteien sorgen innerhalb des Hoheitsgebietes ihres jeweiligen Staates für die Durchführung der erforderlichen Sicherheitsinspektionen und für die Einhaltung dieses Abkommens.

Artikel 5

Vernichtung und Rückgabe von Verschlusssachen

(1) Verschlusssachen sind zu vernichten, wenn

a) sie nicht im Einklang mit diesem Abkommen geschützt oder verwendet werden können oder

b) die herausgebende Vertragspartei ihre Vernichtung verlangt.

(2) Schriftliche Verschlusssachen sind so zu vernichten, dass die Wiederherstellung der in ihnen enthaltenen vertraulichen Informationen ausgeschlossen ist.

(3) Die Vernichtung schriftlicher Verschlusssachen erfolgt im Einklang mit den innerstaatlichen Gesetzen und sonstigen Vorschriften der Vertragsparteien.

(4) Gegenständliche Verschlusssachen sind so zu vernichten, dass sie nicht wiederzuerkennen sind, oder so zu verändern, dass die vollständige oder teilweise Wiederherstellung der vertraulichen Informationen ausgeschlossen ist.

(5) Die herausgebende Vertragspartei ist unverzüglich über die Vernichtung zu informieren.

(6) Auf Ersuchen der herausgebenden Vertragspartei werden Verschlusssachen zurückgegeben.

Artikel 6

Vergabe von Verschlusssachenaufträgen

(1) Vor Vergabe eines Verschlusssachenauftrags holt der Auftraggeber über die für ihn zuständige Behörde bei der für den Auftragnehmer zuständigen Behörde einen Sicherheitsbescheid ein, um sich vergewissern zu können, ob der in Aussicht genommene Auftragnehmer der Geheimschutzaufsicht durch die zuständige Behörde dieser Vertragspartei unterliegt und ob er die für die Durchführung des Verschlusssachenauftrags erforderlichen Geheimschutzvorkehrungen getroffen hat. Ist ein Auftragnehmer noch nicht in der Geheimschutzbetreuung, kann hierum ersucht werden.

(2) Ein Sicherheitsbescheid ist auch dann einzuholen, wenn ein Unternehmen zur Abgabe eines Angebots aufgefordert worden ist und im Rahmen des Ausschreibungsverfahrens bereits vor Erteilung des Verschlusssachenauftrags Verschlusssachen übergeben werden müssen.

(3) In den Fällen der Absätze 1 und 2 wird das folgende Verfahren angewendet:

1. Ersuchen um Ausstellung eines Sicherheitsbescheids für Auftragnehmer aus dem Staat der anderen Vertragspartei enthalten Angaben über das Vorhaben sowie die Art, den Umfang und den Geheimhaltungsgrad der dem Auftragnehmer voraussichtlich zu überlassenden oder bei ihm entstehenden Verschlusssachen.

2. Sicherheitsbescheide müssen neben der vollständigen Bezeichnung des

Unternehmens, seiner Postanschrift und dem Namen des Sicherheitsbevollmächtigten sowie dessen Telefon- und Faxnummern und gegebenenfalls E-Mail-Adresse insbesondere Angaben darüber erhalten, in welchem Umfang und bis zu welchem Geheimhaltungsgrad bei dem betreffenden Unternehmen Geheimschutzmaßnahmen auf der Grundlage innerstaatlicher Gesetze und sonstiger Vorschriften getroffen worden sind.

3. Die zuständigen Behörden der Vertragsparteien teilen es einander mit, wenn sich die den ausgestellten Sicherheitsbescheiden zugrunde liegenden Sachverhalte ändern.

4. Der Austausch dieser Mitteilungen zwischen den zuständigen Behörden der Vertragsparteien erfolgt in der Landessprache der zu unterrichtenden Behörde oder in englischer Sprache.

5. Sicherheitsbescheide und an die jeweils zuständigen Behörden der Vertragsparteien gerichtete Ersuchen um Ausstellung von Sicherheitsbescheiden sind schriftlich zu übermitteln.

Artikel 7

Durchführung von Verschlusssachenaufträgen

(1) Verschlusssachenaufträge müssen eine Geheimschutzklausel enthalten, der zufolge der Auftragnehmer verpflichtet ist, die zum Schutz von Verschlusssachen erforderlichen Vorkehrungen in Übereinstimmung mit den innerstaatlichen Gesetzen und sonstigen Vorschriften seines Staates zu treffen.

(2) Außerdem sind folgende Bestimmungen in die Geheimschutzklausel aufzunehmen:

1. die Bestimmung des Begriffs „Verschlusssachen“ und der vergleichbaren

Geheimhaltungsgrade der beiden Vertragsparteien in Übereinstimmung mit diesem Abkommen;

2. der Name der jeweils zuständigen Behörde der Vertragsparteien, die zur Genehmigung der Überlassung von Verschlusssachen, die mit dem Verschlusssachenauftrag in Zusammenhang stehen, und zur Koordinierung des Schutzes dieser Verschlusssachen ermächtigt sind;

3. die Wege, über die Verschlusssachen zwischen den zuständigen Behörden und beteiligten Auftragnehmern weiterzugeben sind;

4. die Verfahren und Mechanismen für die Mitteilung von Änderungen, die sich möglicherweise in Bezug auf Verschlusssachen aufgrund von Änderungen ihres Geheimhaltungsgrads oder wegen des Wegfalls der Einstufungsnotwendigkeit ergeben;

5. die Verfahren für die Genehmigung von Besuchen oder des Zugangs von Personal der Auftragnehmer;

6. die Verfahren für die Übermittlung von Verschlusssachen an Auftragnehmer, bei denen solche Verschlusssachen verwendet und aufbewahrt werden sollen;

