PARLAMENT ČESKÉ REPUBLIKY

Poslanecká sněmovna

2010

6. volební období

140

Vládní návrh,

kterým se předkládá Parlamentu České republiky k vyslovení souhlasu s ratifikací

Smlouva mezi Českou republikou a Španělským královstvím 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 Českou republikou a Španělským královstvím o výměně a vzájemné ochraně utajovaných informací

Poslanecká sněmovna

vyslovuje souhlas s ratifikací Smlouvy mezi Českou republikou a Španělským královstvím o výměně a vzájemné ochraně utajovaných informací.

PŘEDKLÁDACÍ ZPRÁVA PRO PARLAMENT

Důvody uzavírání smluv o výměně a vzájemné ochraně utajovaných informací

Závazky vyplývající z členství v Organizaci Severoatlantické smlouvy (dále jen „NATO") a v Evropské unii (dále jen „EU"), stejně jako ekonomické, vojenské a politické vztahy České republiky s sebou přinášejí nutnost výměny utajovaných informací (dále jen „UI"). Vzhledem k tomu, že neexistuje žádná multilaterální smlouva, která by tuto problematiku upravovala, a to ani mezi členskými státy NATO nebo EU, je nutné právní rámec pro výměnu a vzájemnou ochranu UI 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, jako jim poskytuje ČR. K dnešnímu dni byly tyto smlouvy sjednány s Bulharskou republikou, Estonskou republikou, Finskou republikou, Francouzskou republikou, Italskou republikou, Státem Izrael, Litevskou republikou, Lotyšskou republikou, Norským královstvím, Spolkovou republikou Německo, Polskou republikou, Portugalskou republikou, Rakouskou republikou, Republikou Makedonie, Ruskou federací, Slovenskou republikou, Švédským královstvím, Ukrajinou a Spojeným královstvím Velké Británie a Severního Irska. V působnosti Ministerstva obrany byly navíc sjednány smlouvy o vzájemné ochraně vojenských UI s Jihoafrickou republikou, Rumunskem a Spojenými státy americkými (při sjednávání Dohody o změně byla gesce svěřena Úřadu).

Sjednání Smlouvy o UI se jeví vhodné a pro obě strany výhodné z několika důvodů. Lze se důvodně domnívat, že hospodářská, případně i vědecko-technická spolupráce bude dříve či později vyžadovat výměnu UI. Oba státy jsou členskými zeměmi jak NATO, tak i EU. Členství v těchto organizacích s sebou přináší spolupráci v oblastech bezpečnosti. Tato spolupráce je podmíněna nejen výměnou UI NATO či UI EU, ale i národních UI. Španělsko se navíc aktivně podílí na několika multinárodních zbrojních projektech v rámci organizace OCCAR *(Organisation Conjointe de Coopération en matière d'Armement)*. Jedná se zejména o participaci na vývoji víceúčelového vrtulníku TIGER nebo nákladního letounu A400M. Španělsko je dále jedním ze států, které se účastní projektu vývoje nadzvukového letounu Eurofighter EF-2000 Typhoon, raket vzduch-vzduch IRIS-T a v neposlední řadě i projektu Galileo.

Ochrana UI je ve Španělsku upravena v zákonu č. 9/1968, o státním tajemství, v jeho prováděcí vyhlášce č. 242/1969 a dále pak v nařízeních úřadu Oficina Nacional de Seguridad (národní bezpečnostní úřad, dále jen „NSA ESP") a Pokynu ministerstva obrany o UI poskytnutých podnikatelům č. 76/2006. Trestání v případě porušení ochrany UI je upraveno v trestním zákoně (č. 10/1995) a ve vojenském trestním zákoně (č. 13/1985).

Odpovědnost za ochranu národních UI a UI cizí moci ve Španělsku náleží NSA ESP. V rámci struktury ústředních orgánů státní správy je NSA ESP podřízen Secretario de Estado Director del Centro Nacional de Inteligencia. NSA ESP je zodpovědný za provádění bezpečnostních řízení a vydávání příslušných osvědčení fyzické osoby nebo podnikatele (včetně certifikátů pro NATO a EU), výkon státního dozoru na úseku ochrany UI, zajišťování poučení před prvním přístupem k UI, přípravu právních předpisů v oblasti ochrany UI, zajišťování činnosti ústředního registru, certifikaci informačních systémů, certifikaci technických prostředků, schvalování zahraničních návštěv v prostorech, kde může dojít k seznámení se s UI. Na rozdíl od Úřadu nedisponuje pravomocemi v oblasti kryptografické ochrany, neboť tato je v gesci Centro Criptológico Nacional (Národní kryptologické ústředí), které je spadá též pod Secretario de Estado Director del Centro Nacional de Inteligencia.

Stejně jako v ostatních členských státech NATO a EU je přístup k UI umožněn pouze osobám, které jsou držiteli osvědčení pro příslušný stupeň utajení, jsou poučeny a přístup k UI nezbytně potřebují pro výkon své funkce. Stupně utajení jsou čtyři: DIFUSIÓN LIMITADA (VYHRAZENÉ), CONFIDENCIAL (DŮVĚRNÉ), RESERVADO (TAJNÉ), SECRETO (PŘÍSNĚ TAJNÉ).

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 národními 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 České republiky prosazeny v největší možné míře.

Vzhledem k tomu, že Španělské království je členským státem NATO, a tudíž i spojencem České republiky, a dále členem EU, je sjednání předložené Smlouvy plně v souladu se zahraničně-politickými zájmy České republiky.

Informace o souhlasném stanovisku španělské strany

Španělská strana s návrhem textu Smlouvy vyslovila souhlas bez výhrady.

Charakteristika smlouvou přejímaných závazků

Preambule

Preambule deklaruje přání smluvních stran zajistit vzájemnou ochranu vyměněných UI.

Článek 1 - Vymezení pojmů

V zájmu zajištění jednotného výkladu jsou pro účely Smlouvy definovány následující pojmy: „utajovaná informace", „utajovaná smlouva", „poskytující strana", „přijímající strana" a „třetí strana". Pro poskytující stranu byl použit anglický název *„Originating Party"*, který je významově mnohem širší, než běžně používaný *Releasing Party.* Dle našeho názoru je termín *„Originating Party"* použitelný jak v případech, kdy tato strana je původcem UI, tak i za situace, kdy předává UI třetí strany. Pro účely překladu byl použit termín poskytující strana.

Za UI je považována taková informace nebo materiál, který bez ohledu na svoji formu vyžaduje podle vnitrostátních právních předpisů některé ze smluvních stran ochranu proti vyzrazení, zneužití nebo ztrátě, a který byl jako utajovaný určen a náležitě označen. Rozsah neoprávněného nakládání vychází z *„Directive on the Security of Information AC/35-D/2002 Rev 3"* vydané NATO Office of Security.

Utajovanou smlouvou se rozumí smlouva, která obsahuje UI nebo v souvislosti s níž může dojít k přístupu k UI. V definici není explicitně stanoveno, že utajovaná smlouva musí být označena stupněm utajení, neboť pakliže tato bude obsahovat UI, bude se na ni vztahovat definice utajované informace.

Poskytující stranou je ta ze smluvních stran, která UI poskytuje. Přijímající stranou je ta ze smluvních stran, která UI přijme. Třetí stranou se rozumí stát nebo mezinárodní organizace, které nejsou smluvními stranami této Smlouvy.

Článek 2 – Stupně utajení a jejich rovnocennost

UI poskytnutá podle této Smlouvy se označí příslušným stupněm utajení v souladu s vnitrostátními právními předpisy států smluvních stran. Na základě úrovně ochrany, která je poskytována každou ze smluvních stran národním UI jednotlivých stupňů utajení, je dovozena jejich rovnocennost, která je vyjádřena v tabulce.

Článek 3 - Bezpečnostní úřady

V článku 3 jsou výslovně uvedeny bezpečnostní úřady, tj. orgány smluvních stran odpovědné za výkon státní správy v oblasti ochrany UI a k provádění této Smlouvy. V České republice je bezpečnostním úřadem Národní bezpečnostní úřad a ve Španělském království Secretario de Estado Director del Centro Nacional de Inteligencia - Oficina Nacional se Seguridad. Na explicitním uvedení těchto úřadů se delegace expertů shodly z několika důvodů.

Ve většině zemí se na výkonu státní správy v oblasti ochrany UI podílí více orgánů (zejména národní bezpečnostní úřady a zpravodajské služby). Tyto orgány mají navíc mnohdy složitou vnitřní strukturu a dělenou kompetenci. Proto je praktické jednoznačně určit orgán, který ponese ve vztahu k České republice odpovědnost za ochranu poskytnutých UI, bude plnit funkci kontaktního místa (*„point of contact"*) a vykonávat další činnosti spojené s prováděním Smlouvy.

Kromě toho 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.

Vzhledem k tomu, že ve Smlouvě nejsou uvedeny adresy bezpečnostních úřadů, je zde stanovena povinnost vzájemně se informovat o svých kontaktních údajích.

Článek 4 - 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 právních předpisů druhé smluvní strany mají mít přístup k UI.

Článek 5 - Omezení využití utajovaných informací

V souladu s principem kontroly původce nesmí být poskytnutá UI předána třetí straně bez předchozího písemného souhlasu poskytující strany. Přijímající strana dále může UI použít pouze k účelu, za kterým byla poskytnuta a v souladu s omezeními stanovenými poskytující stranou.

Článek 6 - Ochrana utajovaných informací

Článek stanoví základní principy, resp. základní povinnosti poskytující a přijímající strany, které mají zajistit ochranu UI.

Poskytující strana je povinna UI označit příslušným stupněm utajení podle vnitrostátních právních předpisů. Dále musí informovat přijímající stranu, že poskytnutá informace nebo materiál je UI, a že tato vyžaduje ochranu podle této Smlouvy. Účelem je, aby si přijímající strana byla vědoma, že se jedná o UI, jejíž ochrana je upravena touto Smlouvou. Poskytující strana může stanovit další podmínky, za kterých UI poskytne, nebo omezit nakládání s ní. Účelem je umožnit poskytující straně upravit rozsah ochrany takovým způsobem, který odpovídá konkrétním potřebám dané situace, a umožnit i v těchto případech jejich výměnu (např. přesné vymezení osob, které mohou mít přístup k UI, doba jejího povoleného využití). Aby byla poskytnuté UI zajištěna co největší míra ochrany a zároveň aby informace nebyla utajována po dobu delší, než je nezbytně nutné, stanovuje se poskytující straně notifikační povinnost vztahující se na pozdější změny stupňů utajení UI.

Základní povinností přijímající strany je zajistit poskytnuté UI úroveň ochrany srovnatelnou s tou, kterou jí poskytuje druhá smluvní strana. Srovnatelná úroveň ochrany UI vychází z rovnocennosti stupňů utajení (viz výše). Přijímající straně se stanovuje povinnost označit přijatou UI v souladu s článkem 2. Přijímající strana se dále zavazuje, že bez písemného souhlasu poskytující strany nebude měnit stupeň utajení, a tudíž ani úroveň ochrany, která je UI poskytována.

Článek 7 - Bezpečnostní spolupráce

Aby bylo možné zajistit srovnatelnou úroveň ochrany UI poskytovaných na základě této Smlouvy, bezpečnostní úřady smluvních stran se informují o předpisech upravujících ochranu UI, uplatňovaných postupech a zkušenostech získaných při jejich provádění. Za účelem umožnění kontroly bezpečnostních opatření přijatých k ochraně poskytnutých UI mohou bezpečnostní úřady provádět vzájemné návštěvy. Bezpečnostním úřadům se dále stanovuje vzájemná notifikační povinnost o všech aktuálních hrozbách, které by mohly ohrozit poskytnutou UI.

V průběhu bezpečnostního řízení může vzniknout potřeba dožádat informace týkající se účastníka řízení od bezpečnostního úřadu cizí moci. Z tohoto důvodu se

stanovuje na základě žádosti a v souladu s vnitrostátními právními předpisy povinnost spolupráce 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. 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.

Smluvní strany se dále zavazují, že si budou uznávat osvědčení fyzických osob a podnikatelů za předpokladu reciprocity a splnění formálních požadavků stanovených vnitrostátními právními předpisy. Účelem tohoto ustanovení je usnadnit mobilitu fyzických osob, které jsou oprávněny k přístupu k UI a podporovat rozvoj obchodních vztahů mezi smluvními státy, které předpokládají nebo při kterých dochází k výměně UI. Uznávání předpokládá a formální požadavky, které musí být splněny, stanoví § 62 zákona č. 412/2005 Sb.

V souvislosti s uznáváním osvědčení fyzických osob nebo podnikatelů se bezpečnostním úřadům stanovuje notifikační povinnost o změnách týkajících se vzájemně uznaných osvědčení (zejména v případech zrušení nebo uplynutí doby jejich platnosti).

Bezpečnostní úřady se dále na vyžádání vzájemně informují o tom, zda-li podnikatel nebo fyzická osoba, která se podílí na sjednání nebo implementaci utajované smlouvy je držitelem osvědčení pro přístup k UI příslušného stupně utajení, tj. o jejich bezpečnostním statutu.

Za účelem usnadnění komunikace mezi smluvními stranami bylo stanoveno, že spolupráce podle této Smlouvy bude probíhat v jazyce anglickém.

Článek 8 - Utajované smlouvy

Hospodářské vztahy, při kterých vznikají UI nebo dochází k jejich výměně, předpokládají uzavírání smluv, které jsou označeny jako utajované. Smluvní strana, která zamýšlí uzavřít utajovanou smlouvu s kontrahentem druhé smluvní strany obdrží na základě žádosti písemné ujištění od bezpečnostního úřadu, že tento je držitelem osvědčení podnikatele pro příslušný stupeň utajení.

Utajované smlouvy musí v zájmu zajištění odpovídající ochrany UI, jejichž výměnu nebo zpracovávání předpokládají, obsahovat příslušnou bezpečnostní sekci. Tato určí jaké UI budou poskytnuty nebo vzniknou v rámci plnění utajované smlouvy, stanoví stupně jejich utajení a dále konkrétní bezpečnostní procedury (způsob komunikace změn stupňů utajení, způsob přepravy UI atd.).

Aby bylo možné zajistit kontrolu ochrany UI, kopie bezpečnostních sekcí všech utajovaných smluv se zasílá bezpečnostnímu úřadu té ze smluvních stran, na jejímž území bude utajovaná smlouva prováděna.

Všichni sub-kontrahenti musí splňovat stejné bezpečnostní požadavky jako kontrahenti. Toto ustanovení upravuje subdodavatelské vztahy pouze v rámci utajované smlouvy, kterou se, v souladu s článkem 1 – Vymezení pojmů, rozumí smlouva obsahující utajovanou informaci, nebo v souvislosti s níž může k seznámení se s utajovanou informací dojít.

Článek 9 - Předávání utajovaných informací

Pokud se bezpečnostní úřady nedohodnou jinak, předávání UI mezi smluvními stranami se děje diplomatickou cestou prostřednictvím ústředních registrů. Pro předání UI lze, v případě že to požaduje poskytující strana, použít kurýra, který je k výkonu kurýrní činnosti oprávněn v souladu s vnitrostátními právními předpisy a je vybaven kurýrním listem.

Každá přeprava rozměrné UI nebo velkého množství UI podléhá schválení bezpečnostních úřadů. Schválení podléhají i bezpečnostní postupy pro předávání UI elektronickou cestou.

Článek 10 - Překlad, reprodukce a zničení

V tomto článku jsou stanoveny postupy při vyhotovování překladů a reprodukcí UI nebo při ničení UI.

Překlady i reprodukce UI musí být označeny příslušným stupněm utajení a musí jim být poskytnuta stejná úroveň ochrany jako původní UI. Vyhotovení překladů a počet vyhotovených reprodukcí je omezen účelem, za kterým je jejich vyhotovení požadováno. Překlad musí být opatřen poznámkou v jazyce překladu, která vysvětluje, že tento obsahuje UI druhé smluvní strany. Účelem předmětného ustanovení je zajistit, že z UI je zřejmé, kdo je poskytující stranou, a tedy podle jaké právní úpravy se nakládání s touto UI řídí (např. Smlouva).

V souladu s principem kontroly původce lze překlad nebo reprodukci UI stupně utajení PŘÍSNĚ TAJNÉ/SECRETO vyhotovit pouze na základě písemného souhlasu bezpečnostního úřadu poskytující strany. Toto ustanovení je plně v souladu s ustanovením § 21 odst. 6 zákona č. 412/2005 Sb.

UI do stupně utajení DŮVĚRNÉ/CONFIDENCIAL lze zničit v souladu s vnitrostátními právními předpisy přijímající strany. Před zničením UI stupně utajení TAJNÉ/RESERVADO je nutný předchozí písemný souhlas poskytující strany. UI stupně utajení PŘÍSNĚ TAJNÉ/SECRETO nesmí být zničena a musí být vrácena bezpečnostnímu úřadu poskytující strany.

Článek 11 - Návštěvy

Režim návštěv je standardní procedurou vycházející z bezpečnostních předpisů NATO, která zjednodušuje spolupráci předpokládající poskytování UI mezi ústředními orgány státní správy, ozbrojenými silami nebo pracovníky společností participujícími na utajovaných smlouvách. Cílem je zajistit, že přístup k UI bude umožněn toliko osobám, které jsou držiteli 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.

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

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.

Žádost o povolení návštěvy se podává prostřednictvím bezpečnostních úřadů alespoň dvacet dnů před jejím zahájením. V naléhavých případech může být žádost o povolení návštěvy podána ve lhůtě pěti dní.

Žádost o povolení návštěvy obsahuje:

- jméno a příjmení návštěvníka, místo a datum narození, státní občanství, číslo pasu nebo průkazu totožnosti;
- pracovní zařazení návštěvníka a určení subjektu, který zastupuje;
- stupeň utajení, pro který bylo návštěvníkovi osvědčení fyzické osoby vydáno včetně data ukončení jeho platnosti;
- datum a délku návštěvy. V případě opakované návštěvy se uvede její celková délka;
- účel návštěvy včetně nejvyššího stupně utajení informací, ke kterým bude přístup vyžadován;
- název, adresu, telefonní/faxové číslo, e-mailovou adresu a kontaktní osobu subjektu, který bude navštíven;
- datum, podpis a otisk úředního razítka bezpečnostního úřadu.

Návštěva se povoluje na období, které nepřesáhne dvanáct měsíců. Předpokládá-li se, že délka návštěvy tuto dobu překročí, předkládá se žádost nová.

Veškeré UI zpřístupněné návštěvníkovi při takové návštěvě se považují za poskytnuté podle této Smlouvy, a proto je jim třeba zajistit odpovídající ochranu.

Článek 12 - Bezpečnostní incidenty

Prvořadým cílem Smlouvy je zajistit odpovídající ochranu UI, které si smluvní strany vymění. V případě bezpečnostního incidentu, při kterém dojde ke ztrátě, zneužití nebo vyzrazení poskytnuté utajované informace, nebo vyskytne-li se podezření na takový incident, bezpečnostnímu úřadu přijímající strany se stanovuje písemná notifikační povinnost bezpečnostnímu úřadu poskytující strany a dále povinnost zajistit vyšetření tohoto incidentu. Rozsah událostí nebo jednání, který je třeba druhé smluvní straně oznamovat, je vymezen škodlivým následkem.

Pokud je to vyžadováno (ať již poskytující nebo přijímající stranou), poskytující smluvní strana spolupracuje při vyšetřování. Poskytující strana je vždy informována o okolnostech bezpečnostního incidentu, vzniklé škodě, opatřeních přijatých za účelem jejího zmírnění a výsledku vyšetřování.

Článek 13 - Náklady

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

Článek 14 - Výklad a řešení sporů

Spory vzniklé při výkladu či provádění této Smlouvy budou řešeny cestou jednání smluvních stran. Tím je vyloučeno zejména soudní nebo rozhodčí řízení, v jejichž průběhu by mohlo dojít k ohrožení ochrany UI, které se to týká.

Článek 15 – Závěrečná ustanovení

Tato Smlouva se sjednává na dobu neurčitou. Vstoupí v platnost první den druhého měsíce po doručení pozdějšího z oznámení mezi smluvními stranami diplomatickou cestou informujících o tom, že byly splněny všechny vnitrostátní právní podmínky pro vstup této Smlouvy v platnost. Všem utajovaným informacím vyměněným před vstupem této Smlouvy v platnost bude poskytnuta ochrana v souladu s ustanoveními této Smlouvy.

Smlouva může být změněna po vzájemném písemném souhlasu smluvních stran. Tato změna vstupuje v platnost dnem doručení pozdějšího z písemných oznámení diplomatickou cestou mezi smluvními stranami informujících o tom, že byly splněny všechny vnitrostátní právní podmínky pro její vstup v platnost.

Každá ze smluvních stran má možnost tuto Smlouvu vypovědět písemným oznámením druhé smluvní straně. Platnost Smlouvy je ukončena 6 měsíců po dni kdy bylo písemné oznámení o vypovězení Smlouvy doručeno druhé smluvní straně. Aby byla zajištěna ochrana poskytnutých nebo vytvořených UI i po ukončení platnosti Smlouvy, smluvní strany se zavazují poskytovat jim nadále ochranu v souladu s touto Smlouvou dokud poskytující strana nezprostí přijímající stranu této povinnosti.

Smlouva je sjednávána v jazyce smluvních stran a v jazyce anglickém s tím, že anglické znění je rozhodné.

Zajištění provádění smlouvy

Odpovědnost za implementaci této Smlouvy mají v České republice Národní bezpečnostní úřad a ve Španělsku Secretario de Estado Director del Centro Nacional de Inteligencia - Oficina Nacional de Seguridad. Obě instituce jsou ve Smlouvě uvedeny jako bezpečnostní úřady a jejich funkce je jasně definována.

Dopad na státní rozpočet

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

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

Navrhovaný text Smlouvy je v souladu s ústavním pořádkem, s ostatními součástmi právního řádu České republiky a mezinárodními závazky ČR (včetně práva EU a bezpečnostních standardů NATO). Z právních předpisů EU se jedná zejména o rozhodnutí Rady EU 2001/264/ES ze dne 19. března 2001, ve znění pozdějších rozhodnutí (2004/194/ES ze dne 10. února 2004, 2005/571/ES ze dne 12. července 2005 a 2005/952/ES ze dne 20. prosince 2005), kterým byly přijaty bezpečnostní předpisy Rady a dále rozhodnutí Komise 2001/844/ES ze dne 29. listopadu 2001, ve znění pozdějších rozhodnutí (2005/94/ES, Euratom ze dne 3. února 2005, 2006/70/ES, Euratom ze dne 31. ledna 2006 a 2006/548/EC, Euratom ze dne 2. srpna 2006), které novelizovalo její jednací řád. 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.

V obou státech je smlouva sjednávána jako smlouva nejvyšší právní síly. Z tohoto důvodu nese všechny znaky smlouvy prezidentské. Na výslovnou žádost španělské strany nebyly do smlouvy vloženy ratifikační klauzule.

Vláda vyslovila se sjednáním Smlouvy souhlas svým usnesením č. 720 ze dne 27. června 2007.

Smlouva byla podepsána v Madridu dne 8. října 2009 ředitelem Národního bezpečnostního úřadu Ing. Dušanem Navrátilem a Félixem Sanz Roldánem, tajemníkem státního ředitele Národního zpravodajského centra (*Centro Nacional de Inteligencia).*

Senát Parlamentu České republiky vyslovil s ratifikací smlouvy souhlas svým usnesením č. 408 ze dne 18. března 2010. Vzhledem k tomu, že Poslanecká sněmovna Parlamentu České republiky neprojednala návrh během 5. volebního období, je z důvodu diskontinutity tento návrh předkládán Parlamentu České republiky znovu.

V Praze dne 13. října 2010

RNDr. Petr Nečas, v.r.
předseda vlády

SMLOUVA

MEZI

ČESKOU REPUBLIKOU

A

ŠPANĚLSKÝM KRÁLOVSTVÍM

O VÝMĚNĚ

A VZÁJEMNÉ OCHRANĚ

UTAJOVANÝCH INFORMACÍ

Česká republika a Španělské království (dále jen „smluvní strany"), přejíce si zajistit ochranu utajovaných informací vyměněných mezi nimi, se v zájmu své národní bezpečnosti dohodly takto:

ČLÁNEK 1
VYMEZENÍ POJMŮ

Pro účely této Smlouvy jsou vymezeny následující pojmy:

a) **„Utajovanou informací"** se rozumí informace nebo materiál, který podle vnitrostátních právních předpisů některé ze smluvních stran vyžaduje ochranu proti vyzrazení, zneužití nebo ztrátě, a který byl jako takový určen a náležitě označen bez ohledu na svoji formu.

b) **„Utajovanou smlouvou"** se rozumí smlouva, která obsahuje utajovanou informaci, nebo v souvislosti s níž může k přístupu k utajované informaci dojít.

c) **„Poskytující stranou"** se rozumí smluvní strana, která poskytne utajovanou informaci druhé smluvní straně.

d) **„Přijímající stranou"** se rozumí smluvní strana, která přijme utajovanou informaci od poskytující strany.

e) **„Třetí stranou"** se rozumí stát nebo mezinárodní organizace, která není smluvní stranou této Smlouvy.

ČLÁNEK 2
STUPNĚ UTAJENÍ A JEJICH ROVNOCENNOST

Rovnocennost stupňů utajení je následující:

V České republice	Ve Španělském království
PŘÍSNĚ TAJNÉ	SECRETO
TAJNÉ	RESERVADO
DŮVĚRNÉ	CONFIDENCIAL
VYHRAZENÉ	DIFUSIÓN LIMITADA

ČLÁNEK 3
BEZPEČNOSTNÍ ÚŘADY

1. Bezpečnostními úřady odpovědnými za provádění této Smlouvy jsou:

   V České republice:
   Národní bezpečnostní úřad

   Ve Španělském království:
   Secretario de Estado Director del Centro Nacional de Inteligencia (CNI)
   Oficina Nacional de Seguridad

2. Bezpečnostní úřady si vzájemně poskytnou oficiální kontaktní údaje.

ČLÁNEK 4
PŘÍSTUP K UTAJOVANÝM INFORMACÍM

Přístup k utajovaným informacím poskytnutým na základě této Smlouvy lze umožnit pouze osobám k tomu oprávněným podle vnitrostátních právních předpisů příslušné smluvní strany.

ČLÁNEK 5
OMEZENÍ POUŽITÍ UTAJOVANÝCH INFORMACÍ

1. Přijímající strana nezveřejní nebo neposkytne přijatou utajovanou informaci třetí straně bez předchozího písemného povolení bezpečnostního úřadu poskytující strany.

2. Přijímací strana použije přijatou utajovanou informaci pouze k účelu, za kterým byla poskytnuta, a v souladu s omezeními stanovenými poskytující stranou.

ČLÁNEK 6
OCHRANA UTAJOVANÝCH INFORMACÍ

1. Poskytující strana:

   a) zajistí označení utajované informace příslušným stupněm utajení v souladu s vnitrostátními právními předpisy;

   b) informuje přijímající stranu, že poskytnutá informace nebo materiál je utajovanou informací a vyžaduje ochranu podle této Smlouvy;

   c) informuje přijímající stranu o podmínkách poskytnutí utajované informace a omezeních při nakládání s ní;

   d) informuje přijímající stranu o následných změnách stupně utajení.

2. Přijímající strana:

   a) poskytne, v souladu se svými vnitrostátními právními předpisy, utajované informaci rovnocennou úroveň ochrany jako poskytující strana;

   b) zajistí označení přijaté utajované informace rovnocenným stupněm utajení v souladu s článkem 2 této Smlouvy;

   c) zajistí, že stupeň utajení nebude bez písemného souhlasu poskytující strany změněn.

ČLÁNEK 7
BEZPEČNOSTNÍ SPOLUPRÁCE

1. Bezpečnostní úřady mohou provádět vzájemné návštěvy za účelem ověření bezpečnostních opatření použitých při ochraně poskytnutých utajovaných informací a na požádání se informují o vnitrostátních právních předpisech upravujících ochranu utajovaných informací, o uplatňovaných postupech a zkušenostech získaných při jejich ochraně.

2. Pokud jsou splněny procesní podmínky stanovené vnitrostátními právními předpisy, smluvní strany si vzájemně uznají osvědčení fyzických osob a osvědčení podnikatelů. Článek 2 této Smlouvy se použije obdobně.

3. Bezpečnostní úřady si bezodkladně oznámí všechny změny týkající se vzájemně uznaných osvědčení fyzických osob a osvědčení podnikatelů.

4. Na základě žádosti se bezpečnostní úřady informují o bezpečnostním statusu podnikatelů usazených na území druhé smluvní strany a fyzických osob, které se podílejí na sjednávání nebo provádění utajovaných smluv.

5. Bezpečnostní úřady si na vyžádání a v souladu s příslušnými vnitrostátními právními předpisy poskytnou součinnost při provádění bezpečnostních řízení o vydání osvědčení fyzické osoby a osvědčení podnikatele.

6. Bezpečnostní úřady se informují o aktuálních bezpečnostních rizicích, která mohou ohrozit poskytnutou utajovanou informaci.

7. Spolupráce podle této Smlouvy bude uskutečňována v jazyce anglickém.

ČLÁNEK 8
UTAJOVANÉ SMLOUVY

1. Smluvní strana, která zamýšlí uzavřít utajovanou smlouvu s kontrahentem druhé smluvní strany, obdrží na základě žádosti písemné ujištění bezpečnostního úřadu druhé smluvní strany, že navrhovaný kontrahent je držitelem osvědčení podnikatele pro příslušný stupeň utajení.

2. Utajovaná smlouva uzavřená mezi smluvními stranami v souladu s ustanoveními této Smlouvy obsahuje příslušnou bezpečnostní sekci, která určí následující:

   a) seznam utajovaných informací a směrnici pro stanovení jejich stupně utajení;

   b) postup pro sdělování změn stupňů utajení;

   c) způsob komunikace a prostředky elektromagnetického přenosu;

   d) postup pro předávání utajovaných informací;

   e) příslušné úřady odpovědné za koordinaci ochrany utajovaných informací týkajících se utajované smlouvy;

   f) oznamovací povinnost v případě vyzrazení, zneužití nebo ztráty utajované informace, nebo vyskytne-li se takové podezření.

3. Sub-kontrahent musí splňovat stejné bezpečnostní požadavky jako kontrahent.

4. Kopie bezpečnostní sekce utajované smlouvy se zasílá bezpečnostnímu úřadu smluvní strany, kde bude utajovaná smlouva prováděna, za účelem zajištění státního dozoru.

ČLÁNEK 9
PŘEDÁVÁNÍ UTAJOVANÝCH INFORMACÍ

1. Utajované informace jsou předávány diplomatickou cestou, pokud se bezpečnostní úřady nedohodnou jinak.

2. Pokud to požaduje poskytující strana, utajovanou informaci lze předat prostřednictvím kurýrů k tomu oprávněných v souladu s jejími vnitrostátními právními předpisy a vybavených kurýrním listem příslušného bezpečnostního úřadu.

3. Každá přeprava rozměrné utajované informace nebo velkého množství utajovaných informací podléhá schválení bezpečnostními úřady.

4. Smluvní strany si utajovanou informaci mohou předávat elektronicky v souladu s bezpečnostními postupy schválenými bezpečnostními úřady.

ČLÁNEK 10
PŘEKLAD, REPRODUKCE A ZNIČENÍ

1. Překlady a reprodukce utajované informace lze vyhotovit v souladu s následujícími pravidly:

a) překlady a reprodukce musí být označeny stejným způsobem jako původní utajovaná informace a musí být jim poskytnuta stejná úroveň ochrany;

b) vyhotovení překladů a počet reprodukcí musí být omezen požadovaným účelem;

c) překlad musí být opatřen vhodnou poznámkou v jazyce překladu, ze které je zřejmé, že obsahuje utajovanou informaci poskytující strany.

2. Překlad nebo reprodukci utajované informace stupně utajení PŘÍSNĚ TAJNÉ/ SECRETO lze vyhotovit pouze na základě písemného souhlasu bezpečnostního úřadu poskytující strany.

3. Utajovaná informace stupně utajení PŘÍSNĚ TAJNÉ/SECRETO nesmí být zničena a musí být vrácena bezpečnostnímu úřadu poskytující strany.

4. Zničení utajované informace stupně utajení TAJNÉ/RESERVADO je možné s předchozím písemným souhlasem poskytující strany.

5. Při zničení utajované informace do stupně utajení DŮVĚRNÉ/CONFIDENCIAL se postupuje v souladu s vnitrostátními právními předpisy přijímající strany.

ČLÁNEK 11
NÁVŠTĚVY

1. Návštěvy vyžadující přístup k utajovaným informacím podléhají předchozímu písemnému povolení příslušným bezpečnostním úřadem.

2. Žádost o povolení návštěvy je zaslána prostřednictvím bezpečnostních úřadů nejméně dvacet (20) dnů před jejím zahájením a obsahuje:

a) jméno a příjmení návštěvníka, místo a datum narození, státní občanství, číslo pasu nebo průkazu totožnosti;

b) pracovní zařazení návštěvníka a určení subjektu, který zastupuje;

c) stupeň utajení, pro který bylo návštěvníkovi osvědčení fyzické osoby vydáno včetně data ukončení jeho platnosti;

d) datum a délku návštěvy. V případě opakované návštěvy se uvede její 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 kontaktní osobu subjektu, který bude navštíven;

g) datum, podpis a otisk úředního razítka bezpečnostního úřadu.

3. V naléhavých případech může být žádost o povolení návštěvy předložena alespoň pět (5) dnů před jejím zahájením.

4. Návštěva se povoluje na období nepřesahující dvanáct (12) měsíců. Předpokládá-li se, že určitá návštěva přesáhne období dvanácti (12) měsíců, předkládá se nová žádost.

5. Jakákoliv utajovaná informace zpřístupněná návštěvníkovi se považuje za utajovanou informaci poskytnutou podle této Smlouvy.

ČLÁNEK 12
BEZPEČNOSTNÍ INCIDENTY

1. V případě bezpečnostního incidentu, při kterém dojde ke ztrátě, zneužití nebo vyzrazení utajované informace poskytnuté podle této Smlouvy, nebo vyskytne-li se podezření, že k takovému incidentu došlo, bezpečnostní úřad přijímající strany o tom bezodkladně písemně informuje bezpečnostní úřad poskytující strany. Pokud je to vyžadováno, poskytující strana spolupracuje při vyšetřování.

2. Přijímající strana vždy písemně informuje poskytující stranu o okolnostech bezpečnostního incidentu, vzniklé škodě, opatřeních přijatých pro její zmírnění a výsledku vyšetřování.

ČLÁNEK 13
NÁKLADY

Smluvní strany si hradí náklady vzniklé v souvislosti s prováděním této Smlouvy samy.

ČLÁNEK 14
VÝKLAD A ŘEŠENÍ SPORŮ

Jakýkoliv spor týkající se výkladu nebo provádění této Smlouvy bude řešen jednáním mezi smluvními stranami.

ČLÁNEK 15
ZÁVĚREČNÁ USTANOVENÍ

1. Tato Smlouva se sjednává na dobu neurčitou. Vstoupí v platnost první den druhého měsíce po doručení pozdějšího z oznámení mezi smluvními stranami diplomatickou cestou informujících o tom, že byly splněny všechny vnitrostátní právní podmínky pro vstup této Smlouvy v platnost. Všem utajovaným informacím

vyměněným před vstupem této Smlouvy v platnost bude poskytnuta ochrana v souladu s ustanoveními této Smlouvy

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 písemně vypovědět. V takovém případě platnost Smlouvy skončí šest (6) měsíců po dni, kdy bylo písemné oznámení o vypovězení Smlouvy doručeno druhé smluvní straně

4 Bez ohledu na ukončení platnosti této Smlouvy bude veškerým utajovaným informacím poskytnutým nebo vytvořeným podle této Smlouvy zajištěna ochrana v souladu s ustanoveními této Smlouvy do doby, než poskytující strana zprostí přijímající stranu této povinnosti.

Dáno v Madridu dne 8. října 2009
ve dvou původních vyhotoveních, každé z nich v českém, španělském a anglickém jazyce, přičemž všechna znění jsou stejně autentická. V případě rozdílnosti ve výkladu je rozhodující znění v jazyce anglickém.

Za Českou republiku

Za Španělské království

AGREEMENT

BETWEEN

THE CZECH REPUBLIC

AND

THE KINGDOM OF SPAIN

ON THE EXCHANGE

AND MUTUAL PROTECTION

OF CLASSIFIED INFORMATION

The Czech Republic and the Kingdom of Spain (hereafter referred to as "the Parties"), wishing to ensure the protection of Classified Information exchanged between them, have agreed in the interests of their national security on the following:

ARTICLE 1
DEFINITIONS

For the purpose of this Agreement the following terms are defined.

a) **"Classified Information"** means any information or material that, under national laws and regulations of either Party, requires protection against unauthorised disclosure, misappropriation or loss, and has been designated as such and appropriately marked, regardless of its form.

b) **"Classified Contract"** means an agreement that contains or involves access to Classified Information.

c) **"Originating Party"** means the Party, which releases Classified Information to the other Party.

d) **"Recipient Party"** means the Party, which receives Classified Information from the Originating Party.

e) **"Third Party"** means any state or international organisation that is not a party to this Agreement.

ARTICLE 2
SECURITY CLASSIFICATIONS AND EQUIVALENCE

The security classifications markings and their equivalents are as follows:

In the Czech Republic	In the Kingdom of Spain
PŘÍSNĚ TAJNÉ	SECRETO
TAJNÉ	RESERVADO
DŮVĚRNÉ	CONFIDENCIAL
VYHRAZENÉ	DIFUSIÓN LIMITADA

ARTICLE 3
SECURITY AUTHORITIES

1. The Security Authorities responsible for the implementation of this Agreement are:

   In the Czech Republic:

   Národní bezpečnostní úřad

   In the Kingdom of Spain:

   Secretario de Estado Director del Centro Nacional de Inteligencia (CNI)
   Oficina Nacional de Seguridad

2. The Security Authorities shall provide each other with their official contact details.

ARTICLE 4
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 respective Party.

ARTICLE 5
RESTRICTIONS ON USE OF CLASSIFIED INFORMATION

1. The Recipient Party shall not release or disclose the received Classified Information to a Third Party without the prior written authorisation of the Security Authority of the Originating Party.

2. The Recipient Party shall use received Classified Information only for the purpose it has been released for and within the limitations stated by the Originating Party.

ARTICLE 6
PROTECTION OF CLASSIFIED INFORMATION

1. The Originating Party shall:

   a) ensure that Classified Information is marked with an appropriate security classification markings in accordance with national laws and regulations;

   b) inform the Recipient Party that information or material released is Classified Information and requires protection under this Agreement;

   c) inform the Recipient Party of any conditions of release and limitations on its use;

d) inform the Recipient Party of any subsequent changes in classifications.

2. The Recipient Party shall.

a) in accordance with its national laws and regulations afford the equivalent level of protection to Classified Information as afforded by the Originating Party;

b) ensure that received Classified Information is marked with equivalent security classification markings in accordance with Article 2 of this Agreement;

c) ensure that classifications are not altered, except if authorised in writing by the Originating Party.

ARTICLE 7
SECURITY CO-OPERATION

1. The Security Authorities may conduct reciprocal visits in order to check security arrangements applied for the protection of released Classified Information and shall, on request, inform each other about their security standards, procedures and practices for the protection of Classified Information.

2. Subject to procedural requirements laid down in national laws and regulations, the Parties shall mutually recognise their respective Personnel and Facility Security Clearances. The Article 2 of this Agreement shall apply accordingly.

3. The Security Authorities shall promptly notify each other about any changes in mutually recognised Personnel and Facility Security Clearances.

4. On request, the Security Authorities shall notify each other about the security status of facilities residing in the territory of the other Party and individuals participating in pre-contractual negotiations or Classified Contracts.

5. On request, the Security Authorities shall, within the scope of their respective national laws and regulations, assist each other during the Personnel and Facility Security Clearance procedures.

6. The Security Authorities shall inform each other about current security risks that may endanger released Classified Information.

7. The co-operation under this Agreement shall be effected in English language.

ARTICLE 8
CLASSIFIED CONTRACTS

1. The Party wishing to place a Classified Contract with a contractor of the other Party shall obtain upon request a prior written assurance from the Security Authority of the other Party that the proposed contractor holds a Facility Security Clearance of an appropriate level.

2. Every Classified Contract concluded between the Parties, under the provisions of this Agreement, shall include an appropriate security section identifying the following aspects:

    a) Classification guide and list of Classified Information;

    b) Procedure for the communication of changes in the security classifications;

    c) Communication channels and means for electromagnetic transmission;

    d) Procedure for the transmission of Classified Information;

    e) Relevant authorities responsible for the co-ordination of the protection of Classified Information related to the Classified Contract;

    f) An obligation to notify any actual or suspected unauthorised disclosure, misappropriation or loss of Classified Information.

3. Any subcontractor shall fulfil the same security obligations as the contractor

4. A copy of the security section of Classified Contract shall be forwarded to the Security Authority of the Party where the Classified Contract is to be performed to allow adequate security control.

ARTICLE 9
TRANSMISSION OF CLASSIFIED INFORMATION

1. Unless otherwise agreed by the Security Authorities, Classified Information shall be transmitted through diplomatic channels.

2. If required by the Originating Party, transmissions may be undertaken by couriers duly authorised in accordance with its national laws and regulations and furnished with a courier certificate issued by the respective Security Authority.

3. Delivery of large items or quantities of Classified Information arranged on case-by-case basis shall be approved by the Security Authorities.

4. The Parties may transmit Classified Information by electronic means in accordance with security procedures approved by the Security Authorities.

ARTICLE 10
TRANSLATION, REPRODUCTION AND DESTRUCTION

1. Translations and reproductions of Classified Information shall be made in accordance with the following rules:

    a) The translations and the reproductions shall be marked and afforded the same protection as the original Classified Information;

    b) The translations and the number of reproductions shall be limited to that required for official purposes;

    c) The translations shall bear an appropriate note in the language of translation indicating that it contains Classified Information received from the Originating Party.

2. Classified Information marked as PŘÍSNĚ TAJNÉ/SECRETO shall be translated or reproduced only upon the written permission of the Security Authority of the Originating Party.

3. Classified Information marked as PŘÍSNĚ TAJNÉ/SECRETO shall not be destroyed and shall be returned to the Security Authority of the Originating Party.

4. Classified Information marked as TAJNÉ/RESERVADO shall be destroyed with prior written approval of the Originating Party.

5. Classified Information marked up to DŮVĚRNÉ/CONFIDENCIAL shall be destroyed in accordance with national laws and regulations of the Recipient Party.

ARTICLE 11
VISITS

1. Visits entailing access to Classified Information are subject to prior written authorisation given by the respective Security Authority.

2. Request for Visit shall be submitted through Security Authorities at least twenty (20) days before visit and shall include:

    a) First and last name of the visitor, date and place of birth, nationality and passport/ID card number;

    b) Official position of the visitor and specification of the facility, which the visitor represents;

    c) Level of the Personnel Security Clearance of the visitor and date of expiry of the Personnel Security Clearance;

d) Date and duration of the visit, in case of recurring visit 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 point of contact of the facility to be visited;

g) Date, signature and stamping of the official seal of the Security Authority.

3. In urgent cases, the Request for Visit may be submitted at least five (5) working days before the date of the visit.

4. The Request for Visit shall be approved for a period of time not exceeding twelve (12) months. When it is expected that a particular visit shall exceed twelve (12) months, a new Request for Visit shall be submitted.

5. Any Classified Information acquired by a visitor shall be considered as Classified Information released under this Agreement.

ARTICLE 12
BREACHES OF SECURITY

1. In the event of a breach of security resulting in loss, misappropriation or unauthorised disclosure of Classified Information released under this Agreement, or suspicion of such a breach, the Security Authority of the Recipient Party shall immediately inform the Security Authority of the Originating Party in writing. The Originating Party shall, if required, co-operate in the investigation.

2. In any case, the Recipient Party shall inform the Originating 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 13
EXPENSES

Each of the Parties shall bear its own expenses incurred in the course of the implementation of this Agreement.

ARTICLE 14
INTERPRETATION AND DISPUTES

Any dispute regarding the interpretation or application of this Agreement shall be settled by negotiation between the Parties.

ARTICLE 15
FINAL PROVISIONS

1. This Agreement is concluded for an indefinite period of time. This Agreement 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. All Classified Information exchanged before this Agreement enters into force shall be protected in compliance with its provisions.

2. This Agreement may be amended on the basis of the 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 denounce this Agreement in writing. In such case, the validity of this Agreement shall expire after six (6) months following the day on which the other Party receives the written notice of the denunciation.

4. Regardless of the denounce of this Agreement, all Classified Information released or generated pursuant to this Agreement shall be protected in accordance with the provisions set forth herein until the Originating Party dispenses the Recipient Party from this obligation.

Done in Madrid on 8 October 2009 in two originals, each one in the Czech, Spanish and English language, all texts being equally authentic. In case of different interpretation the English text of this Agreement shall prevail.

For the Czech Republic

For the Kingdom of Spain