No. 50403*

Switzerland
and
Denmark

Arrangement between the Federal Department of Defence, Civil Protection and Sport of the Swiss Confederation and the Ministry of Defence of the Kingdom of Denmark concerning the mutual protection of classified information. Bern, 25 April 2012 and Copenhagen, 31 May 2012

Entry into force: *31 May 2012*

Authentic text: *English*

Registration with the Secretariat of the United Nations: *Switzerland, 9 January 2013*

*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.

Suisse
et
Danemark

Accord entre le Département fédéral de la défense, de la protection civile et du sport de la Confédération suisse et le Ministère de la défense du Royaume du Danemark relatif à la protection réciproque des informations classifiées. Berne, 25 avril 2012 et Copenhague, 31 mai 2012

Entrée en vigueur : *31 mai 2012*

Texte authentique : *anglais*

Enregistrement auprès du Secrétariat des Nations Unies : *Suisse, 9 janvier 2013*

Numéro de volume RTNU n'a pas encore été établie pour ce dossier. Les textes réproduits ci-dessous, s'ils sont disponibles, sont les textes authentiques de l'accord/pièce jointe d'action tel que soumises pour l'enregistrement et publication au Secrétariat. Pour référence, ils ont été présentés sous forme de la pagination consécutive. Les traductions, s'ils sont inclus, ne sont pas en form finale et sont fournies uniquement à titre d'information.

[ENGLISH TEXT – TEXTE ANGLAIS]

ARRANGEMENT

between

THE FEDERAL DEPARTMENT OF DEFENCE, CIVIL PROTECTION AND SPORT OF THE SWISS CONFEDERATION

and

THE MINISTRY OF DEFENCE OF THE KINGDOM OF DENMARK

CONCERNING

THE MUTUAL PROTECTION OF CLASSIFIED INFORMATION

Preamble

The Federal Department of Defence, Civil Protection and Sport of the Swiss Confederation and the Ministry of Defence of the Kingdom of Denmark also referred to as the Parties for the purpose of this Arrangement have, in the interests of national security in the defence domain, established the following arrangements which are set out in this General Security Arrangement (GSA) wishing to ensure the protection of classified information concerning defence and military issues exchanged between the two ministries or between legal entities or individuals under the jurisdiction of the Parties.

1. DEFINITIONS

1.1 The following terms are defined in the interests of clarity:

- "**Classified Information**" means any classified item, be it an oral or visual communication of classified contents or the electrical or electronic transmission of a classified message;
- **"Classified Material"** includes any classified item of machinery or equipment or weapons either manufactured or in the process of manufacture or document;
- "**Document**" means any letter, note, minute, report, memorandum, signal/message, sketch, photograph, film, map, chart, plan, notebook, stencil, carbon, typewriter ribbon, diskette etc or other form of recorded information (e.g. tape recording, magnetic recording, punched card, tape, etc);
- **Contractor**" means an individual or legal entity possessing the legal capability to undertake contracts;
- "**Contract**" means an agreement between two or more parties creating and defining enforceable rights and obligations between the parties;
- "**Classified Contract**" means a Contract which contains or involves Classified Information;
- "**National Security Authority (NSA)/ Designated Security Authority (DSA)**" means the Government Authority responsible for Defence Security in each country;
- "**Originating Party**" means the Party releasing Classified Information to the Recipient Party;
- "**Recipient Party**" means the Party which receives the Classified Information from the Originating Party.

1.2 For the purpose of these provisions, the security classifications and their equivalents in the two countries will be limited to:

IN SWITZERLAND	Corresponding English term	IN DENMARK
GEHEIM/SECRET/ SEGRETO	SECRET	HEMMELIGT
VERTRAULICH/ CONFIDENTIEL/ CONFIDENZIALE	CONFIDENTIAL	FORTROLIGT
INTERN/ INTERNE/ AD USO INTERNO	RESTRICTED	TIL TJENESTEBRUG

As a general rule, the levels referred to above are to be considered as equivalent. For example a Swiss VERTRAULICH/CONFIDENTIEL/CONFIDENZIALE marked classified document transmitted to Denmark is to be handled, stored and located in a manner which will afford the same protection as that given to a Danish FORTROLIGT marked classified document. However, exceptionally either Party may ask the other to afford protection at a higher level but not at a lower level than the classification indicated.

