

**ABKOMMEN  
ZWISCHEN  
DER ÖSTERREICHISCHEN BUNDESREGIERUNG  
UND  
DER REGIERUNG DER ITALIENISCHEN REPUBLIK  
ÜBER DEN AUSTAUSCH UND GEGENSEITIGEN SCHUTZ  
KLASSIFIZIERTER INFORMATIONEN**

Die Österreichische Bundesregierung und die Regierung der Italienischen Republik (im Weiteren „die Parteien“ genannt),

*In der Absicht*, den Schutz aller klassifizierten Informationen zu gewährleisten, die gemäß den innerstaatlichen Gesetzen und Verordnungen einer der Parteien als solche eingestuft und gekennzeichnet und an die andere Partei übermittelt wurden,

*Von dem Wunsch geleitet*, Regeln zum gegenseitigen Schutz der ausgetauschten oder im Zuge der Zusammenarbeit zwischen den Parteien entstandenen klassifizierten Informationen vorzusehen,

*Unter Berücksichtigung* der nationalen Interessen und Sicherheit sowie der industriellen Angelegenheiten,

sind wie folgt übereingekommen:

**ARTIKEL 1  
BEGRIFFSBESTIMMUNGEN**

Im Sinne dieses Abkommens bedeutet:

- a) „Klassifizierte Informationen“ jegliche Informationen, unabhängig von ihrer Form, die gemäß den innerstaatlichen Gesetzen und Verordnungen einer der Parteien als klassifiziert eingestuft und gekennzeichnet wurden, um ihren Schutz vor unberechtigter Preisgabe, widerrechtlicher Verwendung oder Verlust zu gewährleisten;
- b) „Zuständige Behörde“ die Nationale Sicherheitsbehörde einer der Parteien und jede andere zuständige Behörde oder Agentur, die gemäß Artikel 2 notifiziert wurde und für die Durchführung dieses Abkommens zuständig ist;

- c) "Sicherheitsunbedenklichkeitsbescheinigung für Personen" die Erklärung durch eine Zuständige Behörde einer der Parteien, die nach dem Abschluss einer Sicherheitsuntersuchung gemäß den innerstaatlichen Gesetzen und Verordnungen erfolgt und die bestätigt, dass eine Person zum Zugang zu Klassifizierten Informationen bis zu einer bestimmten Stufe für eine bestimmte Zeit berechtigt ist;
- d) "Sicherheitsunbedenklichkeitsbescheinigung für Unternehmen" die Erklärung durch eine Zuständige Behörde einer der Parteien gemäß den innerstaatlichen Gesetzen und Verordnungen, dass ein Unternehmen über die organisatorische Fähigkeit verfügt, um den adäquaten Schutz Klassifizierter Informationen für eine bestimmte Klassifizierungsstufe bis zu einem bestimmten Zeitpunkt zu gewährleisten;
- e) „Klassifizierter Vertrag“ ein Vertrag oder Untervertrag zwischen einer juristischen Person, die der Hoheitsgewalt einer der Parteien unterstellt ist und einer juristischen Person, die der Hoheitsgewalt der anderen Partei unterstellt ist, dessen Erfüllung den Zugang oder die Herstellung von Klassifizierten Informationen erfordert;
- f) „Auftragnehmer“ eine juristische Person des öffentlichen oder privaten Rechts, die über die Rechtsfähigkeit verfügt, Klassifizierte Verträge abzuschließen;
- g) „Herausgeber“ die herausgebende Partei sowie jede ihrer Hoheitsgewalt unterstehende juristische Person, die Klassifizierte Informationen erzeugt oder zur Verfügung stellt;
- h) „Empfänger“ die empfangende Partei sowie jede ihrer Hoheitsgewalt unterstehende juristische Person, die Klassifizierte Informationen empfängt;
- i) „Zugangserfordernis (Need to Know)“ der Grundsatz, dass der Zugang zu Klassifizierten Informationen an eine Person ausschließlich dann gewährt wird, wenn der Zugang für die Erfüllung der Aufgaben dieser Person erforderlich ist;
- j) "Dritter" eine juristische oder natürliche Person, die nicht Herausgeber oder Empfänger der Klassifizierten Informationen im Sinne dieses Abkommens ist, oder eine Regierung, die nicht Partei dieses Abkommens ist, oder eine internationale Organisation;
- k) „Besuch“ der Zugang zu den Räumlichkeiten einer juristischen Person des öffentlichen oder privaten Rechts, die der Hoheitsgewalt einer der Parteien unterstellt ist, im Zuge der Vollziehung dieses Abkommens, der den Zugriff auf und den Umgang mit Klassifizierten Informationen umfasst;

