

Hinweise zur Handhabung von nichtdeutschen Verschlussachen

1 Grundsatz

Bei nichtdeutschen Verschlussachen (VS) ist zu differenzieren zwischen VS über- oder zwischenstaatlicher Einrichtungen oder Stellen (NATO, EU, ESA, OCCAR u.a.) und VS ausländischer öffentlicher Stellen (z.B. Frankreich, Spanien u.a.).

Die Regelungen des GHB finden auf Verschlussachen von über- oder zwischenstaatlichen Einrichtungen und Stellen nur dann uneingeschränkt Anwendung, soweit in vertraglichen Vereinbarungen oder projektspezifischen Sicherheitsanweisungen (PSI) auf die Anwendung nationaler Vorschriften verwiesen wird.

In den Fällen, in denen Unternehmen im Rahmen ihrer Beteiligung an Aufträgen über- oder zwischenstaatlicher Einrichtungen oder Stellen vertraglich direkt auf die Einhaltung der Geheimschutzvorschriften solcher Einrichtungen oder auf die Einhaltung von programm- oder projektspezifischen Geheimschutzvereinbarungen (sog. *Programme/Project Security Instructions - PSI*) verpflichtet worden sind, gehen diese Regelungen dem GHB vor. Hier haben die Sicherheitsorganisationen der jeweiligen Einrichtungen/Stellen zudem auch eigenständige Rechte, die Einhaltung ihrer Geheimschutzvorschriften oder von programm- oder projektspezifischen Geheimschutzvereinbarungen bei ihren Auftragnehmern zu kontrollieren.

Im Zusammenhang mit der Aufbewahrung von VS, die Unternehmen von über- oder zwischenstaatlichen Einrichtungen oder Stellen überlassen wurden oder von Unternehmen auf Veranlassung dieser Stellen erstellt werden, können die Anforderungen zum materiellen Geheimschutz aus dem GHB sowie aus den technischen Leitlinien des BSI i.d.R. angewendet werden, soweit sie ein vergleichbares Schutzniveau bieten. Für die Behandlung von VS dieser Einrichtungen in IuK gelten aber oft weitergehende spezifische Anforderungen (z.B. für die Akkreditierung der IuK), die zu berücksichtigen sind.

VS ausländischer öffentlicher Stellen, welche deutschen Unternehmen im Rahmen von bilateralen Abkommen überlassen werden, werden hingegen i.d.R. nach den Vorschriften des GHB behandelt. Dies ergibt sich aus den entsprechenden bilateralen Abkommen, in denen typischerweise eine Äquivalenz der ausländischen mit den deutschen VS-Einstufungsgraden vereinbart wird. Die VS sind dann im Partnerland nach den jeweiligen entsprechenden nationalen Vorschriften zu schützen (d.h. für Unternehmen in Deutschland nach GHB). Soweit es im jeweiligen Partnerland nicht für alle Geheimhaltungsgrade einen vergleichbaren Geheimhaltungsgrad gibt, können bilaterale Abkommen auch Sonderregelungen enthalten.

Diese Anlage enthält Hinweise zu den ggf. abweichenden oder weitergehenden Anforderungen zur Behandlung von nichtdeutschen VS von über- oder zwischenstaatlichen Einrichtungen und Stellen zur Anwendbarkeit des GHB zur Behandlung solcher VS, wobei die Hinweise nicht als abschließende Darstellung der Abweichungen zu werten sind (2), sowie Hinweise zur Behandlung von nichtdeutschen Verschlussachen, welche deutschen Unternehmen im Rahmen von bilateralen Abkommen überlassen werden (3).

2 Handhabung von VS über- oder zwischenstaatlicher Einrichtungen und Stellen

2.1 Kennzeichnung und Erfassung

VS über oder zwischenstaatlicher Einrichtungen oder Stellen sind mit den jeweiligen Geheimhaltungskennzeichnungen dieser Einrichtungen / Stellen versehen.¹

Im Zusammenhang mit VS-Aufträgen durch über- oder zwischenstaatliche Einrichtungen und Stellen spielen internationale Geheimhaltungsgrade des höchsten Levels TOP SECRET (STRENG GEHEIM) i.d.R. keine Rolle.

