

No. 49264*

**Switzerland
and
Czech Republic**

Agreement between the Swiss Federal Council and the Government of the Czech Republic on the exchange and mutual protection of classified information. Prague, 26 January 2011

Entry into force: *1 September 2011 by notification, in accordance with article 16*

Authentic texts: *Czech, English and German*

Registration with the Secretariat of the United Nations: *Switzerland, 6 January 2012*

**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
République tchèque**

Accord entre le Conseil fédéral suisse et le Gouvernement de la République tchèque sur l'échange et la protection réciproque des informations classifiées. Prague, 26 janvier 2011

Entrée en vigueur : *1er septembre 2011 par notification, conformément à l'article 16*

Textes authentiques : *tchèque, anglais et allemand*

Enregistrement auprès du Secrétariat des Nations Unies : *Suisse, 6 janvier 2012*

** Numéro de volume RTNU n'a pas encore été établie pour ce dossier. Les textes reproduits 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.*

[CZECH TEXT – TEXTE TCHÈQUE]

SMLOUVA

MEZI

ŠVÝCARSKOU SPOLKOVOU RADOU

A

VLÁDOU ČESKÉ REPUBLIKY

O

VÝMĚNĚ A VZÁJEMNÉ OCHRANĚ

UTAJOVANÝCH INFORMACÍ

Švýcarská spolková rada a Vláda České republiky (dále jen „smluvní strany“), přejíce si zajistit ochranu utajovaných informací vyměněných mezi nimi nebo mezi právníckými a fyzickými osobami pod jurisdikcí jejich států, se při vzájemném respektování svých státních zájmů a bezpečnosti dohodly takto:

ČLÁNEK 1 ROZSAH PŮSOBNOSTI

1. Účelem této Smlouvy je zajistit ochranu utajovaných informací vyměněných mezi smluvními stranami nebo mezi právníckými a fyzickými osobami pod jurisdikcí jejich států, předaných v rámci provádění a přípravy utajovaných smluv nebo vytvořených v rámci aplikace této Smlouvy.
2. Výměna utajovaných informací mezi orgány činnými v trestním řízení smluvních stran nespadá do působnosti této Smlouvy, ale bude upravena zvláštní smlouvou.

ČLÁNEK 2 VYMEZENÍ POJMŮ

Pro účely této Smlouvy jsou vymezeny následující pojmy:

- 1) „**utajovanou informací**“ se rozumí jakákoliv informace, dokument nebo materiál, předaný nebo vytvořený smluvními stranami nebo právníckými a fyzickými osobami pod jurisdikcí jejich států, který, bez ohledu na svoji formu, podle vnitrostátních právních předpisů státu některé ze smluvních stran vyžaduje ochranu proti jakékoliv formě vyzrazení, zneužití, zničení, ztráty, zveřejnění nebo zpřístupnění neoprávněné osobě, a byl jako takový určen a náležitě označen;
- 2) „**utajovanou smlouvou**“ se rozumí smlouva nebo subdodavatelská smlouva, která obsahuje utajovanou informaci nebo v souvislosti s níž může k přístupu k utajované informaci dojít;
- 3) „**kontrahentem**“ se rozumí fyzická nebo právnícká osoba způsobilá k uzavření utajované smlouvy;
- 4) „**poskytující stranou**“ se rozumí smluvní strana včetně právníckých a fyzických osob pod jurisdikcí jejího státu, která poskytne utajovanou informaci;
- 5) „**přijímající stranou**“ se rozumí smluvní strana včetně právníckých a fyzických osob pod jurisdikcí jejího státu, která přijme utajovanou informaci;

6) „**třetí stranou**“ se rozumí stát včetně právnických a fyzických osob pod jeho jurisdikcí nebo mezinárodní organizace, které nejsou smluvní stranou této Smlouvy;

7) „**bezpečnostním osvědčením**“ se rozumí pozitivní rozhodnutí vycházející z bezpečnostního řízení, které potvrdí loajalitu a důvěryhodnost stejně jako další bezpečnostní aspekty fyzické nebo právníké osoby v souladu s vnitrostátními právními předpisy.

ČLÁNEK 3 NÁRODNÍ BEZPEČNOSTNÍ ÚŘADY

1. Národními bezpečnostními úřady odpovědnými za ochranu utajovaných informací a aplikaci této Smlouvy jsou:

Ve Švýcarské konfederaci:

EIDGENÖSSISCHES DEPARTEMENT FÜR VERTEIDIGUNG,
BEVÖLKERUNGSSCHUTZ UND SPORT,
INFORMATIONEN- UND OBJEKTSICHERHEIT
(Federaální ministerstvo pro obranu, civilní ochranu a sport,
informační bezpečnost a ochranu objektů)

V České republice:

NÁRODNÍ BEZPEČNOSTNÍ ÚŘAD

2. Národní bezpečnostní úřady si sdělí oficiální kontaktní údaje.

3. Národní bezpečnostní úřady se informují o určených bezpečnostních úřadech, které jsou rovněž odpovědné za aplikaci této Smlouvy.

ČLÁNEK 4 STUPNĚ UTAJENÍ

Rovnocennost označení národních stupňů utajení je následující:

Ve Švýcarské konfederaci	V České republice	Ekvivalent v anglickém jazyce
<i>bez ekvivalentu</i>	PŘÍSNĚ TAJNÉ	TOP SECRET
GEHEIM / SECRET / SEGRETO	TAJNÉ	SECRET
VERTRAULICH / CONFIDENTIEL / CONFIDENZIALE	DŮVĚRNÉ	CONFIDENTIAL
INTERN / INTERNE / AD USO INTERNO	VYHRAZENÉ	RESTRICTED

ČLÁNEK 5 PŘÍSTUP K UTAJOVANÝM INFORMACÍM

Přístup k utajovaným informacím poskytnutým podle této Smlouvy lze umožnit pouze osobám k tomu oprávněným v souladu s vnitrostátními právními předpisy státu příslušné smluvní strany.

ČLÁNEK 6 OMEZENÍ POUŽITÍ UTAJOVANÝCH INFORMACÍ

1. Přijímající strana neposkytne utajovanou informaci třetí straně bez předchozího písemného souhlasu poskytlující strany.
2. Přijímající strana použije utajovanou informaci pouze v souladu s účelem, za kterým byla poskytnuta, a s požadavky na nakládání s ní stanovenými poskytlující stranou.