1) „Sicherheitsverletzung“ eine Handlung oder eine Unterlassung, die gegen dieses Abkommen oder innerstaatliche Gesetze und Verordnungen der Parteien verstößt und zu einer unberechtigten Preisgabe, zum Verlust, zur widerrechtlichen Verwendung oder zu einer sonstigen Form der Kenntnisnahme durch Unbefugte der Klassifizierten Informationen führen kann.

## **ARTIKEL 2 ZUSTÄNDIGE BEHÖRDEN**

(1) Die Zuständigen Behörden, die von den Parteien für die Durchführung dieses Abkommens bestimmt wurden, sind:

**Für die Bundesrepublik Österreich:**

Bundeskanzleramt  
Büro der Informationssicherheitskommission

**Für die Italienische Republik:**

Presidenza del Consiglio dei Ministri  
Dipartimento delle Informazioni per la Sicurezza  
Ufficio Centrale per la Segretezza

(2) Die Parteien teilen einander auf diplomatischem Weg weitere Zuständige Behörden mit, die für die Durchführung dieses Abkommens verantwortlich sind, sowie jede spätere Änderung der Zuständigkeit.

## **ARTIKEL 3 GLEICHWERTIGKEIT DER KLASSIFIZIERUNGSSTUFEN**

Die Parteien kommen überein, dass folgende Klassifizierungsstufen gleichwertig sind:

Republik Österreich	Italienische Republik	Englische Entsprechung
STRENG GEHEIM	SEGRETISSIMO	TOP SECRET
GEHEIM	SEGRETO	SECRET
VERTRAULICH	RISERVATISSIMO	CONFIDENTIAL
EINGESCHRÄNKT	RISERVATO	RESTRICTED

## **ARTIKEL 4 KENNZEICHNUNG**

(1) Klassifizierte Informationen, die unter diesem Abkommen erzeugt, ausgetauscht und herausgegeben werden, werden von dem Empfänger mit der entsprechenden Klassifizierungsstufe gemäß Artikel 3 und gemäß den innerstaatlichen Gesetzen und Verordnungen der Parteien gekennzeichnet.

(2) Klassifizierte Informationen, die von dem Empfänger im Zuge der unter dieses Abkommen fallenden Zusammenarbeit erzeugt, vervielfältigt oder übersetzt werden, werden auch mit der entsprechenden Klassifizierungsstufe gemäß Artikel 3 und gemäß den innerstaatlichen Gesetzen und Verordnungen der Parteien gekennzeichnet.

(3) Die Klassifizierungsstufe darf ausschließlich mit schriftlicher Zustimmung des Herausgebers geändert oder widerrufen werden. Der Herausgeber informiert den Empfänger unverzüglich über jede Änderung oder Widerruf der Klassifizierungsstufe der ausgetauschten Klassifizierten Informationen.

## **ARTIKEL 5 GRUNDSÄTZE DES SCHUTZES KLASSIFIZIERTER INFORMATIONEN**

(1) Die Parteien treffen alle geeigneten Maßnahmen, um den Schutz der ausgetauschten Klassifizierten Informationen zu gewährleisten, und sorgen für die erforderliche Kontrolle dieses Schutzes.

(2) Die Parteien gewähren den ausgetauschten Klassifizierten Informationen zumindest den gleichen Schutzstandard, wie sie ihren eigenen Klassifizierten Informationen der gleichwertigen Klassifizierungsstufe gewähren.