7. die Forderung, dass der Auftragnehmer den Zugang zu einer Verschlusssache nur einer Person gewähren darf, welche die Bedingung „Kenntnis nur, wenn nötig" erfüllt und mit der Durchführung des Verschlusssachenauftrags beauftragt worden oder daran beteiligt ist und – außer im Falle von als შეზღუდული სარგებლობისათვის / VS-NUR FÜR DEN DIENSTGEBRAUCH eingestuften Verschlusssachen – zuvor bis zum entsprechenden Geheimhaltungsgrad sicherheitsüberprüft worden ist;

8. die Forderung, dass eine Verschlusssache nur an Dritte weitergegeben beziehungsweise ihre Weitergabe an Dritte nur gestattet werden darf, wenn die herausgebende Vertragspartei dem zugestimmt hat;

9. die Forderung, dass der Auftragnehmer die für ihn zuständige Behörde unverzüglich über jeden erfolgten oder vermuteten Verlust, eine begangene oder vermutete Indiskretion oder unbefugte Bekanntgabe der unter den Verschlusssachenauftrag fallenden Verschlusssachen zu unterrichten hat.

(3) Die für den Auftraggeber zuständige Behörde benennt dem Auftragnehmer in einer gesonderten Aufstellung (Einstufungsliste) sämtliche Vorgänge, die einer Verschlusssacheneinstufung bedürfen, legt den erforderlichen Geheimhaltungsgrad fest und veranlasst, dass diese Aufstellung dem Verschlusssachenauftrag als Anhang beigefügt wird. Die für den Auftraggeber zuständige Behörde hat diese Aufstellung auch der für den Auftragnehmer zuständigen Behörde zu übermitteln oder ihre Übermittlung zu veranlassen.

(4) Die für den Auftraggeber zuständige Behörde stellt sicher, dass dem Auftragnehmer Verschlusssachen erst dann zugänglich gemacht werden, wenn der entsprechende Sicherheitsbescheid der für den Auftragnehmer zuständigen Behörde vorliegt.

Artikel 8
Übermittlung von Verschlusssachen

(1) Verschlusssachen des Geheimhaltungsgrads განსაკუთრებული მნიშვნელობის / STRENG GEHEIM werden zwischen den Vertragsparteien ausschließlich auf diplomatischem Wege befördert.

(2) Verschlusssachen der Geheimhaltungsgrade საიდუმლო / VS-VERTRAULICH und

სრულიად საიდუმლო / GEHEIM werden von einem Staat in den anderen grundsätzlich auf amtlichem Kurierweg befördert. Die zuständigen Behörden der Vertragsparteien können alternative Übermittlungswege vereinbaren. Der Empfang einer Verschlusssache wird von der zuständigen Behörde oder auf deren Veranlassung bestätigt und die Verschlusssache nach Maßgabe der innerstaatlichen Gesetze und sonstigen Vorschriften an den Empfänger weitergeleitet.

(3) Die zuständigen Behörden können für ein genau bezeichnetes Vorhaben – allgemein oder unter Festlegung von Beschränkungen – vereinbaren, dass Verschlusssachen der Geheimhaltungsgrade საიდუმლო / VS-VERTRAULICH und სრულიად საიდუმლო / GEHEIM auf einem anderen als dem amtlichen Kurierweg befördert werden dürfen, sofern die Einhaltung des amtlichen Kurierwegs den Transport oder die Ausführung eines Verschlusssachenauftrags unangemessen erschweren würde. In derartigen Fällen

1. muss der Beförderer zum Zugang zu Verschlusssachen des vergleichbaren Geheimhaltungsgrads ermächtigt sein;

2. muss bei der absendenden zuständigen Behörde ein Verzeichnis der beförderten Verschlusssachen verbleiben; ein Exemplar dieses Verzeichnisses ist dem Empfänger zur Weiterleitung an die zuständige Behörde zu übergeben;

3. müssen die Verschlusssachen nach den für die Inlandsbeförderung geltenden innerstaatlichen Gesetzen und sonstigen Vorschriften verpackt sein;

4. muss die Übergabe der Verschlusssachen gegen Empfangsbescheinigung erfolgen und

5. muss der Beförderer einen Kurierausweis mit sich führen, der von der zuständigen Behörde des Staates der absendenden oder der empfangenden Behörde ausgestellt wurde.

(4) Für die Beförderung von Verschlusssachen von erheblichem Umfang werden Transport, Transportweg und Begleitschutz in jedem Einzelfall durch die zuständigen Behörden auf der Grundlage eines detaillierten Transportplans festgelegt.

(5) Verschlusssachen der Geheimhaltungsgrade საიდუმლო / VS-VERTRAULICH und höher dürfen auf elektronischem Wege nicht unverschlüsselt übermittelt werden. Für die Verschlüsselung von Verschlusssachen dieser Geheimhaltungsgrade dürfen nur Verschlüsselungssysteme eingesetzt werden, die von den zuständigen Behörden der Vertragsparteien in gegenseitigem Einvernehmen zugelassen worden sind.

(6) Verschlusssachen des Geheimhaltungsgrads შეზღუდული სარგებლობისათვის / VS-NUR FÜR DEN DIENSTGEBRAUCH können unter Berücksichtigung der innerstaatlichen Gesetze und sonstigen Vorschriften und unter der Voraussetzung, dass sich Absender und Empfänger zuvor über die beabsichtigte Übertragung geeinigt haben, an Empfänger im Hoheitsgebiet des Staates der anderen Vertragspartei mit der Post oder anderen Zustelldiensten übermittelt werden.