ČLÁNEK 7 NAKLÁDÁNÍ S UTAJOVANÝMI INFORMACEMI

1. Poskytlující strana:
 - a) zajistí, že poskytnutá utajovaná informace je označena příslušným stupněm utajení a doplňujícím označením v souladu s vnitrostátními právními předpisy;
 - b) informuje přijímající stranu o všech podmínkách poskytnutí utajované informace;
 - c) informuje přijímající stranu o všech následných změnách nebo zrušení stupně utajení.

2. Přijímající strana:
 - a) zajistí označení utajované informace rovnocenným stupněm utajení v souladu s článkem 4 této Smlouvy. Utajované informace České republiky označené PŘÍSNĚ TAJNÉ budou ve Švýcarské konfederaci označeny GEHEIM / SECRET / SEGRETO;
 - b) zajistí utajované informaci stejnou úroveň ochrany jako poskytuje národním utajovaným informacím rovnocenného stupně utajení. Utajované informace České republiky označené PŘÍSNĚ TAJNÉ budou ve Švýcarské konfederaci chráněny jako utajované informace označené GEHEIM / SECRET / SEGRETO;
 - c) zajistí, že stupeň utajení utajované informace nebude bez písemného souhlasu poskytovající strany změněn nebo zrušen.
3. Smluvní strany zajistí, že budou v souladu s vnitrostátními právními předpisy uplatněna veškerá bezpečnostní opatření k zajištění ochrany utajovaných informací.

ČLÁNEK 8 BEZPEČNOSTNÍ SPOLUPRÁCE

1. Za účelem udržení srovnatelných bezpečnostních standardů si národní bezpečnostní úřady na vyžádání sdělují informace o vnitrostátních právních předpisech upravujících ochranu utajovaných informací a o uplatňovaných postupech a zkušenostech získaných při jejich provádění.
2. Národní bezpečnostní úřady si na vyžádání a v souladu s vnitrostátními právními předpisy poskytnou součinnost při provádění bezpečnostních řízení o vydání bezpečnostního osvědčení fyzické osoby a bezpečnostního osvědčení podnikatele.
3. Smluvní strany si v souladu s vnitrostátními právními předpisy uznají bezpečnostní osvědčení fyzických osob a bezpečnostní osvědčení podnikatelů. Článek 4 této Smlouvy se použije obdobně. Na žádost příslušného národního bezpečnostního úřadu může být švýcarské bezpečnostní osvědčení umožňující přístup k utajovaným informacím označeným GEHEIM / SECRET / SEGRETO uznáno tak, aby umožňovalo přístup také k českým utajovaným informacím označeným PŘÍSNĚ TAJNÉ. České bezpečnostní osvědčení umožňující přístup k utajovaným informacím označeným PŘÍSNĚ TAJNÉ a TAJNÉ bude uznáno jako umožňující přístup ke švýcarským utajovaným informacím označeným GEHEIM / SECRET / SEGRETO.
4. Národní bezpečnostní úřady si bezodkladně oznámí změny týkající se uznaných bezpečnostních osvědčení fyzických osob a bezpečnostních

osvědčení podnikatelů, zejména v případech jejich zrušení nebo uplynutí doby platnosti.

ČLÁNEK 9 UTAJOVANÉ SMLOUVY

1. Národní bezpečnostní úřady si na vyžádání potvrdí, že navrhovaní kontrahenti utajované smlouvy nebo fyzické osoby účastníci se sjednávání nebo provádění utajované smlouvy jsou držiteli příslušného bezpečnostního osvědčení.
2. Národní bezpečnostní úřady mohou požadovat provedení bezpečnostní inspekce subjektu s cílem zajistit, že vnitrostátní právní předpisy upravující ochranu utajovaných informací jsou nadále dodržovány.
3. Utajované smlouvy obsahují bezpečnostní pokyny, které určují bezpečnostní požadavky a stupně utajení jednotlivých fází a částí utajované smlouvy. Kopie bezpečnostních pokynů se zasilá národnímu bezpečnostnímu úřadu státu smluvní strany, pod jehož jurisdikcí bude utajovaná smlouva prováděna.

ČLÁNEK 10 PŘEDÁVÁNÍ UTAJOVANÝCH INFORMACÍ

1. Utajované informace se předávají diplomatickou nebo vojenskou cestou, nebo jiným způsobem, na kterém se národní bezpečnostní úřady dohodnou.
2. Smluvní strany si mohou utajované informace předávat elektronicky v souladu s bezpečnostními postupy schválenými národními bezpečnostními úřady.

ČLÁNEK 11 REPRODUKCE, PŘEKLAD A ZNIČENÍ UTAJOVANÝCH INFORMACÍ

1. Veškeré reprodukce a překlady utajované informace musí být označeny příslušným stupněm utajení a doplňujícím označením a musí jim být poskytnuta stejná ochrana jako původní utajované informaci. Počet vyhotovených překladů a požadovaných reprodukcí se omezí na nezbytné minimum.
2. Veškeré překlady musí být opatřeny poznámkou v jazyce překladu, ze které je zřejmé, že obsahují utajovanou informaci poskytující strany.
3. Překlad nebo reprodukci utajované informace stupně utajení **TAJNÉ** nebo vyššího lze vyhotovit pouze s předchozím písemným souhlasem poskytující strany.

4. Utajovaná informace stupně utajení **TAJNÉ** nebo vyššího nesmí být v případě, kdy již není dále využitelná, zničena a musí být v souladu s vnitrostátními právními předpisy vrácena poskytující straně.
5. Utajované informace stupně utajení **DŮVĚRNÉ** nebo nižšího musí být zničeny v souladu s vnitrostátními právními předpisy státu přijímající strany způsobem, který vylučuje jejich částečné nebo úplné obnovení.

ČLÁNEK 12 NÁVŠTĚVY

1. Návštěvy vyžadující přístup k utajovaným informacím nebo do prostor, kde jsou utajované informace vytvářeny, ukládány, přenášeny nebo kde je s nimi nakládáno, podléhají předchozímu písemnému povolení příslušného národního bezpečnostního úřadu, pokud se národní bezpečnostní úřady nedohodnou jinak.
2. Žádost o povolení návštěvy se podává prostřednictvím národních bezpečnostních úřadů alespoň dvacet dnů před jejím zahájením. V naléhavých případech může být žádost o povolení návštěvy podána na základě předchozí součinnosti národních bezpečnostních úřadů ve lhůtě kratší.
3. Žádost o povolení návštěvy obsahuje:
 - a) jméno a příjmení, datum a místo narození, státní občanství, číslo cestovního pasu nebo průkazu totožnosti každého návštěvníka;
 - b) pracovní zařazení návštěvníka a určení subjektu, který zastupuje;
 - c) stupeň utajení, pro který bylo návštěvníkovi bezpečnostní osvědčení fyzické osoby vydáno, včetně doby jeho platnosti;
 - d) datum a délku návštěvy; v případě opakovaných návštěv se uvede jejich celková délka;
 - e) účel návštěvy včetně nejvyššího stupně utajení informací, ke kterým bude přístup vyžadován;
 - f) název, adresu, telefonní/faxové číslo, e-mailovou adresu a jméno a příjmení, pracovní zařazení a/nebo funkci hostitele nebo kontaktní osoby subjektu, který bude navštíven;
 - g) datum, podpis a otisk úředního razítka příslušného národního bezpečnostního úřadu;
 - h) jméno a příjmení, pracovní zařazení a/nebo funkci hostitele.
4. Národní bezpečnostní úřady se mohou dohodnout na seznamu osob, jimž jsou povoleny opakované návštěvy. Na podrobnostech opakovaných návštěv se národní bezpečnostní úřady dohodnou.
5. Utajovaná informace zpřístupněná návštěvníkovi se považuje za utajovanou informaci poskytnutou podle této Smlouvy.

ČLÁNEK 13 BEZPEČNOSTNÍ INCIDENTY

1. Smluvní strany se bezodkladně písemně informují o jakémkoli bezpečnostním incidentu, při kterém došlo například ke ztrátě, zneužití nebo vyzrazení utajované informace, nebo o podezření, že k takovému incidentu došlo.
2. Smluvní strana, v jejíž jurisdikci k incidentu došlo, zahájí bezodkladně vyšetřování. Druhá smluvní strana se zúčastní vyšetřování, pokud je to vyžadováno.
3. Smluvní strana, v jejíž jurisdikci k incidentu došlo, v každém případě písemně informuje druhou smluvní stranu o okolnostech bezpečnostního incidentu, způsobené škodě, opatřeních přijatých pro její zmírnění a o výsledku vyšetřování.

ČLÁNEK 14 NÁKLADY

Náklady vzniklé v souvislosti s aplikací této Smlouvy si smluvní strany hradí samy.

ČLÁNEK 15 VÝKLAD A ŘEŠENÍ SPORŮ

Jakýkoliv spor týkající se výkladu nebo aplikace této Smlouvy bude řešen jednáním mezi smluvními stranami a nebude předán k urovnání žádnému vnitrostátnímu nebo mezinárodnímu soudu nebo třetí straně.

ČLÁNEK 16 ZÁVĚREČNÁ USTANOVENÍ

1. Tato Smlouva se sjednává na dobu neurčitou. Tato Smlouva vstoupí v platnost první den druhého měsíce následujícího po doručení pozdějšího oznámení mezi smluvními stranami diplomatickou cestou, informujícího o tom, že byly splněny všechny vnitrostátní podmínky pro vstup této Smlouvy v platnost.
2. Tuto Smlouvu lze změnit na základě souhlasu smluvních stran. Změny vstoupí v platnost v souladu s ustanovením odstavce 1 tohoto článku.

3. Každá ze smluvních stran má právo tuto Smlouvu kdykoliv písemně vypovědět. V takovém případě je platnost Smlouvy ukončena šest měsíců po dni, kdy bylo písemné oznámení o vypovědi doručeno druhé smluvní straně.
4. Veškerým utajovaným informacím poskytnutým nebo vytvořeným podle této Smlouvy bude zajištěna ochrana podle této Smlouvy i po ukončení její platnosti do doby, než poskytující strana zprostí přijímající stranu této povinnosti.

Na důkaz toho níže uvedení zástupci, řádně zmocnění k tomuto účelu, podepsali tuto Smlouvu.

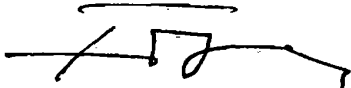
Dáno v Praze dne 26. ledna 2011 ve dvou původních vyhotoveních, každé v německém, českém a anglickém jazyce, přičemž všechna znění jsou stejně autentická. V případě rozdílnosti ve výkladu je rozhodující znění v jazyce anglickém.

Za Švýcarskou konfederaci

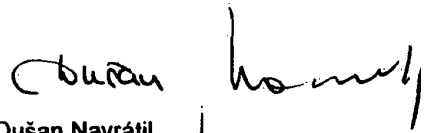
Za vládu České republiky

ředitel Ředitelství
pro bezpečnost informací
a ochranu objektů

Ředitel Národního bezpečnostního
úřadu



Urs FREIBURGH AUS



Dušan Navrátil

[ENGLISH TEXT – TEXTE ANGLAIS]

AGREEMENT
BETWEEN
THE SWISS FEDERAL COUNCIL
AND
THE GOVERNMENT OF THE CZECH REPUBLIC
ON THE EXCHANGE
AND MUTUAL PROTECTION
OF CLASSIFIED INFORMATION

The Swiss Federal Council and the Government of the Czech Republic, hereinafter referred to as "the Parties", wishing to ensure the protection of Classified Information exchanged between them or between legal entities or individuals under the jurisdiction of their states have, in mutual respect for national interests and security agreed upon the following:

ARTICLE 1 SCOPE OF APPLICATION

1. The purpose of this Agreement is to protect Classified Information exchanged between the Parties or between legal entities or individuals under the jurisdiction of their states, transmitted within the context of the implementation as well as the preparation of Classified Contracts or generated within the scope of application of this Agreement.
2. The Exchange of Classified Information between the law enforcement bodies of the Parties shall not fall under this Agreement, but is governed by a separate agreement.

ARTICLE 2 DEFINITIONS

For the purpose of this Agreement:

- 1) "**Classified Information**" means any information, document or material transmitted or generated between the Parties or between legal entities or individuals under the jurisdiction of their states that, regardless of its form, under the national laws and regulations of the state of either Party, requires protection against any form of unauthorised disclosure, misappropriation, destruction, loss, publication or access to unauthorized persons and has been designated as such and appropriately marked.
- 2) "**Classified Contract**" means a contract or a subcontract that contains or involves access to Classified Information.
- 3) "**Contractor**" means an individual or legal entity, possessing the capability to conclude Classified Contracts.
- 4) "**Originating Party**" means the Party including legal entities or individuals under the jurisdiction of its state, which releases Classified Information.
- 5) "**Recipient Party**" means the Party including legal entities or individuals under the jurisdiction of its state, which receives Classified Information.

6) **“Third Party”** means any state including legal entities or individuals under its jurisdiction or international organisation that is not a party to this Agreement.

7) **“Security Clearance”** means the positive determination stemming from a vetting procedure that shall ascertain loyalty and trustworthiness as well as other security aspects of an individual or legal entity in accordance with national laws and regulations.

ARTICLE 3 NATIONAL SECURITY AUTHORITIES

1. The National Security Authorities responsible for the protection of Classified Information as well as the application of this Agreement are:

In the Swiss Confederation:

EIDGENÖSSISCHES DEPARTEMENT FÜR VERTEIDIGUNG,
BEVÖLKERUNGSSCHUTZ UND SPORT
INFORMATIONEN- UND OBJEKTSICHERHEIT
(Federal Department of Defence, Civil Protection and Sport,
Directorate for Information Security and Facility Protection)

In the Czech Republic:

NÁRODNÍ BEZPEČNOSTNÍ ÚŘAD
(National Security Authority)

2. The National Security Authorities shall provide each other with official contact details.
3. The National Security Authorities shall notify each other of designated security authorities that are also responsible for the application of this Agreement.

**ARTICLE 4
SECURITY CLASSIFICATION LEVELS**

The equivalence of national security classification level markings is as follows:

In the Swiss Confederation	In the Czech Republic	Equivalent in English language
<i>no equivalent</i>	PŘÍSNĚ TAJNÉ	TOP SECRET
GEHEIM / SECRET / SEGRETO	TAJNÉ	SECRET
VERTRAULICH / CONFIDENTIEL / CONFIDENZIALE	DŮVĚRNÉ	CONFIDENTIAL
INTERN / INTERNE / AD USO INTERNO	VYHRAZENÉ	RESTRICTED

**ARTICLE 5
ACCESS TO CLASSIFIED INFORMATION**

Access to Classified Information released under this Agreement shall be limited only to individuals duly authorised in accordance with the national laws and regulations of the state of the respective Party.

**ARTICLE 6
RESTRICTIONS ON USE OF CLASSIFIED INFORMATION**

1. The Recipient Party shall not release Classified Information to a Third Party without the prior written consent of the Originating Party.
2. The Recipient Party shall use Classified Information only for the purpose it has been released for and in accordance with handling requirements of the Originating Party.

**ARTICLE 7
HANDLING OF CLASSIFIED INFORMATION**

1. The Originating Party shall:
 - a) ensure that Classified Information is marked with appropriate security classification markings in accordance with the national laws and regulations;
 - b) inform the Recipient Party of any conditions of release;
 - c) inform the Recipient Party of any subsequent changes in classifications or declassification.

2. The Recipient Party shall:
 - a) ensure that Classified Information is marked with equivalent security classification level markings in accordance with Article 4 of this Agreement. Czech Classified Information marked PŘÍSNĚ TAJNÉ shall be marked GEHEIM / SECRET / SEGRETO in the Swiss Confederation;
 - b) afford the same degree of protection to Classified Information as afforded to its national Classified Information of equivalent security classification level. Czech Classified Information marked PŘÍSNĚ TAJNÉ shall be protected as Classified Information marked GEHEIM / SECRET / SEGRETO in the Swiss Confederation;
 - c) ensure that Classified Information is not declassified nor its classification changed, except if authorised in writing by the Originating Party.

3. Parties shall ensure that all security measures shall be applied in accordance with national laws and regulations to provide appropriate protection of Classified Information.

**ARTICLE 8
SECURITY CO-OPERATION**

1. In order to maintain comparable standards of security, the National Security Authorities shall, on request, inform each other of national security standards, procedures and practices for the protection of Classified Information.

2. On request, the National Security Authorities shall, within the scope of the national laws and regulations, assist each other during the personnel and facility Security Clearance procedures.

3. The Parties shall recognise their Personnel and Facility Security Clearances in accordance with the national laws and regulations. Article 4 of this Agreement shall apply accordingly. On request of the respective National Security Authority, a Swiss Security Clearance granting access to Classified Information marked GEHEIM /

SECRET / SEGRETO may be recognised to grant access also to Czech Classified Information marked PŘÍSNĚ TAJNĚ. A Czech Security Clearance granting access to Classified Information marked PŘÍSNĚ TAJNĚ as well as TAJNĚ shall be recognised as granting access to Swiss Classified Information marked GEHEIM / SECRET / SEGRETO.

4. The National Security Authorities shall promptly notify each other about changes in recognised Personnel and Facility Security Clearances especially in cases of their revocation or termination.

ARTICLE 9 CLASSIFIED CONTRACTS

1. On request, the National Security Authorities shall confirm that the proposed Contractors of the Classified Contract as well as individuals participating in pre-contractual negotiations or in the implementation of Classified Contracts have appropriate Security Clearances.
2. The National Security Authorities may request that a security inspection is carried out at a facility to ensure continuing compliance with security standards according to the national laws and regulations.
3. Classified Contracts shall contain programme security instructions on the security requirements and on the classification of each aspect or element of the Classified Contract. A copy of the programme security instructions shall be forwarded to the National Security Authority of the state of the Party under whose jurisdiction the Classified Contract is to be implemented.

ARTICLE 10 TRANSMISSION OF CLASSIFIED INFORMATION

1. Classified Information shall be transmitted through diplomatic or military channels or as otherwise agreed between the National Security Authorities.
2. The Parties may transmit Classified Information by electronic means in accordance with security procedures approved by the National Security Authorities.

ARTICLE 11 REPRODUCTION, TRANSLATION AND DESTRUCTION OF CLASSIFIED INFORMATION

1. All reproductions and translations of Classified Information shall bear appropriate security classification markings and shall be protected as the original Classified

Information. The translations and number of reproductions shall be limited to the minimum needed.

2. All translations shall contain a note in the language of translation indicating that they contain Classified Information of the Originating Party.
3. Classified Information of security classification level SECRET or above shall be translated or reproduced only upon the prior written consent of the Originating Party.
4. Classified Information of security classification level SECRET or above shall not be destroyed but shall be returned to the Originating Party in accordance with the national laws and regulations after it is no longer considered necessary.
5. Classified Information of security classification level CONFIDENTIAL or below shall be destroyed in accordance with the national laws and regulations of the state of the Recipient Party in a way preventing its full as well as partial reconstruction.

ARTICLE 12 VISITS

1. Visits requiring access to Classified Information or to premises where Classified Information is being originated, handled, stored or transmitted are subject to the prior written consent of the respective National Security Authority, unless otherwise agreed between the National Security Authorities.
2. The request for visit shall be submitted through the National Security Authorities at least twenty days before the visit. In urgent cases, the request for visit may be submitted at a shorter notice, subject to prior co-ordination between the National Security Authorities.
3. The request for visit shall include:
 - a) first and last name, date and place of birth, nationality and passport/ID card number of every visitor;
 - b) position of the visitor and specification of the facility, which the visitor represents;
 - c) visitor's level of the personnel security clearance and its validity;
 - d) date and duration of the visit; in case of recurring visits the total period of time covered by the visits shall be stated;
 - e) purpose of the visit including the highest level of Classified Information to be involved;
 - f) name, address, phone/fax number, e-mail address and including first and last name, official position and/or function of the host/point of contact;
 - g) date, signature and stamping of the official seal of the respective National Security Authority;
 - h) first and last name, official position and/or function of the host.

4. The National Security Authorities may agree on a list of visitors entitled to recurring visits. Further details of the recurring visits are subject to the co-ordination between the National Security Authorities.
5. Classified Information acquired by a visitor shall be considered as Classified Information released under this Agreement.

**ARTICLE 13
BREACHES OF SECURITY**

1. The Parties shall immediately inform each other in writing of any breach of security resulting in e.g. loss, misappropriation or unauthorised disclosure of Classified Information or suspicion of such a breach.
2. The Party under whose jurisdiction the breach of security occurred shall investigate the incident without delay. The other Party shall, if required, co-operate in the investigation.
3. In any case, the Party under whose jurisdiction the breach of security occurred shall inform the other Party in writing about the circumstances of the breach of security, the extent of the damage, the measures adopted for its mitigation and the outcome of the investigation.

**ARTICLE 14
EXPENSES**

The Parties shall bear their own expenses incurred in the course of the application of this Agreement.

**ARTICLE 15
INTERPRETATION AND DISPUTES**

Any dispute regarding the interpretation or application of this Agreement shall be settled by negotiation between the Parties and shall not be referred to any national or international tribunal or Third Party for settlement.

**ARTICLE 16
FINAL PROVISIONS**

1. This Agreement is concluded for an indefinite period of time. It shall enter into force on the first day of the second month following the date of receipt of the last of

notifications between the Parties, through diplomatic channels, that the internal legal procedures for this Agreement to enter into force have been fulfilled.

2. This Agreement may be amended on the basis of mutual consent of the Parties. Such amendments shall enter into force in accordance with paragraph 1 of this Article.
3. Each of the Parties is entitled to terminate this Agreement in writing at any time. In such a case, the validity of this Agreement shall expire after six months following the day on which the other Party receives the written notice of the termination.
4. Regardless of the termination of this Agreement, all Classified Information released or generated under this Agreement shall be protected in accordance with the provisions set forth herein until the Originating Party dispenses the Recipient Party from this obligation.

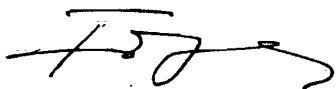
In witness of which, the undersigned, duly authorised to this effect, have signed this Agreement.

Done in Prague on January 26, 2011 in two originals, in the German, Czech, and English languages, each text being equally authentic. In case of different interpretations the English text shall prevail.

For the Swiss Federal Council

For the Government of the Czech Republic

Director for Information Security
and Facility Protection



Urs FREIBURGHaus

Director of the National Security Authority



Dušan NAVRÁTIL

[GERMAN TEXT – TEXTE ALLEMAND]

ABKOMMEN

ZWISCHEN

DEM SCHWEIZERISCHEN BUNDESRAT

UND

DER REGIERUNG DER TSCHECHISCHEN REPUBLIK

ÜBER DEN AUSTAUSCH

UND DEN GEGENSEITIGEN SCHUTZ

VON KLASSIFIZIERTEN INFORMATIONEN

Der Schweizerische Bundesrat und die Regierung der Tschechischen Republik, nachstehend "die Vertragsparteien" genannt, vom Wunsch geleitet, den Schutz von klassifizierten Informationen zu gewährleisten, die zwischen ihnen oder zwischen juristischen oder natürlichen Personen gemäss ihren rechtlichen Bestimmungen ausgetauscht werden, sind in gegenseitiger Achtung der nationalen Interessen und der nationalen Sicherheit wie folgt übereingekommen:

ARTIKEL 1 GELTUNGSBEREICH

1. Das vorliegende Abkommen hat den Zweck, klassifizierte Informationen zu schützen, die zwischen den Vertragsparteien oder zwischen juristischen oder natürlichen Personen gemäss ihren rechtlichen Bestimmungen ausgetauscht werden, im Zusammenhang mit der Implementierung und der Vorbereitung von klassifizierten Verträgen übermittelt werden oder innerhalb des Geltungsbereichs des vorliegenden Abkommens ausgearbeitet werden.
2. Der Austausch von klassifizierten Informationen zwischen den Strafverfolgungsbehörden der Vertragsparteien fällt nicht unter den Geltungsbereich des vorliegenden Abkommens, sondern wird in einem separaten Abkommen geregelt.

ARTIKEL 2 DEFINITIONEN

Im vorliegenden Abkommen werden folgende Begriffe verwendet:

- 1) **"Klassifizierte Informationen"** umfasst alle zwischen den Vertragsparteien oder zwischen juristischen oder natürlichen Personen gemäss ihren rechtlichen Bestimmungen übermittelten oder erarbeiteten Informationen, Unterlagen und Materialien, die ungeachtet ihrer Form gemäss den innerstaatlichen Gesetzen und sonstigen Vorschriften einer der Vertragsparteien Schutz vor irgendeiner Form von unbefugter Weitergabe, widerrechtlicher Aneignung, Zerstörung, Verlust, Veröffentlichung oder Zugang von nicht autorisierten Personen benötigen und als solche bezeichnet und angemessen gekennzeichnet wurden.
- 2) **"Klassifizierter Vertrag"** bezeichnet einen Vertrag oder Untervertrag, der klassifizierte Informationen enthält oder sich auf den Zugang zu klassifizierten Informationen bezieht.
- 3) **"Auftragnehmer"** bezeichnet eine natürliche oder juristische Person, die klassifizierte Verträge abschliessen kann.

- 4) **“bereitstellende Partei”** bezeichnet die Vertragspartei, einschliesslich juristischer oder natürlicher Personen gemäss ihren rechtlichen Bestimmungen, die klassifizierte Informationen freigibt.
- 5) **“empfangende Partei”** bezeichnet die Vertragspartei, einschliesslich juristischer oder natürlicher Personen gemäss ihren rechtlichen Bestimmungen, die klassifizierte Informationen entgegennimmt.
- 6) **“Dritte”** bezeichnet irgendeinen Staat, einschliesslich juristischer oder natürlicher Personen gemäss seinen rechtlichen Bestimmungen, oder eine internationale Organisation, der/die nicht Vertragspartei des vorliegenden Abkommens ist.
- 7) **“Sicherheitsbescheinigung”** bezeichnet den positiven Entscheid, der aus einem Prüfverfahren resultiert, und der die Loyalität und Vertrauenswürdigkeit sowie andere Sicherheitsaspekte hinsichtlich einer natürlichen oder juristischen Person in Übereinstimmung mit nationalem Recht und sonstigen Vorschriften bestätigt.

ARTIKEL 3 NATIONALE SICHERHEITSBEHÖRDEN

1. Für den Schutz von klassifizierten Informationen und die Umsetzung des vorliegenden Abkommens sind die folgenden Nationalen Sicherheitsbehörden zuständig:

In der Schweizerischen Eidgenossenschaft:

**EIDGENÖSSISCHES DEPARTEMENT FÜR VERTEIDIGUNG,
BEVÖLKERUNGSSCHUTZ UND SPORT
INFORMATIONEN- UND OBJEKTSICHERHEIT**

In der Tschechischen Republik:

**NÁRODNÍ BEZPEČNOSTNÍ ÚŘAD
(Nationale Sicherheitsbehörde)**

2. Die Nationalen Sicherheitsbehörden lassen sich gegenseitig die offiziellen Kontaktdaten zukommen.
3. Die Nationalen Sicherheitsbehörden teilen sich gegenseitig mit, welche Sicherheitsbehörde für die Anwendung des vorliegenden Abkommens zuständig ist.

ARTIKEL 4 Klassifizierungsstufen

Es bestehen die folgenden nationalen Klassifizierungsstufen:

In der Schweizerischen Eidgenossenschaft	In der Tschechischen Republik	Entsprechender Begriff auf Englisch
<i>Kein entsprechender Begriff</i>	PŘÍSNĚ TAJNÉ	<i>TOP SECRET</i>
GEHEIM / SECRET / SEGRETO	TAJNÉ	<i>SECRET</i>
VERTRAULICH / CONFIDENTIEL / CONFIDENZIALE	DŮVĚRNÉ	<i>CONFIDENTIAL</i>
INTERN / INTERNE / AD USO INTERNO	VYHRAZENÉ	<i>RESTRICTED</i>

ARTIKEL 5 ZUGANG ZU KLASSIFIZIERTEN INFORMATIONEN

Der Zugang zu klassifizierten Informationen, die gemäss dem vorliegenden Abkommen freigegeben werden, ist ausschliesslich auf Personen beschränkt, die entsprechend den innerstaatlichen Gesetzen und sonstigen Vorschriften der betreffenden Vertragspartei ordnungsgemäss ermächtigt sind.

ARTIKEL 6 EINSCHRÄNKUNGEN BEZÜGLICH DER VERWENDUNG VON KLASSIFIZIERTEN INFORMATIONEN

1. Die empfangende Partei gibt klassifizierte Informationen nicht ohne vorgängige schriftliche Einwilligung der bereitstellenden Partei an Dritte weiter.
2. Die empfangende Partei verwendet klassifizierte Informationen nur für den Zweck, für den sie freigegeben wurden, und beachtet dabei die Benutzungsvorgaben der bereitstellenden Partei.

**ARTIKEL 7
UMGANG MIT KLASSIFIZIERTEN INFORMATIONEN**

1. Die bereitstellende Partei:
 - a) stellt sicher, dass klassifizierte Informationen gemäss den innerstaatlichen Gesetzen und sonstigen Vorschriften mit einer angemessenen Klassifizierungsstufe gekennzeichnet werden;
 - b) setzt die empfangende Partei über alle Bedingungen der Freigabe in Kenntnis;
 - c) setzt die empfangende Partei über alle nachfolgenden Änderungen der Klassifizierungsstufe oder eine Aufhebung der Klassifizierung in Kenntnis.

2. Die empfangende Partei:
 - a) stellt sicher, dass klassifizierte Informationen gemäss Artikel 4 des vorliegenden Abkommens mit einer gleichwertigen Klassifizierungsstufe gekennzeichnet werden; tschechische klassifizierte Informationen, die mit PRÍSNE TAJNÉ gekennzeichnet sind, werden in der Schweizerischen Eidgenossenschaft mit GEHEIM / SECRET / SEGRETO gekennzeichnet;
 - b) stellt für klassifizierte Informationen den gleichen Grad von Schutz sicher, der für ihre innerstaatlichen klassifizierten Informationen der gleichen Klassifizierungsstufe gewährleistet wird; tschechische klassifizierte Informationen, die mit PRÍSNE TAJNÉ gekennzeichnet sind, werden in gleicher Weise geschützt wie klassifizierte Informationen, die in der Schweizerischen Eidgenossenschaft mit GEHEIM / SECRET / SEGRETO gekennzeichnet sind;
 - c) stellt sicher, dass bei klassifizierten Informationen ohne schriftliche Einwilligung der bereitstellenden Partei weder die Klassifizierung aufgehoben noch die Klassifizierungsstufe geändert wird.

3. Beide Vertragsparteien gewährleisten, dass entsprechend den innerstaatlichen Gesetzen und sonstigen Vorschriften alle Sicherheitsmassnahmen angewandt werden, die erforderlich sind, um einen angemessenen Schutz von klassifizierten Informationen sicherzustellen.

**ARTIKEL 8
ZUSAMMENARBEIT IM BEREICH DER SICHERHEIT**

1. Um vergleichbare Sicherheitsstandards aufrechtzuerhalten, setzen sich die Nationalen Sicherheitsbehörden auf Ersuchen gegenseitig über die nationalen Sicherheitsstandards, -verfahren und -praktiken für den Schutz von klassifizierten Informationen in Kenntnis.

2. Auf Ersuchen unterstützen sich die Nationalen Sicherheitsbehörden im Rahmen der innerstaatlichen Gesetze und sonstigen Vorschriften gegenseitig bei den Verfahren für die Ermächtigung zum Zugang zu klassifizierten Informationen in Bezug auf die Sicherheitsbescheinigung von Personen und Einrichtungen.
3. Die Vertragsparteien anerkennen entsprechend den innerstaatlichen Gesetzen und sonstigen Vorschriften ihre Personen- und Firmensicherheitsbescheinigungen zum Zugang zu klassifizierten Informationen. Artikel 4 des vorliegenden Abkommens gelangt dementsprechend zur Anwendung. Auf Ersuchen der betreffenden Nationalen Sicherheitsbehörde kann eine schweizerische Sicherheitsbescheinigung für den Zugang zu klassifizierten Informationen, die mit GEHEIM / SECRET / SEGRETO gekennzeichnet sind, so anerkannt werden, dass auch der Zugang zu tschechischen klassifizierten Informationen gewährt wird, die mit PŘÍSNĚ TAJNÉ gekennzeichnet sind. Eine tschechische Sicherheitsbescheinigung für den Zugang zu klassifizierten Informationen, die mit PŘÍSNĚ TAJNÉ oder TAJNÉ gekennzeichnet sind, wird so anerkannt, dass auch der Zugang zu schweizerischen klassifizierten Informationen gewährt wird, die mit GEHEIM / SECRET / SEGRETO gekennzeichnet sind.
4. Die Nationalen Sicherheitsbehörden setzen sich gegenseitig unverzüglich über Änderungen von anerkannten Personen- und Firmensicherheitsbescheinigungen für den Zugang zu klassifizierten Informationen in Kenntnis. Dies gilt insbesondere bei einer Annullierung oder Beendigung von solchen Ermächtigungen.

ARTIKEL 9 KLASSIFIZIERTE VERTRÄGE

1. Auf Ersuchen bestätigen die Nationalen Sicherheitsbehörden, dass die vorgeschlagenen vertragschliessenden Partner des klassifizierten Vertrags sowie die Personen, die an den vorvertraglichen Verhandlungen oder an der Umsetzung von klassifizierten Verträgen beteiligt sind, über eine angemessene Sicherheitsbescheinigung zum Zugang zu klassifizierten Informationen verfügen.
2. Die Nationalen Sicherheitsbehörden können verlangen, dass in einer Einrichtung eine Sicherheitsüberprüfung durchgeführt wird, um zu gewährleisten, dass die Sicherheitsstandards gemäss den innerstaatlichen Gesetzen und sonstigen Vorschriften weiterhin erfüllt werden.
3. Klassifizierte Verträge enthalten Programmsicherheitsanweisungen zu den Sicherheitsanforderungen und zur Klassifizierung aller Aspekte und Elemente des klassifizierten Vertrags. Ein Exemplar der Programmsicherheitsanweisungen wird der Nationalen Sicherheitsbehörde der empfangenden Partei übergeben, gemäss deren rechtlichen Bestimmungen der klassifizierte Vertrag umzusetzen ist.

**ARTIKEL 10
ÜBERMITTLUNG VON KLASSIFIZIERTEN INFORMATIONEN**

1. Klassifizierte Informationen werden im Rahmen von diplomatischen oder militärischen Kanälen oder gemäss anderen Vereinbarungen zwischen den Nationalen Sicherheitsbehörden übermittelt.
2. Die Vertragsparteien können klassifizierte Informationen gemäss den Sicherheitsverfahren, die von den Nationalen Sicherheitsbehörden genehmigt wurden, mit Hilfe von elektronischen Mitteln übermitteln.

**ARTIKEL 11
VERVIELFÄLTIGUNG, ÜBERSETZUNG UND VERNICHTUNG VON
KLASSIFIZIERTEN INFORMATIONEN**

1. Alle Vervielfältigungen und Übersetzungen von klassifizierten Informationen werden mit einer angemessenen Klassifizierungsstufe gekennzeichnet und gleich wie das Original der klassifizierten Information geschützt. Die Übersetzungen und die Anzahl Vervielfältigungen werden auf das notwendige Minimum beschränkt.
2. Alle Übersetzungen enthalten einen Vermerk in der Sprache der Übersetzung, mit dem darauf hingewiesen wird, dass sie klassifizierte Informationen der bereitstellenden Partei enthalten.
3. Klassifizierte Informationen der Klassifizierungsstufe GEHEIM oder einer höheren Klassifizierungsstufe dürfen nur mit einer vorgängigen schriftlichen Einwilligung der bereitstellenden Partei übersetzt oder vervielfältigt werden.
4. Wenn klassifizierte Informationen der Klassifizierungsstufe GEHEIM oder einer höheren Klassifizierungsstufe nicht mehr benötigt werden, werden sie nicht zerstört, sondern der bereitstellenden Partei gemäss den innerstaatlichen Gesetzen und sonstigen Vorschriften zurückgegeben.
5. Klassifizierte Informationen mit der Klassifizierungsstufe VERTRAULICH oder einer tieferen Klassifizierungsstufe werden gemäss den innerstaatlichen Gesetzen und sonstigen Vorschriften so vernichtet, dass ihre vollständige oder partielle Wiederherstellung unmöglich ist.

**ARTIKEL 12
BESUCHE**

1. Vorbehaltlich anderer Vereinbarungen zwischen den Nationalen Sicherheitsbehörden, bedürfen Besuche, für die der Zugang zu klassifizierten Informationen oder zu Räumlichkeiten erforderlich ist, in denen klassifizierte Informationen hergestellt, bearbeitet, aufbewahrt oder übermittelt werden, einer

- vorgängigen schriftlichen Einwilligung der betreffenden Nationalen Sicherheitsbehörde.
2. Das Gesuch für einen Besuch ist über die Nationalen Sicherheitsbehörden mindestens 20 Tage vor dem Besuch einzureichen. In dringenden Fällen kann, vorbehaltlich einer vorgängigen Koordination zwischen den Nationalen Sicherheitsbehörden, das Gesuch für einen Besuch auch kurzfristiger eingereicht werden.
 3. Das Gesuch für einen Besuch hat die folgenden Elemente zu enthalten:
 - a) Vor- und Nachname, Geburtsdatum, Geburtsort, Staatsangehörigkeit und Nummer des Passes/der Identitätskarte jedes Besuchers;
 - b) Stellung des Besuchers und spezifische Angaben zur Einrichtung, die der Besucher vertritt;
 - c) Grad der Sicherheitsbescheinigung für den Zugang zu klassifizierten Informationen des Besuchers und Gültigkeitsdauer der Sicherheitsbescheinigung;
 - d) Datum und Dauer des Besuchs; bei periodisch wiederkehrenden Besuchen ist die Gesamtdauer der Besuche anzugeben;
 - e) Zweck des Besuchs, einschliesslich der höchsten Klassifizierungsstufe der betreffenden klassifizierten Informationen;
 - f) Name, Adresse, Telefon-/Faxnummer, E-Mail-Adresse und Vor- und Nachname, offizielle Stellung und/oder Funktion des Gastgebers / der Kontaktstelle der für den Besuch vorgesehenen Einrichtung;
 - g) Datum, Unterschrift und offizieller Stempel der betreffenden Nationalen Sicherheitsbehörde;
 - h) Vor- und Nachname, offizielle Stellung und/oder Funktion des Gastgebers.
 4. Die Nationalen Sicherheitsbehörden können sich auf eine Liste von Besuchern einigen, die zu periodisch wiederkehrenden Besuchen berechtigt sind. Weitere Einzelheiten der periodisch wiederkehrenden Besuche unterliegen der Koordination zwischen den Nationalen Sicherheitsbehörden.
 5. Klassifizierte Informationen, in deren Besitz ein Besucher gelangt, gelten im Rahmen des vorliegenden Abkommens als freigegebene klassifizierte Informationen.

ARTIKEL 13 VERSTÖSSE GEGEN DIE SICHERHEITSBESTIMMUNGEN

1. Die Vertragsparteien setzen sich gegenseitig umgehend schriftlich über jeglichen Verstoß gegen die Sicherheitsbestimmungen und über jeden Verdacht bezüglich eines solchen Verstosses in Kenntnis, der mit einem Verlust, einer widerrechtlichen Aneignung oder einer unbefugten Weitergabe von klassifizierten Informationen zusammenhängt.

2. Die Vertragspartei, in deren Rechtsordnung der Verstoss gegen die Sicherheitsbestimmungen erfolgte, untersucht den Vorfall unverzüglich. Die andere Vertragspartei beteiligt sich bei Bedarf an der Untersuchung des Vorfalls.
3. Die Vertragspartei, in deren Rechtsordnung der Verstoss gegen die Sicherheitsbestimmungen erfolgte, setzt die andere Vertragspartei auf jeden Fall schriftlich über die Umstände des Verstosses gegen die Sicherheitsbestimmungen, das Ausmass des Schadens, die für die Reduktion des Schadens getroffenen Massnahmen und das Ergebnis der Untersuchung in Kenntnis.

ARTIKEL 14 KOSTEN

Die Vertragsparteien tragen ihre eigenen Kosten, die sich im Rahmen der Anwendung des vorliegenden Abkommens ergeben.

ARTIKEL 15 AUSLEGUNG UND STREITIGKEITEN

Alle Streitigkeiten im Zusammenhang mit der Auslegung oder Anwendung des vorliegenden Abkommens werden durch Verhandlungen zwischen den Vertragsparteien beigelegt und nicht einem nationalen oder internationalen Gericht oder einem Dritten zur Beilegung unterbreitet.

ARTIKEL 16 SCHLUSSBESTIMMUNGEN

1. Das vorliegende Abkommen wird auf unbefristete Dauer abgeschlossen. Es tritt am ersten Tag des zweiten Monats nach dem Datum in Kraft, an dem auf diplomatischem Weg die letzte der Mitteilungen zwischen den Vertragsparteien eingegangen ist, gemäss der die innerstaatlichen rechtlichen Verfahren für das Inkrafttreten des vorliegenden Abkommens abgeschlossen wurden.
2. Das vorliegende Abkommen kann auf der Grundlage eines gegenseitigen Einverständnisses der Vertragsparteien geändert werden. Solche Änderungen treten gemäss Absatz 1 dieses Artikels in Kraft.
3. Jede Vertragspartei kann das vorliegende Abkommen jederzeit schriftlich kündigen. In einem solchen Fall erlischt die Gültigkeit des vorliegenden Abkommens sechs Monate nach dem Tag, an dem die andere Vertragspartei die schriftliche Kündigung erhalten hat.

4. Ungeachtet der Kündigung des vorliegenden Abkommens sind alle klassifizierten Informationen, die im Rahmen des vorliegenden Abkommens freigegeben oder erarbeitet wurden, entsprechend den im vorliegenden Abkommen festgehaltenen Bestimmungen geschützt, bis die bereitstellende Partei die empfangende Partei von dieser Verpflichtung entbindet.

Zu Urkund dessen haben die zu diesem Zweck gehörig befugten Unterzeichneten das vorliegende Abkommen unterzeichnet.

Geschehen zu Prag am 26. Januar 2011 in zwei Urschriften, in deutscher, tschechischer, und englischer Sprache, wobei jeder Wortlaut gleichermaßen verbindlich ist. Bei einer unterschiedlichen Auslegung ist der englische Wortlaut massgebend.

Für den Schweizerischen Bundesrat

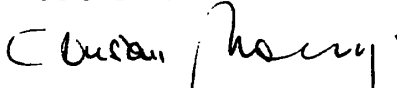
Chef Informations- und Objektsicherheit



Urs FREIBURGH AUS

**Für die Regierung der
Tschechischen Republik**

Direktor der Nationalen
Sicherheitsbehörde



Dušan NAVRÁTIL