(3) Ausgetauschte Klassifizierte Informationen dürfen nur zu dem Zweck, für den sie herausgegeben wurden, und nur im Rahmen der vom Herausgeber festgelegten Beschränkungen verwendet werden.

(4) Empfangene Klassifizierte Informationen werden nur Personen zugänglich gemacht, die gemäß den innerstaatlichen Gesetzen und Verordnungen zum Zugang zu Klassifizierten Informationen der gleichwertigen Klassifizierungsstufe ermächtigt sind und die Voraussetzungen des Zugangserfordernisses (Need to Know) erfüllen.

(5) Eine Partei macht Dritten ohne vorherige schriftliche Zustimmung des Herausgebers Klassifizierte Informationen nicht zugänglich.

(6) Klassifizierte Informationen, die im Zuge der unter dieses Abkommen fallenden Zusammenarbeit erzeugt werden, genießen den gleichen Schutz wie ausgetauschte Klassifizierte Informationen.

## **ARTIKEL 6**

### **SICHERHEITSUNBEDENKLICHKEITSBESCHEINIGUNGEN FÜR PERSONEN**

(1) Im Rahmen dieses Abkommens anerkennt jede Partei die von der anderen Partei ausgestellten Sicherheitsunbedenklichkeitsbescheinigungen für Personen.

(2) Die Zuständigen Behörden unterstützen einander auf Ersuchen und gemäß den innerstaatlichen Gesetzen und Verordnungen bei den für die Anwendung dieses Abkommens notwendigen Sicherheitsüberprüfungen.

(3) Im Rahmen dieses Abkommens informieren die Zuständigen Behörden einander unverzüglich über Widerruf und alle Änderungen von Sicherheitsunbedenklichkeitsbescheinigungen für Personen, insbesondere über eine Änderung der Klassifizierungsstufe.

(4) Auf Ersuchen der Zuständigen Behörde einer Partei stellt die Zuständige Behörde der anderen Partei eine schriftliche Bestätigung aus, dass eine Person zum Zugang zu Klassifizierten Informationen berechtigt ist.

(5) Nur Personen, die die Voraussetzungen des Zugangserfordernisses (Need to Know) erfüllen und die entsprechend unterwiesen wurden, wird der Zugang zu Informationen, die als EINGESCHRÄNKT / RISERVATO / RESTRICTED eingestuft und gekennzeichnet sind, gewährt.

(6) Nur Personen, die die Voraussetzungen des Zugangserfordernisses (Need to Know) erfüllen, über eine Sicherheitsunbedenklichkeitsbescheinigung für eine entsprechende Klassifizierungsstufe verfügen und entsprechend regelmäßig unterwiesen werden, wird der Zugang zu Informationen, die als VERTRAULICH / RISERVATISSIMO / CONFIDENTIAL und höher eingestuft und gekennzeichnet sind, gewährt.

**ARTIKEL 7**  
**SICHERHEITSUNBEDENKLICHKEITSBESCHEINIGUNGEN FÜR**  
**UNTERNEHMEN UND KLASSIFIZIERTE VERTRÄGE**

(1) Ein Klassifizierter Vertrag enthält Bestimmungen über die Sicherheitsanforderungen und Klassifizierungsstufe der herauszugebenden Information. Eine Kopie der Bestimmungen wird an die Zuständige Behörde der Partei weitergeleitet.

(2) Bevor Klassifizierte Informationen, die als VERTRAULICH / RISERVATISSIMO / CONFIDENTIAL und höher eingestuft und gekennzeichnet sind und im Zusammenhang mit dem klassifizierten Vertrag stehen, dem Auftragnehmer oder den potenziellen Auftragnehmern zur Verfügung gestellt werden, muss die empfangende Partei sicherstellen, dass:

- a. Solche Auftragnehmer oder potenzielle Auftragnehmer und ihre Einrichtungen über die organisatorische Fähigkeit verfügen, um den adäquaten Schutz Klassifizierter Informationen zu gewährleisten;
- b. Auftragnehmer und deren Subauftragnehmer und ihre Einrichtungen vor der Erfüllung des Vertrages über die Sicherheitsunbedenklichkeitsbescheinigung für die entsprechende Stufe verfügen;
- c. Personen, die Aufgaben wahrnehmen, die den Zugang zu Klassifizierten Informationen erforderlich machen, über eine entsprechende Sicherheitsunbedenklichkeitsbescheinigung verfügen;
- d. Personen, die den Zugang zu Klassifizierten Informationen haben, über ihre Aufgaben und Pflichten für den Schutz Klassifizierter Informationen gemäß den innerstaatlichen Gesetzen und Verordnungen der empfangenden Partei informiert sind.

(3) Im Rahmen von Klassifizierten Verträgen erkennt jede Partei die Sicherheitsunbedenklichkeitsbescheinigung für Unternehmen der anderen Partei an.

(4) Im Rahmen der Vorbereitungen oder des Abschlusses von Klassifizierten Verträgen bestätigen die Zuständigen Behörden auf Ersuchen, dass eine gültige Sicherheitsunbedenklichkeitsbescheinigung für Unternehmen ausgestellt wurde oder dass die entsprechenden Verfahren eingeleitet wurden, sowie über die Sicherheitsanforderungen für die betroffenen Klassifizierten Informationen.

(5) Die Zuständigen Behörden informieren einander über den Abschluss von Klassifizierten Verträgen, die unter dieses Abkommen fallen.

(6) Die Zuständigen Behörden informieren einander unverzüglich über Widerruf und alle Änderungen von Sicherheitsunbedenklichkeitsbescheinigungen für Unternehmen, die unter diesen Artikel fallen, insbesondere über eine Änderung der Klassifizierungsstufe.

(7) Die Zuständige Behörde des Herausgebers übermittelt dem Empfänger und der Zuständigen Behörde des Empfängers die Sicherheitsanweisungen für das Programm (*Programme Security Instructions*) und den Sicherheitsklassifizierungsleitfaden (*Security Classification Guide*), die im Rahmen des Klassifizierten Vertrages erstellt wurden.

(8) Ein Auftragnehmer kann einen Subauftragnehmer heranziehen, um einen Teil des Klassifizierten Vertrags zu erfüllen. Subauftragnehmer unterliegen den gleichen Sicherheitserfordernissen wie der Auftragnehmer.

## **ARTIKEL 8**

### **SCHUTZ KLASSIFIZIERTER INFORMATIONEN IN KOMMUNIKATIONS- UND INFORMATIONSSYSTEMEN**

Jede Partei stellt sicher, dass im Rahmen ihrer innerstaatlichen Gesetze und Verordnungen und gemäß Artikel 5 geeignete Maßnahmen zum Schutz Klassifizierter Informationen getroffen werden, die über Kommunikations- und Informationssysteme verarbeitet, gespeichert und übermittelt werden. Diese Maßnahmen gewährleisten unter anderem die Vertraulichkeit, Integrität, Verfügbarkeit und gegebenenfalls die Nichtzurückweisung und die Authentizität Klassifizierter Informationen, sowie ein angemessenes Maß an Verantwortlichkeit und Nachverfolgbarkeit der Handlungen in Bezug auf Klassifizierte Informationen.

## **ARTIKEL 9**

### **ÜBERMITTLUNG**

(1) Klassifizierte Informationen werden auf diplomatischem Weg oder auf jedem anderen zwischen den Zuständigen Behörden der Parteien vereinbarten sicheren Weg übermittelt.

(2) Der Empfang Klassifizierter Informationen, die als VERTRAULICH / RISERVATISSIMO / CONFIDENTIAL und höher eingestuft und gekennzeichnet sind, ist schriftlich zu bestätigen.

(3) Klassifizierte Informationen, die als STRENG GEHEIM / SEGRETISSIMO / TOP SECRET eingestuft und gekennzeichnet sind, sind nur auf diplomatischem Weg gemäß innerstaatlichen Gesetzen und Verordnungen zu übermitteln.

