SPORAZUM

MED

VLADO REPUBLIKE SLOVENIJE

IN

VLADO KRALJEVINE ŠVEDSKE

O IZMENJAVI

IN MEDSEBOJNEM VAROVANJU

TAJNIH PODATKOV

UVOD

Vlada Republike Slovenije in Vlada Kraljevine Švedske (v nadaljevanju: pogodbenici) sta se v interesu nacionalne varnosti in v želji, da bi zagotovili varovanje tajnih podatkov, izmenjanih med njima, dogovorili:

1. ČLEN
POMEN IZRAZOV

V tem sporazumu izrazi pomenijo:

(1) **tajni podatek**: tako označeni podatek, ki se ne glede na obliko izmenja ali nastane med pogodbenicama in po zakonih pogodbenic zahteva varovanje pred izgubo, nepooblaščenim razkritjem ali drugim ogrožanjem;

(2) **pogodbenica izvora**: pogodbenica, vključno z javnimi ali zasebnimi subjekti v njeni pristojnosti, ki daje tajne podatke drugi pogodbenici;

(3) **pogodbenica prejemnica**: pogodbenica, vključno z javnimi ali zasebnimi subjekti v njeni pristojnosti, ki prejme tajne podatke od druge pogodbenice;

(4) **pogodba s tajnimi podatki**: pogodba, ki vsebuje ali vključuje tajne podatke;

(5) **načelo potrebe po seznanitvi**: načelo, s katerim se posamezniku lahko dovoli dostop do tajnih podatkov za opravljanje njegovih uradnih dolžnosti in nalog.

2. ČLEN
OZNAKE STOPNJE TAJNOSTI

(1) Nacionalnim oznakam stopnje tajnosti so enakovredne te oznake:

v Republiki Sloveniji:	v Kraljevini Švedski:	
	obrambni organi	drugi organi
STROGO TAJNO	HEMLIG/TOP SECRET	HEMLIG AV SYNNERLIG BETYDELSE FÖR RIKETS SÄKERHET
TAJNO	HEMLIG/SECRET	HEMLIG
ZAUPNO	HEMLIG/CONFIDENTIAL	—
INTERNO	HEMLIG/RESTRICTED	—

(2) Podatki iz Kraljevine Švedske, ki imajo samo oznako HEMLIG, se obravnavajo kot podatki stopnje TAJNO v Republiki Sloveniji, razen če pogodbenica izvora ne zahteva drugače.

(3) Pogodbenica izvora brez odlašanja obvesti pogodbenico prejemnico o vsaki spremembi stopnje tajnosti danih tajnih podatkov.

(4) Pogodbenica izvora:

a) zagotovi, da so tajni podatki označeni z ustrezno oznako stopnje tajnosti v skladu z njenimi notranjimi zakoni in predpisi;

b) obvesti pogodbenico prejemnico o pogojih za dajanje tajnih podatkov ali omejitvah pri njihovi uporabi.

(5) Pogodbenica prejemnica zagotovi, da so tajni podatki označeni z enakovredno nacionalno oznako stopnje tajnosti v skladu s prvim odstavkom.

(6) Pogodbenici se obveščata o vseh spremembah nacionalnih oznak stopenj tajnosti.

3. ČLEN
VAROVANJE TAJNIH PODATKOV

(1) Pogodbenici skladno s svojimi notranjimi zakoni in predpisi zagotovita prejetim tajnim podatkom stopnjo varovanja v skladu s svojo enakovredno stopnjo tajnosti, navedeno v 2. členu.

(2) Nobena določba v tem sporazumu ne posega v notranje zakone in predpise pogodbenic o dostopu javnosti do dokumentov oziroma dostopu do informacij javnega značaja, varstvu osebnih podatkov ali varovanju tajnih podatkov.

(3) Pogodbenica zagotovi, da se izvajajo ustrezni ukrepi za varovanje tajnih podatkov, ki se obdelujejo, hranijo ali prenašajo v komunikacijskih in informacijskih sistemih. Ti ukrepi zagotovijo zaupnost, celovitost, razpoložljivost, in kadar je mogoče, nezatajljivost in verodostojnost tajnih podatkov ter ustrezno raven odgovornosti in sledljivosti dejanj, povezanih s takimi podatki.

4. ČLEN
RAZKRITJE IN UPORABA TAJNIH PODATKOV

(1) Pogodbenica zagotovi, da se za dane ali izmenjane tajne podatke po tem sporazumu:

a) ne zniža ali prekliče stopnja tajnosti brez predhodnega pisnega soglasja pogodbenice izvora;

b) da se ti podatki ne uporabijo za druge namene od tistih, ki jih opredeli pogodbenica izvora;

c) da se ti podatki ne razkrijejo tretji državi ali mednarodni organizaciji brez predhodnega pisnega soglasja pogodbenice izvora ter ustreznega sporazuma ali dogovora o varovanju tajnih podatkov s tretjo državo ali mednarodno organizacijo.

(2) V skladu z ustavnimi zahtevami, notranjimi zakoni in predpisi pogodbenica spoštuje načelo soglasja organa, pri katerem so podatki nastali.

5. ČLEN
DOSTOP DO TAJNIH PODATKOV

(1) Pogodbenica zagotovi, da se dostop do tajnih podatkov dovoli le na podlagi načela potrebe po seznanitvi.

(2) Pogodbenica zagotovi, da so vsi posamezniki, ki imajo dostop do tajnih podatkov, seznanjeni s svojo odgovornostjo za varovanje takih podatkov v skladu z ustreznimi varnostnimi predpisi.

(3) Pogodbenici jamčita, da je dostop do tajnih podatkov stopnje tajnosti ZAUPNO / HEMLIG/CONFIDENTIAL ali višje stopnje dovoljen samo posameznikom, ki imajo ustrezno dovoljenje za dostop do tajnih podatkov ali so drugače pravilno pooblaščeni zaradi svoje funkcije v skladu z notranjimi zakoni in predpisi.

(4) V skladu s svojimi notranjimi zakoni in predpisi pogodbenica zagotovi, da je vsak subjekt v njeni pristojnosti, v katerem lahko nastanejo tajni podatki ali jih lahko prejme, ustrezno varnostno preverjen in sposoben zagotavljati primerno varovanje z ustrezno stopnjo tajnosti, kot določa prvi odstavek 3. člena.

6. ČLEN
PREVAJANJE, RAZMNOŽEVANJE IN UNIČEVANJE TAJNIH PODATKOV

(1) Vsi prevodi tajnih podatkov so označeni z ustrezno stopnjo tajnosti in so varovani kot tajni podatki izvirnika.

(2) Vsak prevod tajnih podatkov ima v jeziku prevoda ustrezno navedbo, da prevod vsebuje tajne podatke pogodbenice izvora.

(3) Tajni podatki z oznako stopnje tajnosti STROGO TAJNO / HEMLIG/TOP SECRET / HEMLIG AV SYNNERLIG BETYDELSE FÖR RIKETS SÄKERHET se prevajajo ali razmnožujejo izključno s predhodnim pisnim dovoljenjem pogodbenice izvora.

(4) Tajni podatki z oznako stopnje tajnosti STROGO TAJNO / HEMLIG/TOP SECRET / HEMLIG AV SYNNERLIG BETYDELSE FÖR RIKETS SÄKERHET se ne smejo uničiti. Pogodbenica prejemnica jih vrne pogodbenici izvora, ko jih ne potrebuje več.

(5) Tajni podatki stopnje tajnosti TAJNO / HEMLIG ali nižje stopnje tajnosti se uničijo v skladu z notranjimi zakoni in predpisi, ko jih pogodbenica prejemnica ne potrebuje več.

7. ČLEN
PRENOS TAJNIH PODATKOV

(1) Tajni podatki se v skladu z notranjimi zakoni in predpisi pogodbenice izvora med pogodbenicama pošiljajo po diplomatski poti ali po drugi varni poti, za katero se skupaj dogovorijo pristojni varnostni organi pogodbenic.

(2) Tajni podatki z oznako stopnje tajnosti INTERNO / HEMLIG/RESTRICTED se lahko prenašajo ali pošiljajo tudi na drug način v skladu z notranjimi zakoni in predpisi pogodbenice izvora.

(3) Pogodbenici se lahko za izvajanje tega sporazuma dogovorita za ločen sporazum o komunikacijski varnosti za ureditev varnega medsebojnega pošiljanja tajnih podatkov in varne medsebojne komunikacije.

8. ČLEN
OBISKI

(1) Za obiske organizacij, ki ravnajo s tajnimi podatki ali jih hranijo, je potrebno predhodno dovoljenje pristojnega varnostnega organa pogodbenice gostiteljice, razen če ni drugače dogovorjeno.

(2) Zaprosilo za obisk se predloži pristojnemu varnostnemu organu pogodbenice gostiteljice in vsebuje navedene podatke, ki se uporabljajo samo za namene obiska:

a) ime in priimek obiskovalca, datum in kraj rojstva, državljanstvo in številko osebne izkaznice ali potnega lista;

b) položaj obiskovalca s podatki o delodajalcu, ki ga obiskovalec zastopa;

c) podatke o projektu, pri katerem obiskovalec sodeluje;

d) veljavnost in stopnjo tajnosti obiskovalčevega dovoljenja za dostop do tajnih podatkov, če je potrebno;

e) ime, naslov, telefonsko številko, številko telefaksa, elektronski naslov organizacije, v kateri bo obisk, in osebo za stike v tej organizaciji;

f) namen obiska, vključno z najvišjo stopnjo tajnosti obravnavanih podatkov;

g) datum in trajanje obiska; za večkratne obiske se navede skupno obdobje, v katerem bodo obiski opravljeni;

h) datum in podpis pristojnega varnostnega organa pošiljatelja.

(3) Zaprosilo za obisk se predloži vsaj 20 dni pred obiskom, razen če se pristojna varnostna organa ne dogovorita drugače.

(4) Tajni podatki, ki jih pridobi obiskovalec, veljajo za tajne podatke po tem sporazumu. Obiskovalec spoštuje varnostne predpise pogodbenice gostiteljice.

(5) Pristojna varnostna organa se lahko dogovorita o seznamu obiskovalcev, ki imajo pravico do večkratnih obiskov. Seznam velja za začetno obdobje do 12 mesecev in se lahko podaljša za največ 12 mesecev. Zaprosilo za večkratne obiske se predloži v skladu s tretjim odstavkom tega člena. Ko je seznam potrjen, se lahko sodelujoče organizacije o obiskih dogovarjajo neposredno.

9. ČLEN
POGODBE S TAJNIMI PODATKI

(1) Če namerava pristojni varnostni organ pogodbenice izvora dovoliti pogajanja za sklenitev pogodbe s tajnimi podatki z izvajalcem, ki je v pristojnosti pogodbenice prejemnice, na podlagi zaprosila pridobi od pristojnega

varnostnega organa pogodbenice prejemnice vsa ustrezna varnostna dovoljenja v skladu z notranjimi zakoni in predpisi.

(2) Pristojni varnostni organ lahko zahteva, da se izvede varnostni inšpekcijski pregled organizacije druge pogodbenice zaradi stalnega zagotavljanja skladnosti z varnostnimi standardi po notranjih zakonih in predpisih te pogodbenice.

(3) Pogodba s tajnimi podatki vsebuje določbe o varnostnih zahtevah in stopnji tajnosti vsakega njenega vidika ali dela. Zaradi varnostnega nadzora se izvod teh določb predloži pristojnima varnostnima organoma pogodbenic.

10. ČLEN
PRISTOJNI VARNOSTNI ORGANI IN VARNOSTNO SODELOVANJE

(1) Po tem sporazumu so pristojni varnostni organi:

v Republiki Sloveniji:

Urad Vlade Republike Slovenije za varovanje tajnih podatkov (nacionalni varnostni organ);

v Kraljevini Švedski:

Švedske oborožene sile, Vojaška varnostna služba (nacionalni varnostni organ),

Uprava za obrambne nabave (imenovani varnostni organ).

(2) Pogodbenici si zagotavljata podatke o pristojnih varnostnih organih, ki so potrebni za stike.

(3) Pogodbenici se obveščata o vseh poznejših spremembah pristojnih varnostnih organov.

(4) Pogodbenici si priznavata dovoljenja za dostop do tajnih podatkov in varnostna dovoljenja organizacij ter se takoj obvestita o vsaki spremembi v medsebojno priznanih varnostnih dovoljenjih.

(5) Zaradi doseganja in ohranjanja primerljivih varnostnih standardov se pristojni varnostni organi na podlagi zaprosila obveščajo o nacionalnih varnostnih standardih, postopkih in praksah za varovanje tajnih podatkov. V ta namen se lahko pristojni varnostni organi obiskujejo.

(6) Pristojni varnostni organi se, kot je določeno, obveščajo o posebnih varnostnih tveganjih, ki lahko ogrozijo dane tajne podatke.

(7) Na podlagi zaprosila si pogodbenici pomagata pri izvajanju postopkov varnostnega preverjanja.

(8) Če pristojni varnostni organ začasno prekliče ali prekliče dostop do tajnih podatkov, ki je bil na podlagi varnostnega dovoljenja dovoljen državljanu druge pogodbenice, se druga pogodbenica o tem obvesti in navedejo razlogi za tako ukrepanje.

11. ČLEN
IZGUBA ALI OGROŽANJE TAJNIH PODATKOV

(1) V skladu s svojimi notranjimi zakoni in predpisi pogodbenici izvajata ustrezne ukrepe za preiskovanje primerov, za katere je znano ali pa obstajajo utemeljeni razlogi za sum, da so tajni podatki ogroženi ali izgubljeni.

(2) Pogodbenica, ki odkrije ogrožanje ali izgubo, po ustrezni poti o tem takoj obvesti pogodbenico izvora in nato še o končnih rezultatih preiskave in popravljalnih ukrepih za preprečitev ponovnega ogrožanja ali izgube. Na podlagi zaprosila pogodbenica izvora lahko pomaga pri preiskavi.

12. ČLEN
RAZLAGA IN SPORI

Vsi spori med pogodbenicama zaradi razlage ali uporabe tega sporazuma se rešujejo s posvetovanji med njima.

13. ČLEN
STROŠKI

Vsaka pogodbenica krije svoje stroške, ki nastanejo pri izvajanju tega sporazuma.

14. ČLEN
KONČNE DOLOČBE

(1) Sporazum je sklenjen za nedoločen čas. Odobren mora biti v skladu z notranjepravnimi postopki pogodbenic in začne veljati prvi dan drugega meseca po datumu zadnjega uradnega obvestila pogodbenic o tem, da so izpolnjene vse zahteve, potrebne za začetek veljavnosti tega sporazuma.

(2) Sporazum se lahko spremeni z medsebojnim pisnim soglasjem pogodbenic. Spremembe začnejo veljati v skladu s prvim odstavkom tega člena.

(3) Sporazum lahko vsaka pogodbenica kadar koli pisno odpove. V takem primeru sporazum preneha veljati šest (6) mesecev po dnevu, ko je druga pogodbenica prejela obvestilo o odpovedi sporazuma.

(4) Ne glede na prenehanje veljavnosti tega sporazuma se vsi tajni podatki, dani na podlagi tega sporazuma, še naprej varujejo v skladu z njegovimi določbami.

(5) Pogodbenici se takoj obvestita o vsaki spremembi notranjih zakonov in predpisov, ki vplivajo na varovanje tajnih podatkov, danih na podlagi tega sporazuma. V takem primeru se pogodbenici posvetujeta o morebitnih spremembah tega sporazuma. V tem času se vsi tajni podatki še naprej varujejo v skladu s tem sporazumom, razen če ni pogodbenica izvora pisno zahtevala drugače.

Sestavljeno v Stockholmu, 16. 11. 2011 v dveh izvirnikih v slovenskem, švedskem in angleškem jeziku, pri čemer so vsa besedila enako verodostojna. Pri razlikah v razlagi prevlada angleško besedilo.

Da bi to potrdila, sta podpisnika, ki sta ju za to pravilno pooblastili njuni vladi, podpisala ta sporazum.

Za Vlado
Republike Slovenije

Za Vlado
Kraljevine Švedske

AVTAL

MELLAN

REPUBLIKEN SLOVENIENS REGERING

OCH

KONUNGARIKET SVERIGES REGERING

OM UTBYTE OCH

ÖMSESIDIGT SKYDD

AV SÄKERHETSSKYDDSKLASSIFICERADE UPPGIFTER

INGRESS

Republiken Sloveniens regering och Konungariket Sveriges 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, inbegripet alla offentliga och privata aktörer inom dess jurisdiktion, som lämnar ut de säkerhetsskyddsklassificerade uppgifterna till den andra parten.

3. *mottagande part*: den part, inbegripet 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 hänför sig till säkerhetsskyddsklassificerade uppgifter.

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

ARTIKEL 2
SÄKERHETSSKYDDSKLASSIFICERINGAR

1. De nationella säkerhetsskyddsmarkeringarna motsvarar varandra enligt följande:

I Republiken Slovenien	I Konungariket Sverige	
	Försvarsmyndigheter	Andra myndigheter
STROGO TAJNO	HEMLIG/ TOP SECRET	HEMLIG AV SYNNERLIG BETYDELSE FÖR RIKETS SÄKERHET
TAJNO	HEMLIG/ SECRET	HEMLIG
ZAUPNO	HEMLIG/ CONFIDENTIAL	—
INTERNO	HEMLIG/ RESTRICTED	—

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

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

4. Ursprungsparten ska

   a) se till 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 av eller begränsningar i användningen av de säkerhetsskyddsklassificerade uppgifterna.

5. Den mottagande parten ska se till att säkerhetsskyddsklassificerade uppgifter förses med en motsvarande nationell säkerhetsskyddsmarkering i enlighet med punkt 1.

6. 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 säkerhetsskyddsklassificerade uppgifter är likvärdig med den säkerhetsskyddsklassificeringsnivå som anges i artikel 2.

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 överlämnas i kommunikations- eller informationssystem. Dessa åtgärder ska säkerställa de säkerhetsskyddsklassificerade uppgifternas konfidentialitet, integritet, tillgänglighet och, där det 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 placeras på en lägre säkerhetsskyddsklassificeringsnivå eller att uppgifterna förklaras inte längre vara säkerhetsskyddsklassificerade utan föregående skriftligt medgivande från ursprungsparten,

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

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

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

ARTIKEL 5
TILLGÅNG TILL SÄKERHETSSKYDDSKLASSIFICERADE UPPGIFTER

1. Varje part ska se till att tillgång till säkerhetsskyddsklassificerade uppgifter beviljas enligt principen om behovsenlig behörighet.

2. Varje part ska se till att alla enskilda personer som beviljats tillgång till säkerhetsskyddsklassificerade uppgifter informeras om sin skyldighet att skydda sådana uppgifter i enlighet med vederbörliga säkerhetsbestämmelser.

3. Parterna ska garantera att tillgång till säkerhetsskyddsklassificerade uppgifter på säkerhetsskyddsklassificeringsnivån ZAUPNO / HEMLIG/CONFIDENTIAL eller högre endast beviljas enskilda personer som har genomgått lämplig säkerhetsprövning 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 de enheter inom dess jurisdiktion som eventuellt kan erhålla eller generera säkerhetsskyddsklassificerade uppgifter har genomgått lämplig säkerhetsprövning och i enlighet med artikel 3.1 kan ge ett ändamålsenligt skydd på lämplig säkerhetsnivå.

ARTIKEL 6
ÖVERSÄTTNING, KOPIERING OCH FÖRSTÖRING AV SÄKERHETSSKYDDSKLASSIFICERADE UPPGIFTER

1. Alla översättningar 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 notering på det översatta språket om att de innehåller ursprungspartens säkerhetsskyddsklassificerade uppgifter.

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

4. Säkerhetsskyddsklassificerade uppgifter med markeringen STROGO 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 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 INTERNO / 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 ett särskilt avtal om säker kommunikation för att överföringen av de säkerhetsskyddsklassificerade uppgifterna och kommunikation mellan parterna ska vara säker.

ARTIKEL 8
BESÖK

1. Besök vid anläggningar där säkerhetsskyddsklassificerade uppgifter hanteras eller förvaras ska godkännas i förväg av värdpartens behöriga säkerhetsskyddsmyndighet om inte något annat har överenskommits.

2. En framställan om besök ska lämnas till värdpartens behöriga säkerhetsmyndighet. Den ska innehålla följande uppgifter som endast får användas i besökssyfte:

   a) besökarens namn, födelsedatum och födelseort, medborgarskap och id-kortsnummer eller passnummer,

   b) besökarens befattning med en detaljerad beskrivning av den arbetsgivare som besökaren företräder,

   c) en detaljerad beskrivning av det projekt som besökaren deltar i,

   d) besökarens säkerhetsprövnings giltighet och nivå, om det krävs,

   e) namn, adress, telefon-/faxnummer, e-postadress och kontaktpunkt för den anläggning som ska besökas,

   f) ändamålet med besöket, inbegripet den högsta säkerhetsskyddsklassificerings-nivån för de berörda säkerhetsskyddsklassificerade uppgifterna,

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

   h) datum och underskrift från den behöriga säkerhetsmyndigheten som skickar besökaren.

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

4. Säkerhetsskyddsklassificerade uppgifter som en besökare kommer över 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 12 månader och får förlängas i en ytterligare tidsperiod om högst 12 månader. En framställan om återkommande besök ska lämnas in i enlighet med punkt 3 i detta avtal. När förteckningen har godkänts kan besöken skötas direkt av de berörda anläggningarna.

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 erhålla tillämplig säkerhetsprövning från den mottagande partens behöriga säkerhetsmyndighet.

2. De behöriga säkerhetsskyddsmyndigheterna får begära att det ska genomföras en säkerhetsskyddsinspektion på den andra partens anläggningar 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 tillställas parternas behöriga säkerhetsmyndigheter så att de kan utöva tillsyn.

ARTIKEL 10
BEHÖRIGA SÄKERHETSMYNDIGHETER OCH SÄKERHETSSAMARBETE

1. Följande myndigheter är enligt detta avtal behöriga säkerhetsmyndigheter:

I Republiken Slovenien:

Regeringskansliet för skydd av säkerhetsskyddsklassificerade uppgifter (nationell säkerhetsmyndighet)

I Konungariket Sverige:

Försvarsmakten, militära säkerhetstjänsten (nationell säkerhetsmyndighet)

Försvarets materielverk (utsedd säkerhetsmyndighet)

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

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

4. Parterna ska erkänna varandras säkerhetsprövning av personal och anläggning och utan dröjsmål informera varandra om den ömsesidigt erkända säkerhetsprövningen 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 upplysa varandra om särskilda säkerhetsrisker som kan äventyra de utlämnade säkerhetsskyddsklassificerade uppgifterna.

7. På begäran ska parterna lämna ömsesidigt bistånd vid genomförandet av säkerhetsprövningen.

8. Om någon av de behöriga säkerhetsmyndigheterna upphäver eller vidtar åtgärder för att upphäva den rätt att ta del av säkerhetsskyddsklassificerade uppgifter som en medborgare i den andra parten har beviljats med stöd av en säkerhetsprövning 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 undersöka fall där det är känt eller det finns rimliga skäl att misstänka att säkerhetsskyddsklassificerade uppgifter har röjts eller gått förlorade.

2. En part som upptäcker att uppgifterna har röjts eller gått förlorade ska via lämpliga kanaler omedelbart informera ursprungsparten om det inträffade och därefter informera ursprungsparten om slutresultatet av undersökningen och om de korrigerande åtgärder som vidtagits för att förhindra en upprepning. Ursprungsparten får på begäran hjälpa till vid utredningen.

ARTIKEL 12
TOLKNING OCH TVISTER

Eventuella tvister mellan parterna i fråga om tolkningen eller tillämpningen av detta avtal ska lösas genom samråd mellan parterna.

ARTIKEL 13
KOSTNADER

Vardera parten ska stå för sina egna kostnader i samband med detta avtal.

ARTIKEL 14
SLUTBESTÄMMELSER

1. Detta avtal ingås på obestämd tid. Det ska godkännas i enlighet med parternas nationella rättsliga förfaranden och träder i kraft den första dagen i den andra månaden efter den dag då det sista meddelandet mottogs mellan parterna om att de nödvändiga kraven för att detta avtal ska kunna träda i kraft är uppfyllda.

2. Avtalet får ändras efter skriftligt samtycke från båda parter. Sådana ändringar träder i kraft i enlighet med punkt 1 i denna artikel.

3. Parterna får när som helst säga upp detta avtal skriftligen. I sådana fall upphör avtalet att gälla sex (6) månader från den dag då meddelandet om uppsägning lämnades till den andra parten.

4. 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.

5. Parterna ska utan dröjsmål underrätta varandra om alla ändringar i sina respektive nationella lagar och andra författningar som påverkar skyddet av de säkerhetsskyddsklassificerade uppgifter som har lämnats ut enligt detta avtal. Parterna ska vid sådana ändringar konsultera varandra 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 Stockholm den 16/11 2011 i två original på slovenska, svenska och engelska språken, vilka alla texter är lika giltiga. I händelse av skiljaktighet beträffande tolkningen ska den engelska texten gälla.

Till bekräftelse härav har undertecknade, därtill vederbörligen bemyndigade av sina respektive regeringar, undertecknat detta avtal.

För Republiken Sloveniens regering

För Konungariket Sveriges regering

AGREEMENT

BETWEEN

THE GOVERNMENT OF THE REPUBLIC OF SLOVENIA

AND

THE GOVERNMENT OF THE KINGDOM OF SWEDEN

ON THE EXCHANGE AND

MUTUAL PROTECTION

OF CLASSIFIED INFORMATION

PREAMBLE

The Government of the Republic of Slovenia and the Government of the Kingdom of Sweden (hereinafter: the Parties), have, in the interest of national security and for the purpose of ensuring the protection of Classified Information exchanged between them, 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.

ARTICLE 2
SECURITY CLASSIFICATIONS

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

In the Republic of Slovenia	In the Kingdom of Sweden	
	Defence Authorities	Other Authorities
STROGO TAJNO	HEMLIG/TOP SECRET	HEMLIG AV SYNNERLIG BETYDELSE FÖR RIKETS SÄKERHET
TAJNO	HEMLIG/SECRET	HEMLIG
ZAUPNO	HEMLIG/CONFIDENTIAL	—
INTERNO	HEMLIG/RESTRICTED	—

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

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

(4) 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.

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

(6) 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.

(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) downgraded or declassified 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 ZAUPNO / HEMLIG/CONFIDENTIAL or above is granted only to individuals who hold an appropriate security clearance 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 Article 3(1), at the appropriate security level.

ARTICLE 6
TRANSLATION, REPRODUCTION AND DESTRUCTION OF CLASSIFIED INFORMATION

(1) All translations 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 STROGO 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 STROGO 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 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 INTERNO / 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 Agreement 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 competent security authority of 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) the date and signature of the competent security authority sending the visitor.

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

(4) Any Classified Information acquired by 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 12 months and may be extended for a further period of time not exceeding 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 Republic of Slovenia:

Government Office for the Protection of Classified Information (National Security Authority)

In the Kingdom of Sweden:

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

Defence Materiel Administration (Designated Security Authority)

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

(3) The Parties shall inform each other 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 will 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 compromised or lost.

(2) A Party that discovers such a compromise or loss 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 and of the corrective measures taken to prevent a recurrence. Upon request, the Originating Party may provide investigative assistance.

ARTICLE 12
INTERPRETATION AND DISPUTES

Any dispute between Parties relating to interpretation or application of this Agreement shall be settled through consultation between the Parties.

ARTICLE 13
EXPENSES

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

ARTICLE 14
FINAL PROVISIONS

(1) This Agreement is concluded for an indefinite period of time. It is subject to approval in accordance with the national legal procedures of the Parties and shall enter into force on the first day of the second month following the date of the last notification between the Parties that the necessary requirements for this Agreement to enter into force have been met.

(2) This Agreement may be amended with the mutual written consent of both Parties. Such amendments shall enter into force in accordance with Paragraph 1 of this Article.

(3) Each Party may terminate this Agreement in writing at any time. In this case, the Agreement will expire after six (6) months from the day on which the termination notice was served to the other Party.

(4) 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.

(5) 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 in Stockholm on 16/11 2021 in two original copies, each in the Slovene, Swedish and English languages, all texts being equally authentic. In case of divergences of interpretation, the English text shall prevail.

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

On behalf of the Government of the Republic of Slovenia

On behalf of the Government of the Kingdom of Sweden