2. NATIONAL SECURITY AUTHORITIES / DESIGNATED SECURITY AUTHORITIES

The Government Authorities responsible for the implementation of this Arrangement in each country are the following:

FOR SWITZERLAND

Department of Defence, Civil Protection and Sport
Directorate for Information Security and Facility Protection (IOS)
CH-3003 Bern
SWITZERLAND

FOR DENMARK

Danish Defence Intelligence Service
Kastellet 30
DNK-2100 Copenhagen OE
DENMARK

3. RESTRICTIONS ON USE AND DISCLOSURE

3.1 Without express written consent the Recipient Party will not disclose or use, or permit the disclosure or use, of any Classified Information except for purposes and within any limitations stated by or on behalf of the Originating Party.

3.2 The Recipient Party will not pass or disclose to a Government official, Contractor, Contractor's employee or to any other person holding the nationality of any third country, or to any international organisation, any Classified Information, supplied under the provisions of this Agreement without the prior consultation of the Originating Party, nor will it publicly disclose any Classified Information without the prior written permission of the Originating Party. Furthermore, the Recipient Party will not disclose to any third party any information supplied in confidence, whether classified or not, without the prior consultation of the Originating Party.

3.3 Nothing in this Agreement will be taken as an authority for, or to govern the release, use, exchange or disclosure of information in which intellectual property rights exists, until the specific written authorisation of the owner of these rights has first been obtained, whether the owner is one of the Parties or a third party.

3.4 The exchange of Classified Information between the Intelligence Services of the two Parties shall not be subject of the present GSA.

4. PROTECTION OF CLASSIFIED INFORMATION

4.1 The Originating Party will ensure that the Recipient Party is informed of:

(a) The security classification of the information and of any conditions of release or limitations on its use, and that documents are so marked.

(b) Any subsequent change in security classification.

4.2 The Recipient Party will:

(a) In accordance with its national laws and regulations, afford information received

from the other Party a level of security protection that is afforded to Classified Information of an equivalent security classification originated by the Recipient Party.

(b) Ensure that Classified Information is marked with its own security classification in accordance with paragraph 1.2 above.

(c) Ensure that security classifications are not altered, except as authorised in writing by or on behalf of the Originating Party.

4.3 In order to achieve and maintain comparable standards of security, each NSA/DSA will, on request, provide to the other information about its security standards, procedures and practices for safeguarding Classified Information, and will for this purpose facilitate visits by security representatives of the other NSA/DSA.

5. ACCESS TO CLASSIFIED INFORMATION

Access to Classified Information marked FORTROLIGT or VERTRAULICH/ CONFIDENTIEL/CONFIDENZIALE or above will be limited to those persons who have a "need to know", and who have been security cleared by the recipient NSA/DSA, in accordance with its national standards, to the level appropriate to the security classification of the information to be accessed.

6. TRANSMISSION OF CLASSIFIED INFORMATION

Classified Information will be transmitted between the two Parties through Government to Government channels, but other arrangements, such as hand carriage, secure communications (encryption), may be established, if mutually acceptable to both Parties.

7. VISITS

7.1 The prior approval of the NSA/DSA of the host country will be required in respect of visitors, including those on detached duty from the other country, where access is required to Classified Information at the Swiss VERTRAULICH/CONFIDENTIEL/ CONFIDENZIALE and/or GEHEIM/SECRET/SEGRETO or Danish FORTROLIGT and/or HEMMELIGT levels or to defence establishments/defence contractor premises engaged in classified work at these levels. Requests for such visits will be submitted through the NSA/DSA.

7.2 Requests will include the following information:

7.2.1 Name, date and place of birth, nationality and passport number/identity card number of proposed visitor(s).

7.2.2 Official status of the visitor(s) together with the name of the establishment, company or organisation which he/she represents or to which they belong.