## **ARTIKEL 10 VERVIELFÄLTIGUNG UND ÜBERSETZUNG**

(1) Alle Vervielfältigungen, Übersetzungen und Kopien sind mit einer entsprechenden Klassifizierungsstufe zu kennzeichnen und wie die Originale zu schützen. Die Übersetzungen und die Anzahl der Vervielfältigungen und Kopien sind auf ein Minimum zu beschränken. Die Vervielfältigung, Übersetzung und das Kopieren klassifizierter Informationen kann vom Herausgeber eingeschränkt oder ausgeschlossen werden.

(2) Klassifizierte Informationen, die als STRENG GEHEIM / SEGRETISSIMO / TOP SECRET eingestuft und gekennzeichnet sind, dürfen nur mit schriftlicher Zustimmung des Herausgebers vervielfältigt, übersetzt oder kopiert werden.

(3) Klassifizierte Informationen werden nur von Personen übersetzt, die zum Zugang zu klassifizierten Informationen der jeweiligen Klassifizierungsstufe gemäß den innerstaatlichen Gesetzen und Verordnungen berechtigt sind.

## **ARTIKEL 11 VERNICHTUNG**

(1) Klassifizierte Informationen, die als VERTRAULICH / RISERVATISSIMO / CONFIDENTIAL oder GEHEIM / SEGRETO / SECRET eingestuft und gekennzeichnet sind, werden nachweislich und auf eine Weise vernichtet, die eine vollständige oder teilweise Wiederherstellung nicht zulässt.

(2) Klassifizierte Informationen, die als STRENG GEHEIM / SEGRETISSIMO / TOP SECRET eingestuft und gekennzeichnet sind, werden nicht vernichtet. Sie sind zurück an den Herausgeber zu übermitteln, wenn sie für den Empfänger nicht mehr erforderlich sind.

(3) Im Falle einer Krisensituation, in der es unmöglich ist Klassifizierte Informationen, die in Anwendung dieses Abkommens ausgetauscht oder erzeugt wurden, zu schützen oder rückzuübermitteln, werden die Klassifizierten Informationen umgehend vernichtet. Der

Empfänger informiert die Zuständige Behörde des Herausgebers ohne ungebührliche Verzögerung über diese Vernichtung.

## **ARTIKEL 12**

### **BESUCHE**

(1) Besuche, die den Zugang zu Klassifizierten Informationen erfordern, unterliegen der vorherigen Genehmigung durch die Zuständige Behörde der gastgebenden Partei. Die Genehmigung wird nur Personen erteilt, die gemäß den innerstaatlichen Gesetzen und Verordnungen zum Zugang zu Klassifizierten Informationen der entsprechenden Klassifizierungsstufe ermächtigt sind.

(2) Besuchsansträge werden mindestens fünfzehn Arbeitstage vor dem Besuch bei der Zuständigen Behörde der gastgebenden Partei gestellt, oder in dringenden Fällen innerhalb eines kürzeren Zeitraums. Die Zuständigen Behörden informieren einander über die Einzelheiten des Besuchs und gewährleisten den Schutz personenbezogener Daten.

(3) Besuchsansträge werden in englischer Sprache gestellt und enthalten insbesondere folgende Angaben:

- a) Zweck und vorgesehenes Datum des Besuchs;
- b) Vor- und Familienname, Geburtsdatum und -ort, Staatsangehörigkeit und Pass- oder Personalausweisnummer des Besuchers;
- c) Funktion des Besuchers und Name der vertretenen Behörde oder Stelle oder des vertretenen Unternehmens;
- d) Gültigkeit und Klassifizierungsstufe der Sicherheitsunbedenklichkeitsbescheinigung für Personen des Besuchers;
- e) Name, Adresse, Telefon- und Faxnummer, E-Mail-Adresse und Ansprechpartner der Behörden, Stellen oder Einrichtungen, die besucht werden sollen;
- f) Datum des Antrags und Unterschrift der Zuständigen Behörde.

