Amtsblatt der Europäischen Union

C 126

Ausgabe in deutscher Sprache

Mitteilungen und Bekanntmachungen

61. Jahrgang

10. April 2018

Inhalt

IV *Informationen*

INFORMATIONEN DER ORGANE, EINRICHTUNGEN UND SONSTIGEN STELLEN DER EUROPÄISCHEN UNION

2018/C 126/01 Beschluss der Hohen Vertreterin der Union für Außen- und Sicherheitspolitik vom 19. September 2017 über die Sicherheitsvorschriften für den Europäischen Auswärtigen Dienst — ADMIN(2017) 10 1

DE

IV

(Informationen)

INFORMATIONEN DER ORGANE, EINRICHTUNGEN UND SONSTIGEN STELLEN DER EUROPÄISCHEN UNION

EUROPÄISCHER AUSWÄRTIGER DIENST

Beschluss der Hohen Vertreterin der Union für Außen- und Sicherheitspolitik vom 19. September 2017 über die Sicherheitsvorschriften für den Europäischen Auswärtigen Dienst

ADMIN(2017) 10

(2018/C 126/01)

DIE HOHE VERTRETERIN DER UNION FÜR AUßEN- UND SICHERHEITSPOLITIK —

gestützt auf den Beschluss 2010/427/EU des Rates vom 26. Juli 2010 über die Organisation und die Arbeitsweise des Europäischen Auswärtigen Dienstes ([1]) (*EAD*),

gestützt auf die Stellungnahme des in Artikel 9 Absatz 6 des Beschlusses der Hohen Vertreterin vom 15. Juni 2011 über die Sicherheitsvorschriften für den Europäischen Auswärtigen Dienst ([2]) genannten Ausschusses,

in Erwägung nachstehender Gründe:

(1) Als eine funktional eigenständige Einrichtung der Europäischen Union (EU) sollte der EAD nach Artikel 10 Absatz 1 des Beschlusses 2010/427/EU des Rates über Sicherheitsvorschriften verfügen.

(2) Der Hohe Vertreter der Union für Außen- und Sicherheitspolitik (im Folgenden „Hoher Vertreter“) sollte Sicherheitsvorschriften für den EAD beschließen, die für alle Aspekte der Sicherheit in Zusammenhang mit der Funktionsweise des EAD gelten, sodass er den Risiken für das ihm unterstehende Personal, seine materiellen Werte, seine Informationen und seine Besucher wirksam entgegenwirken und seinen Sorgfaltspflichten in dieser Hinsicht nachkommen kann.

(3) So sollte insbesondere dem Personal, das dem EAD untersteht, den materiellen Werten des EAD, einschließlich seiner Kommunikations- und Informationssysteme, seinen Informationen und Besuchern ein Schutzniveau gewährt werden, das mit den bewährten Verfahren des Rates, der Kommission, der Mitgliedstaaten und gegebenenfalls internationaler Organisationen im Einklang steht.

(4) Die Sicherheitsvorschriften für den EAD sollten dazu beitragen, einen kohärenteren und umfassenderen allgemeinen Rahmen in der Europäischen Union für den Schutz von EU-Verschlusssachen (im Folgenden „EU-VS“) zu schaffen, wobei die Sicherheitsvorschriften des Rates der Europäischen Union (im Folgenden „Rat“) und der Europäischen Kommission zugrunde gelegt werden und größtmögliche Kohärenz mit ihnen gewahrt werden soll.

(5) Der EAD, der Rat und die Kommission sind entschlossen, gleichwertige Sicherheitsstandards für den Schutz von EU-VS anzuwenden.

(6) Dieser Beschluss lässt die Artikel 15 und 16 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV) und die zu ihrer Durchführung erlassenen Rechtsakte unberührt.

([1]) ABl. L 201 vom 3.8.2010, S. 30.
([2]) ABl. C 304 vom 15.10.2011, S. 7.

(7) Die Organisation der Sicherheit im EAD und die Zuweisung der Sicherheitsaufgaben müssen festgelegt werden.

(8) Der Hohe Vertreter sollte gegebenenfalls auf einschlägige Fachkenntnisse in den Mitgliedstaaten, dem Generalsekretariat des Rates und der Europäischen Kommission zurückgreifen.