(7) Verschlusssachen des Geheimhaltungsgrads შეზღუდული სარგებლობისათვის / VS-NUR FÜR DEN DIENSTGEBRAUCH können mithilfe von Geräten, die von den zuständigen Behörden der Vertragsparteien zugelassen worden sind, elektronisch übertragen oder zugänglich gemacht werden. Eine unverschlüsselte Übermittlung von Verschlusssachen dieses Geheimhaltungsgrads ist nur zulässig, wenn innerstaatliche Gesetze und sonstige Vorschriften dem nicht entgegenstehen, ein zugelassenes Verschlüsselungssystem nicht verfügbar ist, die Übermittlung ausschließlich innerhalb von Festnetzen erfolgt und Absender und Empfänger sich zuvor über die beabsichtigte Übertragung geeinigt haben.

Artikel 9

Besuche

(1) Besuchern aus dem Hoheitsgebiet des Staates einer Vertragspartei wird im Hoheitsgebiet des Staates der anderen Vertragspartei Zugang zu Verschlusssachen sowie zu Einrichtungen, in denen an diesen gearbeitet wird, grundsätzlich nur mit vorheriger Erlaubnis der zuständigen Behörde des Staates der zu besuchenden Vertragspartei gewährt. Sie wird nur Personen erteilt, welche die Bedingung „Kenntnis nur, wenn nötig" nachweislich erfüllen und im Einklang mit den jeweiligen innerstaatlichen Gesetzen und sonstigen Vorschriften der Vertragsparteien zum Zugang zu Verschlusssachen ermächtigt sind.

(2) Besuchsanmeldungen sind rechtzeitig und in Übereinstimmung mit den Gesetzen und sonstigen Vorschriften des Staates der Vertragspartei, in dessen Hoheitsgebiet die Besucher einzureisen wünschen, der zuständigen Behörde dieser Vertragspartei vorzulegen. Die zuständigen Behörden teilen einander die Einzelheiten der Anmeldungen mit und stellen den Schutz personenbezogener Daten sicher.

(3) Besuchsanmeldungen sind in der Sprache des zu besuchenden Staates oder in englischer Sprache und mit folgenden Angaben versehen vorzulegen:

1. Vor- und Familienname, Geburtsdatum und -ort sowie die Pass- oder Personalausweisnummer des Besuchers;

2. Staatsangehörigkeit des Besuchers;

3. Dienstbezeichnung des Besuchers und Name der Behörde oder Stelle, die er vertritt;

4. Grad der Ermächtigung des Besuchers für den Zugang zu Verschlusssachen;

5. Besuchszweck sowie vorgesehenes Besuchsdatum und

6. Angabe der Stellen, Ansprechpartner und Einrichtungen, die besucht werden sollen.

Artikel 10
Konsultationen

(1) Die zuständigen Behörden der Vertragsparteien nehmen von den im Hoheitsgebiet des Staates der jeweils anderen Vertragspartei geltenden Bestimmungen über den Schutz von Verschlusssachen Kenntnis.

(2) Um eine enge Zusammenarbeit bei der Durchführung dieses Abkommens zu gewährleisten, konsultieren die zuständigen Behörden einander auf Ersuchen einer dieser Behörden.

(3) Jede Vertragspartei erlaubt darüber hinaus der zuständigen Behörde der anderen Vertragspartei, Besuche im Hoheitsgebiet ihres Staates zu machen, um mit ihren zuständigen Behörden ihre Verfahren und Einrichtungen zum Schutz von Verschlusssachen, die ihr von der anderen Vertragspartei zur Verfügung gestellt wurden, zu erörtern. Jede Vertragspartei unterstützt diese zuständige Behörde bei der Feststellung, ob solche Verschlusssachen, die ihr von der anderen Vertragspartei zur Verfügung gestellt wurden, ausreichend geschützt werden. Die Einzelheiten der Besuche werden von den zuständigen Behörden festgelegt.

Artikel 11

Streitbeilegung

Streitigkeiten zwischen den Vertragsparteien über die Auslegung oder Anwendung dieses Abkommens werden durch Konsultationen oder Verhandlungen der Vertragsparteien beigelegt und nicht an nationale oder internationale Gerichte oder Dritte zur Beilegung verwiesen.

Artikel 12

Verletzung der Bestimmungen über den gegenseitigen Schutz von Verschlusssachen

(1) Wenn eine unbefugte Bekanntgabe von Verschlusssachen nicht auszuschließen ist, vermutet oder festgestellt wird, ist dies der anderen Vertragspartei unverzüglich mitzuteilen.

(2) Verletzungen der Bestimmungen über den Schutz von Verschlusssachen werden von den zuständigen Behörden und Gerichten der Vertragspartei, deren Zuständigkeit gegeben ist, nach den innerstaatlichen Gesetzen und sonstigen Vorschriften dieser Vertragspartei untersucht und verfolgt. Die andere Vertragspartei soll diese Ermittlungen auf Ersuchen unterstützen und ist über das Ergebnis zu unterrichten.

Artikel 13

Kosten

Jede Vertragspartei trägt die ihr bei der Durchführung dieses Abkommens entstehenden Kosten.

Artikel 14

Zuständige Behörden

(1) Im Sinne dieses Abkommens sind die für die Durchführung dieses Abkommens zuständigen Behörden

1. für die Bundesrepublik Deutschland:
   das Bundesministerium des Innern (nationale Sicherheitsbehörde),
   das Bundesministerium für Wirtschaft und Energie (bezeichnete Sicherheitsbehörde),
   das Bundesministerium der Verteidigung (militärische Sicherheitsbehörde);

2. für Georgien:
   der staatliche Sicherheitsdienst Georgiens.

(2) Nach Inkrafttreten dieses Abkommens teilen die zuständigen Behörden einander unmittelbar ihre Kontaktinformationen und etwaige Änderungen mit.