VS solcher Einrichtungen, die Unternehmen überlassen werden, können in den Unternehmen nach Eingang zusätzlich mit dem vergleichbaren deutschen Geheimhaltungsgrad gekennzeichnet werden, wobei der originale Geheimhaltungsgrad aber deutlich erkennbar beibehalten und die VS mit dem internationalen Geheimhaltungsgrad in Bestandsbüchern vereinnahmt werden muss. Eine solche Kennzeichnung besagt aber nicht, dass die VS in jedem Fall auch entsprechend den Anforderungen an deutsche VS mit vergleichbarem Geheimhaltungsgrad zu behandeln sind.

Soweit Unternehmen im Rahmen von Aufträgen oder Unteraufträgen solcher Einrichtungen/Stellen selbst VS erstellen müssen, sind diese VS mit dem entsprechenden Geheimhaltungsgrad der Einrichtungen/Stellen zu kennzeichnen und in den VS-Tagebüchern als internationale VS mit der jeweiligen Abkürzung zu erfassen.

Weitere Vorgaben zur Anbringung von Zusatzkennzeichnungen zur Klarstellung von Weitergabe- oder zu Nutzungsbeschränkungen finden sich ggf. in den jeweiligen programm- oder projektspezifischen Geheimschutzvereinbarungen (Programme/Project Security Instructions - PSI).

Die Aufbewahrung internationaler VS sollte für Zwecke von Inspektionen durch die Sicherheitsbehörden der internationalen Einrichtungen/Stelle getrennt von anderen VS in zugelassenen VS-Verwahrzellen oder VS-Sperrzonen aufbewahrt werden.

Internationale VS, die mit anderen als den in dieser Anlage beschriebenen VS-Kennzeichnungen gekennzeichnet sind, sind in Deutschland nicht als VS zu behandeln. In Zweifelsfällen sollte aber Rücksprache mit BMWK gehalten werden.

2.2 Rechte des öffentlichen internationalen VS-Herausgebers

Die Rechte des VS-Herausgebers liegen bei VS von über oder zwischenstaatlicher Einrichtungen oder Stellen bei der jeweiligen Einrichtung/Stelle. Soweit Unternehmen im Rahmen eines Auftrages VS auf Veranlassung eines internationalen VS-Herausgebers (sog. „originator“) einstufen, sind sie stets nur deren Ersteller. Sie sind dabei nicht selbst der VS-Herausgeber bzw. haben selbst nicht das Recht über eine Änderung der VS-Einstufung oder über die Weitergabe der VS an Empfänger außerhalb der jeweiligen Organisation zu entscheiden (siehe auch 1.9.1 GHB).

Dies ist vor allem für die Weitergabe solcher VS, z.B. an nicht an einem Projekt beteiligte ausländische staatliche Stellen oder an Unterauftragnehmer in solchen Ländern von Bedeutung, da hierfür stets die Zustimmung des Auftraggebers oder amtlichen VS-Herausgebers der VS eingeholt werden muss (sog. *release approvals*).

Die Prozesse zur Einholung von Weitergabegenehmigungen (*release approvals*) oder zur Unterauftragsvergabe finden sich i.d.R. ebenfalls in den jeweiligen programm- oder projektspezifischen Geheimschutzvereinbarungen (Programme/Project Security Instructions - PSI). Dabei ersetzt die Genehmigung zur Weitergabe der VS an einen

¹ Eine Auflistung der gängigen vergleichbaren Geheimhaltungsgrade über- oder zwischenstaatlicher Einrichtungen oder Stellen findet sich in Anlage 31 zum GHB

ausländischen Empfänger allerdings nicht die nach nationalen Vorschriften zusätzlich erforderliche Ausfuhrgenehmigung.

2.3 Nachweis der Sicherheitsüberprüfungen für Mitarbeiter/innen von Unternehmen

Soweit Mitarbeiter/innen von Unternehmen Besuche in über- oder zwischenstaatlichen Einrichtungen oder Stellen oder in nichtdeutschen Unternehmen durchführen müssen, bei denen sie Zugang zu VS ab CONFIDENTIAL (VS-VERTRAULICH) oder höher erhalten oder erhalten können, muss grundsätzlich online ein Besuchsantrag (*Request for Visit*) beim BMWK gestellt werden (zum Besuchskontrollverfahren siehe Kapitel 5 GHB).

BMWK prüft das Vorliegen einer VS-Ermächtigung für die Firmenmitarbeiter/innen und leitet den Besuchsantrag an die zuständige ausländische Sicherheitsbehörde weiter. In bestimmten Fällen werden die Besuchsanträge auch an das Bundesamt für Ausrüstung, Informationstechnik und Nutzung der Bundeswehr (BAAINBw) zur weiteren Bearbeitung weitergeleitet. Dies gilt allerdings nur, soweit in den jeweiligen programm-/projektspezifischen Sicherheitsvereinbarungen nicht eine direkte Anmeldung von Besuchern zwischen der den Besuchenden entsendenden und der zu besuchenden Stelle (d.h. ohne Beteiligung der zuständigen Sicherheitsbehörden) vereinbart worden ist. Dann können Besuchsanträge von dem/der SiBe der Besuchenden direkt an die für Besuche verantwortlichen Stellen des zu besuchenden Unternehmens oder der nichtdeutschen öffentlichen Stelle übermittelt werden.

Besuche, bei denen es lediglich um den Zugang zu internationalen VS bis zum Geheimhaltungsgrad RESTRICTED geht, können i.d.R. ohne formale Anforderungen direkt zwischen den beteiligten Einrichtungen angemeldet werden. Allerdings fordern dennoch einige ausländische Stellen für den Zutritt zu ihren militärischen Einrichtungen generell einen Besuchsantrag mit Nachweis der Sicherheitsüberprüfung des Besuchenden.

2.4 Sicherheitsvorschriften der NATO

Die maßgeblichen Bestimmungen zu Austausch, Schutz und Handhabung von NATO-VS sind in Dokument C-M(2002)49 und den jeweiligen Implementierungsvorschriften in der jeweils gültigen Fassung festgeschrieben. Diese Bestimmungen sind in der Bundesrepublik Deutschland geltendes Recht. Sie finden auf Unternehmen aber nur dann unmittelbar Anwendung, wenn die Unternehmen in VS-Aufträgen auf die Einhaltung dieser Vorschriften vertraglich verpflichtet wurden.

2.4.1 NATO-Geheimhaltungsgrade

COSMIC TOP SECRET (CTS) - vergleichbar STRENG GEHEIM

NATO SECRET (NS) - vergleichbar GEHEIM

NATO CONFIDENTIAL - vergleichbar VS-VERTRAULICH

NATO RESTRICTED (NR) - vergleichbar VS-NUR FÜR DEN DIENSTGEBRAUCH

NATO-VS können zusätzlich zum Geheimhaltungsgrad auch mit Zusatzvermerken (sog. Warn- oder Sperrvermerke) versehen sein. Hierzu zählen auch Schutzworte, welche zusätzliche Weitergabe- oder Zugangsbeschränkung für Personen klarstellen. Solche NATO-VS sind in einer eigenen VS-Registrierung zu erfassen und aufzubewahren (sog. Schutzwortregistrierung) und dürfen nur Personen zugänglich gemacht werden, die entsprechend eine Sonderverpflichtung und Belehrung erhalten haben.

2.4.2 Behandlung von NATO VS

Zugang zu NATO VS darf unter strikter Einhaltung des Grundsatzes „Kenntnis nur, wenn nötig“ (*Need-to-Know*) gewährt werden und ab dem Geheimhaltungsgrad NATO CONFIDENTIAL nur erhalten, wer nach Maßgabe des GHB und des SÜG bis zur Höhe des vergleichbaren deutschen Geheimhaltungsgrades (also bei NATO CONFIDENTIAL bis VS-VERTRAULICH und bei NATO SECRET bis GEHEIM) entsprechend sicherheitsüberprüft und ermächtigt worden ist.

Firmen, die Zugang zu NATO VS ab dem Geheimhaltungsgrad NATO CONFIDENTIAL benötigen, müssen in das Geheimschutzverfahren des BMWK aufgenommen werden und es muss ein Sicherheitsbescheid für den vergleichbaren deutschen Geheimhaltungsgrad vorliegen. Für ausländische Unterauftragnehmer mit Zugang zu NATO CONFIDENTIAL oder NATO SECRET ist beim BMWK eine *NATO Facility Security Clearance Assurance* einzuholen.

Alle Personen, die Zugang zu NATO VS erhalten beziehungsweise erhalten können, sind regelmäßig und nachweislich über ihre Rechte und Pflichten im Umgang mit NATO VS zu unterrichten.

Für die Behandlung von NATO CONFIDENTIAL und NATO SECRET in Informations- und Kommunikationssystemen (*Communication and Information Systems - CIS*) sowie deren Akkreditierung gibt es weitergehende Anforderungen, welche u.a. in der *NATO Management Directive on CIS Security* (NATO Dokument AC/35-D/2005-REV5) sowie weiteren einschlägigen NATO- Infosec Vorschriften beschrieben sind. Für weitere Auskünfte stehen die zuständigen Mitarbeiter/innen des BMWK zur Verfügung.

2.4.3 Behandlung von NATO RESTRICTED (NR)

Für den Zugang zu NATO RESTRICTED ist nach den NATO-Vorschriften weder eine Personen- noch eine Firmenüberprüfung erforderlich. Einige NATO-Mitgliedstaaten fordern aber nach ihren nationalen Vorschriften dennoch Clearances für Personal und für Unternehmen mit Zugang zu NATO RESTRICTED. In den einschlägigen NATO-Vorschriften wurde aber vereinbart, dass diese Länder bei der Auftragsvergabe oder bei Ausschreibungen keine Firmen aus Ländern benachteiligen dürfen, in denen es solche Forderungen nicht gibt.

NATO RESTRICTED müssen in zugangskontrollierten Bereichen aufbewahrt und bearbeitet werden (sog. *Administrative Zones*). Für NATO RESTRICTED gibt es keine Verpflichtung zur Registrierung.

Auch für die Behandlung von NATO RESTRICTED in Informations- und Kommunikationssystemen (*Communication and Information Systems - CIS*) gibt es weitergehende Anforderungen, welche in einem gesonderten Dokument i.d.R. als Anhang zu den Aufträgen oder zu den PSIs für NATO-Projekte beschrieben sind. U.a. ist für NATO RESTRICTED CIS eine spezielle Akkreditierung erforderlich, wobei für Unternehmen mit Sitz in Deutschland aber von der Möglichkeit Gebrauch gemacht wurde, diese Akkreditierung auf den VS-Auftragnehmer zu delegieren. Hierbei setzen die Unternehmen die NATO-Anforderungen in eigener Verantwortung (d.h. ohne Einbindung des BMWK) um. Dem VS-Auftraggeber ist auf Verlangen ein Nachweis über die Akkreditierung in Übereinstimmung mit den NATO-Anforderungen vorzulegen (sog. *Statement of Compliance*).

Für die elektronische Übertragung von NATO RESTRICTED sind Verschlüsselungsprodukte einzusetzen, die dafür von der NATO oder vom BSI explizit zugelassen sind.

2.4.4 Behandlung von NATO UNCLASSIFIED (NU)

Nicht als VS eingestufte NATO-Informationen sind als NATO UNCLASSIFIED (NU) gekennzeichnet.

Dabei handelt es sich nicht um einen Geheimhaltungsgrad. Dennoch sind solche Informationen weder für die Weitergabe an Nicht-NATO-Staaten oder an die Öffentlichkeit freigegeben, es sei denn hierfür liegt die Genehmigung des NATO-Herausgebers vor. Weitere Informationen zur Behandlung von NATO UNCLASSIFIED sind den NATO-Dokumenten C-M(2002)60 und C-M(2007)0118 in ihrer gültigen Fassung enthalten.

2.5 EU

Die maßgeblichen Bestimmungen zu Austausch, Schutz und Handhabung von EU VS sind in den Geheimschutzvorschriften des Rates (*Council Security Regulations* - Ratsdokument 2013/488) sowie den Geheimschutzvorschriften der Europäischen Kommission (*Commission security rules for protecting EU classified information* - Kommissionsentscheidung 2015/444) sowie den jeweiligen Implementierungsvorschriften in dessen gültigen Fassungen festgeschrieben.

Diese Bestimmungen finden in der Bundesrepublik Deutschland aber keine unmittelbare Anwendung. Die EU-Mitgliedstaaten sind jedoch gehalten, diese Vorschriften zu respektieren um ein gleichwertiges Schutzniveau für EU VS in den Mitgliedstaaten zu gewährleisten. Dies ist vor allem für Unternehmen wichtig, damit diese ihre vertraglichen Verpflichtungen (z.B. hinsichtlich des Einsatzes von sicherheitsüberprüftem Personal, dem Vorliegen oder der Durchführung von VS-Transporten) erfüllen können.

Unternehmen werden aber i.d.R. vertraglich auf die Einhaltung der Sicherheitsvorschriften des Rates oder der Kommission bzw. der jeweiligen projektspezifischen Sicherheitsvereinbarungen (PSI) verpflichtet. So bilden die Sicherheitsvorschriften der Kommission die Grundlage für den Schutz von EU VS, z.B. im Rahmen von GNSS (Galileo), den Sicherheitsforschungsprojekten im Rahmen HORIZON 2020 oder den Projekten im Rahmen des Europäischen Verteidigungsfonds (EDF).

2.5.1 EU-Geheimhaltungsgrade

TRES SECRET UE/EU TOP SECRET (TS-UE/EU-TS) - vergleichbar STRENG GEHEIM

SECRET UE/EU SECRET (S-UE/EU-S) - vergleichbar GEHEIM

CONFIDENTIEL UE/EU CONFIDENTIAL (C-UE/EU-C) - vergleichbar VS-VERTRAULICH

RESTREINT UE/EU RESTRICTED (R-UE/EU-R) - vergleichbar VS-NUR FÜR DEN DIENSTGEBRAUCH

2.5.2 Behandlung von EU-VS

EU VS des Rates der Europäischen Union, die vor dem 15. Oktober 2013 (Veröffentlichung der Sicherheitsvorschriften des Rates) sowie EU VS der Europäischen Kommission, die vor dem 18. März 2015 entstanden sind, tragen lediglich französischsprachige Kennzeichnungen. Solche EU VS gelten aber dennoch als korrekt gekennzeichnet und sind dementsprechend zu behandeln.

Einige Agenturen des Rates und der Kommission verwenden nach wie vor Kennzeichnungen, die von den offiziellen VS-Kennzeichnungen des Rates und der

Kommission abweichen. In Zweifelsfällen ist beim BMWK die Gültigkeit solcher Kennzeichnungen zu erfragen.

Auch für die Behandlung von EU VS gelten die Hinweise für die Behandlung von NATO VS unter den Abschnitten 2.4.2 und 2.4.3 im Wesentlichen analog.

Für die elektronische Übertragung von RESTREINT UE/EU RESTRICTED sind Verschlüsselungsprodukte einzusetzen, die dafür vom Sicherheitsausschuss des Rates explizit zugelassen sind.

Nicht als VS eingestufte oder markierte Dokumente und Informationen der EU sind grundsätzlich nicht ohne Zustimmung des Herausgebers für die Weitergabe an die Öffentlichkeit zugelassen. Dokumente (z.B. des Rates) können die Kennzeichnung LIMITE tragen. Dabei handelt es sich nicht um einen weiteren Geheimhaltungsgrad, sondern um eine Verbreitungsbeschränkung. Informationen mit der Kennzeichnung LIMITE sind auf vertraglicher Basis nach den Vorgaben des EU-Auftraggebers zu behandeln. Gleiches gilt für von der Europäischen Kommission zur Verfügung gestellte Informationen mit Kennzeichnungen, wie z.B. „SENSITIVE (NON CLASSIFIED)“ oder „SPECIAL HANDLING“.

2.6 Europäische Raumfahrtagentur ESA

Die Europäische Weltraumagentur ist keine Agentur der Europäischen Union. Sie verfügt als eigenständige internationale Organisation über eigene Regeln zur Handhabung ihrer VS, die in den Sicherheitsvorschriften der ESA (ESA Security Regulations) beschrieben sind.

Nach den Bestimmungen des Geheimschutzabkommens der ESA mit ihren Mitgliedstaaten von 2003 ist Deutschland verpflichtet, die Mindeststandards der ESA Geheimschutzvorschriften zu beachten. Diese Mindeststandards werden im Wesentlichen durch das GHB erfüllt.

Allerdings werden Unternehmen i.d.R. auch von der ESA vertraglich auf die Einhaltung der ESA-Sicherheitsvorschriften bzw. der jeweiligen projektspezifischen Sicherheitsvereinbarungen (PSI) verpflichtet.

Ansonsten gelten auch die Hinweise für die Behandlung von NATO VS unter den Abschnitten 2.4.2 und 2.4.3 im Wesentlichen analog.

ESA-Geheimhaltungsgrade

ESA TOP SECRET - vergleichbar STRENG GEHEIM

ESA SECRET - vergleichbar GEHEIM

ESA CONFIDENTIAL - vergleichbar VS-VERTRAULICH

ESA RESTRICTED - vergleichbar VS-NUR FÜR DEN DIENSTGEBRAUCH

2.7 Organisation Conjointe de Coopération en Matière d'Armement (OCCAR)

Die OCCAR ist keine Agentur der Europäischen Union. Sie verfügt als eigenständige internationale Organisation über eigene Regeln zur Handhabung von VS, die im Rahmen von Aufträgen durch die OCCAR Verwaltung (*OCCAR Executive Agency- OCCAR-EA*) im Rahmen von OCCAR Programmen erstellt werden (OCCAR VS).

Die Bestimmungen des Geheimschutzabkommens der OCCAR mit ihren Mitgliedstaaten von 2005 sind nach Maßgabe der Bestimmungen der OCCAR Konvention von 1998 in den OCCAR-Mitgliedstaaten geltendes Recht.

Die OCCAR Geheimschutzvorschriften (*OCCAR Security Regulations*) sind in der OMP 11 (*OCCAR Management Procedures No. 11*) in ihrer gültigen Fassung festgelegt.

Im Rahmen von Verträgen mit Bearbeitung von OCCAR-VS werden Auftragnehmer vertraglich direkt auf die Einhaltung der OCCAR Security Regulations sowie der ergänzenden Regelungen in den jeweiligen Programme Security Instructions (PSI) verpflichtet.

Zusätzlich werden Auftragnehmer vertraglich auf Behandlung von nicht eingestuft, aber anderweitig als sensitiv zu betrachtenden Informationen (*OCCAR Sensitive Information*) verpflichtet. Die Anforderungen für OCCAR Sensitive Information sind in der OCCAR Management Directive Nr. 12 (OMP 12) festgelegt.

OCCAR Geheimhaltungsgrade

OCCAR SECRET - vergleichbar GEHEIM

OCCAR CONFIDENTIAL - vergleichbar VS-VERTRAULICH

OCCAR RESTRICTED - vergleichbar VS-NUR FÜR DEN DIENSTGEBRAUCH

Ansonsten gelten auch für Aufträge im Rahmen von OCCAR-Programmen die Hinweise für die Behandlung von NATO-VS unter den Abschnitten 2.4.2 und 2.4.3 im Wesentlichen analog.