(9) Der Hohe Vertreter sollte mit Unterstützung der Mitgliedstaaten, des Generalsekretariats des Rates und der Kommission alle angemessenen und zur Anwendung dieser Vorschriften erforderlichen Maßnahmen ergreifen.

(10) Der Generalsekretär des EAD ist die Sicherheitsbehörde des EAD und Artikel 1 des Beschlusses ADMIN (2015)34 des Generalsekretärs des Europäischen Auswärtigen Dienstes vom 14. September 2015 sieht vor, dass die in den EAD-Sicherheitsvorschriften vorgesehenen Sicherheitsfunktionen der Sicherheitsbehörde vom Generaldirektor für Haushalt und Verwaltung wahrgenommen werden —

HAT FOLGENDEN BESCHLUSS ERLASSEN:

Artikel 1

Gegenstand und Anwendungsbereich

In diesem Beschluss werden die Sicherheitsvorschriften für den Europäischen Auswärtigen Dienst (im Folgenden „*EAD-Sicherheitsvorschriften*“) festgelegt.

Dieser Beschluss gilt nach Artikel 10 Absatz 1 des Beschlusses 2010/427/EU des Rates vom 26. Juli 2010 über die Organisation und die Arbeitsweise des Europäischen Auswärtigen Dienstes für das gesamte Personal des EAD und das gesamte Personal der Delegationen der Union, unabhängig von ihrer dienstrechtlichen Stellung oder Herkunft, und er schafft den allgemeinen Regelungsrahmen, um den Risiken für das dem EAD unterstehende Personal gemäß Artikel 2, für die Räumlichkeiten des EAD, seine materiellen Werte, seine Informationen und seine Besucher effektiv entgegenzuwirken.

Artikel 2

Begriffsbestimmungen

Für die Zwecke dieses Beschlusses bezeichnet der Ausdruck

a) „Personal des EAD“ Beamte und sonstige Bedienstete des EAD, einschließlich zu Bediensteten auf Zeit ernannter Mitglieder des Personals der diplomatischen Dienste der Mitgliedstaaten, sowie abgeordnete nationale Sachverständige gemäß Artikel 6 des Beschlusses 2010/427/EU des Rates vom 26. Juli 2010 über die Organisation und die Arbeitsweise des Europäischen Auswärtigen Dienstes;

b) „dem EAD unterstehendes Personal“ das Personal des EAD in der Zentrale und den Delegationen der Union sowie das gesamte sonstige Personal in den Delegationen der Union, unabhängig von dessen dienstrechtlicher Stellung oder Herkunft, sowie im Rahmen dieses Beschlusses der Hohe Vertreter und gegebenenfalls sonstiges Personal, das in Räumlichkeiten der EAD-Zentrale tätig ist;

c) „Angehörige“ die beim Außenministerium des Gastlandes gemeldeten und im Haushalt lebenden Familienmitglieder des dem EAD unterstehenden Personals in Delegationen der Union;

d) „Räumlichkeiten des EAD“ alle Einrichtungen des EAD, einschließlich aller Gebäude, Büros, Räume und sonstigen Bereiche, sowie die Bereiche, in denen Kommunikations- und Informationssysteme (auch solche zur Bearbeitung von EU-VS) untergebracht sind, die vom EAD ständig oder zeitweilig für die Ausübung seiner Tätigkeiten genutzt werden;

e) „Sicherheitsinteressen des EAD“ das dem EAD unterstehende Personal, Räumlichkeiten des EAD, Angehörige, materielle Werte einschließlich Kommunikations- und Informationssystemen, Informationen und Besucher;

f) „EU-VS“ alle mit einem EU-Geheimhaltungsgrad gekennzeichneten Informationen oder Materialien, deren unbefugte Offenlegung den Interessen der Europäischen Union oder eines oder mehrerer ihrer Mitgliedstaaten in unterschiedlichem Maße schaden könnte;

g) „Delegation der Union“ Delegationen in Drittländern und bei internationalen Organisationen im Sinne von Artikel 1 Absatz 4 des Beschlusses 2010/427/EU des Rates vom 26. Juli 2010 über die Organisation und die Arbeitsweise des Europäischen Auswärtigen Dienstes.

Weitere Begriffsbestimmungen sind in den jeweiligen Anhängen und in Anlage A aufgeführt.

Artikel 3

Sorgfaltspflicht

(1) Die EAD-Sicherheitsvorschriften gewährleisten, dass den Sorgfaltspflichten des EAD nachgekommen wird.

(2) Die Sorgfaltspflicht des EAD bezeichnet die Verpflichtung, mit der gebotenen Sorgfalt alle geeigneten Maßnahmen zur Umsetzung der Sicherheitsmaßnahmen zu ergreifen, um jeden nach vernünftigem Ermessen vorhersehbaren Schaden von den Sicherheitsinteressen des EAD abzuwenden.

Dazu gehören sowohl Schutz- als auch Sicherheitsmaßnahmen, einschließlich Maßnahmen in Not- oder Krisensituationen, gleich welcher Art.

(3) Um der Sorgfaltspflicht der Mitgliedstaaten, der EU-Organe und -Einrichtungen und anderer Parteien, deren Personal in Delegationen der Union und/oder Räumlichkeiten dieser Delegationen tätig ist, sowie der Sorgfaltspflicht des EAD für Delegationen der Union, die in Räumlichkeiten der vorstehend genannten anderen Parteien eingerichtet sind, Rechnung zu tragen, schließt der EAD mit jeder dieser Parteien Verwaltungsvereinbarungen, in denen die jeweiligen Funktionen und Zuständigkeiten, Aufgaben und Kooperationsmechanismen festgelegt sind.

Artikel 4

Materieller Geheimschutz und Sicherheit der Infrastruktur

(1) Der EAD trifft alle geeigneten (dauerhaften oder vorübergehenden) Maßnahmen für den materiellen Geheimschutz, einschließlich Zugangskontrollen, in allen Räumlichkeiten des EAD, um die Sicherheitsinteressen des EAD zu schützen. Diesen Maßnahmen wird beim Entwurf und der Planung neuer Räumlichkeiten und vor der Anmietung bereits bestehender Räumlichkeiten Rechnung getragen.

(2) Dem Personal, das dem EAD untersteht, und den Angehörigen können aus Sicherheitsgründen für einen bestimmten Zeitraum und in bestimmten Bereichen besondere Pflichten oder Beschränkungen auferlegt werden.

(3) Die Maßnahmen nach den Absätzen 1 und 2 müssen dem festgestellten Risiko entsprechen.

Artikel 5

Alarmstufen und Krisenmanagement

(1) Es ist Sache der Sicherheitsbehörde des EAD im Sinne von Artikel 13 Abschnitt I Absatz 1, im Vorgriff oder als Reaktion auf Bedrohungen und Vorfälle, die die Sicherheit des EAD beeinträchtigen, geeignete Alarmstufen-Maßnahmen sowie Maßnahmen für das Krisenmanagement einzuführen.

(2) Die in Absatz 1 genannten Alarmstufen-Maßnahmen entsprechen der jeweiligen Stufe der Sicherheitsbedrohung. Die Alarmstufen werden in enger Zusammenarbeit mit den zuständigen Dienststellen anderer Organe, Einrichtungen und Agenturen der Union, der Mitgliedstaaten oder jener Mitgliedstaaten, in denen sich die Räumlichkeiten des EAD befinden, definiert.

(3) Die Sicherheitsbehörde des EAD ist die Kontaktstelle für Alarmstufen und Krisenmanagement.

Artikel 6

Schutz von Verschlusssachen

(1) Für den Schutz von EU-VS gelten die in diesem Beschluss, insbesondere in Anhang A, festgelegten Vorschriften. Der Besitzer jedweder EU-VS ist für den entsprechenden Schutz dieser EU-VS verantwortlich.

(2) Der EAD gewährleistet, dass der Zugang zu Verschlusssachen nur Personen gewährt wird, die die Anforderungen gemäß Anhang A Artikel 5 erfüllen.

(3) Im Einklang mit den Vorschriften über den Schutz von EU-VS in Anhang A legt der Hohe Vertreter auch die Voraussetzungen fest, unter denen örtliche Bedienstete Zugang zu EU-VS erhalten.

(4) Die für Sicherheit zuständige Direktion des EAD verwaltet eine Datenbank, in der der Sicherheitsstatus des gesamten dem EAD unterstehenden Personals sowie der Auftragnehmer des EAD erfasst ist.

(5) Bringt ein Mitgliedstaat Verschlusssachen, die mit einem nationalen Geheimhaltungsgrad gekennzeichnet sind, in die Strukturen oder Netze des EAD ein, so schützt der EAD diese Verschlusssachen nach Maßgabe der Anforderungen, die für EU-VS mit gleichwertigem Geheimhaltungsgrad gemäß der Entsprechungstabelle in Anlage B gelten.

(6) Die Bereiche im EAD, in denen als „CONFIDENTIEL UE/EU CONFIDENTIAL“ oder höher oder mit entsprechendem Geheimhaltungsgrad eingestufte Verschlusssachen aufbewahrt werden, werden im Einklang mit den Vorschriften nach Anhang A II als abgesicherte Bereiche eingerichtet und von der Sicherheitsbehörde des EAD genehmigt.

(7) Die Verfahren, nach denen der Hohe Vertreter seine Aufgaben im Rahmen von Abkommen oder Verwaltungsvereinbarungen über den Austausch von EU-VS mit Drittstaaten oder internationalen Organisationen wahrnimmt, sind in den Anhängen A und A VI aufgeführt.

(8) Der Generalsekretär legt die Bedingungen fest, unter denen er in seinem Besitz befindliche EU-VS an andere Organe, Einrichtungen oder sonstige Stellen der Union weitergibt. Dazu wird ein geeigneter Rahmen geschaffen, unter anderem gegebenenfalls durch entsprechende interinstitutionelle oder sonstige Vereinbarungen.

(9) Mit einem solchen Rahmen wird sichergestellt, dass EU-VS ihrem Geheimhaltungsgrad entsprechend sowie nach Grundsätzen und Mindeststandards geschützt werden, die denen in diesem Beschluss festgelegten Grundsätzen und Mindeststandards gleichwertig sind.

Artikel 7

Sicherheitsvorfälle und Notfälle

(1) Um eine rasche und wirksame Reaktion auf einen Sicherheitsvorfall zu gewährleisten, legt der EAD ein Verfahren für die Meldung solcher Vorfälle und Notfälle fest, das rund um die Uhr, sieben Tage die Woche und bei jeglicher Art von Sicherheitsvorfällen oder Bedrohungen der Sicherheitsinteressen des EAD (z. B. durch Unfälle, Konflikte, böswillige Handlungen, Straftaten, Entführungen und Geiselnahmen oder medizinische Notfälle, Störungen der Kommunikations- und Informationssysteme, Cyber-Angriffe usw.) einsatzbereit ist.

(2) Zwischen der EAD-Zentrale, den Delegationen der Union, dem Rat, der Kommission, den EU-Sonderbeauftragten und den Mitgliedstaaten werden Kanäle für die Notfallkommunikation eingerichtet, um sie beim Management von Sicherheitsvorfällen, von denen das Personal betroffen ist, und deren Folgen zu unterstützen; dies schließt auch die Notfallplanung ein.

(3) Das Management von Sicherheitsvorfällen umfasst u. a.

— Verfahren zur wirksamen Unterstützung der Beschlussfassung im Zusammenhang mit einem Sicherheitsvorfall, von dem das Personal betroffen ist, einschließlich Beschlüssen über den Abzug oder die Aussetzung einer Mission, und

— ein Konzept und Verfahren für die Rettung des eingesetzten Personals — z. B. im Falle vermisster Personen oder im Falle von Entführungen und Geiselnahmen — unter Berücksichtigung der besonderen Zuständigkeiten der Mitgliedstaaten, der EU-Organe und des EAD in dieser Hinsicht. In diesem Zusammenhang sind die für das Management solcher Einsätze erforderlichen speziellen Fähigkeiten und eine mögliche Bereitstellung entsprechender Ressourcen durch die Mitgliedstaaten zu berücksichtigen.

(4) Der EAD wird geeignete Verwaltungsvereinbarungen für die Berichterstattung über Sicherheitsvorfälle in den Delegationen der Union einführen. Gegebenenfalls werden die Mitgliedstaaten, die Kommission, sonstige zuständige Behörden sowie die zuständigen Sicherheitsausschüsse unterrichtet.

(5) Die Abläufe des Vorfallmanagements sollten regelmäßig geübt und überprüft werden.