(3) Die Vertragsparteien unterrichten einander auf diplomatischem Wege über alle Änderungen der zuständigen Behörden und ihrer Kontaktinformationen.

(4) Eine Änderung der zuständigen Behörden führt nicht zur Einleitung einer Änderung dieses Abkommens.

Artikel 15

Verhältnis zu anderen Abkommen, Vereinbarungen und Absprachen

Alle bestehenden Abkommen, Vereinbarungen und Absprachen zwischen den

Vertragsparteien oder den zuständigen Behörden über den Schutz von Verschlusssachen bleiben von diesem Abkommen unberührt, soweit sie diesem nicht entgegenstehen.

Artikel 16

Schlussbestimmungen

(1) Dieses Abkommen tritt an dem Tag in Kraft, an dem die Regierung von Georgien der Regierung der Bundesrepublik Deutschland notifiziert hat, dass die innerstaatlichen Voraussetzungen für das Inkrafttreten erfüllt sind. Maßgebend ist der Tag des Eingangs der Notifikation.

(2) Dieses Abkommen wird auf unbestimmte Zeit geschlossen.

(3) Dieses Abkommen kann einvernehmlich in Schriftform von den Vertragsparteien geändert werden. Jede Vertragspartei kann jederzeit schriftlich eine Änderung dieses Abkommens beantragen. Stellt eine Vertragspartei einen entsprechenden Antrag, so führen die Vertragsparteien Verhandlungen über die Änderung dieses Abkommens durch. Solche Änderungen treten nach Absatz 1 in Kraft.

(4) Jede Vertragspartei kann dieses Abkommen unter Einhaltung einer Frist von sechs Monaten auf diplomatischem Wege schriftlich kündigen. Im Falle der Kündigung sind die aufgrund dieses Abkommens übermittelten oder beim Auftragnehmer entstandenen Verschlusssachen weiterhin nach Artikel 4 zu behandeln, solange das Bestehen der Einstufung dies rechtfertigt.

(5) Die Registrierung dieses Abkommens beim Sekretariat der Vereinten Nationen nach Artikel 102 der Charta der Vereinten Nationen wird unverzüglich nach seinem Inkrafttreten von der Vertragspartei veranlasst, in deren Staatsgebiet das Abkommen geschlossen wird. Die andere Vertragspartei wird unter Angabe der VN-Registriernummer von der erfolgten Registrierung unterrichtet, sobald diese vom Sekretariat der Vereinten Nationen bestätigt worden ist.

Geschehen zu Tiflis am 16. November 2017 in zwei Urschriften in georgischer, deutscher und englischer Sprache, wobei jeder Wortlaut verbindlich ist. Bei unterschiedlicher Auslegung des georgischen und des deutschen Wortlauts ist der englische Wortlaut maßgebend.

Für die Regierung von Georgien

Für die Regierung der Bundesrepublik Deutschland

[TRANSLATION – TRADUCTION]

ACCORD ENTRE LE GOUVERNEMENT DE LA GÉORGIE ET LE GOUVERNEMENT DE LA RÉPUBLIQUE FÉDÉRALE D'ALLEMAGNE SUR L'ÉCHANGE ET LA PROTECTION MUTUELLE DES INFORMATIONS CLASSIFIÉES

Le Gouvernement de la Géorgie et le Gouvernement de la République fédérale d'Allemagne(ci-après dénommés collectivement les « Parties contractantes » et individuellement la « Partie contractante »),

Aspirant à garantir la protection des informations classifiées échangées entre les autorités compétentes de la Géorgie et de la République fédérale d'Allemagne ainsi qu'avec des contractants sur le territoire de l'État de l'autre Partie contractante ou entre des contractants des deux Parties contractantes,

Désireux d'établir un accord relatif à la protection réciproque d'informations classifiées qui s'applique à tous les accords de coopération conclus entre les Parties contractantes, ainsi qu'aux contrats impliquant l'échange d'informations classifiées,

Sont convenus de ce qui suit :

Article premier. Définitions

1) Aux fins du présent Accord :

1. le terme « information classifiée » désigne :

a. en République fédérale d'Allemagne : les faits, éléments ou renseignements qui, quelle que soit leur présentation, doivent être tenus secrets dans l'intérêt public. Ils sont classifiés par un organe officiel, ou à sa demande, conformément à ses besoins en matière de protection ;
b. en Géorgie : les données/informations ou éléments matériels (quelle que soit leur forme ou leur nature) qui ont été traités ou sont en cours de traitement et qui doivent être protégés contre toute manipulation non autorisée, y compris les données/informations contenant des secrets d'État dans les domaines de la défense, de l'économie, des relations étrangères, du renseignement, de la sécurité de l'État et de la protection de l'ordre public et qui constituent des secrets d'État conformément à la législation de la Géorgie ;

2. le terme « contrat classifié » désigne un contrat ou un contrat de sous-traitance entre une autorité ou une entreprise du pays d'une Partie contractante (ci-après dénommée le « chargé de contrat ») et une autorité ou une entreprise du pays de l'autre Partie contractante (ci-après dénommée le « contractant ») ; dans le cadre de ce contrat, des informations classifiées de l'État du chargé de contrat doivent être divulguées au contractant, recueillies par le contractant ou rendues accessibles aux membres du personnel du contractant qui doivent effectuer des tâches dans les installations du chargé de contrat.

2) Les niveaux de classification de sécurité sont définis comme suit :

1. en République fédérale d'Allemagne, les informations classifiées sont placées dans les catégories suivantes :

a. « STRENG GEHEIM » si le fait que des personnes non autorisées en prennent connaissance risque de porter atteinte à l'existence ou aux intérêts vitaux de la République fédérale d'Allemagne ou de l'un de ses États fédérés (Länder) ;
b. « GEHEIM » si le fait que des personnes non autorisées en prennent connaissance risque de porter atteinte à la sécurité de la République fédérale d'Allemagne ou de l'un de ses États fédérés (Länder) ou de nuire sérieusement à leurs intérêts ;
c. « VS-VERTRAULICH » si le fait que des personnes non autorisées en prennent connaissance risque de porter atteinte aux intérêts de la République fédérale d'Allemagne ou de l'un de ses États fédérés (Länder) ;
d. « VS-NUR FÜR DEN DIENSTGEBRAUCH » si le fait que des personnes non autorisées en prennent connaissance risque de nuire aux intérêts de la République fédérale d'Allemagne ou de l'un de ses États fédérés (Länder) ;

2. En Géorgie, les informations classifiées sont placées dans les catégories suivantes :

a. « » (équivalent de « TRÈS SECRET ») : les données dont la diffusion ou la perte risque d'avoir un effet négatif important sur les intérêts de la Géorgie dans les domaines de la défense, de l'économie, de la sécurité de l'État, de la protection de l'ordre public et de la politique de l'État, ou d'entraîner les conséquences les plus graves pour un État ou une organisation qui est partie à un traité international dont la Géorgie est signataire ;
b. « » (équivalent de « SECRET ») : les données dont la diffusion ou la perte risque d'avoir de graves conséquences pour la défense, la sécurité de l'État, la protection de l'ordre public et les intérêts politiques et économiques de la Géorgie, ainsi que pour les intérêts des personnes qui coopèrent ou ont coopéré à titre confidentiel dans les domaines du renseignement, de la sécurité de l'État et de la protection de l'ordre public avec les différentes autorités géorgiennes compétentes, ou les données dont la divulgation peut avoir de graves conséquences pour un État ou une organisation qui est partie à un traité international dont la Géorgie est signataire ;
c. « » (équivalent de « CONFIDENTIEL ») : les données dont la diffusion risque de porter atteinte à la défense, à la sécurité de l'État, à la protection de l'ordre public, aux intérêts politiques et économiques de la Géorgie, ainsi qu'aux intérêts des personnes faisant l'objet d'un programme de protection spécial dans le cadre d'une participation à des procédures pénales, ou les données dont la divulgation peut porter atteinte aux intérêts d'un État ou d'une organisation qui est partie à un traité international dont la Géorgie est signataire ;
d. « » (équivalent de « RESTREINT ») : les données dont la diffusion risque d'avoir un effet négatif sur la défense, la sécurité de l'État, la protection de l'ordre public, les intérêts politiques et économiques de la Géorgie, ou sur les intérêts et activités d'un État ou d'une organisation qui est partie à un traité international dont la Géorgie est signataire.

Article 2. Équivalence

Les Parties contractantes disposent que les niveaux de classification de sécurité suivants sont équivalents :

Géorgie	République fédérale d'Allemagne	Équivalent français
განსაკუთრებული მნიშვნელობის	STRENG GEHEIM	TRÈS SECRET
სრულიად საიდუმლო	GEHEIM	SECRET
საიდუმლო	VS-VERTRAULICH	CONFIDENTIEL
შეზღუდული სარგებლობისათვის	VS-NUR FÜR DEN DIENSTGEBRAUCH	RESTREINT

Article 3. Marquage

1) Les informations classifiées transmises se voient apposer la marque du niveau de classification de sécurité nationale équivalent prévu à l'article 2 par l'autorité compétente de la Partie contractante destinataire ou à la demande de cette dernière.

2) Les informations classifiées qui sont produites par la Partie contractante destinataire dans le cadre de contrats classifiés ainsi que les copies qui en sont faites par ladite Partie contractante doivent également porter une marque de classification.

3) À la demande de l'autorité compétente de la Partie contractante d'origine, les niveaux de classification de sécurité sont modifiés ou révoqués par l'autorité compétente de la Partie contractante destinataire de l'information classifiée concernée, ou à sa demande. L'autorité compétente de la Partie contractante d'origine informe sans délai l'autorité compétente de l'autre Partie contractante de son intention de modifier ou de révoquer un niveau de classification de sécurité.

4) La traduction, la reproduction et la destruction des informations classifiées s'effectuent conformément aux exigences prévues par les lois et règlements nationaux des Parties contractantes.

Article 4. Mesures prises au niveau national

1) Dans le cadre de leurs lois et règlements nationaux, les Parties contractantes prennent toutes les mesures appropriées pour garantir la protection des informations classifiées produites, échangées ou détenues conformément aux dispositions du présent Accord. Elles accordent à ces informations classifiées, dans les limites de leurs lois et règlements nationaux respectifs, un degré de protection au moins égal à celui qu'exige la Partie contractante destinataire pour ses propres informations classifiées relevant du niveau de classification de sécurité équivalent.

2) La durée de la classification est définie par les lois et règlements nationaux de la Partie contractante d'origine.

3) Les informations classifiées ne sont utilisées qu'aux fins précisées. La Partie contractante destinataire ne divulgue ni n'exploite ni ne permet la divulgation ou l'exploitation d'informations classifiées à des fins autres que celles indiquées par la Partie contractante d'origine ou à sa demande et dans le cadre des limites posées par ladite Partie contractante. La Partie contractante d'origine doit avoir donné son consentement écrit à tout arrangement contraire à cette disposition.

4) L'accès aux informations classifiées peut être accordé conformément aux lois et règlements nationaux respectifs des Parties contractantes. L'habilitation de sécurité n'est accordée qu'au terme d'une enquête de sécurité menée selon des normes non moins strictes que celles qui s'appliquent à l'accès aux informations classifiées nationales relevant du niveau de classification de sécurité équivalent.

5) L'accès aux informations classifiées de niveau « VS-VERTRAULICH » / « » ou de niveau supérieur est accordé sans autorisation préalable par la Partie contractante d'origine à une personne ayant la nationalité d'une Partie contractante.

6) Les habilitations de sécurité personnelles des ressortissants de l'État de la Partie contractante qui y résident et y demandent l'accès à des informations classifiées sont accordées par les autorités compétentes de cet État.

7) Toutefois, les habilitations de sécurité personnelles des ressortissants de l'État d'une Partie contractante qui résident légalement dans l'État de l'autre Partie contractante depuis au moins cinq ans et qui y postulent pour un emploi sensible sur le plan de la sécurité sont accordées par l'autorité compétente de cette autre Partie contractante, conformément à ses lois et règlements nationaux ; cette autorité compétente demande à celle de la première Partie contractante de procéder aux contrôles de sécurité appropriés.

8) Les Parties contractantes, sur leurs territoires nationaux respectifs, veillent à ce que les inspections de sécurité nécessaires soient réalisées et à ce que les dispositions du présent Accord soient respectées.

Article 5. Destruction et restitution des informations classifiées

1) Les informations classifiées sont détruites si :

a. elles ne peuvent pas être protégées ou utilisées conformément au présent Accord, ou si
b. la Partie contractante d'origine exige leur destruction.

2) Les documents classifiés sont détruits d'une manière excluant toute possibilité de reconstituer les informations classifiées qu'ils contiennent.

3) La destruction des documents classifiés s'effectue conformément aux lois et règlements nationaux des Parties contractantes.

4) Le matériel classifié est détruit de façon à rendre impossible toute reconnaissance, ou modifié de façon à empêcher la reconstitution des informations classifiées en tout ou en partie.

5) La Partie contractante d'origine est informée sans délai de la destruction.

6) À la demande de la Partie contractante d'origine, les informations classifiées seront restituées.

Article 6. Attribution de contrats classifiés

1) Avant l'attribution d'un contrat classifié, le chargé de contrat obtient, par l'intermédiaire de son autorité compétente, une habilitation de sécurité des installations auprès de l'autorité compétente du contractant afin de déterminer si le contractant potentiel fait l'objet d'un contrôle de sécurité par l'autorité compétente de sa Partie contractante et s'il a pris les précautions de sécurité nécessaires à l'exécution du contrat classifié. Lorsqu'un contractant n'est pas encore soumis à un contrôle de sécurité, une demande peut être faite à cette fin.

2) Une habilitation de sécurité des installations est également obtenue si une entreprise a été invitée à soumettre une offre et si des informations classifiées doivent être divulguées avant l'attribution d'un contrat classifié dans le cadre de la procédure d'appel d'offres.

3) Dans les cas visés aux paragraphes 1 et 2 du présent article, la procédure suivante est appliquée :

1. les demandes de délivrance d'une habilitation de sécurité des installations à l'égard de contractants de l'État de l'autre Partie contractante contiennent des informations sur le projet ainsi que sur la nature, la portée et le niveau de classification de sécurité des informations classifiées susceptibles d'être divulguées au contractant ou produites par ce dernier ;

2. outre la désignation complète de l'entreprise, son adresse postale et le nom de son responsable en matière de sécurité, son numéro de téléphone et de télécopie et, s'il y a lieu, son adresse électronique, les habilitations de sécurité des installations doivent notamment contenir des informations sur l'ampleur des mesures de sécurité prises par l'entreprise concernée conformément aux lois et règlements nationaux ainsi que sur le niveau de classification de sécurité correspondant à ces mesures ;

3. les autorités compétentes des Parties contractantes s'informent mutuellement de toute modification apportée aux faits auxquels s'applique l'habilitation de sécurité des installations délivrée ;

4. les échanges relatifs à ces informations entre les autorités compétentes des Parties contractantes s'effectuent soit dans la langue du pays des autorités qui doivent être informées, soit en anglais ;

5. les habilitations de sécurité des installations et les demandes adressées aux autorités compétentes respectives des Parties contractantes concernant la délivrance de telles habilitations sont transmises par écrit.

Article 7. Exécution de contrats classifiés

1) Les contrats classifiés doivent contenir une clause de sécurité au titre de laquelle le contractant est tenu de prendre les dispositions nécessaires à la protection des informations classifiées conformément aux lois et règlements nationaux de son État.

2) En outre, la clause de sécurité contient les dispositions suivantes :

1. la définition du terme « informations classifiées » et des niveaux de classification de sécurité équivalents des deux Parties contractantes, conformément aux dispositions du présent Accord ;

2. le nom de l'autorité compétente de chacune des deux Parties contractantes habilitée à autoriser la divulgation des informations classifiées ainsi qu'à coordonner la sauvegarde des informations classifiées faisant l'objet du contrat classifié ;

3. les voies de communication à utiliser pour le transfert des informations classifiées entre les autorités compétentes et les contractants concernés ;

4. les procédures et mécanismes de communication des éventuelles modifications portant sur les informations classifiées dues au fait que le niveau de classification de sécurité a changé ou que la classification n'est plus requise ;

5. les procédures d'approbation des visites ou de l'accès par le personnel des contractants ;

6. les procédures de transmission d'informations classifiées aux contractants lorsque de telles informations doivent être utilisées ou détenues ;

7. l'obligation pour le contractant de n'accorder l'accès aux informations classifiées qu'à une personne qui a le besoin d'en connaître et qui est responsable de l'exécution du contrat classifié ou qui y contribue, et (excepté dans le cas d'informations classifiées de niveau « VS-NUR FÜR DEN DIENSTGEBRAUCH » / « ») qui a préalablement obtenu une habilitation de sécurité au niveau approprié ;

8. l'obligation de ne divulguer des informations classifiées à un tiers ou de ne permettre la divulgation d'informations classifiées à un tiers que si cela a été approuvé par la Partie contractante d'origine ;

9. l'obligation pour le contractant d'aviser immédiatement son autorité compétente de tout risque de perte, de fuite ou de divulgation non autorisée d'informations classifiées relevant du contrat classifié.

3) L'autorité compétente du chargé de contrat fournit au contractant une liste séparée (guide de classification) des dossiers de documents exigeant une classification de sécurité, détermine le niveau de classification de sécurité requis et veille à ce que ladite liste soit ajoutée en annexe au contrat classifié. En outre, elle communique la liste à l'autorité compétente du contractant, ou prend les mesures nécessaires à cette communication.

4) L'autorité compétente du chargé de contrat veille à ce que le contractant n'ait pas accès aux informations classifiées avant que l'autorité compétente du contractant n'ait reçu l'habilitation de sécurité des installations pertinente.

Article 8. Transmission d'informations classifiées

1) Les informations classifiées de niveau « STRENG GEHEIM » / « » ne sont transmises entre les Parties contractantes que par la voie diplomatique de gouvernement à gouvernement.

2) Par principe, les informations classifiées de niveau « VS-VERTRAULICH » / « » et de niveau « GEHEIM » / « » sont transmises d'un État à l'autre par courrier officiel. Les autorités compétentes des Parties contractantes peuvent convenir d'autres voies de transmission. La réception des informations classifiées est confirmée par l'autorité compétente, ou à sa demande, et ces informations classifiées sont transmises au destinataire conformément aux lois et règlements nationaux.

3) Pour un projet expressément désigné, les autorités compétentes peuvent convenir, de manière générale ou sous réserve de restrictions, que les informations classifiées de niveau « VS-VERTRAULICH » / « » et de niveau « GEHEIM » / « » peuvent être transmises par des voies

autres que le courrier officiel dans le cas où le recours au service de courrier officiel engendrerait des difficultés excessives vis-à-vis du transport des informations ou de l'exécution d'un contrat classifié. Dans de tels cas :

1. le porteur doit être habilité à accéder aux informations classifiées relevant du niveau de classification de sécurité équivalent ;

2. l'autorité compétente chargée de l'envoi doit conserver une liste des informations classifiées transmises ; une copie de cette liste est communiquée au destinataire pour transmission à l'autorité compétente ;

3. les informations classifiées sont conditionnées conformément aux lois et règlements nationaux régissant le transport sur le territoire national ;

4. les informations classifiées doivent être remises contre accusé de réception ;

5. le porteur doit être muni d'un ordre de mission de messager remis par l'autorité compétente de l'État de l'autorité d'envoi ou de l'autorité destinataire.

4) Lorsqu'un volume important d'informations classifiées doit être transmis, le moyen de transport, l'itinéraire et l'escorte sont déterminés au cas par cas et sur la base d'un plan de transport détaillé par les autorités compétentes.

5) La transmission électronique d'informations classifiées de niveau « VS-VERTRAULICH » / « » et d'un niveau supérieur doit dans tous les cas avoir lieu sous une forme codée. Les informations classifiées à ces niveaux de classification de sécurité sont impérativement codées selon une méthode approuvée d'un commun accord par les autorités compétentes des Parties contractantes.

6) Les informations classifiées de niveau « VS-NUR FÜR DEN DIENSTGEBRAUCH » / « » peuvent être transmises par les services postaux ou autres services de livraison aux destinataires situés sur le territoire de l'État de l'autre Partie contractante, compte tenu des lois et règlements nationaux et à condition que l'expéditeur et le destinataire se soient entendus à l'avance sur la transmission proposée.

7) Les informations classifiées de niveau « VS-NUR FÜR DEN DIENSTGEBRAUCH » / « » peuvent être transmises ou mises à disposition par voie électronique au moyen de dispositifs approuvés par les autorités compétentes des Parties contractantes. À ce niveau de classification de sécurité, lesdites informations classifiées peuvent être transmises autrement que sous une forme codée uniquement si les lois et règlements nationaux ne s'y opposent pas, si aucun système approuvé de codage n'est disponible, si la transmission se fait exclusivement au sein des réseaux établis et si l'expéditeur et le destinataire se sont entendus à l'avance sur la transmission proposée.

Article 9. Visites

1) En principe, les visiteurs en provenance du territoire de l'État d'une Partie contractante ne pourront, sur le territoire de l'État de l'autre Partie contractante, accéder aux informations classifiées et aux installations dans lesquelles des informations classifiées sont traitées qu'avec l'autorisation préalable de l'autorité compétente de la Partie contractante devant accueillir la visite. Cette autorisation n'est accordée qu'aux personnes dont le besoin d'en connaître est établi et qui ont été autorisées à accéder à des informations classifiées conformément aux lois et règlements nationaux respectifs des Parties contractantes.

2) Les demandes de visite sont soumises à l'autorité compétente de la Partie contractante dont les visiteurs souhaitent entrer sur le territoire, en temps utile et conformément aux lois et règlements nationaux de cette Partie contractante. Les autorités compétentes des deux Parties contractantes se communiquent des informations détaillées concernant ces demandes et veillent à la protection des informations à caractère personnel.

3) Les demandes de visites sont soumises dans la langue de l'État à visiter ou en anglais et contiennent les informations suivantes :

1. le nom et le prénom du visiteur, la date et le lieu de naissance ainsi que le numéro du passeport ou de la carte d'identité ;

2. la nationalité du visiteur ;

3. la désignation du service auquel appartient le visiteur, ainsi que le nom de l'autorité ou de l'agence dont ce service fait partie ;

4. le niveau d'habilitation de sécurité du visiteur eu égard à l'accès aux informations classifiées ;

5. le but de la visite et la date proposée pour la visite ;

6. la désignation des agences, interlocuteurs et installations auxquels il sera rendu visite.

Article 10. Consultations

1) L'autorité compétente de chaque Partie contractante prend note des réglementations en vigueur sur le territoire de l'État de l'autre Partie contractante concernant la protection des informations classifiées.

2) Pour assurer une étroite coopération lors de la mise en œuvre du présent Accord, les autorités compétentes se consultent à la demande de l'une ou l'autre d'entre elles.

3) En outre, chaque Partie contractante autorise l'autorité compétente de l'autre Partie contractante à effectuer des visites sur son territoire national en vue d'examiner, avec sa propre autorité compétente, ses procédures et installations de protection des informations classifiées qui lui ont été transmises par l'autre Partie contractante. Chaque Partie contractante aide également cette autorité compétente à déterminer si les informations classifiées mises à sa disposition par l'autre Partie contractante sont dûment protégées. Les détails de ces visites sont arrêtés par les autorités compétentes.

Article 11. Règlement des différends

Tout différend entre les Parties contractantes concernant l'interprétation ou la mise en œuvre du présent Accord est réglé par des consultations ou des négociations entre les Parties contractantes et ne saurait être référé ni à aucun tribunal national ou international, ni à aucune tierce partie aux fins de son règlement.

Article 12. Violations des dispositions régissant la protection mutuelle des informations classifiées

1) Lorsque la transmission non autorisée d'informations classifiées ne peut être exclue ou lorsqu'une telle infraction est présumée ou constatée, l'autre Partie contractante en est immédiatement informée.

2) Les infractions aux dispositions régissant la protection d'informations classifiées font l'objet d'enquêtes et de poursuites judiciaires pertinentes de la part des autorités compétentes des tribunaux de la Partie contractante ayant juridiction, conformément aux lois et règlements nationaux de ladite Partie. L'autre Partie contractante, sur demande, appuie ces enquêtes et est informée de leurs résultats.

Article 13. Frais

Chaque Partie contractante prend en charge les dépenses qu'elle a engagées pour la mise en œuvre des dispositions du présent Accord.

Article 14. Autorités compétentes

1) Aux fins du présent Accord, les autorités compétentes chargées de la mise en œuvre du présent Accord sont :

1. pour la République fédérale d'Allemagne :

le Ministère fédéral de l'intérieur (autorité de sécurité nationale),
le Ministère fédéral de l'économie et de l'énergie (autorité de sécurité désignée),
le Ministère fédéral de la défense (autorité de sécurité militaire) ;

2. pour la Géorgie :
le Service de sécurité de l'État de Géorgie.

2) Dès l'entrée en vigueur du présent Accord, les autorités compétentes s'informent directement de leurs coordonnées et de toute modification de celles-ci.

3) Les Parties contractantes s'informent mutuellement, par la voie diplomatique, de tout changement apporté aux autorités compétentes et à leurs coordonnées.

4) Un changement apporté aux autorités compétentes n'entraîne pas la modification du présent Accord.

Article 15. Relation avec d'autres accords, arrangements et mémorandums d'accord

Les accords, arrangements et mémorandums d'accord existants entre les Parties contractantes ou les autorités compétentes en matière de protection des informations classifiées ne sont pas concernés par le présent Accord dans la mesure où ils ne sont pas en contradiction avec ses dispositions.

Article 16. Dispositions finales

1) Le présent Accord entre en vigueur le jour où le Gouvernement de la Géorgie informe le Gouvernement de la République fédérale d'Allemagne qu'il a accompli toutes les procédures internes nécessaires à son entrée en vigueur. La date effective est la date de réception de cette notification.

2) Le présent Accord est conclu pour une durée indéterminée.

3) Le présent Accord peut être modifié par écrit d'un commun accord entre les Parties contractantes. Chacune des Parties contractantes peut à tout moment demander par écrit une

modification du présent Accord. Si une telle demande est présentée par une Partie contractante, les Parties contractantes entament des négociations aux fins de cette modification. Ladite modification entre en vigueur conformément aux modalités énoncées au paragraphe 1 du présent article.

4) Chaque Partie contractante peut, par la voie diplomatique, dénoncer le présent Accord avec notification écrite préalable de six mois. En cas de dénonciation, les informations classifiées qui ont été transmises, ou qui ont été produites par le contractant, sur la base du présent Accord continuent d'être traitées conformément aux dispositions de l'article 4 du présent Accord aussi longtemps que l'existence de la classification de sécurité est justifiée.

5) L'enregistrement du présent Accord au Secrétariat des Nations Unies, conformément à l'Article 102 de la Charte des Nations Unies, est effectué par la Partie contractante sur le territoire national de laquelle ledit Accord est conclu immédiatement après son entrée en vigueur. L'autre Partie contractante est informée dudit enregistrement et du numéro d'enregistrement attribué par l'Organisation des Nations Unies dès que l'accomplissement de cette formalité est confirmé par le Secrétariat.

FAIT à Tbilissi, le 16 novembre 2017, en double exemplaire en langues géorgienne, allemande et anglaise, les trois textes faisant également foi. En cas de divergence d'interprétation entre les textes géorgien et allemand, le texte anglais prévaut.

Pour le Gouvernement de la Géorgie :

[SIGNÉ]

Pour le Gouvernement de la République fédérale d'Allemagne :

[SIGNÉ]