3 Behandlung von nichtdeutschen VS aus bilateralen Abkommen

Für VS, welche Unternehmen im Rahmen von bi- oder multilateralen Projekten oder von nichtdeutschen VS-Auftraggebern auf der Grundlage bilateraler Geheimschutzabkommen überlassen werden, finden die Regelungen des GHB uneingeschränkt Anwendung, soweit in den jeweiligen Abkommen keine abweichenden Vereinbarungen getroffen worden sind. Die jeweiligen Abkommen halten fest, welche Geheimschutzgrade als äquivalent betrachtet werden und verweisen somit auf das jeweilige Schutzniveau. Im Einzelfall enthält das anwendbare Abkommen noch spezielle Regelungen.

3.1 Formen von Abkommen

3.1.1 Regierungsgeheimschutzabkommen

Regierungsgeheimschutzabkommen (General Security Agreement - GSA) sind zweiseitige völkerrechtliche Verträge zwischen der Regierung der Bundesrepublik Deutschland und der Regierung eines anderen Staates oder dem entsprechenden Exekutivorgan einer internationalen Organisation. Regierungsgeheimschutzabkommen binden die Bundesrepublik Deutschland als Völkerrechtssubjekt in ihrer Gesamtheit und ermöglichen den Austausch von VS mit Regierungseinrichtungen oder Auftragnehmern im jeweiligen Partnerstaat.

3.1.2 Ressortgeheimschutzabkommen

Ressortgeheimschutzabkommen werden zwischen einem Bundesressort und dessen Pendant in einem Partnerstaat geschlossen. Sie genießen dieselbe völkerrechtliche Stellung wie Regierungsgeheimschutzabkommen und binden ebenfalls die Bundesrepublik Deutschland als Völkerrechtssubjekt in ihrer Gesamtheit. Allerdings können auf Grundlage von Ressortgeheimschutzabkommen nur VS der jeweils betreffenden Ressorts und Behörden ihres Geschäftsbereichs ausgetauscht werden. Für bilaterale Verteidigungsprojekte sind i.d.R. die vom BMVg geschlossenen Ressortgeheimschutzabkommen relevant.

3.1.3 Memoranda of Understanding (MoU), Memoranda of Agreement (MoA) oder vergleichbare nicht rechtsverbindliche Vereinbarungen

Obwohl Instrumente dieser Art Absprachen zur Handhabung von VS enthalten können, fehlt ihnen die rechtliche Verbindlichkeit zum gegenseitigen Schutz von VS. Sie können daher genuine Regierungs- beziehungsweise Ressortgeheimschutzabkommen nicht ersetzen und daher dürfen auf der Grundlage solcher Vereinbarungen auch keine deutschen VS an ausländische Regierungseinrichtungen oder Auftragnehmer gegeben werden.

Eine Liste der in Kraft befindlicher Geheimschutzabkommen ist im geschützten Bereich des Geheimschutzservers abrufbar. Für weitere Fragen zu einzelnen Geheimschutzabkommen steht BMWK zur Verfügung.

3.1.4 Hinweise zur Kennzeichnung nichtdeutscher VS

Nichtdeutsche VS, welche deutschen Unternehmen auf der Grundlage eines bilateralen Geheimschutzabkommens überlassen werden, sind zusätzlich mit dem korrespondierenden deutschen Geheimhaltungsgrad zu kennzeichnen.

Dies erfolgt jeweils unterhalb des Originalgeheimhaltungsgrades. Bei zusammenhängenden VS reicht es aus, wenn diese zusätzliche Kennzeichnung nur auf der ersten Seite erfolgt.

Solche nichtdeutschen VS sind mit dem vergleichbaren deutschen Geheimhaltungsgrad in den VS-Tagebüchern zu erfassen. Auch nichtdeutsche VS sollten in den VS-Verwahrgelassen in nach Ländern getrennten Ordnern aufbewahrt werden.

Keinesfalls darf der Originalgeheimhaltungsgrad durchgestrichen, überschrieben oder durch die zusätzliche Kennzeichnung geändert werden.