Sveriges internationella överenskommelser

ISSN 1102-3716

Utgiven av utrikesdepartementet

SÖ 2016:5

Nr 5
Avtal mellan Konungariket Sveriges regering och Förbundsrepubliken Tysklands regering om ömsesidigt skydd av säkerhetsklassificerade uppgifter
Stockholm den 31 mars 2016

Regeringen beslutade den 6 mars 2014 att underteckna avtalet. Avtalet trädde i kraft vid undertecknandet.

Avtal
mellan
Konungariket Sveriges regering
och
Förbundsrepubliken Tysklands regering
om
ömsesidigt skydd av säkerhetsskyddsklassificerade uppgifter

Konungariket Sveriges regering

och

Förbundsrepubliken Tysklands regering (nedan kallade *parterna*),

som önskar säkerställa skyddet av säkerhetsskyddsklassificerade uppgifter,

som önskar förstärka samarbetet, forskningen, utvecklingen, produktionen och upphandlingen inom försvarsområdet,

som inser att ett sådant samarbete kan kräva utbyte av säkerhetsskyddsklassificerade uppgifter mellan behöriga myndigheter och försvarsindustrin,

som erkänner ramavtalet mellan Republiken Frankrike, Republiken Italien, Konungariket Spanien, Förenade konungariket Storbritannien och Nordirland, Konungariket Sverige och Förbundsrepubliken Tyskland om åtgärder för att underlätta omstrukturering och drift av den europeiska försvarsindustrin av den 27 juli 2000,

har kommit överens om följande.

Artikel 1
Definitioner

Enligt detta avtal gäller följande definitioner:

1. *säkerhetsskyddsklassificerade uppgifter*: uppgift som, oavsett form, enligt endera partens lagar och andra författningar kräver skydd mot förlust, otillåtet röjande eller annan blottläggning och som har angetts som sådan enligt artikel 4.1 i detta avtal,

2. *säkerhetsskyddsklassificerat kontrakt*: ett avtal mellan två eller flera parter, som innehåller eller inbegriper säkerhetsskyddsklassificerade uppgifter och preciserar rättigheter och skyldigheter som kan göras gällande mellan parterna,

3. *ursprungspart*: den part, inklusive offentliga och privata juridiska personer inom dess jurisdiktion, som lämnar ut säkerhetsskyddsklassificerade uppgifter till den andra parten och beslutar om uppgifternas säkerhetsklass,

4. *mottagande part*: den part, inklusive offentliga och privata aktörer inom dess jurisdiktion, som tar emot säkerhetsskyddsklassificerade uppgifter från ursprungsparten.

Artikel 2
Allmänna bestämmelser

Parternas skyldigheter enligt detta avtal ska tolkas i enlighet med respektive parts nationella lagar och andra författningar.

Artikel 3
Behöriga säkerhetsmyndigheter

1. I syfte att tillämpa detta avtal är följande myndigheter behöriga säkerhetsmyndigheter:

a) I Konungariket Sverige:

Försvarsmakten, Militära säkerhetstjänsten (nationell säkerhetsmyndighet)

Försvarets materielverk (utsedd säkerhetsmyndighet)

b) I Förbundsrepubliken Tyskland:

Förbundsrepubliken Tysklands inrikesdepartement (nationell säkerhetsmyndighet)

Förbundsrepubliken Tysklands närings- och energidepartement (utsedd säkerhetsmyndighet)

Förbundsrepubliken Tysklands försvarsdepartement (militär säkerhetsmyndighet)

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

Artikel 4
Jämförbara säkerhetsskyddsklassificeringar

1. Parterna är överens om att följande säkerhetsskyddsklassificeringar ska vara jämförbara och omfattas av detta avtal:

I Förbundsrepubliken Tyskland	I Konungariket Sverige	
	försvarsmyndigheter	andra myndigheter
STRENG GEHEIM	HEMLIG/ TOP SECRET	HEMLIG av synnerlig betydelse för rikets säkerhet
GEHEIM	HEMLIG/SECRET	HEMLIG
VS-VERTRAULICH	HEMLIG/ CONFIDENTIAL	se punkt 2 nedan
VS-NUR FÜR DEN DIENSTGEBRAUCH	HEMLIG/ RESTRICTED	se punkt 2 nedan

2. Information från Förbundsrepubliken Tyskland som har försetts med VS-NUR FÜR DEN DIENSTGEBRAUCH och VS-VERTRAULICH ska behandlas som HEMLIG av andra myndigheter än försvarsmyndigheter i

Konungariket Sverige om inte ursprungsparten begär något annat. Den ska behålla sin tyska beteckning.

3. Tyska säkerhetsskyddsklassificerade uppgifter i säkerhetsklasserna VS-NUR FÜR DEN DIENSTGEBRAUCH och VS-VERTRAULICH som skickas tillbaka till Tyskland ska skyddas enligt den ursprungliga tyska säkerhetsklassen.

4. När en part ändrar sin nationella säkerhetsklass ska den andra parten underrättas om detta.

5. I särskilda fall får en part be den andra partens behöriga säkerhetsmyndigheter att skydda uppgifterna enligt en annan säkerhetsklass än den motsvarande klassificeringen anger. Den ändrade klassificeringen måste synas tydligt och undertecknas av en behörig säkerhetsansvarig.

Artikel 5
Inskränkningar i fråga om användning och röjande

Parterna får inte, utan föregående samråd, lämna ut, röja eller använda säkerhetsskyddsklassificerade uppgifter eller tillåta att säkerhetsskyddsklassificerade uppgifter lämnas ut, röjs eller används för annat än för det ändamål och med de begränsningar som ursprungsparten har angett.

Artikel 6
Skydd av säkerhetsskyddsklassificerade uppgifter

1. Ursprungsparten ska

a) säkerställa att säkerhetsskyddsklassificerade uppgifter som lämnas ut förses med lämplig nationell säkerhetsskyddsbeteckning i enlighet med artikel 4.1,

b) i förekommande fall informera den mottagande parten om eventuella villkor för utlämnandet eller begränsningar i användningen av de säkerhetsskyddsklassificerade uppgifterna,

c) informera den mottagande parten om efterföljande ändringar av säkerhetsskyddsklassificeringen för de utlämnade säkerhetsskyddsklassificerade uppgifterna.

2. Den mottagande parten ska

a) ge mottagna säkerhetsskyddsklassificerade uppgifter ett säkerhetsskydd som är likvärdigt med det skydd som ges egna säkerhetsskyddsklassificerade uppgifter,

b) säkerställa att säkerhetsskyddsklassificerade uppgifter förses med den egna motsvarande klassificeringen i enlighet med artikel 4,

c) säkerställa att säkerhetsskyddsklassificeringarna inte ändras utan skriftligt tillstånd från ursprungsparten eller på ursprungspartens vägnar.

Artikel 7

1. Rätten att ta del av säkerhetsskyddsklassificerade uppgifter ska vara förbehållen personer som har behov av dem i tjänsten och, med undantag av säkerhetsskyddsklassificerade uppgifter i säkerhetsklassen VS-NUR FÜR DEN DIENSTGEBRAUCH ; HEMLIG/RESTRICTED, har blivit godkända vid säkerhetsprövningen i enlighet med nationella lagar och andra författningar för den aktuella säkerhetsklassen och har informerats om hur säkerhetsskyddsklassificerade uppgifter skyddas. En säkerhetsprövning är inte obligatorisk för personer som i enlighet med nationella lagar och andra författningar är behöriga att ta del av säkerhetsskyddsklassificerade uppgifter på grund av sina arbetsuppgifter.

2. Om formföreskrifterna i nationella lagar och andra författningar är uppfyllda ska parterna erkänna varandras intyg om säkerhetsgodkännande av personal.

3. Säkerhetsprövning av medborgare i en part som är lagligen bosatta i den andra parten och som söker en tjänst som är känslig ur säkerhetssynpunkt i det landet, ska genomföras av den behöriga säkerhetsmyndigheten i det landet, som vid behov utför kontroller i utlandet.

Artikel 8
Överföring av säkerhetsskyddsklassificerade uppgifter

1. Säkerhetsskyddsklassificerade uppgifter ska överföras mellan de båda länderna i enlighet med de nationella lagarna och andra författningar i ursprungsparten. Normalt ska överföringen ske via officiell diplomatisk väg mellan regeringarna, men andra arrangemang får göras, såsom personligt överlämnande eller säker kommunikation (kryptering), om de båda parterna godkänner detta.

2. I brådskande fall, dvs. endast när användningen av de diplomatiska vägarna mellan regeringarna inte uppfyller kraven, får säkerhetsskyddsklassificerade uppgifter i säkerhetsklassen VS-VERTRAULICH ; HEMLIG/CONFIDENTIAL överföras med kommersiella budfirmor, under förutsättning att följande kriterier är uppfyllda:

1) Budfirman finns inom parternas territorium och har inrättat ett skyddsprogram för hantering av värdefulla försändelser med en signeringstjänst, inklusive ett protokoll över det kontinuerliga ansvaret för försändelserna antingen genom ett signerings- och avprickningsprotokoll eller genom ett elektroniskt spårningssystem.

2) Budfirman måste erhålla och förse avsändaren med en leveransbekräftelse på signerings- och avprickningsprotokollet, eller erhåller mottagningskvitton av vilket försändelsens nummer framgår.

3) Budfirman måste garantera att försändelsen levereras till mottagaren en viss tid och ett visst datum, normalt inom 24 timmar.

4) Budfirman får anförtro uppdraget åt ett godkänt ombud eller en godkänd underleverantör. Ansvaret för att uppfylla ovanstående krav vilar dock fortfarande på budfirman.

3. Säkerhetsskyddsklassificerade uppgifter i säkerhetsklassen VS-NUR FÜR DEN DIENSTGEBRAUCH ; HEMLIG/RESTRICTED ska överföras mellan parterna i enlighet med avsändarens nationella bestämmelser, vilket kan inbegripa användning av kommersiella budfirmor.

4. Säkerhetsskyddsklassificerade uppgifter i säkerhetsklasserna VS-VERTRAULICH ; HEMLIG/CONFIDENTIAL och GEHEIM ; HEMLIG/SECRET eller HEMLIG får inte överföras elektroniskt i klartext. Endast kryptografiska system som är godkända av de behöriga säkerhetsmyndigheterna i fråga får användas för krypteringen av säkerhetsskyddsklassificerade uppgifter i säkerhetsklasserna VS-VERTRAULICH ; HEMLIG/CONFIDENTIAL och GEHEIM ; HEMLIG/SECRET eller HEMLIG, oavsett överföringsmetod. Säkerhetsskyddsklassificerade uppgifter i säkerhetsklassen VS-NUR FÜR DEN DIENSTGEBRAUCH ; HEMLIG/RESTRICTED får överföras eller finnas tillgängliga elektroniskt (t.ex. genom punkt-till-punkt-förbindelse mellan datorer) via ett allmänt nätverk som internet, endast om sådan kommersiell krypteringsutrustning används som de behöriga säkerhetsmyndigheterna i de båda parterna har godkänt.

5. När stora mängder säkerhetsskyddsklassificerade uppgifter ska överföras, ska transportsättet, vägen och eskorten, i förekommande fall, bestämmas gemensamt från fall till fall av parternas behöriga säkerhetsmyndigheter. En överföringsplan ska upprättas av den sändande parten och godkännas av den mottagande parten innan överföringen får ske.

Artikel 9
Besök

1. Besök vid verksamhetsställen där säkerhetsskyddsklassificerade uppgifter hanteras eller förvaras ska godkännas i förväg av värdpartens behöriga säkerhetsmyndighet i enlighet med tillämpliga regler och förfaranden, om inte parterna kommer överens om annat. Tillstånd ska endast ges till personer som har behov av det i tjänsten och – med undantag för säkerhetsskyddsklassificerade uppgifter i säkerhetsklass VS-NUR FÜR DEN DIENSTGEBRAUCH ; HEMLIG/RESTRICTED – som är behöriga att ta del av säkerhetsskyddade uppgifter.

2. En framställan om besök ska normalt överlämnas till värdpartens behöriga säkerhetsmyndighet minst 20 dagar före besöket. Den ska innehålla följande uppgifter:

1) Besökarens namn, födelsedatum och födelseort, medborgarskap och pass- eller id-kortsnummer.

2) Besökarens befattning tillsammans med en utförlig beskrivning av det verksamhetsställe som besökaren företräder.

3) Uppgifter om besökarens intyg om säkerhetsgodkännande av personal.

4) Uppgifter om det verksamhetsställe som ska besökas.

5) Syftet med besöket.

6) Besökets/besökens tidpunkt och längd.

3. Säkerhetsskyddsklassificerade uppgifter som röjs för besökare från en part ska behandlas som om de har lämnats ut till den parten och ska skyddas

på vederbörligt sätt. Alla besökare ska uppfylla värdpartens säkerhetsskyddsföreskrifter.

4. Besök som omfattar säkerhetsskyddsklassificerade uppgifter i säkerhetsklass VS-NUR FÜR DEN DIENSTGEBRAUCH; HEMLIG/RESTRICTED får arrangeras direkt mellan det sändande verksamhetsstället och det verksamhetsställe som ska besökas utan samråd med parternas behöriga säkerhetsmyndigheter.

Artikel 10
Säkerhetsskyddsklassificerade kontrakt

1. Innan ett säkerhetsskyddsklassificerat kontrakt tilldelas ska den upphandlande enheten, genom dess behöriga säkerhetsmyndighet, erhålla ett säkerhetsgodkännande av verksamhetsställe från uppdragstagarens behöriga säkerhetsmyndighet. Syftet med säkerhetsgodkännandet av verksamhetsställe är att få en försäkran om att den presumtiva uppdragstagaren är föremål för den nationella behöriga säkerhetsmyndighetens säkerhetstillsyn och om att vederbörande har vidtagit de säkerhetsåtgärder som är nödvändiga för att fullgöra kontraktet. Om en uppdragstagare ännu inte är föremål för säkerhetstillsyn kan en ansökan göras i detta syfte.

2. Ett säkerhetsgodkännande av verksamhetsställe ska också erhållas om ett företag har ombetts att lämna ett anbud och om säkerhetsskyddsklassificerade uppgifter måste lämnas ut före tilldelningen av ett kontrakt under anbudsförfarandet.

3. I de fall som avses i punkterna 1 och 2 ovan ska följande förfarande tillämpas:

1) Framställningar om utfärdande av ett säkerhetsgodkännande av verksamhetsställe ska innehålla information om projektet och de säkerhetsskyddsklassificerade uppgifternas karaktär, omfattning och säkerhetsnivå, som förväntas lämnas ut till uppdragstagaren eller tas fram av denne.

2) Ett säkerhetsgodkännande av verksamhetsställe ska innehålla företagets fullständiga namn, postadress, namnet på säkerhetsansvarig person på företaget, telefon- och faxnummer och, i förekommande fall, e-postadress. Ett säkerhetsgodkännande av verksamhetsställe ska även innehålla information om i vilken utsträckning, och upp till vilken säkerhetsklass, säkerhetsåtgärder har vidtagits av respektive företag på grundval av nationella säkerhetsbestämmelser.

3) Parternas behöriga säkerhetsmyndigheter ska informera varandra om de uppgifter som omfattas av utfärdade säkerhetsgodkännanden av verksamhetsställe ändras.

4) Säkerhetsgodkännanden av verksamhetsställe och framställningar riktade till respektive behöriga säkerhetsmyndigheter för utfärdande av säkerhetsgodkännanden av verksamhetsställe ska överlämnas skriftligen.

4. Parterna ska säkerställa att uppdragstagare och presumtiva uppdragstagare som tar emot säkerhetsskyddsklassificerade uppgifter är medvetna om följande:

1) Definitionen av säkerhetsskyddsklassificerade uppgifter och parternas jämförbara säkerhetsskyddsklassificeringar i enlighet med bestämmelserna i detta avtal.

2) Namn på de nationella behöriga säkerhetsmyndigheter som är behöriga att godkänna utlämnandet och att samordna skyddet av säkerhetsskyddsklassificerade uppgifter som rör det säkerhetsskyddsklassificerade kontraktet.

3) De tillvägagångssätt som ska användas för att överföra de säkerhetsskyddsklassificerade uppgifterna mellan de myndigheter och/eller uppdragstagare som är inblandade.

4) Förfaranden och mekanismer för kommunikation av ändringar som kan uppkomma i fråga om säkerhetsskyddsklassificerade uppgifter antingen på grund av att säkerhetsklassen ändras eller på grund av att det inte längre behövs något skydd.

5) Besöksregler.

6) Att uppdragstagaren får röja säkerhetsskyddsklassificerade uppgifter endast till personer som har behov av dem i tjänsten och, med undantag för säkerhetsklassen VS-NUR FÜR DEN DIENSTGEBRAUCH; HEMLIG/ RESTRICTED, är behöriga och har anlitats för eller medverkar i utförandet av det säkerhetsskyddsklassificerade kontraktet.

7) Att uppdragstagaren inte får röja säkerhetsskyddsklassificerade uppgifter eller tillåta att de röjs till personer som inte skriftligen har godkänts av behörig säkerhetsmyndighet att ta del av dessa.

8) Att uppdragstagaren har en skyldighet att omedelbart meddela behörig säkerhetsmyndighet om faktisk eller misstänkt förlust, läcka eller blottläggning av säkerhetskyddsklassificerade uppgifter i detta kontrakt.

5. Alla säkerhetsskyddsklassificerade kontrakt ska innehålla en vägledning om säkerhetsskyddskraven och klassificeringen av varje aspekt av eller del i kontraktet.

6. Den behöriga säkerhetsmyndigheten i ursprungsparten ska överföra en kopia av de relevanta delarna i det säkerhetsskyddsklassificerade kontraktet till den behöriga säkerhetsmyndigheten i den mottagande parten, för att möjliggöra en adekvat säkerhetskontroll.

Artikel 11
Tillämpning av säkerhetsskyddskrav

I syfte att uppnå och upprätthålla jämförbara normer för säkerhetsskyddet ska var och en av parterna, på begäran, förse den andra parten med information om dess normer, förfaranden och rutiner för att skydda de säkerhetsskyddsklassificerade uppgifterna, och ska i detta syfte göra sitt yttersta för att underlätta besök av den andra partens behöriga säkerhetsmyndighet.

Artikel 12
Förlust eller otillåtet röjande av säkerhetsskyddsklassificerade uppgifter

1. I händelse av förlust eller otillåtet röjande av säkerhetsskyddsklassificerade uppgifter eller vid misstanke om detta ska den mottagande partens behöriga säkerhetsmyndighet omedelbart skriftligen underrätta ursprungspartens behöriga säkerhetsmyndighet.

2. Lämpliga myndigheter i den mottagande parten (vid behov biträdda av ursprungspartens behöriga myndigheter) ska omedelbart undersöka händelsen i enlighet med sina nationella lagar och andra författningar. Den mottagande parten ska utan dröjsmål informera ursprungsparten om omständigheterna kring händelsen, eventuella skador som åsamkats, vilka åtgärder som har vidtagits för att förhindra eller begränsa förlusten eller skadan och resultatet av utredning.

Artikel 13
Kostnader och tvister

1. Alla kostnader som en part har i samband med fullgörandet av skyldigheterna i detta avtal ska den parten svara för.

2. Tvister mellan parterna om tolkningen eller tillämpningen av detta avtal ska lösas genom samråd mellan parterna och får inte hänskjutas till nationell eller internationell domstol eller annan tredje part för avgörande.

Artikel 14
Slutbestämmelser

1. Detta avtal träder i kraft vid dagen för undertecknandet. Avtalet av den 1 december 1969 mellan Konungariket Sveriges regering och Förbundsrepubliken Tysklands regering om ömsesidigt skydd av hemliga uppgifter, ska upphöra att gälla i samband med att detta avtal träder i kraft. Detsamma gäller för den svensk-tyska tilläggsöverenskommelsen av den 1 december 1969 enligt artikel 6 i nämnda avtal, liksom andra befintliga bilagor och tillägg.

2. Detta avtal gäller till dess någon av parterna säger upp det genom att på diplomatisk väg skriftligen meddela den andra parten sex månader i förväg. När avtalet har upphört att gälla ska båda parterna vara ansvariga för skyddet av alla säkerhetsskyddsklassificerade uppgifter som har utbytts i enlighet med bestämmelserna i detta avtal.

3. Detta avtal får skriftligen ändras om parterna kommer överens om det. Var och en av parterna får när som helst överlämna en formell begäran om ändring av detta avtal. Om en sådan begäran överlämnas av en av parterna ska parterna inleda förhandlingar om ändring av avtalet.

4. Den part, inom vars territorium detta avtal ingås, ska omedelbart efter avtalets i kraftträdande skicka avtalet till Förenta nationernas sekretariat för registrering i enlighet med artikel 102 i Förenta nationernas (FN) stadga. Den andra parten ska informeras om registreringen och om registreringsnumret hos FN så snart detta har bekräftats av sekretariatet.

Undertecknat i Stockholm den 31 mars 2016 i två exemplar på svenska, tyska och engelska språken, vilka alla tre är lika giltiga. Vid skiljaktiga tolkningar av den tyska och svenska texten ska den engelska texten gälla.

För Konungariket Sveriges regering	För Förbundsrepubliken Tysklands regering
Julius Liljeström	Michael Bock

Abkommen
zwischen
der Regierung des Königreichs Schweden
und
der Regierung der Bundesrepublik Deutschland
über
den gegenseitigen Schutz von Verschlusssachen

Die Regierung des Königreichs Schweden

und

die Regierung der Bundesrepublik Deutschland
(im Folgenden als „Vertragsparteien“ bezeichnet) –

in dem Wunsch, den Geheimschutz von Verschlusssachen zu gewährleisten,

in dem Wunsch, die Zusammenarbeit, Forschung, Entwicklung, Herstellung und Beschaffung im Rüstungsbereich zu verbessern,

in der Erkenntnis, dass diese Zusammenarbeit den Austausch von Verschlusssachen zwischen den zuständigen Behörden und Unternehmen der Rüstungsindustrie erfordern kann,

in Anerkennung des Rahmenübereinkommens vom 27. Juli 2000 zwischen dem Königreich Schweden, der Bundesrepublik Deutschland, der Französischen Republik, der Italienischen Republik, dem Königreich Spanien und dem Vereinigten Königreich Großbritannien und Nordirland über Maßnahmen zur Erleichterung der Umstrukturierung und der Tätigkeit der europäischen Rüstungsindustrie –

sind wie folgt übereingekommen:

Artikel 1
Begriffsbestimmungen

Im Sinne dieses Abkommens gelten die folgenden Begriffsbestimmungen:

1. Verschlusssachen: Informationen, unabhängig von ihrer Form, die nach den Gesetzen und sonstigen Vorschriften der Vertragsparteien gegen Verlust, unbefugte Bekanntgabe oder eine andere Form der Preisgabe zu schützen sind und nach Artikel 4 Absatz 1 als solche gekennzeichnet sind;

2. Verschlusssachenauftrag: eine Vereinbarung zwischen zwei oder mehr Parteien, die Verschlusssachen beinhaltet oder einbezieht und mit der im Rechtsweg durchsetzbare Rechte und Pflichten zwischen den Parteien bestimmt werden;

3. herausgebende Vertragspartei: die Vertragspartei, einschließlich der ihrer Gerichtsbarkeit unterstehenden öffentlichen oder privaten Rechtsträger, die

Verschlusssachen an die andere Vertragspartei freigibt und den Geheimhaltungsgrad dieser Informationen festlegt;

4. empfangende Vertragspartei: die Vertragspartei, einschließlich der ihrer Gerichtsbarkeit unterstehenden öffentlichen oder privaten Rechtsträger, die Verschlusssachen von der herausgebenden Vertragspartei erhält.

Artikel 2
Allgemeine Bestimmungen

Die Pflichten der Vertragsparteien aus diesem Abkommen sind im Einklang mit den innerstaatlichen Gesetzen und sonstigen Vorschriften jeder Vertragspartei auszulegen.

Artikel 3
Zuständige Sicherheitsbehörden

(1) Für die Durchführung dieses Abkommens sind die zuständigen Sicherheitsbehörden die folgenden:
a) in der Bundesrepublik Deutschland:
Bundesministerium des Innern (nationale Sicherheitsbehörde),
Bundesministerium für Wirtschaft und Energie (beauftragte Sicherheitsbehörde)
Bundesministerium der Verteidigung (militärische Sicherheitsbehörde)
b) im Königreich Schweden:
Militärischer Nachrichtendienst (nationale Sicherheitsbehörde)
Wehrmaterialverwaltung (beauftragte Sicherheitsbehörde)

(2) Jede Vertragspartei stellt der anderen die erforderlichen Kontaktdaten ihrer zuständigen Sicherheitsbehörden zur Verfügung.

Artikel 4
Vergleichbare Geheimhaltungsgrade

(1) Die Vertragsparteien legen fest, dass die folgenden Geheimhaltungsgrade vergleichbar und von diesem Abkommen erfasst sind:

Im Königreich Schweden		In der Bundesrepublik Deutschland
Behörden des Verteidigungsbereichs	Andere Behörden	
HEMLIG/ TOP SECRET	HEMLIG av synnerlig betydelse för rikets säkerhet	STRENG GEHEIM
HEMLIG/SECRET	HEMLIG	GEHEIM
HEMLIG/ CONFIDENTIAL	siehe Absatz 2	VS-VERTRAULICH
HEMLIG/ RESTRICTED	siehe Absatz 2	VS-NUR FÜR DEN DIENSTGEBRAUCH

(2) Informationen der Bundesrepublik Deutschland, die als VS-NUR FÜR DEN DIENSTGEBRAUCH und VS-VERTRAULICH gekennzeichnet sind,

werden im Königreich Schweden von Behörden außerhalb des Verteidigungsbereichs als HEMLIG behandelt, es sei denn, die herausgebende Vertragspartei stellt ein anderslautendes Ersuchen. Sie behalten ihre deutsche Kennzeichnung.

(3) Bei Rückgabe von deutschen Verschlusssachen der Geheimhaltungsgrade VS-NUR FÜR DEN DIENSTGEBRAUCH und VS-VERTRAULICH werden diese in Deutschland entsprechend ihrem ursprünglichen deutschen Geheimhaltungsgrad geschützt.

(4) Ändert eine Vertragspartei ihre innerstaatlichen Geheimhaltungsgrade, so unterrichtet sie die andere Vertragspartei hiervon nachträglich.

(5) In besonderen Fällen kann eine Vertragspartei die zuständige Sicherheitsbehörde der anderen Vertragspartei darum ersuchen, einen anderen als den durch den entsprechenden Geheimhaltungsgrad angezeigten Schutz zu gewähren. Die Änderung des Geheimhaltungsgrads muss deutlich sichtbar sein und von einem dazu ermächtigten Sicherheitsbeamten unterzeichnet werden.

Artikel 5
Beschränkungen hinsichtlich Nutzung und Bekanntgabe

Die Vertragsparteien dürfen ohne vorherige Rücksprache Verschlusssachen weder freigeben, bekanntgeben oder nutzen, noch deren Freigabe, Bekanntgabe oder Nutzung zulassen, es sei denn, dies geschieht zu dem von der herausgebenden Vertragspartei festgelegten Zweck und mit den von ihr festgelegten Einschränkungen.

Artikel 6
Schutz von Verschlusssachen

(1) Die herausgebende Vertragspartei

a) stellt sicher, dass freigegebene Verschlusssachen mit einer geeigneten Kennzeichnung des innerstaatlichen Geheimhaltungsgrads nach Artikel 4 Absatz 1 gekennzeichnet werden;

b) unterrichtet die empfangende Vertragspartei über etwaige Bedingungen für eine Freigabe beziehungsweise Beschränkungen hinsichtlich der Nutzung von Verschlusssachen;

c) unterrichtet die empfangende Vertragspartei über nachträgliche Änderungen des Geheimhaltungsgrads freigegebener Verschlusssachen.

(2) Die empfangende Vertragspartei

a) gewährt empfangenen Verschlusssachen den ihren eigenen Verschlusssachen entsprechenden Grad an Geheimschutz;

b) stellt sicher, dass Verschlusssachen mit ihren eigenen entsprechenden Geheimhaltungsgraden nach Artikel 4 gekennzeichnet werden;

c) stellt sicher, dass Geheimhaltungsgrade nicht geändert werden, es sei denn, dies wurde von der herausgebenden Vertragspartei oder in deren Auftrag schriftlich genehmigt.

Artikel 7
Zugang zu Verschlusssachen

(1) Der Zugang zu Verschlusssachen ist auf Personen zu beschränken, die die Bedingung „Kenntnis nur, wenn nötig“ erfüllen und die – außer im Fall von Verschlusssachen des Geheimhaltungsgrads HEMLIG/RESTRICTED / VS-NUR FÜR DEN DIENSTGEBRAUCH – zum Zugang zu Verschlusssachen des jeweiligen Geheimhaltungsgrads im Einklang mit den innerstaatlichen Gesetzen und sonstigen Vorschriften bereits ermächtigt und über den Schutz von Verschlusssachen belehrt worden sind. Eine Sicherheitsüberprüfung ist nicht vorgeschrieben für Personen, die nach den innerstaatlichen Gesetzen und sonstigen Vorschriften aufgrund ihrer Funktion zum Zugang zu Verschlusssachen ermächtigt sind.

(2) Vorbehaltlich der Erfüllung der in den innerstaatlichen Gesetzen und sonstigen Vorschriften niedergelegten Verfahrensvorschriften erkennen die Vertragsparteien die jeweiligen Sicherheitsüberprüfungsbescheinigungen der anderen Vertragspartei an.

(3) Sicherheitsüberprüfungen von Staatsangehörigen einer Vertragspartei, die ihren rechtmäßigen Aufenthalt im Staat der anderen Vertragspartei haben und sich dort um eine sicherheitsempfindliche Stellung bewerben, werden von der zuständigen Sicherheitsbehörde dieses Staates durchgeführt, wobei gegebenenfalls Sicherheitsauskünfte im Ausland eingeholt werden.

Artikel 8
Übermittlung von Verschlusssachen

(1) Verschlusssachen werden zwischen den beiden Staaten nach den innerstaatlichen Gesetzen und sonstigen Vorschriften der herausgebenden Vertragspartei übermittelt. Üblicher Transportweg ist der offizielle diplomatische Kurier von Regierung zu Regierung, jedoch können andere Vereinbarungen wie beispielsweise eine Beförderung von Hand zu Hand oder sichere Kommunikationsverbindungen (verschlüsselt) getroffen werden, sofern beide Vertragsparteien dem zustimmen.

(2) In dringenden Fällen, das heißt, nur wenn die Nutzung des diplomatischen Kuriergepäcks von Regierung zu Regierung den Erfordernissen nicht gerecht wird, dürfen Verschlusssachen des Geheimhaltungsgrads HEMLIG/ CONFIDENTIAL / VS-VERTRAULICH durch zugelassene kommerzielle Kurierdienste übermittelt werden, sofern die folgenden Voraussetzungen erfüllt sind:

1. Der Kurierdienst ist im Hoheitsgebiet der Vertragsparteien ansässig und hat für die Beförderung von Wertgegenständen ein Sicherheitssystem mit Unterschriftsleistung und lückenlosem Nachweis der Verantwortlichkeit für den Gewahrsam mittels eines Quittungs- und Nachweisbuchs oder eines elektronischen Ermittlungs- beziehungsweise Nachforschungssystems eingerichtet;

2. der Kurierdienst muss über Annahme und Auslieferung einer Sendung ein Quittungs- und Nachweisbuch führen, anhand dessen er dem Absender einen Auslieferungsbeleg vorlegt, oder der Kurier muss auf einem Frachtbeleg mit Registriernummer den Empfangsnachweis führen;

3. der Kurierdienst muss gewährleisten, dass die Sendung dem Empfänger unter normalen Umständen innerhalb einer Frist von 24 Stunden bis zu einem bestimmten Datum und Zeitpunkt überbracht wird;

4. der Kurierdienst kann einen zugelassenen Beauftragten oder Subunternehmer beauftragen. Die Verantwortung für die Erfüllung der genannten Voraussetzungen muss jedoch beim Kurierdienst verbleiben.

(3) Verschlusssachen des Geheimhaltungsgrads HEMLIG/RESTRICTED / VS-NUR FÜR DEN DIENSTGEBRAUCH werden zwischen den Vertragsparteien nach den innerstaatlichen Vorschriften des Absenders übermittelt, die auch die Nutzung kommerzieller Kurierdienste vorsehen können.

(4) Verschlusssachen der Geheimhaltungsgrade HEMLIG/CONFIDENTIAL / VS-VERTRAULICH und HEMLIG/SECRET beziehungsweise HEMLIG / GEHEIM dürfen auf elektronischem Weg nicht im Klartext übermittelt werden. Unabhängig von der Art der Übermittlung sind für die Verschlüsselung von Verschlusssachen der Geheimhaltungsgrade HEMLIG/ CONFIDENTIAL / VS-VERTRAULICH und HEMLIG/SECRET beziehungsweise HEMLIG / GEHEIM nur Verschlüsselungssysteme zu verwenden, die von den betreffenden zuständigen Sicherheitsbehörden zugelassen wurden. Verschlusssachen des Geheimhaltungsgrads HEMLIG/RESTRICTED / VS-NUR FÜR DEN DIENSTGEBRAUCH können elektronisch (zum Beispiel mittels Punkt-zu-Punkt-Computerverbindungen) über ein öffentliches Netz wie das Internet nur unter Verwendung handelsüblicher, von den zuständigen Sicherheitsbehörden gegenseitig anerkannter Verschlüsselungseinrichtungen übermittelt oder abgerufen werden.

(5) Sind Verschlusssachen von erheblichem Umfang zu übermitteln, so werden das Beförderungsmittel, der Transportweg und gegebenenfalls der Begleitschutz im jeweiligen Einzelfall von den zuständigen Sicherheitsbehörden der Vertragsparteien gemeinsam festgelegt. Bevor die Beförderung stattfindet, wird ein Beförderungsplan von der absendenden Vertragspartei erstellt und von der empfangenden Vertragspartei genehmigt.

Artikel 9
Besuche

(1) Sofern nichts anderes vereinbart wird, unterliegen Besuche in Einrichtungen, in denen mit Verschlusssachen gearbeitet wird oder in denen diese aufbewahrt werden, der vorherigen Zustimmung der zuständigen Sicherheitsbehörde der gastgebenden Vertragspartei im Einklang mit den geltenden Vorschriften und Verfahren. Die Erlaubnis wird nur Personen erteilt, die die Bedingung „Kenntnis nur, wenn nötig“ erfüllen und die – außer im Fall von Verschlusssachen des Geheimhaltungsgrads HEMLIG/RESTRICTED / VS-NUR FÜR DEN DIENSTGEBRAUCH – zum Zugang zu Verschlusssachen ermächtigt sind.

(2) Besuchsanmeldungen sind der zuständigen Sicherheitsbehörde der gastgebenden Vertragspartei im Normalfall mindestens 20 Tage vor dem Besuch mit folgenden Angaben vorzulegen:

1. Name, Geburtsdatum und ort, Staatsangehörigkeit sowie Pass- oder Personalausweisnummer des Besuchers;
2. Stellung des Besuchers und genaue Bezeichnung der von ihm vertretenen Einrichtung;
3. Einzelheiten zur Sicherheitsüberprüfung des Besuchers;
4. genaue Bezeichnung der zu besuchenden Einrichtung;
5. Besuchszweck;
6. Datum und Dauer des Besuchs/der Besuche.

(3) Besuchern einer Vertragspartei gegenüber bekanntgegebene Verschlusssachen werden so behandelt, als seien sie an diese Vertragspartei freigegeben worden, und entsprechend geschützt. Sämtliche Besucher haben die Sicherheitsvorschriften der gastgebenden Vertragspartei einzuhalten.

(4) Besuche im Zusammenhang mit Verschlusssachen des Geheimhaltungsgrads HEMLIG/RESTRICTED / VS-NUR FÜR DEN DIENSTGEBRAUCH können unmittelbar ohne Einschaltung der zuständigen Sicherheitsbehörden der Vertragsparteien zwischen der entsendenden und der zu besuchenden Einrichtung vereinbart werden.

Artikel 10
Verschlusssachenaufträge

(1) Vor der Vergabe eines Verschlusssachenauftrags holt die auftraggebende Stelle über ihre zuständige Sicherheitsbehörde bei der zuständigen Sicherheitsbehörde des Auftragnehmers einen Sicherheitsbescheid ein. Zweck des Sicherheitsbescheids ist es, sich vergewissern zu können, ob der in Aussicht genommene Auftragnehmer der Geheimschutzaufsicht durch die nationale zuständige Sicherheitsbehörde unterliegt und ob er die für die Auftragsdurchführung erforderlichen Geheimschutzvorkehrungen getroffen hat. Unterliegt ein Auftragnehmer noch nicht der Geheimschutzaufsicht, so kann dies beantragt werden.

(2) Ein Sicherheitsbescheid ist auch dann einzuholen, wenn ein Unternehmen zur Abgabe eines Angebots aufgefordert worden ist und im Rahmen des Ausschreibungsverfahrens bereits vor Auftragserteilung Verschlusssachen überlassen werden müssen.

(3) In den Fällen der Absätze 1 und 2 wird das folgende Verfahren angewendet:
1. Ersuchen um Ausstellung eines Sicherheitsbescheids enthalten Angaben über das Vorhaben sowie die Art, den Umfang und den Geheimhaltungsgrad der dem Auftragnehmer voraussichtlich zu überlassenden oder bei ihm entstehenden Verschlusssachen;
2. ein Sicherheitsbescheid enthält die vollständige Bezeichnung des Unternehmens, seine Postanschrift und den Namen des Sicherheitsbevollmächtigten sowie dessen Telefon- und Faxverbindung und gegebenenfalls EMail-Adresse. Ein Sicherheitsbescheid enthält ferner insbesondere Angaben darüber, in welchem Umfang und bis zu welchem Geheimhaltungsgrad bei dem betreffenden Unternehmen Geheimschutzmaßnahmen auf der Grundlage innerstaatlicher Geheimschutzvorschriften getroffen worden sind;

3. die zuständigen Sicherheitsbehörden der Vertragsparteien teilen es einander mit, wenn sich die den ausgestellten Sicherheitsbescheiden zugrundeliegenden Sachverhalte ändern;

4. Sicherheitsbescheide und an die jeweiligen zuständigen Sicherheitsbehörden gerichtete Ersuchen um Ausstellung von Sicherheitsbescheiden sind schriftlich zu übermitteln.

(4) Die Vertragsparteien stellen sicher, dass Auftragnehmern oder zukünftigen Auftragnehmern, die Verschlusssachen erhalten, die folgenden Bestimmungen bekannt sind:

1. die Bestimmung des Begriffs „Verschlusssache“ und der vergleichbaren Geheimhaltungsgrade der Vertragsparteien in Übereinstimmung mit diesem Abkommen;

2. der jeweilige Name der nationalen zuständigen Sicherheitsbehörden, die zur Genehmigung der Freigabe von Verschlussachen, die mit einem Verschlusssachenauftrag im Zusammenhang stehen, und zur Koordinierung des Schutzes dieser Verschlusssachen ermächtigt sind;

3. die Wege, über die Verschlusssachen zwischen den Behörden beziehungsweise den beteiligten Auftragnehmern weiterzugeben sind;

4. die Verfahren und Mechanismen für die Mitteilung der Änderungen, die sich in Bezug auf Verschlusssachen aufgrund von Änderungen des ihnen zugewiesenen Geheimhaltungsgrads oder aufgrund des Wegfalls der Schutzbedürftigkeit möglicherweise ergeben;

5. die Verfahren für Besuche;

6. die dem Auftragnehmer obliegende Pflicht, Verschlusssachen nur solchen Personen bekanntzugeben, die die Bedingung „Kenntnis nur, wenn nötig“ erfüllen und die – außer im Fall des Geheimhaltungsgrads HEMLIG/RESTRICTED / VS-NUR FÜR DEN DIENSTGEBRAUCH – mit der Durchführung eines Verschlusssachenauftrags beauftragt oder daran beteiligt beziehungsweise dazu ermächtigt sind;

7. die dem Auftragnehmer obliegende Pflicht, keine Verschlusssachen an Personen weiterzugeben, die nicht von der entsprechenden zuständigen Sicherheitsbehörde schriftlich zum Zugang ermächtigt worden sind, beziehungsweise eine solche Weitergabe nicht zu gestatten;

8. die dem Auftragnehmer obliegende Pflicht, die entsprechende zuständige Sicherheitsbehörde unverzüglich über jeden erfolgten oder mutmaßlichen Verlust sowie jede begangene oder mutmaßliche Indiskretion oder Preisgabe der unter den Auftrag fallenden Verschlusssachen zu unterrichten.

(5) Jeder Verschlusssachenauftrag enthält Hinweise zu den Sicherheitsanforderungen und zum Geheimhaltungsgrad jedes Aspekts beziehungsweise Elements des Auftrags.

(6) Um eine angemessene Sicherheitsüberwachung zu ermöglichen, leitet die zuständige Sicherheitsbehörde der herausgebenden Vertragspartei der zuständigen Sicherheitsbehörde der empfangenden Vertragspartei eine Kopie der einschlägigen Teile des Verschlusssachenauftrags zu.

Artikel 11

Um vergleichbare Sicherheitsnormen zu erreichen und aufrechtzuerhalten, stellt jede Vertragspartei der anderen Vertragspartei auf deren Ersuchen Informationen über ihre Sicherheitsnormen und verfahren sowie ihre Sicherheitspraxis zur Gewährleistung des Schutzes von Verschlusssachen zur Verfügung; zu diesem Zweck bemüht sie sich nach besten Kräften, Besuche durch die zuständigen Sicherheitsbehörden der anderen Vertragspartei zu erleichtern.

Artikel 12
Verlust oder unbefugte Bekanntgabe von Verschlusssachen

(1) Im Fall des Verlusts oder der unbefugten Bekanntgabe von Verschlusssachen oder einer entsprechenden Vermutung unterrichtet die zuständige Sicherheitsbehörde der empfangenden Vertragspartei die zuständige Sicherheitsbehörde der herausgebenden Vertragspartei unverzüglich schriftlich.

(2) Die einschlägigen Behörden der empfangenden Vertragspartei führen (erforderlichenfalls mit Hilfe der zuständigen Behörden der herausgebenden Vertragspartei) im Einklang mit ihren innerstaatlichen Gesetzen und sonstigen Vorschriften unverzüglich Ermittlungen bezüglich des Vorfalls durch. Die empfangende Vertragspartei unterrichtet die herausgebende Vertragspartei unverzüglich über die Umstände des Vorfalls, einen etwaigen Schaden, die zur Verhinderung oder Eindämmung des Verlusts oder Schadens ergriffenen Maßnahmen und das Ermittlungsergebnis.

Artikel 13
Kosten und Streitigkeiten

(1) Jede Vertragspartei trägt die von ihr bei der Erfüllung der Verpflichtungen aus diesem Abkommen verursachten Kosten.

(2) Streitigkeiten zwischen den Vertragsparteien über die Auslegung oder Anwendung dieses Abkommens werden durch Konsultationen der Vertragsparteien beigelegt und nicht an nationale oder internationale Gerichte oder Dritte zur Beilegung verwiesen.

Artikel 14
Schlussbestimmungen

(1) Dieses Abkommen tritt am Tag seiner Unterzeichnung in Kraft. Mit Inkrafttreten dieses Abkommens treten die Vereinbarung vom 1. Dezember 1969 zwischen der Regierung des Königreichs Schweden und der Regierung der Bundesrepublik Deutschland über den gegenseitigen Schutz von Verschlusssachen sowie die schwedisch-deutsche Zusatzvereinbarung vom 1. Dezember 1969 gemäß Artikel 6 der vorgenannten Vereinbarung sowie jegliche andere gegebenenfalls vorhandenen Zusätze oder Ergänzungen außer Kraft.

(2) Dieses Abkommen bleibt in Kraft, solange es nicht von einer der Vertragsparteien unter Einhaltung einer Frist von sechs Monaten gegenüber der anderen Vertragspartei auf diplomatischem Weg schriftlich gekündigt wird. Beide Vertragsparteien bleiben nach der Kündigung für den Schutz aller nach diesem Abkommen ausgetauschten Verschlusssachen verantwortlich.

(3) Dieses Abkommen kann einvernehmlich in Schriftform von den Vertragsparteien geändert werden. Jede Vertragspartei kann jederzeit ein förmliches Ersuchen um Änderung dieses Abkommens vorlegen. Legt eine Vertragspartei ein solches Ersuchen vor, so treten die Vertragsparteien in Verhandlungen über die Änderung des Abkommens ein.

(4) Die Registrierung dieses Abkommens beim Sekretariat der Vereinten Nationen nach Artikel 102 der Charta der Vereinten Nationen wird unverzüglich nach seinem Inkrafttreten von der Vertragspartei veranlasst, in deren Staatsgebiet das Abkommen geschlossen wird. Die andere Vertragspartei wird unter Angabe der VNRegistriernummer von der erfolgten Registrierung unterrichtet, sobald diese vom Sekretariat der Vereinten Nationen bestätigt worden ist.

Geschehen zu Stockholm am 31 März 2016 in zwei Urschriften, jede in schwedischer, deutscher und englischer Sprache, wobei jeder Wortlaut verbindlich ist. Bei unterschiedlicher Auslegung des schwedischen und des deutschen Wortlauts ist der englische Wortlaut maßgebend.

Für die Regierung des Königreichs Schweden	Für die Regierung der Bundesrepublik Deutschland
Julius Liljeström	Michael Bock

Agreement
between
the Government of the Kingdom of Sweden
and
the Government of the Federal Republic of Germany
concerning
the Mutual Protection of Classified Information

The Government of the Kingdom of Sweden

and

the Government of the Federal Republic of Germany

(hereinafter referred to as the Parties),

wishing to ensure the protective security of Classified Information;

wishing to enhance the cooperation, research, development, production and procurement in the area of defence;

realising that such cooperation may require exchange of Classified Information between competent authorities and defence industries;

recognising the Framework Agreement between the French Republic, the Federal Republic of Germany, the Italian Republic, the Kingdom of Spain, the Kingdom of Sweden and the United Kingdom of Great Britain and Northern Ireland concerning Measures to Facilitate the Restructuring and Operation of the European Defence Industry on 27 July 2000,

have agreed as follows:

Article 1
Definitions

For the purposes of this Agreement, the following definitions shall apply:

1. Classified Information: information, regardless of its form, that under the laws and regulations of either Party requires protection against loss, unauthorised disclosure or other compromise, and has been so designated according to Article 4 Paragraph (1) of this Agreement;

2. Classified Contract: an Agreement between two or more parties, containing or involving Classified Information and defining enforceable rights and obligations between the parties;

3. Originating Party: the Party, including any public or private entities under its jurisdiction, which releases Classified Information to the other Party and decides the level of classification of such information;

4. Recipient Party: the Party, including any public or private entities under its jurisdiction, which receives Classified Information from the Originating Party.

Article 2
General Provisions

The Parties' obligations under this Agreement are to be interpreted in accordance with each Party's national laws and regulations.

Article 3
Competent Security Authorities

(1) For the purpose of implementing this Agreement, the Competent Security Authorities are:

a) In the Federal Republic of Germany:

Federal Ministry of the Interior (National Security Authority)

Federal Ministry for Economic Affairs and Energy (Designated Security Authority)

Federal Ministry of Defence (Military Security Authority)

b) In the Kingdom of Sweden:

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

The Defence Materiel Administration (Designated Security Authority)

(2) Each Party shall provide the other with the necessary contact data of their Competent Security Authorities.

Article 4
Comparable Security Classifications

(1) The Parties determine that the following security classifications shall be comparable and covered by this Agreement:

In the Kingdom of Sweden		In the Federal Republic of Germany
defence authorities	other authorities	
HEMLIG/ TOP SECRET	HEMLIG av synnerlig betydelse för rikets säkerhet	STRENG GEHEIM
HEMLIG/SECRET	HEMLIG	GEHEIM
HEMLIG/ CONFIDENTIAL	cf. paragraph 2 below	VS-VERTRAULICH
HEMLIG/ RESTRICTED	cf. paragraph 2 below	VS-NUR FÜR DEN DIENSTGEBRAUCH

(2) Information from the Federal Republic of Germany bearing the marking of VS-NUR FÜR DEN DIENSTGEBRAUCH and VS-VERTRAULICH shall be treated as HEMLIG by other authorities than defence authorities in the Kingdom of Sweden unless otherwise requested by the Originating Party. It shall retain its German marking.

(3) Any German Classified Information at the VS-NUR FÜR DEN DIENSTGEBRAUCH and the VS-VERTRAULICH levels that is returned to Germany shall be protected at its original German level of classification.

(4) When a Party alters its national classification, it shall notify the other Party subsequently.

(5) On specific occasions one Party may ask the other Party's Competent Security Authorities to afford protection at another level than the equivalent classification indicates. The change of classification must be clearly visible and signed by an authorised security officer.

Article 5
Restrictions on Use and Disclosure

The Parties shall not, without prior consultation, release, disclose, use or permit the release, disclosure or use of any Classified Information except for the purpose and within the limitations stated by the Originating Party.

Article 6
Protection of Classified Information

(1) The Originating Party shall:

a) ensure that released Classified Information is marked with an appropriate national security classification marking according to Article 4 Paragraph (1);

b) inform the Recipient Party of any conditions of release or limitations on the use of the Classified Information, as applicable;

c) inform the Recipient Party of any subsequent changes in the security classification of released Classified Information.

(2) The Recipient Party shall:

a) afford the equivalent level of security protection to received Classified Information as afforded to its own Classified Information;

b) ensure that Classified Information is marked with its own equivalent classification in accordance with Article 4;

c) ensure that security classifications are not altered, except if authorised in writing by or on behalf of the Originating Party.

Article 7
Access to Classified Information

(1) Access to Classified Information shall be limited to those persons who have a need-to-know and, except for Classified Information at the level of HEMLIG/RESTRICTED / VS-NUR FÜR DEN DIENSTGEBRAUCH, have been previously security cleared in accordance with national laws and regulations to the appropriate classification level and have been briefed on Classified Information protection. A security clearance is not mandatory for persons who are authorised in accordance with national laws and regulations to have access to Classified Information by virtue of their function.

(2) Subject to fulfilment of procedural requirements laid out in national laws and regulations, the Parties shall mutually recognise their respective certificates of Personnel Security Clearance.

(3) Personnel Security Clearances for nationals of one Party who are legally resident in the country of the other Party and apply for a security-sensitive position in that country shall be undertaken by the Competent Security Authority of that country, conducting overseas checks as appropriate.

Article 8
Transmission of Classified Information

(1) Classified information shall be transmitted between the two countries in accordance with the national laws and regulations of the Originating Party. The normal route shall be through official diplomatic Government-to-Government channels, but other arrangements may be established, such as hand carriage or secure communications (encryption), if mutually approved by both Parties.

(2) In cases of urgency, i.e. only when the use of Government-to-Government diplomatic channels cannot meet the requirements, Classified Information at the HEMLIG/CONFIDENTIAL / VS-VERTRAULICH level may be transmitted via approved commercial courier companies, provided that the following criteria are met:

1. The courier company is located within the territory of the Parties and has established a protective security programme for handling valuable items with a signature service, including a record of continuous accountability on custody through either a signature and tally record, or an electronic tracking or tracing system;
2. The courier company must obtain and provide to the sender proof of delivery on the signature and tally record, or it must obtain receipts against package numbers;
3. The courier company must guarantee that the consignment shall be delivered to the recipient by a specific time and date, under normal circumstances within a 24-hour period;
4. The courier company may charge an approved commissioner or subcontractor. However, the responsibility for fulfilling the above requirements must remain with the courier company.

(3) Classified Information at the HEMLIG/RESTRICTED / VS-NUR FÜR DEN DIENSTGEBRAUCH level shall be transmitted between the Parties in accordance with the national regulations of the sender, which may include the use of commercial courier companies.

(4) Classified Information at the HEMLIG/CONFIDENTIAL / VS-VERTRAULICH and HEMLIG/SECRET or HEMLIG / GEHEIM levels must not be transmitted electronically in clear text. Only cryptographic systems approved by the Competent Security Authorities concerned shall be used for the encryption of Classified Information at the HEMLIG/CONFIDENTIAL / VS-VERTRAULICH and HEMLIG/SECRET or HEMLIG / GEHEIM levels, irrespective of the method of transmission. Classified Information at the HEM-

LIG/RESTRICTED / VS-NUR FÜR DEN DIENSTGEBRAUCH level may be transmitted or accessed electronically (e.g. by means of point-to-point computer links) via a public network like the Internet, only using commercial encryption devices mutually accepted by the Competent Security Authorities.

(5) When large volumes of Classified Information are to be transmitted, the means of transport, the route and the escort if any shall be jointly determined on a case-by-case basis by the Competent Security Authorities of the Parties. A transportation plan shall be established by the sending Party and approved by the recipient Party before the transport shall take place.

Article 9
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 following the applicable rules and procedures, unless otherwise agreed. Permission shall be given only to persons having a need-to-know and – except in the case of Classified Information at the HEMLIG/RESTRICTED / VS-NUR FÜR DEN DIENSTGEBRAUCH level – having been authorised to have access to Classified Information.

(2) A request for a visit shall be submitted to the Competent Security Authority of the host Party, normally at least 20 days prior to the visit, and shall include the following:

1. name of the visitor, date and place of birth, nationality and ID or passport number;
2. position of the visitor together with a specification of the facility which the visitor represents;
3. details of the Personnel Security Clearance of the visitor;
4. specification of the facility to be visited;
5. purpose of the visit;
6. dates and duration of the visit(s).

(3) Classified Information disclosed to visitors from a Party shall be treated as if released to that Party, and shall be protected accordingly. All visitors shall comply with the security regulations of the host Party.

(4) Visits relating to Classified Information at the HEMLIG/RESTRICTED / VS-NUR FÜR DEN DIENSTGEBRAUCH level may be arranged directly between the sending facility and the facility to be visited without consultation of the Competent Security Authorities of the Parties.

Article 10
Classified Contracts

(1) Prior to the award of a Classified Contract, the contracting entity shall, through its Competent Security Authority, obtain a Facility Security Clearance from the Competent Security Authority of the contractor. The purpose of the Facility Security Clearance is to obtain assurance as to whether the prospective contractor is subject to security oversight by the national Competent

Security Authority and whether it has taken the security precautions required for discharging the performance of the contract. Where a contractor is not yet subject to security oversight, an application may be made to that end.

(2) A Facility Security Clearance shall also be obtained if an enterprise has been requested to submit a bid and if Classified Information will have to be released prior to the award of a contract under the bidding procedure.

(3) In the cases referred to in paragraphs (1) and (2) above, the following procedure shall be applied:

1. Requests for the issuance of a Facility Security Clearance shall contain information on the project as well as the nature, the scope and the level of security classification of the Classified Information expected to be released to the contractor or to be generated by him;

2. A Facility Security Clearance shall include the full name of the enterprise, its postal address, the name of its security official, its telephone and fax number and, if applicable, its e-mail address. A Facility Security Clearance shall also include information in particular on the extent to which, and the level of security classification up to which, security measures have been taken by the respective enterprise on the basis of national security regulations;

3. The Competent Security Authorities of the Parties shall inform each other of any changes in the facts covered by issued Facility Security Clearances;

4. Facility Security Clearances and requests addressed to the respective Competent Security Authorities for the issuance of Facility Security Clearances shall be transmitted in writing.

(4) The Parties shall ensure that contractors or prospective contractors that receive Classified Information are aware of the following provisions:

1. the definition of Classified Information and of the comparable levels of security classification of the Parties in accordance with the provisions of this Agreement;

2. the name of the national Competent Security Authorities empowered to authorise the release and to coordinate the safeguarding of Classified Information related to the Classified Contract;

3. the channels to be used for the transfer of the Classified Information between the government authorities and/or contractors involved;

4. the procedures and mechanisms for communicating the changes that may arise in respect of Classified Information either because of changes in its security classification or because protection is no longer necessary;

5. the procedures for visits;

6. an obligation that the contractor shall disclose the Classified Information only to a person who has a need-to-know and, except for the level of HEMLIG/RESTRICTED / VS-NUR FÜR DEN DIENSTGEBRAUCH, has been authorised and is employed on or engaged in the carrying out of the Classified Contract;

7. an obligation that the Contractor shall not disclose the Classified Information or permit it to be disclosed to any person not cleared in writing by the relevant Competent Security Authority to have such access;

8. an obligation that the contractor shall immediately notify the relevant Competent Security Authority of any actual or suspected loss, leak or compromise of the Classified Information of this contract.

(5) Each Classified Contract shall contain guidance on the security requirements and on the classification of each aspect or element of the contract.

(6) The Competent Security Authority of the Originating Party shall pass a copy of the relevant parts of the Classified Contract to the Competent Security Authority of the Recipient Party, to allow adequate security monitoring.

Article 11
Implementation of Security Requirements

In order to achieve and maintain comparable standards of security each Party shall, on request, provide to the other Party information about its security standards, procedures and practices for safeguarding Classified Information, and shall for this purpose make its best effort to facilitate visits by the Competent Security Authorities of the other Party.

Article 12
Loss or Unauthorised Disclosure of Classified Information

(1) In the event of the loss or unauthorised disclosure of Classified Information, or suspicion thereof, the Competent Security Authority of the Recipient Party shall immediately inform the Competent Security Authority of the Originating Party in writing.

(2) The appropriate authorities of the Recipient Party (assisted by competent authorities of the Originating Party, if required) shall carry out an immediate investigation of the incident in accordance with their national laws and regulations. The Recipient Party shall without delay inform the Originating Party about the circumstances of the incident, any damage caused, measures adopted to prevent or to mitigate the loss or damage and the outcome of the investigation.

Article 13
Costs and Disputes

(1) All costs incurred by one Party in the fulfilment of the obligations in this Agreement shall be borne by that Party.

(2) Any dispute between the Parties regarding the interpretation or application of this Agreement shall be resolved by consultation between the Parties and shall not be referred to any national or international tribunal or third party for settlement.

Article 14
Final Provisions

(1) This Agreement shall enter into force on the date of signature thereof. The Agreement of 1 December 1969 between the Government of the Kingdom of Sweden and the Government of the Federal Republic of Germany concerning the Mutual Protection of Classified Information as well as the Swedish-German Supplementary Agreement of 1 December 1969 according to Article 6 of the aforementioned Agreement and any other existing supplements or amendments shall cease to have effect upon the entry into force of the present Agreement.

(2) This Agreement shall remain in force until terminated by either Party giving the other Party six months written notice of termination through diplomatic channels. Both Parties shall remain responsible after termination for the safeguarding of all Classified Information exchanged under the provisions of this Agreement.

(3) This Agreement may, by mutual consent, be amended in writing by the Parties. Either Party may at any time submit a formal request for the amendment of this Agreement. If such a request is submitted by one of the Parties, the Parties shall initiate negotiations on the amendment of the Agreement.

(4) Registration of this Agreement with the Secretariat of the United Nations, in accordance with Article 102 of the Charter of the United Nations, shall be initiated by the Party on whose national territory the Agreement is concluded immediately following its entry into force. The other Party shall be informed of registration, and of the UN registration number, as soon as this has been confirmed by the Secretariat.

Done at Stockholm on 31 March 2016 in two originals, in the Swedish, German and English languages, all three texts being authentic. In case of divergent interpretations of the Swedish and German text, the English text shall prevail.

For the Government of the Kingdom of Sweden	For the Government of the Federal Republic of Germany
Julius Liljeström	Michael Bock