Sveriges internationella överenskommelser

ISSN 1102-3716

Utgiven av utrikesdepartementet

SÖ 2014:22

Nr 22
Avtal med republiken Kroatiens regering om utbyte och ömsesidigt skydd av säkerhetsskyddsklassificerade uppgifter Zagreb den 14 januari 2014

Regeringen beslutade den 18 april 2013 att ingå avtalet. Avtalet trädde i kraft efter notväxling den 1 oktober 2014.

AVTAL MELLAN KONUNGARIKET SVERIGES REGERING OCH REPUBLIKEN KROATIENS REGERING OM UTBYTE OCH ÖMSESIDIGT SKYDD AV SÄKERHETSSKYDDSKLASSIFICERADE UPPGIFTER

Konungariket Sveriges regering och Republiken Kroatiens regering (nedan kallade *parterna*) har,

med hänsyn till rikets säkerhet och i syfte att trygga skyddet av säkerhetsskyddsklassificerade uppgifter som utbyts mellan dem,

kommit överens om följande.

ARTIKEL 1
DEFINITIONER

I detta avtal gäller följande definitioner:

1. *säkerhetsskyddsklassificerad uppgift*: uppgift som oavsett form och som enligt endera partens lagstiftning kräver skydd mot förlust, otillåtet röjande eller annan blottläggning och som har klassificerats som sådan och som utbyts mellan eller genereras av parterna.

2. *ursprungspart*: den part, inklusive alla offentliga och privata aktörer inom dess jurisdiktion, som lämnar ut de säkerhetsskyddsklassificerade uppgifterna till den andra parten.

3. *mottagande part*: den part, inklusive alla offentliga och privata aktörer inom dess jurisdiktion, som tar emot de säkerhetsskyddsklassificerade uppgifterna från den andra parten.

4. *säkerhetsskyddsklassificerat kontrakt*: ett kontrakt som innehåller eller inbegriper säkerhetsskyddsklassificerade uppgifter.

5. *principen om behovsgrundad behörighet*: en princip som innebär att en enskild person kan få ta del av säkerhetsskyddsklassificerade uppgifter för att kunna utföra sitt arbete.

6. *röjande*: alla former av missbruk, skada eller obehörig åtkomst, förvanskning, utlämnande eller förstöring av säkerhetsskyddsklassificerade uppgifter, samt annan handling eller underlåtenhet, som leder till sekretessbrott, förlust av okränkbarheten eller tillgängligheten.

7. *försvarsmyndigheter*: myndigheter i Konungariket Sverige för vilka Försvarsmaktens föreskrifter om säkerhetsskydd gäller.

8. *andra myndigheter*: myndigheter i Konungariket Sverige för vilka Rikspolisstyrelsens föreskrifter om säkerhetsskydd gäller.

ARTIKEL 2
SÄKERHETSSKYDDSKLASSIFICERINGAR

1. De nationella säkerhetsskyddsmarkeringarna motsvarar varandra enligt följande:

I Republiken Kroatien	I Konungariket Sverige	
	Försvarsmyndigheter	Andra myndigheter
VRLO TAJNO	HEMLIG/ TOP SECRET	HEMLIG AV SYNNERLIG BETYDELSE FÖR RIKETS SÄKERHET
TAJNO	HEMLIG/SECRET	HEMLIG
POVJERLJIVO	HEMLIG/ CONFIDENTIAL	–
OGRANIČENO	HEMLIG/ RESTRICTED	–

2. Uppgifter från Konungariket Sverige som endast bär markeringen HEMLIG ska behandlas som TAJNO i Republiken Kroatien om inte ursprungsparten begär något annat.

3. Information från Republiken Kroatien som bär beteckningen POVJERLJIVO eller OGRANIČENO ska behandlas som HEMLIG av andra myndigheter i Konungariket Sverige om inte ursprungsparten begär något annat.

4. Ursprungsparten ska utan dröjsmål meddela den mottagande parten om säkerhetsskyddsklassificeringen ändras för de utlämnade säkerhetsskyddsklassificerade uppgifterna.

5. Ursprungsparten ska
a) säkerställa att säkerhetsskyddsklassificerade uppgifter förses med lämplig säkerhetsskyddsmarkering i enlighet med nationella lagar och andra författningar,
b) informera den mottagande parten om eventuella villkor för utlämnandet eller begränsningar i användningen av de säkerhetsskyddsklassificerade uppgifterna.

6. Den mottagande parten ska säkerställa att säkerhetsskyddsklassificerade uppgifter förses med en motsvarande nationell säkerhetsskyddsmarkering i enlighet med punkt 1 i denna artikel.

7. Parterna ska underrätta varandra om de nationella säkerhetskyddsmarkeringarna ändras.

ARTIKEL 3
SKYDD AV SÄKERHETSSKYDDSKLASSIFICERADE UPPGIFTER

1. Parterna ska i enlighet med sina respektive nationella lagar och andra författningar vidta alla lämpliga åtgärder för att säkerställa att den säkerhetsnivå som ges mottagna säkerhetsskydds-klassificerade uppgifter är likvärdig med den säkerhetsskyddsklassificeringsnivå som anges i artikel 2 i detta avtal.

2. Ingenting i detta avtal ska påverka tillämpningen av parternas nationella lagar och andra författningar när det gäller allmänhetens rätt att ta del av handlingar eller av offentlig information, personuppgiftsskyddet eller skyddet av säkerhetsskyddsklassificerade uppgifter.

3. Varje part ska säkerställa att lämpliga åtgärder vidtas för skydd av de säkerhetsskyddsklassificerade uppgifter som behandlas, förvaras eller överförs i kommunikations- eller informationssystem. Dessa åtgärder ska säkerställa de säkerhetsskyddsklassificerade uppgifternas sekretess, okränkbarhet, tillgänglighet och, när så är lämpligt, oavvislighet och äkthet samt en lämplig nivå i fråga om ansvarsskyldighet och spårbarhet för aktiviteter i samband med dessa uppgifter.

ARTIKEL 4
RÖJANDE OCH ANVÄNDNING AV
SÄKERHETSSKYDDSKLASSIFICERADE UPPGIFTER

1. Varje part ska säkerställa att säkerhetsskyddsklassificerade uppgifter som lämnas ut eller utbyts enligt detta avtal

a) inte förklaras vara säkerhetsskyddsklassificerade längre eller placeras på en lägre säkerhetsskyddsklassificeringsnivå utan föregående skriftligt medgivande från ursprungsparten,

b) inte används för andra ändamål än dem som fastställts av ursprungsparten,

c) inte röjs för någon tredje stat eller internationell organisation utan föregående skriftligt medgivande från ursprungsparten och att det finns ett lämpligt avtal eller en överenskommelse för skydd av säkerhetsskyddsklassificerade uppgifter med den berörda tredje staten eller internationella organisationen.

2. Principen om ursprungspartens medgivande ska respekteras av varje part i enlighet med deras konstitutionella bestämmelser, nationella lagar och andra författningar.

ARTIKEL 5
TILLGÅNG TILL SÄKERHETSSKYDDSKLASSIFICERADE
UPPGIFTER

1. Varje part ska säkerställa att rätt att ta del av säkerhetsskyddsklassificerade uppgifter ges enligt principen om behovsgrundad behörighet.

2. Varje part ska se till att alla enskilda personer som ges rätt att ta del av säkerhetsskyddsklassificerade uppgifter informeras om sin skyldighet att skydda sådana uppgifter i enlighet med lämpliga säkerhetsbestämmelser.

3. Parterna ska garantera att rätt att ta del av säkerhetsskyddsklassificerade uppgifter på säkerhetsskyddsklassificeringsnivån POVJERLJIVO/HEMLIG/CONFIDENTIAL eller högre endast ges enskilda personer som innehar ett lämpligt intyg om säkerhetsgodkännande eller som på annat sätt i kraft av sina arbetsuppgifter vederbörligen bemyndigas i enlighet med nationella lagar och andra författningar.

4. I enlighet med nationella lagar och andra författningar ska varje part se till att alla enheter inom dess jurisdiktion som kan ta emot eller generera säkerhetsskyddsklassificerade uppgifter har genomgått lämplig säkerhetsprövning och kan ge ett ändamålsenligt skydd, i enlighet med artikel 3.1 i detta avtal, på lämplig säkerhetsnivå.

ARTIKEL 6
ÖVERSÄTTNING, KOPIERING OCH FÖRSTÖRING AV SÄKERHETSSKYDDSKLASSIFICERADE UPPGIFTER

1. Alla översättningar och kopior av säkerhetsskyddsklassificerade uppgifter ska förses med lämplig säkerhetsskyddsmarkering och skyddas på samma sätt som de ursprungliga säkerhetsskyddsklassificerade uppgifterna.

2. Alla översättningar av säkerhetsskyddsklassificerade uppgifter ska innehålla en lämplig kommentar på det översatta språket om att de innehåller ursprungspartens säkerhetsskyddsklassificerade uppgifter.

3. Säkerhetsskyddsklassificerade uppgifter med markeringen VRLO TAJNO/HEMLIG/TOP SECRET/HEMLIG AV SYNNERLIG BETYDELSE FÖR RIKETS SÄKERHET får endast översättas eller kopieras efter det att ett skriftligt tillstånd har inhämtats från ursprungsparten.

4. Säkerhetsskyddsklassificerade uppgifter med markeringen VRLO TAJNO/HEMLIG/TOP SECRET/HEMLIG/AV SYNNERLIG BETYDELSE FÖR RIKETS SÄKERHET får inte förstöras. De ska återsändas till ursprungsparten när den mottagande parten anser att de inte längre behövs.

5. Uppgifter med klassificeringen TAJNO/HEMLIG/SECRET eller lägre ska förstöras när den mottagande parten anser att de inte längre behövs, i enlighet med nationella lagar och andra författningar.

ARTIKEL 7
ÖVERFÖRING AV SÄKERHETSSKYDDSKLASSIFICERADE UPPGIFTER

1. Säkerhetsskyddsklassificerade uppgifter ska överföras mellan parterna i enlighet med ursprungspartens nationella lagar och andra författningar på diplomatisk väg eller på annat sätt som parternas behöriga säkerhetsmyndigheter kommer överens om.

2. Uppgifter med klassificeringen OGRANIČENO/HEMLIG/RESTRICTED får överföras i en annan form i enlighet med ursprungspartens nationella lagar och andra författningar.

3. Parterna får, för att tillämpa detta avtal, ingå en särskild överenskommelse om säker kommunikation för att överföringen av de säkerhetsskyddsklassificerade uppgifterna och kommunikationen mellan parterna ska vara säker.

ARTIKEL 8
BESÖK

1. Besök vid verksamhetsställen där säkerhetsskyddsklassificerade uppgifter hanteras eller förvaras ska godkännas i förväg av värdpartens behöriga säkerhetsmyndighet om inte parterna kommer överens om annat.

2. En framställan om besök ska lämnas in till värdparten och ska innehålla följande uppgifter som endast får användas i besökssyfte:

a) Besökarens namn, födelsedatum och födelseort, medborgarskap och idkortsnummer eller passnummer.

b) Besökarens befattning med en beskrivning av den arbetsgivare som besökaren företräder.

c) En beskrivning av det projekt som besökaren deltar i.

d) Säkerhetsgodkännandets giltighet och nivå för besökaren, om det krävs.

e) Namn, adress, telefon-/faxnummer, e-postadress och kontaktpunkt för det verksamhetsställe som ska besökas.

f) Ändamålet med besöket, inklusive den högsta säkerhetsskyddsklassificeringsnivån för de berörda säkerhetsskyddsklassificerade uppgifterna.

g) Besökets tidpunkt och varaktighet. För återkommande besök anges den totala tid som besöken omfattar.

h) Andra uppgifter om de behöriga säkerhetsmyndigheterna kommer överens om det.

i) Datum och underskrift.

3. En framställan om besök ska lämnas in minst tjugo (20) dagar före besöket om de behöriga säkerhetsmyndigheterna inte kommer överens om annat.

4. Säkerhetsskyddsklassificerade uppgifter som lämnas ut till en besökare ska betraktas som säkerhetsskyddsklassificerade uppgifter enligt detta avtal. En besökare ska uppfylla värdpartens säkerhetsskyddsföreskrifter.

5. De behöriga säkerhetsmyndigheterna kan komma överens om en förteckning över besökare som är berättigade till återkommande besök. Förteckningen ska vara giltig i en inledande period om högst tolv (12) månader och får förlängas i ytterligare en tidsperiod om högst tolv (12) månader. En framställan om återkommande besök ska lämnas in i enlighet med punkt 3 i detta avtal. När förteckningen har godkänts kan besöken anordnas direkt av de berörda verksamhetsställena.

ARTIKEL 9
SÄKERHETSSKYDDSKLASSIFICERADE KONTRAKT

1. Om ursprungspartens behöriga säkerhetsmyndighet avser att tillåta förhandlingar om att ingå ett säkerhetsskyddsklassificerat kontrakt med en uppdragstagare inom den mottagande partens jurisdiktion ska den på begäran och i enlighet med nationella lagar och andra författningar inhämta alla erforderliga intyg om säkerhetsgodkännande från den mottagande partens behöriga säkerhetsmyndighet.

2. De behöriga säkerhetsmyndigheterna får begära att det ska genomföras en säkerhetsskyddsinspektion på den andra partens verksamhetsställe för att försäkra sig om att säkerhetsskyddsnormerna fortsatt följer den partens nationella lagar och andra författningar.

3. Ett säkerhetsskyddsklassificerat kontrakt ska innehålla bestämmelser om säkerhetsskyddskraven och klassificeringen av varje aspekt av eller del i det säkerhetsskyddsklassificerade kontraktet. En kopia av dessa bestämmelser ska lämnas in till parternas behöriga säkerhetsmyndigheter så att de kan utöva säkerhetstillsyn.

ARTIKEL 10
BEHÖRIGA SÄKERHETSMYNDIGHETER OCH SÄKERHETSSAMARBETE

1. Följande myndigheter är enligt detta avtal behöriga säkerhetsmyndigheter:

I Republiken Kroatien:

Avdelningen för det nationella säkerhetsrådet
(nationell säkerhetsmyndighet/utsedd säkerhetsmyndighet)

I Konungariket Sverige:

Försvarsmakten, militära säkerhetstjänsten
(nationell säkerhetsmyndighet)

Försvarets materielverk
(utsedd säkerhetsmyndighet)

2. Parterna ska skriftligen förse varandra med nödvändiga kontaktuppgifter till sina respektive behöriga säkerhetsmyndigheter.

3. Parterna ska skriftligen underrätta varandra om de behöriga säkerhetsmyndigheterna ändras.

4. Parterna ska erkänna varandras intyg om säkerhetsgodkännande av personal och verksamhetsställe och utan dröjsmål underrätta varandra om de ömsesidigt erkända säkerhetsgodkännandena ändras.

5. För att uppnå och bibehålla ett likvärdigt säkerhetsskydd ska de behöriga säkerhetsmyndigheterna på begäran informera varandra om de nationella

säkerhetsnormer, säkerhetsförfaranden och säkerhetsrutiner som tillämpas för att skydda säkerhetsskyddsklassificerade uppgifter. De behöriga säkerhetsmyndigheterna får besöka varandra i detta syfte.

6. De behöriga säkerhetsmyndigheterna ska i förekommande fall underrätta varandra om särskilda säkerhetsrisker som kan äventyra de utlämnade säkerhetsskyddsklassificerade uppgifterna.

7. På begäran ska parterna hjälpa varandra vid genomförandet av säkerhetsgodkännande-förfarandet.

8. Om någon av de behöriga säkerhetsmyndigheterna upphäver eller vidtar åtgärder för att återkalla den rätt att ta del av säkerhetsskyddsklassificerade uppgifter som en medborgare i den andra parten har beviljats med stöd av ett intyg om säkerhetsgodkännande ska den andra parten underrättas och delges motiven för dessa åtgärder.

ARTIKEL 11
FÖRLUST ELLER RÖJANDE AV SÄKERHETSSKYDDSKLASSIFICERADE UPPGIFTER

1. Parterna ska i enlighet med sina respektive nationella lagar och andra författningar vidta alla lämpliga åtgärder för att utreda fall där det är känt eller där det finns rimlig anledning att misstänka att säkerhetsskyddsklassificerade uppgifter har gått förlorade eller röjts.

2. En part som upptäcker att uppgifterna har gått förlorade eller röjts ska via lämpliga kanaler omedelbart informera ursprungsparten om det inträffade och därefter informera ursprungsparten om slutresultatet av den utredning som avses i punkt 1 i denna artikel och om de rättelser som har vidtagits för att förhindra en upprepning. Ursprungsparten får på begäran hjälpa till vid utredningen.

ARTIKEL 12
KOSTNADER

Varje part ska stå för sina egna kostnader i samband med tillämpningen av detta avtal.

ARTIKEL 13
TVISTLÖSNING

Tvister mellan parterna i fråga om tolkningen eller tillämpningen av detta avtal får endast lösas genom samråd eller förhandlingar mellan parterna.

ARTIKEL 14
SLUTBESTÄMMELSER

1. Detta avtal träder i kraft den första dagen av den andra månaden efter mottagandet av det sista meddelandet genom vilket parterna på diplomatisk

väg har informerat varandra om att deras respektive nationella rättsliga krav för att det ska träda i kraft är uppfyllda.

2. När detta avtal träder i kraft ska avtalet mellan det federala verkställande rådet i Socialistiska federativa republiken Jugoslaviens församling och Konungariket Sveriges regering om skydd av sekretessbelagd information om försvarsprojekt, upprättat i Belgrad den 25 januari 1984 upphöra att gälla mellan parterna.

3. Detta avtal får när som helst ändras om parterna skriftligen kommer överens om det. Sådana ändringar träder i kraft i enlighet med punkt 1 i denna artikel.

4. Detta avtal ingås på obestämd tid. Varje part får när som helst säga upp detta avtal genom en skriftlig underrättelse på diplomatisk väg till den andra parten. I sådana fall upphör avtalet att gälla sex (6) månader från den dag då meddelandet om uppsägning togs emot av den andra parten.

5. Alla säkerhetsskyddsklassificerade uppgifter som lämnas ut enligt detta avtal ska fortsätta att skyddas i enlighet med bestämmelserna i detta avtal även om avtalet sägs upp.

6. Parterna ska utan dröjsmål underrätta varandra om alla ändringar i sina respektive nationella lagar och andra författningar som påverkar skyddet av de säkerhetsskydds-klassificerade uppgifter som har lämnats ut enligt detta avtal. Parterna ska vid sådana ändringar samråda och överväga eventuella ändringar av detta avtal. De säkerhetsskyddsklassificerade uppgifterna ska under tiden fortsätta att vara skyddade i enlighet med detta avtal om inte ursprungsparten skriftligen begär något annat.

Upprättat i Zagreb den 14 januari 2014 i två original på svenska, kroatiska och engelska, vilka alla texter är lika giltiga. I händelse av skiljaktighet beträffande tolkningen ska den engelska texten gälla.

Lars Schmidt	*Ivica Panenic*
För Konungariket Sveriges regering	**För Republiken Kroatiens regering**

UGOVOR
IZMEĐU
VLADE KRALJEVINE ŠVEDSKE

I

VLADE REPUBLIKE HRVATSKE
O RAZMJENI I
UZAJAMNOJ ZAŠTITI
KLASIFICIRANIH PODATAKA

Vlada Kraljevine Švedske i Vlada Republike Hrvatske (u daljnjem tekstu: stranke),

u interesu nacionalne sigurnosti i u svrhu osiguravanja zaštite klasificiranih podataka razmijenjenih između njih,

sporazumjele su se kako slijedi:

ČLANAK 1.
DEFINICIJE

U ovom Ugovoru koriste se sljedeće definicije:

1. **Klasificirani podaci:** podaci, neovisno o njihovom obliku, koje je u skladu sa zakonima svake od stranaka potrebno zaštititi od gubitka, neovlaštenog otkrivanja ili druge povrede sigurnosti, koji su određeni kao takvi, a koji se razmjenjuju između stranaka ili koje stranke stvaraju.
2. **Stranka pošiljateljica:** stranka, uključujući sve javne ili privatne subjekte pod njezinom nadležnošću, koja ustupa klasificirane podatke drugoj stranci.
3. **Stranka primateljica:** stranka, uključujući sve javne ili privatne subjekte pod njezinom nadležnošću, koja prima klasificirane podatke od druge stranke.
4. **Klasificirani ugovor:** ugovor koji sadrži ili uključuje klasificirane podatke.
5. **Načelo nužnosti pristupa podacima za obavljanje poslova iz djelokruga**: načelo prema kojem se pristup klasificiranim podacima omogućava pojedincu kako bi mogao obavljati službene dužnosti i zadaće.
6. **Povreda**: svaki oblik zlouporabe, oštećivanja ili neovlaštenog pristupa, izmjene, otkrivanja ili uništavanja klasificiranih podataka, kao i bilo koja druga aktivnost ili nedostatak iste koja rezultira gubitkom njihove povjerljivosti, cjelovitosti ili raspoloživosti.
7. **Obrambena tijela**: tijela u Kraljevini Švedskoj za koja se primjenjuju propisi Švedskih oružanih snaga o zaštiti sigurnosti.
8. **Ostala tijela**: tijela u Kraljevini Švedskoj za koja se primjenjuju propisi Nacionalnog policijskog odbora o zaštiti sigurnosti.

ČLANAK 2.
STUPNJEVI TAJNOSTI

(1) Istoznačnost nacionalnih oznaka stupnjeva tajnosti je sljedeća:

U Kraljevini Švedskoj		U Republici Hrvatskoj
Obrambena tijela	Ostala tijela	
HEMLIG/ TOP SECRET	HEMLIG AV SYNNERLIG BETYDELSE FÖR RIKETS SÄKERHET	VRLO TAJNO
HEMLIG/ SECRET	HEMLIG	TAJNO
HEMLIG/ CONFIDENTIAL	–	POVJERLJIVO
HEMLIG/ RESTRICTED	–	OGRANIČENO

(2) S podacima iz Kraljevine Švedske koji imaju samo oznaku HEMLIG postupa se kao s podacima označenim TAJNO u Republici Hrvatskoj, osim ako stranka pošiljateljica ne zatraži drugačije.

(3) S podacima iz Republike Hrvatske koji imaju oznaku POVJERLJIVO ili OGRANIČENO postupa se kao s podacima označenim HEMLIG od strane ostalih tijela u Kraljevini Švedskoj, osim ako stranka pošiljateljica ne zatraži drugačije.

(4) Stranka pošiljateljica bez odgode obavještava stranku primateljicu o svim promjenama stupnja tajnosti ustupljenih klasificiranih podataka.

(5) Stranka pošiljateljica:

a) osigurava da se klasificirani podaci označavaju odgovarajućom oznakom stupnja tajnosti u skladu s njezinim nacionalnim zakonima i propisima;

b) obavještava stranku primateljicu o svim uvjetima ustupanja ili ograničenjima korištenja klasificiranih podataka.

(6) Stranka primateljica osigurava da se klasificirani podaci označavaju istoznačnom nacionalnom oznakom stupnja tajnosti u skladu sa stavkom 1. ovog članka.

(7) Stranke obavještavaju jedna drugu o svim promjenama nacionalnih oznaka stupnjeva tajnosti.

ČLANAK 3.
ZAŠTITA KLASIFICIRANIH PODATAKA

(1) Stranke poduzimaju sve odgovarajuće mjere u skladu sa svojim nacionalnim zakonima i propisima kako bi osigurale da je primljenim klasificiranim podacima dodijeljen stupanj zaštite u skladu s njihovim istoznačnim stupnjem tajnosti, kako je navedeno u članku 2. ovog Ugovora.

(2) Ništa u ovom Ugovoru ne dovodi u pitanje nacionalne zakone i propise stranaka koji se odnose na javni pristup dokumentima ili pristup podacima od javnog značaja, zaštitu osobnih podataka ili zaštitu klasificiranih podataka.

(3) Svaka stranka osigurava provedbu odgovarajućih mjera za zaštitu klasificiranih podataka koji se obrađuju, pohranjuju ili prenose u komunikacijskim i informacijskim sustavima. Takvim mjerama osigurava se povjerljivost, cjelovitost, raspoloživost i, kada je to moguće, neporecivost i autentičnost klasificiranih podataka, kao i odgovarajuća razina odgovornosti i sljedivosti postupanja u vezi s tim podacima.

ČLANAK 4.
USTUPANJE I KORIŠTENJE KLASIFICIRANOG PODATKA

(1) Svaka stranka osigurava da se klasificirani podaci dostavljeni ili razmijenjeni u skladu s ovim Ugovorom ne:

a) deklasificiraju ili im se smanjuje stupanj tajnosti bez prethodne pisane suglasnosti stranke pošiljateljice;

b) koriste za druge svrhe osim onih koje je odredila stranka pošiljateljica;

c) ustupaju bilo kojoj trećoj državi ili međunarodnoj organizaciji bez prethodne pisane suglasnosti stranke pošiljateljice i odgovarajućeg ugovora ili sporazuma za zaštitu klasificiranih podataka s predmetnom trećom državom ili međunarodnom organizacijom.

(2) Načelo suglasnosti vlasnika podatka poštuje svaka stranka u skladu sa svojim ustavnim odredbama, nacionalnim zakonima i propisima.

ČLANAK 5.
PRISTUP KLASIFICIRANIM PODACIMA

(1) Svaka stranka osigurava da se pristup klasificiranim podacima omogućava na temelju načela nužnosti pristupa podacima za obavljanje poslova iz djelokruga.

(2) Svaka stranka osigurava da su sve osobe kojima je omogućen pristup klasificiranim podacima informirane o svojim odgovornostima za zaštitu takvih podataka u skladu s odgovarajućim sigurnosnim propisima.

(3) Stranke jamče da se pristup klasificiranim podacima koji nose oznaku stupnja tajnosti HEMLIG/CONFIDENTIAL/POVJERLJIVO ili višu omogućava samo osobama koje posjeduju odgovarajuće uvjerenje o sigurnosnoj provjeri ili koje su na drugi način propisno ovlaštene temeljem svojih funkcija u skladu s nacionalnim zakonima i propisima.

(4) U skladu sa svojim nacionalnim zakonima i propisima, svaka stranka osigurava da svako tijelo pod njezinom nadležnošću koje može primiti ili kod kojeg mogu nastati klasificirani podaci posjeduje odgovarajuće uvjerenje o sigurnosnoj provjeri i da može pružiti odgovarajuću zaštitu, kako je predviđeno u stavku 1. članka 3. ovog Ugovora, sukladno odgovarajućoj razini sigurnosti.

ČLANAK 6.
PREVOĐENJE, UMNOŽAVANJE I UNIŠTAVANJE KLASIFICIRANIH PODATAKA

(1) Svi prijevodi i umnoženi primjerci klasificiranih podataka nose odgovarajuće oznake stupnja tajnosti i štite se kao i izvorni klasificirani podaci.

(2) Svi prijevodi klasificiranih podataka sadrže odgovarajuću napomenu na jeziku prijevoda kojom se naznačuje da oni sadrže klasificirane podatke stranke pošiljateljice.

(3) Klasificirani podaci označeni HEMLIG/TOP SECRET/HEMLIG AV SYNNERLIG BETYDELSE FÖR RIKETS SÄKERHET/VRLO TAJNO prevode se ili umnožavaju samo na temelju prethodnog pisanog dopuštenja stranke pošiljateljice.

(4) Klasificirani podaci označeni HEMLIG/TOP SECRET/HEMLIG AV SYNNERLIG BETYDELSE FÖR RIKETS SÄKERHET/VRLO TAJNO ne uništavaju se. Ti se podaci vraćaju stranci pošiljateljici nakon što ih stranka primateljica prestane smatrati potrebnima.

(5) Podaci označeni HEMLIG/SECRET/TAJNO ili niže uništavaju se nakon što ih stranka primateljica prestane smatrati potrebnima, u skladu s nacionalnim zakonima i propisima.

ČLANAK 7.
DOSTAVA KLASIFICIRANIH PODATAKA

(1) Klasificirani podaci dostavljaju se između stranaka u skladu s nacionalnim zakonima i propisima stranke pošiljateljice, diplomatskim putem ili na drugi način uzajamno odobren od nadležnih sigurnosnih tijela stranaka.

(2) Podaci označeni HEMLIG/RESTRICTED/OGRANIČENO mogu se dostavljati ili prenositi na drugi način, u skladu s nacionalnim zakonima i propisima stranke pošiljateljice.

(3) Stranke se mogu, radi provedbe ovog Ugovora, uzajamno sporazumjeti o posebnom sigurnosnom dogovoru za komunikaciju u svrhu uređenja zaštićenog elektroničkog prijenosa klasificiranih podataka i zaštićene komunikacije između njih.

AK 8.
POSČLANJETI

(1) Posjeti državnim tijelima ili pravnim osobama u kojima se postupa s klasificiranim podacima ili u kojima se klasificirani podaci čuvaju podliježu prethodnom odobrenju nadležnog sigurnosnog tijela stranke domaćina, osim ako uzajamno nije drugačije odobreno.

(2) Zahtjev za posjet podnosi se stranci domaćinu i uključuje sljedeće podatke, koji se koriste samo u svrhu posjeta:

a) ime posjetitelja, datum i mjesto rođenja, državljanstvo i broj identifikacijske iskaznice/putovnice;

b) radno mjesto posjetitelja, s naznakom poslodavca kojeg posjetitelj predstavlja;

c) naznaku projekta u kojem posjetitelj sudjeluje;

d) valjanost i stupanj uvjerenja o sigurnosnoj provjeri posjetitelja, ako je potrebno ;

e) ime, adresu, broj telefona/telefaksa, e-mail i kontakt osobu državnog tijela ili pravne osoba koja se posjećuje;

f) svrhu posjeta, uključujući najviši stupanj tajnosti uključenih klasificiranih podataka;

g) datum i trajanje posjeta. Za ponovljene posjete navodi se ukupno razdoblje posjeta;

h) druge podatke, ukoliko su to dogovorila nadležna sigurnosna tijela;

i) datum i potpis.

(3) Zahtjev za posjet podnosi se najmanje dvadeset (20) dana prije posjeta, osim ako nadležna sigurnosna tijela nisu uzajamno odobrila drugačije.

(4) Svi klasificirani podaci ustupljeni posjetitelju smatraju se klasificiranim podacima u skladu s ovim Ugovorom. Posjetitelj se pridržava sigurnosnih propisa stranke domaćina.

(5) Nadležna sigurnosna tijela mogu dogovoriti popis posjetitelja koji imaju pravo ponavljati posjete. Popis vrijedi tijekom početnog razdoblja ne duljeg od dvanaest (12) mjeseci i može se produljiti za daljnje razdoblje koje ne prelazi dvanaest (12) mjeseci. Zahtjev za ponavljanje posjeta podnosi se u skladu sa stavkom 3. ovog članka. Nakon što se popis odobri, posjeti se mogu dogovarati izravno između državnih tijela ili pravnih osoba koji su u njih uključeni.

ČLANAK 9.
KLASIFICIRANI UGOVORI

(1) Ako nadležno sigurnosno tijelo stranke pošiljateljice namjerava dopustiti pregovore za sklapanje klasificiranog ugovora s ugovarateljem pod nadležnošću stranke primateljice ono, na zahtjev, u skladu s nacionalnim zakonima i propisima, pribavlja sva potrebna uvjerenja o sigurnosnoj provjeri od nadležnog sigurnosnog tijela stranke primateljice.

(2) Svako nadležno sigurnosno tijelo može zatražiti da se provede sigurnosni nadzor u državnom tijelu ili pravnoj osobi druge stranke kako bi se osiguralo trajno pridržavanje sigurnosnih standarda u skladu s nacionalnim zakonima i propisima te stranke.

(3) Klasificirani ugovor sadrži odredbe o sigurnosnim zahtjevima i o klasifikaciji svakog aspekta ili elementa klasificiranog ugovora. Preslika ovih odredbi podnosi se nadležnim sigurnosnim tijelima stranaka kako bi se omogućio sigurnosni nadzor.

ČLANAK 10.
NADLEŽNA SIGURNOSNA TIJELA I SIGURNOSNA SURADNJA

(1) Za potrebe ovog Ugovora nadležna sigurnosna tijela su:

U Kraljevini Švedskoj:

Švedske oružane snage, Vojna sigurnosna služba
(Nacionalno sigurnosno tijelo)

Uprava za obrambeni materijal
(Ovlašteno sigurnosno tijelo)

U Republici Hrvatskoj:

Ured Vijeća za nacionalnu sigurnost
(Nacionalno sigurnosno tijelo/Ovlašteno sigurnosno tijelo)

(2) Svaka stranka dostavlja drugoj potrebne kontakt podatke o svojim nadležnim sigurnosnim tijelima, pisanim putem.

(3) Stranke pisanim putem obavještavaju jedna drugu o svim naknadnim promjenama svojih nadležnih sigurnosnih tijela.

(4) Stranke uzajamno priznaju svoja uvjerenja o sigurnosnoj provjeri osobe i pravne osobe i odmah obavještavaju jedna drugu o svim promjenama u uzajamno priznatim uvjerenjima o sigurnosnoj provjeri.

(5) Kako bi se postigli i održali usporedivi standardi sigurnosti, nadležna sigurnosna tijela, na zahtjev, dostavljaju jedno drugom podatke o svojim nacionalnim sigurnosnim standardima, postupcima i praksama za zaštitu klasificiranih podataka. S tim ciljem nadležna sigurnosna tijela mogu provoditi međusobne posjete.

(6) Nadležna sigurnosna tijela obavještavaju jedno drugo o specifičnim sigurnosnim rizicima koji mogu ugroziti ustupljene klasificirane podatke, kada je moguće.

(7) Na zahtjev, stranke pružaju uzajamnu pomoć u provođenju postupaka izdavanja uvjerenja o sigurnosnoj provjeri.

(8) Ako bilo koje nadležno sigurnosno tijelo onemogući pristup ili poduzme radnju kako bi uskratilo pristup klasificiranim podacima koji je bio omogućen državljaninu druge stranke temeljem uvjerenja o sigurnosnoj provjeri, druga stranka se obavještava i navode se razlozi poduzimanja takve radnje.

ČLANAK 11.
GUBITAK ILI POVREDA KLASIFICIRANIH PODATAKA

(1) Stranke poduzimaju sve odgovarajuće mjere, u skladu s njihovim nacionalnim zakonima i propisima, kako bi istražile slučajeve u kojima je poznato ili u kojima postoje osnovani temelji za sumnju da je došlo do gubitka ili povrede klasificiranih podataka.

(2) Stranka koja otkrije gubitak ili povredu klasificiranih podataka odgovarajućim putem odmah obavještava stranku pošiljateljicu o događaju i naknadno obavještava stranku pošiljateljicu o konačnim rezultatima istrage iz stavka 1. ovog članka i o korektivnim mjerama koje su poduzete kako bi se spriječilo ponavljanje. Na zahtjev, stranka pošiljateljica može pružiti pomoć u istrazi.

ČLANAK 12.
TROŠKOVI

Svaka stranka snosi svoje vlastite troškove koji su nastali u tijeku provedbe ovog Ugovora.

ČLANAK 13.
RJEŠAVANJE SPOROVA

Svaki spor između stranaka u vezi s tumačenjem ili primjenom ovog Ugovora rješavat će se isključivo konzultacijama i pregovorima između stranaka.

ČLANAK 14.
ZAVRŠNE ODREDBE

(1) Ovaj Ugovor stupa na snagu prvog dana drugog mjeseca koji slijedi nakon datuma primitka posljednje pisane obavijesti kojom stranke obavještavaju jedna drugu, diplomatskim putem, da su ispunjeni njihovi unutarnji pravni uvjeti potrebni za njegovo stupanje na snagu.

(2) Datumom stupanja na snagu ovog Ugovora u odnosima između stranaka prestaje Sporazum između Saveznog izvršnog vijeća Skupštine Socijalističke Federativne Republike Jugoslavije i Vlade Kraljevine Švedske o zaštiti klasificiranih podataka vezanih uz projekte obrane, sastavljen u Beogradu, dana 25. siječnja 1984.

(3) Ovaj Ugovor može se izmijeniti i dopuniti u svako doba uzajamnim pisanim pristankom stranaka. Takve izmjene i dopune stupaju na snagu u skladu sa stavkom 1. ovog članka.

(4) Ovaj Ugovor sklapa se na neodređeno vrijeme. Svaka stranka može u svako doba okončati ovaj Ugovor pisanom obaviješću drugoj stranci, diplomatskim putem. U tom slučaju Ugovor prestaje šest (6) mjeseci od datuma kada je druga stranka primila obavijest o prestanku.

(5) Unatoč prestanku ovog Ugovora svi klasificirani podaci ustupljeni u skladu s ovim Ugovorom nastavljaju se štititi u skladu s ovdje utvrđenim odredbama.

(6) Stranke odmah obavještavaju jedna drugu o svim izmjenama u vezi s nacionalnim zakonima i propisima koje utječu na zaštitu klasificiranih podataka ustupljenih u skladu s ovim Ugovorom. U slučaju takvih izmjena, stranke se konzultiraju kako bi razmotrile moguće izmjene ovog Ugovora. U međuvremenu, klasificirani podaci se i dalje nastavljaju štititi kao što je ovdje opisano, osim ako stranka pošiljateljica pisanim putem ne zatraži drukčije.

Sastavljeno u Zagreb dana 14.1.2014 u dva izvornika, svaki na švedskom, hrvatskom i engleskom jeziku, pri čemu su svi tekstovi jednako vjerodostojni. U slučaju razlika u tumačenju, mjerodavan je engleski tekst.

Lars Schmidt

Za Vladu
Kraljevine Švedske

Ivica Panenic

Za Vladu
Republike Hrvatske

AGREEMENT BETWEEN THE GOVERNMENT OF THE KINGDOM OF SWEDEN AND THE GOVERNMENT OF THE REPUBLIC OF CROATIA ON THE EXCHANGE AND MUTUAL PROTECTION OF CLASSIFIED INFORMATION

The Government of the Kingdom of Sweden and the Government of the Republic of Croatia (hereinafter: the Parties),

In the interest of national security and for the purpose of ensuring the protection of Classified Information exchanged between them,

Have agreed as follows:

ARTICLE 1
DEFINITIONS

In this Agreement, the following definitions shall be used:

(1) **Classified Information:** Information, regardless of its form, which under the laws of either Party requires protection against loss, unauthorised disclosure or other compromise, and has been designated as such, and is exchanged between, or generated by, the Parties.

(2) **Originating Party:** The Party, including any public or private entities under its jurisdiction, which releases Classified Information to the other Party.

(3) **Recipient Party:** The Party, including any public or private entities under its jurisdiction, which receives Classified Information from the other Party.

(4) **Classified Contract:** A contract that contains or involves Classified Information.

(5) **Need-to-know principle**: A principle by which access to Classified Information may be granted to an individual in order to be able to perform official duties and tasks.

(6) **Compromise**: Any form of misuse, damage or unauthorized access, alteration, disclosure or destruction of Classified Information, as well as any other action or inaction, resulting in loss of its confidentiality, integrity or availability.

(7) **Defence Authorities**: Authorities in the Kingdom of Sweden for which the Swedish Armed Forces' Protective security regulations apply.

(8) **Other Authorities**: Authorities in the Kingdom of Sweden for which the National Police Board's Protective security regulations apply.

ARTICLE 2
SECURITY CLASSIFICATIONS

(1) The equivalence of national security classification markings shall be as follows:

In the Kingdom of Sweden		In the Republic of Croatia
Defence Authorities	Other Authorities	
HEMLIG/ TOP SECRET	HEMLIG AV SYNNERLIG BETYDELSE FÖR RIKETS SÄKERHET	VRLO TAJNO
HEMLIG/SECRET	HEMLIG	TAJNO
HEMLIG/ CONFIDENTIAL	–	POVJERLJIVO
HEMLIG/ RESTRICTED	–	OGRANIČENO

(2) Information from the Kingdom of Sweden bearing the sole marking of HEMLIG shall be treated as TAJNO in the Republic of Croatia unless otherwise requested by the Originating Party.

(3) Information from the Republic of Croatia bearing the marking POVJERLJIVO or OGRANIČENO shall be treated as HEMLIG by Other Authorities in the Kingdom of Sweden unless otherwise requested by the Originating Party.

(4) The Originating Party shall without delay notify the Recipient Party of any changes to the security classification of released Classified Information.

(5) The Originating Party shall:
a) Ensure that Classified Information is marked with an appropriate security classification marking in accordance with its national laws and regulations;
b) Inform the Recipient Party of any conditions of release or limitations on the use of Classified Information.

(6) The Recipient Party shall ensure that Classified Information is marked with an equivalent national classification marking in accordance with Paragraph 1 of this Article.

(7) The Parties shall notify each other of any changes to national security classification markings.

ARTICLE 3
PROTECTION OF CLASSIFIED INFORMATION

(1) The Parties shall take all appropriate measures in accordance with their respective national laws and regulations to ensure that the level of protection afforded to Classified Information received shall be in accordance with their equivalent security classification level as stated in Article 2 of this Agreement.

(2) Nothing in this Agreement shall cause prejudice to the national laws and regulations of the Parties regarding public access to documents or access to information of public character, the protection of personal data or the protection of Classified Information.

(3) Each Party shall ensure that appropriate measures are implemented for the protection of Classified Information processed, stored or transmitted in communication and information systems. Such measures shall ensure the confidentiality, integrity, availability and, where applicable, non-repudiation and authenticity of Classified Information, as well as an appropriate level of accountability and traceability of actions in relation to that information.

ARTICLE 4
DISCLOSURE AND USE OF CLASSIFIED INFORMATION

(1) Each Party shall ensure that Classified Information provided or exchanged under this Agreement is not:

a) declassified or downgraded without the prior written consent of the Originating Party;

b) used for purposes other than those established by the Originating Party;

c) disclosed to any third state or international organisation without the prior written consent of the Originating Party, and an appropriate agreement or arrangement for the protection of Classified Information with the third state or international organisation concerned.

(2) The principle of originator consent shall be respected by each Party in accordance with its constitutional requirements, national laws and regulations.

ARTICLE 5
ACCESS TO CLASSIFIED INFORMATION

(1) Each Party shall ensure that access to Classified Information is granted on the basis of the Need-to-know principle.

(2) Each Party shall ensure that all individuals granted access to Classified Information are informed of their responsibilities to protect such information in accordance with the appropriate security regulations.

(3) The Parties shall guarantee that access to Classified Information bearing the classification marking POVJERLJIVO / HEMLIG/CONFIDENTIAL or above is granted only to individuals who hold an appropriate security clear-

ance or who are otherwise duly authorised by virtue of their functions in accordance with national laws and regulations.

(4) In accordance with its national laws and regulations, each Party shall ensure that any entity under its jurisdiction that may receive or generate Classified Information is appropriately security cleared and is capable of providing suitable protection, as provided for in Paragraph 1 of Article 3 of this Agreement, at the appropriate security level.

ARTICLE 6
TRANSLATION, REPRODUCTION AND DESTRUCTION OF CLASSIFIED INFORMATION

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

(2) All translations of Classified Information shall contain a suitable annotation in the language of translation, indicating that they contain Classified Information of the Originating Party.

(3) Classified Information marked VRLO TAJNO/HEMLIG/TOP SECRET / HEMLIG AV SYNNERLIG BETYDELSE FÖR RIKETS SÄKERHET shall be translated or reproduced only upon the prior written permission of the Originating Party.

(4) Classified Information marked VRLO TAJNO/HEMLIG/TOP SECRET / HEMLIG AV SYNNERLIG BETYDELSE FÖR RIKETS SÄKERHET shall not be destroyed. It shall be returned to the Originating Party after it is no longer considered necessary by the Recipient Party.

(5) Information classified TAJNO/HEMLIG/SECRET or below shall be destroyed after it is no longer considered necessary by the Recipient Party, in accordance with national laws and regulations.

ARTICLE 7
TRANSFER OF CLASSIFIED INFORMATION

(1) Classified Information shall be transferred between the Parties in accordance with national laws and regulations of the Originating Party, through diplomatic channels or as otherwise mutually approved by the competent security authorities of the Parties.

(2) Information classified OGRANIČENO/HEMLIG/RESTRICTED may be transferred or transmitted by other means in accordance with national laws and regulations of the Originating Party.

(3) The Parties may, for implementation of this Agreement, mutually agree on a separate communication security arrangement for the purpose of regulating secure transmission of Classified Information and secure communication between them.

ARTICLE 8
VISITS

(1) Visits to facilities where Classified Information is handled or stored shall be subject to prior approval by the competent security authority of the host Party, unless otherwise mutually approved.

(2) A request for a visit shall be submitted to the host Party and shall include the following data that shall be used for the purpose of the visit only:

a) the visitor's name, date and place of birth, citizenship and identification card/passport number;

b) the visitor's position, with specification of the employer that the visitor represents;

c) specification of the project in which the visitor is participating;

d) the validity and level of the visitor's Personnel Security Clearance, if required;

e) the name, address, phone/fax number, e-mail and point of contact of the facility to be visited;

f) the purpose of the visit, including the highest security classification level of Classified Information involved;

g) the date and duration of the visit. For recurring visits, the total period covered by the visits shall be stated;

h) other data, if agreed upon by the competent security authorities;

i) date and signature.

(3) A request for a visit shall be submitted at least twenty (20) days prior to the visit unless otherwise mutually approved by the competent security authorities.

(4) Any Classified Information released to a visitor shall be considered as Classified Information under this Agreement. A visitor shall comply with the security regulations of the host Party.

(5) The competent security authorities may agree on a list of visitors entitled to recurring visits. The list shall be valid for an initial period not exceeding twelve (12) months and may be extended for a further period of time not exceeding twelve (12) months. A request for recurring visits shall be submitted in accordance with Paragraph 3 of this Article. Once the list has been approved, visits may be arranged directly between the facilities involved.

ARTICLE 9
CLASSIFIED CONTRACTS

(1) If the competent security authority of the Originating Party intends to permit negotiations for concluding a Classified Contract with a contractor under the jurisdiction of the Recipient Party, it shall, on request, in accordance with national laws and regulations, obtain all relevant security clearances from the competent security authority of the Recipient Party.

(2) Each competent security authority may request that a security inspection is carried out at a facility of the other Party to ensure continuing compliance

with security standards according to national laws and regulations of that Party.

(3) A Classified Contract shall contain provisions on the security requirements and on the classification of each aspect or element of the Classified Contract. A copy of these provisions shall be submitted to the competent security authorities of the Parties to enable security supervision.

ARTICLE 10
COMPETENT SECURITY AUTHORITIES AND SECURITY CO-OPERATION

(1) For the purpose of this Agreement, the competent security authorities shall be:

In the Kingdom of Sweden:

Swedish Armed Forces, Military Security Service
(National Security Authority)

Defence Materiel Administration
(Designated Security Authority)

In the Republic of Croatia:

Office of the National Security Council
(National Security Authority/Designated Security Authority)

(2) Each Party shall provide the other with the necessary contact data of their respective competent security authorities in writing.

(3) The Parties shall inform each other, in writing, of any subsequent changes of their respective competent security authorities.

(4) The Parties shall mutually recognise their respective personnel and facility security clearances, and promptly inform each other about any changes in mutually recognised security clearances.

(5) To achieve and maintain comparable standards of security, the competent security authorities shall, on request, provide each other with information about their national security standards, procedures and practices for the protection of Classified Information. To this end, the competent security authorities may conduct mutual visits.

(6) The competent security authorities shall inform each other of specific security risks that may endanger released Classified Information, as applicable.

(7) Upon request, the Parties shall provide mutual assistance in carrying out security clearance procedures.

(8) If either competent security authority suspends or takes action to revoke access to Classified Information that has been granted to a national of the other Party based upon a security clearance, the other Party shall be notified and given the reasons for such an action.

ARTICLE 11
LOSS OR COMPROMISE OF CLASSIFIED INFORMATION

(1) The Parties shall take all appropriate measures, in accordance with their respective national laws and regulations, to investigate cases where it is known or where there are reasonable grounds for suspecting that Classified Information has been lost or compromised.

(2) A Party that discovers a loss or Compromise shall, through the appropriate channels, immediately inform the Originating Party of the occurrence and subsequently inform the Originating Party of the final results of the investigation referred to in Paragraph 1 of this Article and of the corrective measures taken to prevent a recurrence. Upon request, the Originating Party may provide investigative assistance.

ARTICLE 12
EXPENSES

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

ARTICLE 13
SETTLEMENT OF DISPUTES

Any dispute between the Parties relating to interpretation or application of this Agreement shall be settled through consultations and negotiations between the Parties only.

ARTICLE 14
FINAL PROVISIONS

(1) This Agreement shall enter into force on the first day of the second month following the date of receipt of the last written notification by which the Parties have informed each other, through diplomatic channels, that their internal legal requirements necessary for its entry into force have been fulfilled.

(2) As of the date of entry into force of this Agreement, the Agreement between the Federal Executive Council of the Assembly of the Socialist Federal Republic of Yugoslavia and the Government of the Kingdom of Sweden on the protection of classified information related to defence projects, done at Belgrade on 25 January 1984, shall terminate as between the Parties.

(3) This Agreement may be amended at any time by mutual written consent of the Parties. Such amendments shall enter into force in accordance with Paragraph 1 of this Article.

(4) This Agreement is concluded for an indefinite period of time. Each Party may, at any time, terminate this Agreement by written notification to the other Party, through diplomatic channels. In this case, the Agreement shall terminate after six (6) months from the date on which the termination notice has been received by the other Party.

(5) Notwithstanding the termination of this Agreement, all Classified Information released under this Agreement shall continue to be protected in accordance with the provisions set out herein.

(6) The Parties shall promptly notify each other of any changes to respective national laws and regulations that affect the protection of Classified Information released under this Agreement. In the event of such changes, the Parties shall consult to consider possible changes to this Agreement. In the meantime, the Classified Information shall continue to be protected as described herein, unless otherwise requested by the Originating Party in writing.

Done at Zagreb on 14 January 2014 in two originals, each in the Swedish, Croatian and English languages, all texts being equally authentic. In case of divergences of interpretation, the English text shall prevail.

Lars Schmidt	*Ivica Panenic*
For the Government of the Kingdom of Sweden	For the Government of the Republic of Croatia