(4) Die Zuständigen Behörden der Parteien können Listen von Personen erstellen, die zu wiederholten Besuchen ermächtigt sind. Diese Listen sind für einen anfänglichen Zeitraum von 12 Monaten gültig. Die Bedingungen für die jeweiligen Besuche werden direkt mit den passenden Ansprechpartnern in der juristischen Person, die von diesen Personen besucht werden soll, gemäß den vereinbarten Modalitäten und Bedingungen vorgesehen.

### **ARTIKEL 13**

#### **SICHERHEITSVERLETZUNGEN**

(1) Im Falle einer Sicherheitsverletzung, die zu einer vermuteten oder festgestellten unberechtigten Preisgabe, widerrechtlichen Verwendung oder einem Verlust von unter dieses Abkommen fallenden Klassifizierten Informationen führt, informiert die Zuständige Behörde des Empfängers unverzüglich die Zuständige Behörde des Herausgebers schriftlich.

(2) Verletzungen der Bestimmungen über den Schutz von unter dieses Abkommen fallenden Klassifizierten Informationen werden gemäß den innerstaatlichen Gesetzen und Verordnungen untersucht und verfolgt. Die Parteien unterstützen einander auf Ersuchen.

(3) Im Falle einer Sicherheitsverletzung auf dem Gebiet eines Dritten, informieren die Zuständigen Behörden einander unverzüglich und, wenn möglich, setzen Maßnahmen gemäß Absatz 2 dieses Artikels.

(4) Die Parteien informieren einander über das Ergebnis der Untersuchungen und über die getroffenen Maßnahmen.

### **ARTIKEL 14**

#### **KOSTEN**

Jede Partei trägt ihre eigenen Kosten bei der Durchführung dieses Abkommens gemäß ihren innerstaatlichen Gesetzen und Verordnungen und ohne Überschreitung ihrer verfügbaren ordentlichen Haushaltsmittel.

## **ARTIKEL 15 KONSULTATIONEN**

(1) Die Zuständigen Behörden informieren einander über die jeweiligen innerstaatlichen Gesetze und Verordnungen über den Schutz Klassifizierter Informationen und über alle wesentlichen Änderungen.

(2) Um eine enge Zusammenarbeit bei der Durchführung dieses Abkommens zu gewährleisten, konsultieren die Zuständigen Behörden einander zu allen Fragen im Rahmen dieses Abkommens und erleichtern die notwendigen gegenseitigen Besuche.

## **ARTIKEL 16 STREITBEILEGUNG**

Streitigkeiten über die Anwendung oder Auslegung dieses Abkommens werden im Wege direkter Gespräche und Verhandlungen zwischen den Parteien auf diplomatischem Weg beigelegt.

## **ARTIKEL 17 SCHLUSSBESTIMMUNGEN**

(1) Dieses Abkommen wird auf unbestimmte Zeit geschlossen und tritt am ersten Tag des zweiten Monats nach dem Tag in Kraft, an dem die Parteien einander den Abschluss der für das Inkrafttreten des Abkommens jeweils erforderlichen innerstaatlichen Verfahren mitgeteilt haben.

(2) Dieses Abkommen kann im gegenseitigen schriftlichen Einvernehmen beider Parteien geändert werden. Änderungen treten gemäß Absatz 1 in Kraft.

(3) Jede Partei kann dieses Abkommen jederzeit auf diplomatischem Weg kündigen. In einem solchen Fall tritt das Abkommen sechs Monate nach Erhalt der Kündigungsnote durch die andere Partei außer Kraft. Im Fall der Kündigung bleiben Klassifizierte Informationen, die in Anwendung dieses Abkommens übermittelt oder hergestellt wurden, weiterhin nach den Bestimmungen dieses Abkommens geschützt oder sind alternativ an den Herausgeber rückzuübermitteln.

Geschehen zu ..... am..... in zwei Urschriften in deutscher, italienischer und englischer Sprache, wobei alle Fassungen in gleicher Weise authentisch sind. Im Falle abweichender Auslegung gibt die englische Fassung den Ausschlag.

Für die Österreichische Bundesregierung:      Für die Regierung der Italienischen Republik: