PARLAMENT ČESKÉ REPUBLIKY

Poslanecká sněmovna

2011

6. volební období

263

Vládní návrh,

kterým se předkládá Parlamentu České republiky k vyslovení souhlasu s ratifikací

Smlouva mezi vládou České republiky a Švýcarskou spolkovou radou o výměně a vzájemné ochraně utajovaných informací

Návrh

U S N E S E N Í

Poslanecké sněmovny Parlamentu České republiky

k vládnímu návrhu, kterým se předkládá Parlamentu České republiky k vyslovení souhlasu s ratifikací Smlouva mezi vládou České republiky a Švýcarskou spolkovou radou o výměně a vzájemné ochraně utajovaných informací

Poslanecká sněmovna

vyslovuje souhlas s ratifikací Smlouvy mezi vládou České republiky a Švýcarskou spolkovou radou o výměně a vzájemné ochraně utajovaných informací.

PŘEDKLÁDACÍ ZPRÁVA PRO PARLAMENT

Důvody uzavírání smluv o výměně a vzájemné ochraně utajovaných informací

Ekonomické, vojenské a politické vztahy České republiky (dále jen „ČR") s sebou přinášejí nutnost výměny utajovaných informací (dále jen „UI"). Právní rámec pro výměnu a vzájemnou ochranu národních UI je nutné v mezinárodním styku zajišťovat prostřednictvím bilaterálních smluv.

Při stanovování priorit v této oblasti vychází Národní bezpečnostní úřad (dále jen „Úřad") z praktické potřeby výměny UI s konkrétními státy v souladu se zahraničně-politickými zájmy ČR. Smlouvy o výměně a vzájemné ochraně UI (dále jen „Smlouva o UI") jsou sjednávány jen s těmi státy, které prokáží schopnost zajistit poskytnutým českým UI alespoň takovou úroveň ochrany, jakou jim poskytuje ČR. K dnešnímu dni byly tyto smlouvy sjednány s Bulharskou republikou, Estonskou republikou, Francouzskou republikou, Italskou republikou, Státem Izrael, Litevskou republikou, Lotyšskou republikou, Spolkovou republikou Německo, Polskou republikou, Portugalskou republikou, Ruskou federací, Slovenskou republikou, Ukrajinou, Spojeným královstvím Velké Británie a Severního Irska, Švédským královstvím, Finskou republikou, Norským královstvím, Rakouskou republikou, Republikou Makedonií, Republikou Slovinsko a Gruzií. V působnosti Ministerstva obrany byly navíc sjednány smlouvy o vzájemné ochraně vojenských UI s Jihoafrickou republikou, Rumunskem, Spojenými státy americkými (při sjednávání Dohody o změně byla gesce svěřena Úřadu).

Spolupráce se Švýcarskem

Přestože Švýcarsko vzhledem ke svému tradičně neutrálnímu postavení není členským státem EU ani NATO, úzce s oběmi těmito organizacemi spolupracuje. Od roku 1996 je Švýcarsko členem programu Partnerství pro mír (PfP) a podílelo se i na některých misích NATO (KFOR). Švýcarsko je také členem Mezinárodní pracovní skupiny pro průmyslovou bezpečnost (MISWG), jejímž cílem je vytvoření jednotného rámce ochrany utajovaných informací v oblasti průmyslové bezpečnosti i mimo NATO a EU a tím umožnění snazšího provádění mezinárodních utajovaných smluv. V oblasti ochrany UI Česká republika a Švýcarsko dále spolupracují v rámci Evropské kosmické agentury (ESA).

S ohledem na výše uvedené lze usuzovat, že intenzifikující se bilaterální spolupráce bude vyžadovat výměnu UI. Sjednání Smlouvy o UI se v tomto kontextu jeví jako výhodné pro obě strany.

Ochrana UI je ve Švýcarsku upravena Nařízením o ochraně spolkových informací z roku 2007 a jeho prováděcími předpisy. Kompetence v této oblasti je ve Švýcarsku rozdělena mezi Ministerstvo spravedlnosti a policie (civilní oblast) a Ministerstvo obrany, civilní ochrany a sportu (vojenská oblast), přičemž nejdůležitější roli hraje Ředitelství pro bezpečnost informací a ochranu objektů (DISFP), podřízené Ministerstvu obrany, civilní ochrany a sportu, které je národním bezpečnostním úřadem ve smyslu předpisů NATO. Mezi jeho hlavní činnosti patří příprava legislativy v oblasti ochrany UI, kontrola ochrany UI, včetně vyšetřování porušení bezpečnosti, bezprostřední řízení bezpečnosti v rámci Ministerstva obrany, civilní ochrany a sportu a armády, provádění bezpečnostního řízení pro všechny zaměstnance federální správy, trénink a školení v oblasti ochrany UI a také příprava a provádění bilaterálních smluv o ochraně UI.

UI se dělí do tří stupňů utajení podle újmy, která by byla způsobena národní bezpečnosti jejich vyzrazením, zneužitím nebo ztrátou: GEHEIM / SECRET / SEGRETO (TAJNÉ),

VERTRAULICH / CONFIDENTIEL / CONFIDENZIALE (DŮVĚRNÉ), INTERN / RESTREINT / INTERNO (VYHRAZENÉ). Přístup k UI je ve Švýcarsku umožněn toliko osobám, které jsou prověřeny pro příslušný stupeň utajení a mají „need-to-know", tj. přístup k UI nezbytně potřebují k výkonu své funkce, pracovní nebo jiné činnosti.

Lze konstatovat, že výše uvedená švýcarská právní úprava ochrany UI je plně v souladu se standardy NATO.

Návrh na sjednání Smlouvy mezi vládou České republiky a Švýcarskou spolkovou radou o výměně a vzájemné ochraně UI (dále jen „Smlouva") byl iniciován českou stranou. Expertního jednání se za českou stranu účastnili zástupci oddělení mezinárodní spolupráce a odboru právního a legislativního Úřadu. Švýcarská delegace byla tvořena zástupci DISFP.

Česká delegace expertů při jednání o návrhu Smlouvy postupovala v souladu se vzorovou směrnicí pro expertní jednání o návrzích Smluv o UI. Při jednání bylo dosaženo stanoveného cíle - umožnit výměnu UI mezi smluvními stranami a zajistit jejich odpovídající ochranu. Za tímto účelem se obě smluvní strany zavazují poskytovat vyměněným UI alespoň takovou úroveň ochrany, jakou poskytují UI národním. Zejména se zavazují, že přístup k UI poskytnutým druhou smluvní stranou neumožní neoprávněným subjektům nebo třetím stranám. Návrh Smlouvy dále upravuje srovnatelnost opatření při nakládání s UI a opatření, která mají neoprávněným subjektům znemožnit nebo ztížit přístup k UI. Návrh Smlouvy také obsahuje ustanovení upravující podmínky, za kterých si smluvní strany vzájemně uznávají bezpečnostní oprávnění vydaná příslušnými bezpečnostními úřady podle vnitrostátních právních předpisů. Výslovně jsou určeny orgány smluvních stran kompetentní v otázkách ochrany UI, které jsou příslušné k provádění této smlouvy. Dále jsou stanoveny vzájemné notifikační povinnosti a formy spolupráce (zejména při provádění bezpečnostních řízení).

Lze konstatovat, že při expertních jednáních byly zájmy ČR prosazeny v největší možné míře a sjednání předložené Smlouvy je plně v souladu se zahraničně-politickými zájmy ČR.

Informace o souhlasném stanovisku švýcarské strany

Švýcarská strana s návrhem textu Smlouvy vyslovila souhlas bez výhrady.

Charakteristika Smlouvou přejímaných závazků

Preambule

Preambule deklaruje přání zajistit ochranu UI vyměněných mezi vládou České republiky a Švýcarskou spolkovou radou nebo mezi právnickými a fyzickými osobami pod jurisdikcí jejich států.

Článek 1 – Rozsah působnosti

Tento článek podrobněji vymezuje působnost Smlouvy také na jednotlivé oblasti ochrany UI, vylučuje z její působnosti výměnu UI mezi orgány smluvních stran činnými v trestním řízení. Toto omezení bylo do textu vloženo na žádost švýcarské strany vzhledem ke složitější struktuře legislativy v oblasti ochrany UI ve Švýcarsku a rozdělení kompetencí mezi civilní a vojenské orgány. Z tohoto důvodu bude výměna UI mezi orgány smluvních stran činnými v trestním řízení upravena zvláštní smlouvou (Smlouva mezi Českou republikou a Švýcarskou konfederací o policejní spolupráci v boji proti trestné činnosti, podepsaná v Praze dne 31. května 2005).

Článek 2 - Vymezení pojmů

V zájmu zajištění jednotného výkladu jsou pro účely Smlouvy definovány následující pojmy: „utajovaná informace", „utajovaná smlouva", „kontrahent" „poskytující strana", „přijímající strana", „třetí strana" a „bezpečnostní osvědčení".

UI se rozumí jakákoliv informace, dokument nebo materiál, předaný nebo vytvořený smluvními stranami, který bez ohledu na svoji formu vyžaduje, v souladu s vnitrostátními právními předpisy států smluvních stran, ochranu proti vyzrazení, zneužití, zničení, zveřejnění nebo zpřístupnění neoprávněné osoby, a byl jako takový určen a náležitě označen.

Kontrahentem se rozumí fyzická nebo právnická osoba způsobilá uzavřít utajovanou smlouvu.

Utajovanou smlouvou se rozumí smlouva nebo subdodavatelská smlouva, která obsahuje UI, a/nebo v souvislosti s níž může k přístupu k UI dojít.

Poskytující stranou se rozumí smluvní strana včetně právnických a fyzických osob pod jurisdikcí jejího státu, která poskytne UI.

Přijímající stranou se rozumí smluvní strana včetně právnických a fyzických osob pod jurisdikcí jejího státu, která přijme UI.

Třetí stranou se rozumí stát včetně právnických a fyzických osob pod jeho jurisdikcí nebo mezinárodní organizace, které nejsou smluvní stranou této Smlouvy.

Bezpečnostním osvědčením se rozumí pozitivní rozhodnutí, vycházející z bezpečnostního řízení, které potvrdí loajalitu a důvěryhodnost stejně jako další bezpečnostní aspekty fyzické nebo právnické osoby v souladu s vnitrostátními právními předpisy.

Článek 3 - Národní bezpečnostní úřady

Smlouva upravuje práva a povinnosti osob a některá její ustanovení patří mezi tzv. *„self-executing"*. To znamená, že předpokládá výkon těchto práv bez dalšího. V souladu s principy právní jistoty a veřejnosti je vhodné, aby orgány, které budou v konkrétních případech rozhodovat o těchto právech a povinnostech, byly v textu Smlouvy výslovně určeny.

V článku 3 jsou proto výslovně uvedeny národní bezpečnostní úřady, tj. orgány smluvních stran odpovědné za výkon státní správy v oblasti ochrany UI a za provádění Smlouvy. V ČR je takovým úřadem Národní bezpečnostní úřad a Ve Švýcarsku je to DISFP.

Vzhledem k tomu, že v institucionálním rámci týkajícím se ochrany UI může dojít ke změnám, stanovuje se povinnost národních bezpečnostních úřadů informovat se o kontaktních údajích a vzhledem ke struktuře ochrany UI ve Švýcarsku i o dalších určených bezpečnostních úřadech odpovědných za provádění Smlouvy.

Článek 4 – Stupně utajení

UI poskytnutá podle této Smlouvy se označí příslušným stupněm utajení v souladu s vnitrostátními právními předpisy států smluvních stran. Na základě úrovně ochrany poskytované smluvními stranami národním UI jednotlivých stupňů utajení je dovozena jejich rovnocennost, která je vyjádřena v tabulce. Přestože Švýcarsko nemá ekvivalent pro UI stupně PŘÍSNĚ TAJNÉ, lze říci, že ochrana UI stupně GEHEIM / SECRET / SEGRETO odpovídá ochraně UI stupně PŘÍSNĚ TAJNÉ v ČR. Přesto jsou ve Smlouvě uvedeny jako ekvivalentní stupně utajení TAJNÉ a GEHEIM / SECRET / SEGRETO, protože stejná rovnocennost je uvedena i ve smlouvě o ochraně UI, kterou se Švýcarskem uzavřela EU[1].

[1] viz ÚV 181/58 ze dne 10.7.2008

Článek 5 - Přístup k utajovaným informacím

Ochrana UI sestává z opatření v několika oblastech bezpečnosti. Základním principem v oblasti personální bezpečnosti je umožnit přístup k UI pouze těm osobám, které splňují podmínky stanovené právními předpisy. Okruh osob vychází z principu „need-to-know", tj. přístup je umožněn toliko osobám, které ho nezbytně potřebují k výkonu své funkce, pracovní nebo jiné činnosti, a požadavků na osobnostní způsobilost a bezpečnostní spolehlivost dané osoby. Toto řešení vychází z reciprocity a předpokládá znalost okruhu osob, které podle vnitrostátních právních předpisů druhé smluvní strany mají mít přístup k UI. Splnění podmínek pro přístup k UI je ověřováno v bezpečnostním řízení, jehož výsledkem je vydání rozhodnutí.

Článek 6 - Omezení použití utajovaných informací

V souladu s principem kontroly původce nesmí být poskytnutá UI předána třetí straně bez předchozího písemného souhlasu poskytující strany. Přijímající strana nesmí s poskytnutou UI nakládat jinak než v souladu s účelem, za kterým byla poskytnuta a v souladu s požadavky na nakládání s ní stanovenými poskytující stranou.

Článek 7 – Nakládání s utajovanými informacemi

Tento článek stanoví základní povinnosti smluvních stran při ochraně předaných UI.

Poskytující strana zejména zajistí označení utajované informace příslušným stupněm utajení a doplňujícím označením v souladu s vnitrostátními právními předpisy. Dále informuje přijímající stranu o následných změnách stupně utajení a o podmínkách poskytnutí utajované informace.

Přijímající strana zajistí, že poskytnutá UI je podle tabulky rovnocennosti uvedené v článku 4 označena stupněm utajení rovnocenným tomu, kterým UI označila poskytující strana. Vzhledem k tomu, že v tabulce není uveden ekvivalent českých UI stupně PŘÍSNĚ TAJNÉ, je stanoveno, že budou ve Švýcarské konfederaci chráněny jako UI stupně GEHEIM / SECRET / SEGRETO. Základní povinností přijímající strany je dále zajistit poskytnuté UI úroveň ochrany srovnatelnou s tou, kterou jí poskytuje druhá smluvní strana. Zároveň ale vzhledem k rozdílným stupňům utajení ve Švýcarsku a v ČR může poskytující strana vyžadovat, aby přijímající strana poskytla předané utajované informaci jinou než rovnocennou úroveň ochrany. Přijímající strana také musí zajistit, že stupeň utajení nebude bez předchozího písemného souhlasu poskytující strany změněn nebo zrušen.

Smluvní strany jsou dále povinny zajistit v souladu s vnitrostátními právními předpisy, že budou uplatněna veškerá bezpečnostní opatření k zajištění ochrany UI.

Článek 8 - Bezpečnostní spolupráce

Uzavření smlouvy předchází důkladná analýza právní úpravy ochrany UI a její aplikace ve smluvních státech. Smlouvy jsou prováděny příslušnými bezpečnostními úřady. Ať se jedná o vzájemné informační povinnosti o změnách právní úpravy, struktury orgánů, které se podílejí na zajišťování ochrany UI, bezpečnostních rizicích nebo dalších změnách, které mohou mít vliv na ochranu UI, o spolupráci při provádění úkonů v bezpečnostním řízení na základě dožádání, uznávání bezpečnostních oprávnění, povolování návštěv nebo řešení sporů, smluvní strany předpokládají, že mezi národními bezpečnostními úřady bude probíhat intenzivní komunikace, že otázky společného zájmu budou konzultovány a že při hledání řešení budou tyto úřady spolupracovat. K usnadnění dosažení těchto cílů se strany dohodly, že smlouva bude prováděna v anglickém jazyce.

Aby bylo možné udržet srovnatelnou úroveň ochrany UI poskytovaných na základě této smlouvy, příslušné bezpečnostní úřady smluvních stran se informují o vnitrostátních

právních předpisech upravujících ochranu utajovaných informací a o uplatňovaných postupech a zkušenostech získaných při jejich provádění.

V průběhu bezpečnostního řízení může vzniknout potřeba dožádat informace týkající se účastníka řízení od příslušného bezpečnostního úřadu cizí moci. Z tohoto důvodu se stanovuje povinnost spolupráce příslušných bezpečnostních úřadů smluvních stran při provádění úkonů v bezpečnostním řízení. Spolupráce Úřadu s úřadem cizí moci při provádění bezpečnostního řízení je výslovně umožněna ustanovením § 138 odst. 1 písm. k) zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů. Povinnost Úřadu provádět úkony v bezpečnostním řízení na žádost bezpečnostního úřadu členského státu EU a NATO nebo smluvního partnera je stanovena ustanovením § 110 odst. 2 zákona č. 412/2005 Sb.

Za účelem usnadnění mobility fyzických osob a podnikatelů, kteří jsou oprávněni k přístupu k UI, si smluvní strany tam, kde jsou podmínky pro přístup k UI srovnatelné a bezpečnostní řízení probíhá za srovnatelných podmínek, uznávají bezpečnostní osvědčení fyzických osob a podnikatelů. Uznávání rozhodnutí bezpečnostního úřadu druhé smluvní strany předpokládá reciprocitu a splnění formálních požadavků stanovených vnitrostátními právními předpisy. Uznávání předpokládá a formální požadavky, které musí být splněny, stanoví § 62 zákona č. 412/2005 Sb. Vzhledem k tomu, že ve Švýcarsku neexistuje bezpečnostní osvědčení ekvivalentní českému bezpečnostnímu osvědčení umožňujícímu přístup k UI stupně PŘÍSNĚ TAJNÉ, je stanoveno, že na žádost příslušného národního bezpečnostního úřadu může být švýcarské bezpečnostní osvědčení umožňující přístup k UI označeným GEHEIM / SECRET / SEGRETO uznáno tak, aby umožňovalo přístup také k českým UI označeným PŘÍSNĚ TAJNÉ. V tomto případě by se jednalo zejména o případy, kdy švýcarská strana potvrdí, že daná osoba je držitelem bezpečnostního osvědčení pro přístup k UI stupně označeným GEHEIM / SECRET / SEGRETO mající vliv na politické směřování státu, protože při bezpečnostním řízení je v takovém případě ve Švýcarsku obligatorní činnostní šetření za spolupráce zpravodajských služeb, a tedy svou povahou odpovídá bezpečnostnímu řízení pro vydání bezpečnostního osvědčení pro přístup k UI stupně PŘÍSNĚ TAJNÉ v ČR. Naopak česká bezpečnostní osvědčení umožňující přístup k utajovaným informacím označeným PŘÍSNĚ TAJNÉ a TAJNÉ budou uznána jako umožňující přístup ke švýcarským utajovaným informacím označeným GEHEIM / SECRET / SEGRETO.

Příslušné bezpečnostní úřady si bezodkladně oznamují 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

Hospodářské vztahy, při kterých vznikají UI nebo dochází k jejich výměně, předpokládají uzavírání smluv, které jsou označeny jako utajované. Tyto smlouvy jsou uzavírány a prováděny podle vnitrostátních právních předpisů upravujících ochranu UI příslušné smluvní strany. Na základě žádosti národní bezpečnostní úřad poskytne informaci o tom, je-li navrhovaný kontrahent nebo fyzická osoba, která se účastní sjednávání a provádění utajované smlouvy, držitelem bezpečnostního osvědčení podnikatele nebo bezpečnostního osvědčení fyzické osoby pro přístup k UI požadovaného stupně utajení.

Příslušný národní bezpečnostní úřad může požadovat provedení bezpečnostní inspekce u subjektu druhé smluvní strany s cílem zajistit, že jsou vnitrostátní právní předpisy upravující ochranu utajovaných informací i nadále dodržovány.

Utajované smlouvy musí v zájmu zajištění odpovídající ochrany UI, jejichž výměnu nebo zpracovávání předpokládají, obsahovat bezpečnostní pokyny. Ty určí, jaké UI budou poskytnuty nebo vzniknou v rámci plnění utajované smlouvy, stanoví stupně jejich utajení a dále konkrétní bezpečnostní požadavky k zajištění jejich ochrany.

Národní bezpečnostní úřad poskytující strany zašle kopii bezpečnostních pokynů utajované smlouvy národnímu bezpečnostnímu úřadu strany, pod jejíž jurisdikcí bude utajovaná smlouva prováděna s cílem umožnění státního dozoru.

Článek 10 - Předávání utajovaných informací

Předávání UI mezi smluvními stranami se řídí vnitrostátními právními předpisy státu poskytující strany. Zpravidla se tak děje diplomatickou nebo vojenskou cestou prostřednictvím ústředních registrů. Příslušné bezpečnostní úřady se však mohou dohodnout na jiném způsobu předávání. Využít lze například zabezpečené komunikační systémy nebo další elektromagnetické prostředky schválené a podle vnitrostátních právních předpisů certifikované národními bezpečnostními úřady smluvních stran.

Článek 11 - Reprodukce, překlad a zničení utajovaných informací

Reprodukce a překlady UI musí být označeny příslušným stupněm utajení a doplňujícím označením a musí jim být poskytnuta ochrana jako původní utajované informaci. Překlady musí být dále opatřeny poznámkou v jazyce překladu, která vysvětluje, že obsahuje UI poskytující strany. Účelem tohoto ustanovení je zajistit, že z UI je zřejmé, kdo je poskytující stranou, a tedy podle jaké vnitrostátní právní úpravy se nakládání s touto UI řídí. Počet vyhotovených překladů a reprodukcí se omezí na nezbytné minimum.

V souladu s principem kontroly původce lze překlad nebo reprodukci (kopie, výpis, opis) UI stupně utajení TAJNÉ nebo vyššího vyhotovit pouze s předchozím souhlasem příslušného bezpečnostního úřadu poskytující strany. Toto ustanovení je plně v souladu s ustanovením § 21 odst. 6 zákona č. 412/2005 Sb.

Součástí tohoto článku je ustanovení týkající se ničení UI. UI stupně utajení TAJNÉ nebo vyššího nesmí být zničena a musí být v souladu s vnitrostátními právními předpisy přijímající strany vrácena poskytující straně.

Článek 12 - Návštěvy

Režim návštěv je standardní procedurou vycházející z bezpečnostních předpisů NATO C-M(2002)49, která zjednodušuje spolupráci předpokládající poskytování UI mezi ústředními orgány státní správy, ozbrojenými silami nebo pracovníky společností participujících na utajovaných smlouvách. Cílem je zajistit, že přístup k UI bude umožněn toliko osobám, které jsou držiteli bezpečnostního osvědčení fyzické osoby pro přístup k UI příslušného stupně utajení. V případě návštěv je rozhodující přístup k UI bez ohledu na to, zda-li k němu dojde v budově státní instituce nebo při cvičení ve vojenském prostoru. Vždy je však nutné definovat subjekt, který bude poskytovatelem UI. Jedná se tedy o institut personální bezpečnosti a nikoliv fyzické bezpečnosti. Zpravidla se schvalují pouze návštěvy vyžadující přístup k UI, nicméně švýcarská strana trvala na zavedení povolovacího režimu i na návštěvy do prostor, kde jsou utajované informace vytvářeny, ukládány, přenášeny nebo kde je s nimi nakládáno.

Osoba zašle žádost o povolení návštěvy národnímu bezpečnostnímu úřadu svého domovského státu. Tento na žádosti potvrdí, že je osoba držitelem příslušného bezpečnostního osvědčení fyzické osoby a následně ji zašle národnímu bezpečnostnímu úřadu státu, na jehož území se nachází subjekt, který bude navštíven. Národní bezpečnostní úřad hostitelského státu žádost zpracuje, a návštěvu povolí nebo zamítne.

V ČR lze podle zákona č. 412/2005 Sb. přístup k UI umožnit pouze tehdy, je-li fyzická osoba držitelem osvědčení pro přístup k UI nebo v případech, kdy Úřad uzná bezpečnostní oprávnění vydané úřadem cizí moci, který má ve své kompetenci ochranu UI. Povolení návštěvy je tedy v ČR provázeno i provedením uznání bezpečnostního oprávnění.

Národní bezpečnostní úřady se však mohou dohodnout i na jiném režimu povolování návštěv, zejména jedná-li se o osoby podle § 58 zákona č. 412/2005 Sb.

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 povolena ve lhůtě kratší, nebo jiným způsobem, na kterém se národní bezpečnostní úřady dohodnou.

Žádost o povolení návštěvy obsahuje:

- jméno a příjmení, datum a místo narození, státní občanství, číslo cestovního pasu nebo průkazu totožnosti každého návštěvníka;
- pracovní zařazení návštěvníka a určení subjektu, který zastupuje;
- stupeň utajení, pro který bylo návštěvníkovi bezpečnostní osvědčení fyzické osoby vydáno, včetně doby jeho platnosti;
- datum a délku návštěvy; v případě opakovaných návštěv se uvede jejich celková délka;
- účel návštěvy včetně nejvyššího stupně utajení informací, ke kterým bude přístup vyžadován;
- 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;
- datum, podpis a otisk úředního razítka příslušného národního bezpečnostního úřadu;
- jméno a příjmení, pracovní zařazení a/nebo funkci hostitele.

Národní bezpečnostní úřady se mohou dohodnout na seznamu osob, jimž je povolena opakovaná návštěva. Národní bezpečnostní úřady se mohou dohodnout na dalších podrobnostech opakované návštěvy.

UI zpřístupněná návštěvníkovi během jeho návštěvy se považuje za UI poskytnutou podle této Smlouvy.

Článek 13 – Bezpečnostní incidenty

Smluvní strany se bezodkladně písemně informují o jakémkoli bezpečnostním incidentu, při kterém došlo například ke ztrátě, zneužití nebo vyzrazení UI, nebo o podezření, že k takovému incidentu došlo. Smluvní strana, v jejíž jurisdikci k incidentu došlo, zahájí bezodkladně příslušné vyšetřování. Je-li to vyžadováno (ať již přijímající nebo poskytující stranou) může se druhá smluvní strana účastnit vyšetřování. Smluvní strana v jejíž jurisdikci k incidentu došlo, písemně informuje druhou smluvní stranu o okolnostech bezpečnostního incidentu, způsobené škodě, opatřeních přijatých pro její zmírnění a o výsledku řízení.

Článek 14 - Náklady

Každá smluvní strana si hradí své náklady vzniklé v souvislosti s aplikací této Smlouvy.

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

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. Tuto Smlouvu lze změnit na základě souhlasu smluvních stran. Změny vstoupí v platnost v souladu s ustanovením odstavce 1.

Každá ze smluvních stran má právo tuto Smlouvu kdykoliv diplomatickou cestou vypovědět. V takovém případě je platnost Smlouvy ukončena šest měsíců následujících po dni, kdy bylo písemné oznámení o výpovědi doručeno druhé smluvní straně. Veškerým UI 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.

Zajištění provádění Smlouvy

Odpovědnost za implementaci této Smlouvy mají v ČR Národní bezpečnostní úřad a ve Švýcarsku DISFP. Tyto instituce jsou ve Smlouvě uvedeny jako národní bezpečnostní úřady a jejich funkce je jasně definována.

Dopad na státní rozpočet

Smlouva byla sjednána tak, že se nepředpokládají dopady na schválené rozpočtové kapitoly státního rozpočtu.

Zhodnocení souladu Smlouvy s právním řádem, ústavním pořádkem a mezinárodními závazky ČR

Text Smlouvy je v souladu s ústavním pořádkem, s ostatními součástmi právního řádu ČR a mezinárodně-právními závazky ČR (včetně práva a bezpečnostních standardů EU). Z právních předpisů EU se jedná zejména o rozhodnutí Rady EU 2001/264/ES ze dne 19. března 2001, ve znění pozdějšího rozhodnutí, kterým byly přijaty bezpečnostní předpisy Rady a dále rozhodnutí Komise 2001/844/ES, ESUO, EURATOM ze dne 29. listopadu 2001, ve znění pozdějších rozhodnutí. Smlouva dále reflektuje obecně uznávané principy a uzance mezinárodního práva.

Odůvodnění kategorizace navrhované Smlouvy

Vzhledem k tomu, že Smlouva má upravovat věci, jejichž úprava je vyhrazena zákonu, a dále práva a povinnosti osob, jedná se o smlouvu, k jejíž ratifikaci je v souladu s článkem 49 Ústavy potřebný souhlas obou komor Parlamentu. Ve smyslu Směrnice vlády pro sjednávání, vnitrostátní projednávání, provádění a ukončování platnosti mezinárodních smluv, schválené usnesením vlády č. 131 ze dne 11. února 2004, se jedná o mezinárodní smlouvu prezidentské kategorie. Ve Švýcarsku je tato Smlouva sjednávaná jako vládní, a tudíž má vnější atributy smlouvy vládní.

Vláda vyslovila souhlas se sjednáním Smlouvy svým usnesením č. 449 ze dne 7. června 2010. Podepsána byla dne 26. ledna 2011 v Praze ředitelem NBÚ panem Ing. Dušanem Navrátilem a ředitelem Ředitelství pro bezpečnost informací a ochranu objektů Ursem Freiburghausem.

V Praze dne 14. února 2011

RNDr. Petr Nečas, v.r.
předseda vlády

SMLOUVA

MEZI

VLÁDOU ČESKÉ REPUBLIKY

A

ŠVÝCARSKOU SPOLKOVOU RADOU

O

VÝMĚNĚ A VZÁJEMNÉ OCHRANĚ

UTAJOVANÝCH INFORMACÍ

Vláda České republiky a Švýcarská spolková rada (dále jen „smluvní strany"), přejíce si zajistit ochranu utajovaných informací vyměněných mezi nimi nebo mezi právnickými 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 právnickými 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 právnickými 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 právnická osoba způsobilá k uzavření utajované smlouvy;

4) **„poskytující stranou"** se rozumí smluvní strana včetně právnických a fyzických osob pod jurisdikcí jejího státu, která poskytne utajovanou informaci;

5) **„přijímající stranou"** se rozumí smluvní strana včetně právnických 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 právnické 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:

V České republice:
NÁRODNÍ BEZPEČNOSTNÍ ÚŘAD

Ve Švýcarské konfederaci:

EIDGENÖSSISCHES DEPARTEMENT FÜR VERTEIDIGUNG, BEVÖLKERUNGSSCHUTZ UND SPORT, GENERALSEKRETARIAT VBS, INFORMATIONS- UND OBJEKTSICHERHEIT
(Federální ministerstvo pro obranu, civilní ochranu a sport, Ředitelství pro bezpečnost informací a ochranu objektů)

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:

V České republice	Ve Švýcarské konfederaci	Ekvivalent v anglickém jazyce
PŘÍSNĚ TAJNÉ	*bez ekvivalentu*	*TOP SECRET*
TAJNÉ	GEHEIM / SECRET / SEGRETO	*SECRET*
DŮVĚRNÉ	VERTRAULICH / CONFIDENTIEL / CONFIDENZIALE	*CONFIDENTIAL*
VYHRAZENÉ	INTERN / INTERNE / AD USO INTERNO	*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 poskytující strany.

2. Přijímající strana použije utajovanou informaci pouze v souladu s účelem, za kterým byla poskytnuta, a s požadavky na nakládání s ní stanovenými poskytující stranou.

ČLÁNEK 7
NAKLÁDÁNÍ S UTAJOVANÝMI INFORMACEMI

1. Poskytující 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 poskytující 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 účastnící 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 zasílá 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 jakémkoliv 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 bezodkladné 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 výpovědi 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 zmocněni k tomuto účelu, podepsali tuto Smlouvu.

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

Za Vládu České republiky

Za Švýcarskou konfederaci

AGREEMENT

BETWEEN

THE GOVERNMENT OF THE CZECH REPUBLIC

AND

THE SWISS FEDERAL COUNCIL

ON THE EXCHANGE

AND MUTUAL PROTECTION

OF CLASSIFIED INFORMATION

The Government of the Czech Republic and the Swiss Federal Council, 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 Czech Republic:

   NÁRODNÍ BEZPEČNOSTNÍ ÚŘAD
   (National Security Authority)

   In the Swiss Confederation:

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

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 Czech Republic	**In the Swiss Confederation**	Equivalent in English language
PŘÍSNĚ TAJNÉ	*no equivalent*	TOP SECRET
TAJNÉ	GEHEIM / SECRET / SEGRETO	SECRET
DŮVĚRNÉ	VERTRAULICH / CONFIDENTIEL / CONFIDENZIALE	CONFIDENTIAL
VYHRAZENÉ	INTERN / INTERNE / AD USO INTERNO	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 TAJNÉ. A Czech Security Clearance granting access to Classified Information marked PŘÍSNĚ TAJNÉ as well as TAJNÉ 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 26th January 2011 in two originals, in the Czech, German and English languages, each text being equally authentic. In case of different interpretation the English text shall prevail.

For the Government of the Czech Republic

For the Swiss Federal Council