7.2.3 Certification of level of security clearance of each visitor.

7.2.4 Name and address of the establishment, company or organisation to be visited.

7.2.5 Name and status of the person(s) to be visited, if known.

7.2.6 Purpose of the visit.

7.2.7 Date of the visit. In cases of recurring visits the total period covered by the visits should be stated.

7.3 All visitors will comply with the security regulations of the host country.

7.4 Visit requests should be submitted to the host Party in accordance with the required lead times before the visit takes place (in Switzerland 10 working days / in Denmark 7 working days). In urgent cases short notice visits can be arranged with the approval of the host country.

7.5 In cases involving a specific project or a particular contract it may, subject to the approval of the host country, be possible to establish Recurring Visitors Lists. These Lists will be valid for an initial period not exceeding 12 months and may be extended for a further period of time (not to exceed 12 months) subject to the prior approval of the NSA/DSA. They should be submitted in accordance with the normal procedures of the Recipient Party. Once a list has been approved, visit arrangements may be made directly between the establishments or companies involved in respect of listed individuals.

7.6 Any information which may be provided to visiting personnel, or which may come to the notice of visiting personnel, will be treated by them as if such information had been furnished pursuant to the provisions of this GSA.

8. CONTRACTS

8.1 When proposing to place, or authorising a Contractor in its country to place, a Contract involving Classified Information marked FORTROLIGT or VERTRAULICH/CONFIDENTIEL/CONFIDENZIALE or above with a Contractor in the other country the Originating Party will obtain prior assurance from the NSA/DSA of the other country that the proposed Contractor is security cleared to the appropriate level and also has suitable security safeguards to provide adequate protection for Classified Information. The assurance will carry a responsibility that the security conduct by the cleared Contractor will be in accordance with national security rules and regulations and monitored by his NSA/DSA.

8.2 The NSA/DSA will ensure that Contractors that receive Contracts placed as a consequence of these pre-contract enquiries are aware of the following provisions:

8.2.1 The definition of the term "Classified Information" and of the equivalent levels of security classification of the two Parties in accordance with the provisions of this GSA.

8.2.2 The names of the Government Authority of each of the two countries empowered to authorise the release and to co-ordinate the safeguarding of Classified Information related to the Contract.

8.2.3 The channels to be used for the transfer of the Classified Information between the Government Authorities and/or Contractors involved.

8.2.4 The procedures and mechanisms for communicating the changes that may arise in respect of Classified Information either because of changes in its security classification or because protection is no longer necessary.

8.2.5 The procedures for the approval of visits, access or inspection by personnel of one country to companies of the other country which are covered by the Contract.

8.2.6 An obligation that the Contractor will disclose the Classified Information only to a person who has previously been security cleared for access, who needs to know, and is employed on, or engaged in, the carrying out of the Contract.

8.2.7 An obligation that the Contractor will not disclose the Classified Information or permit it to be disclosed to any person not expressly cleared by his NSA/DSA to have such access.

8.2.8 An obligation that the Contractor will immediately notify his NSA/DSA of any actual or suspected loss, leak or compromise of the Classified Information of the Contract.

8.3 The NSA/DSA of the Originating Party will pass two copies of the relevant parts of the Classified Contract to the Designated Security Authority of the Recipient Party, to allow adequate security monitoring.

8.4 Each Contract will contain guidance on the security requirements and on the classification of each aspect/element of the Contract. The guidance will be contained in specific security clauses or in a Security Aspects Letter (SAL) as appropriate. The guidance must identify each classified aspect of the Contract, or any classified aspect which is to be generated by the contract, and allocate to it a specific security classification. Changes in the requirements or to the aspects/elements will be notified as and when necessary and the Originating Party will notify the Recipient Party if and when any of the information has been declassified.

9. RECIPROCAL INDUSTRIAL SECURITY ARRANGEMENTS

9.1 Each NSA/DSA will notify the security status of a company facility in its country when requested by the other Party. Each NSA/DSA will also notify the security clearance status of one of its nationals when so requested. These notifications will be known as Facility Security Clearance (FSC) assurance and Personnel Security Clearance (PSC) assurance respectively.

9.2 When requested, the NSA/DSA will establish the security clearance status of the company facility/individual which is the subject of the enquiry and forward a FSC/PSC assurance if the company facility/individual is already cleared. If the company facility/individual does not have a security clearance, or the clearance is at a lower security level than that which has been requested, notification will be sent that the assurance cannot be issued immediately, but that action is being taken to process the request. Following successful enquiries an assurance will be provided which will then permit a reciprocal security clearance to be issued.

9.3 A company which is deemed by the NSA/DSA, in the country in which it is registered, to be under the ownership, control or influence of a third country whose aims are not compatible with those of the host Party is not eligible for a security assurance and the requesting NSA/DSA will be notified.

9.4 If either NSA/DSA learns of any derogatory information about an individual for whom a PSC assurance has been issued, it will notify the other NSA/DSA of the nature of the information and the action it intends to take, or has taken. Either NSA/DSA may request a review of any PSC assurance which has been furnished earlier by the other NSA/DSA, provided that the request is accompanied by a reason. The requesting NSA/DSA will be notified of the results of the review and any subsequent action.

9.5 If information becomes available which raises doubts about the suitability of a reciprocally cleared company to continue to have access to Classified Information in the other country then details of this information will be promptly notified to the NSA/DSA to allow an investigation to be carried out.

9.6 If either NSA/DSA suspends or takes action to revoke a reciprocal PSC assurance or suspends or takes action to revoke access which is granted to a national of the other country based upon a security clearance, the other Party will be notified and given the reasons for such an action.

9.7 Each NSA/DSA may request the other to review any FSC assurance, provided that their request is accompanied by the reasons for seeking the review. Following the review, the requesting NSA/DSA will be notified of the results and will be provided with facts supporting any decisions taken.

9.8 If required by the other Party each NSA/DSA will co-operate in reviews and investigations concerning security clearances.

10. LOSS OR COMPROMISE

10.1 In the event of a security infringement involving the loss of Classified Information or Classified Material or suspicion that such information or material has been disclosed to unauthorised persons, the NSA/DSA of the Recipient Party will immediately inform the NSA/DSA of the Originating Party.

10.2 An immediate investigation will be carried out by the Recipient Party (with assistance from the Originating Party if required) in accordance with the regulations in force in

that country for the protection of Classified Information and Classified Material. The Recipient Party will inform the Originating Party about the circumstances, measures adopted and outcome of the investigation as soon as is practicable.

11. COSTS

Any costs incurred in the application of the security provisions of this GSA will be borne by the Party providing the services.

12. AMENDMENT

The provisions of this GSA may be amended with the mutual consent in writing of both Parties.

13. SETTLEMENT OF DISPUTES

Any dispute regarding the interpretation or application of this GSA will be resolved by consultation between the Parties and will not be referred to any national or international tribunal or third party for settlement.

14. ENTRY INTO FORCE, TERMINATION AND REVIEW

14.1 This GSA will enter into effect on the date of the last signature and will continue in effect unless terminated either by mutual consent or by either Party giving six months' notice in writing to the other. In the event of termination each Party will be responsible that any Classified Information or Classified Material already provided and any Classified Information arising under this Arrangement shall be handled in accordance with the provisions of this Arrangement for as long as necessary for the protection of the Classified Information.

14.2 This GSA will be reviewed jointly by the Parties no later than ten years after its effective date.

14.3 The foregoing represents the understandings reached between the Federal Ministry of Defence, Civil Protection and Sport of the Swiss Confederation and the Ministry of Defence of the Kingdom of Denmark upon the matters referred to therein.

Signed in duplicate in the English language.

FOR THE FEDERAL DEPARTMENT OF DEFENCE, CIVIL PROTECTION AND SPORT	FOR THE MINISTRY OF DEFENCE OF THE KINGDOM OF DENMARK
URS FREIBURGHAUS	THOMAS AHRENKIEL
HEAD OF DIRECTORATE FOR INFORMATION SECURITY AND FACILITY PROTECTION	DIRECTOR DANISH DEFENCE INTELLIGENCE SERVICE
Signed	Signed
Date 27. April 2012	Date 31 May 2012
Place Bern	Place Copenhagen