Artikel 8

Sicherheit der Kommunikations- und Informationssysteme

(1) Der EAD schützt Informationen, die in Kommunikations- und Informationssystemen bearbeitet werden, vor Bedrohungen ihrer Vertraulichkeit, Integrität, Verfügbarkeit, Authentizität und Beweisbarkeit.

(2) Entsprechende Vorschriften, Sicherheitsleitlinien und ein Sicherheitsprogramm zum Schutz aller Kommunikations- und Informationssysteme, die sich im Besitz des EAD befinden oder von ihm betrieben werden, werden von der Sicherheitsbehörde des EAD genehmigt.

(3) Vorschriften, Konzept und Programm müssen ebenso wie ihre Umsetzung eng mit denen des Rates und der Kommission und gegebenenfalls mit den Sicherheitskonzepten der Mitgliedstaaten abgestimmt werden.

(4) Alle zur Bearbeitung von Verschlusssachen verwendeten Informations- und Kommunikationssysteme werden einem Akkreditierungsverfahren unterzogen. Der EAD wendet in Absprache mit dem Generalsekretariat des Rates und der Kommission ein System für das Management der Sicherheitsakkreditierung an.

(5) Werden für den Schutz der vom EAD bearbeiteten EU-VS kryptografische Produkte eingesetzt, so müssen diese zuvor auf Empfehlung des Sicherheitsausschusses des Rates von der Krypto-Zulassungsstelle des EAD zugelassen werden.

(6) Von der Sicherheitsbehörde des EAD werden im erforderlichen Umfang folgende Stellen für Informationssicherung geschaffen:

a) eine Stelle für Informationssicherung,

b) eine TEMPEST-Stelle,

c) eine Krypto-Zulassungsstelle,

d) eine Krypto-Verteilungsstelle.

(7) Für jedes System wird die Sicherheitsbehörde des EAD folgende Stellen schaffen:

a) eine Sicherheitsakkreditierungsstelle,

b) eine für den Betrieb zuständige Stelle für Informationssicherung.

(8) Die Bestimmungen zur Anwendung dieses Artikels im Hinblick auf den Schutz von EU-VS sind in den Anhängen A und A IV enthalten.

Artikel 9

Verletzung der Sicherheit und Kenntnisnahme von Verschlusssachen durch Unbefugte

(1) Zu einer Verletzung der Sicherheit kommt es durch eine Handlung oder Unterlassung, die den in diesem Beschluss festgelegten Sicherheitsvorschriften und/oder den gemäß Artikel 21 Absatz 1 genehmigten Sicherheitskonzepten oder -leitlinien mit Maßnahmen zur Anwendung dieses Beschlusses zuwiderläuft.

(2) Eine Kenntnisnahme von Verschlusssachen durch Unbefugte liegt vor, wenn eine Verschlusssache ganz oder teilweise nicht ermächtigten Personen oder Stellen gegenüber offengelegt wurde.

(3) Eine tatsächliche oder vermutete Verletzung der Sicherheit oder eine tatsächliche oder vermutete Kenntnisnahme von Verschlusssachen durch Unbefugte wird unverzüglich der für Sicherheit zuständigen Direktion des EAD gemeldet, die geeignete Maßnahmen nach Anhang A Artikel 11 ergreift.

(4) Nach Anhang A Artikel 11 Absatz 3 können gegen jede Person, die für eine Verletzung der Sicherheitsvorschriften dieses Beschlusses oder die Kenntnisnahme von Verschlusssachen durch Unbefugte verantwortlich ist, Disziplinarmaßnahmen und/oder rechtliche Schritte gemäß den geltenden Rechts- und sonstigen Vorschriften ergriffen werden.

Artikel 10

Untersuchung von Sicherheitsvorfällen, Sicherheitsverletzungen und/oder der Kenntnisnahme durch Unbefugte sowie Abhilfemaßnahmen

(1) Unbeschadet des Artikels 86 (Disziplinarordnung) und des Anhangs IX des Statuts ([1]) kann die für Sicherheit zuständige Direktion des EAD Sicherheitsuntersuchungen durchführen:

a) bei möglichem Verlust oder möglicher Falschbehandlung bzw. unbefugter Kenntnisnahme von EU-VS, Euratom-Verschlusssachen oder nicht als Verschlusssache eingestuften vertraulichen Informationen;

b) zur Abwehr von Angriffen feindlicher Nachrichtendienste gegen den EAD und sein Personal;

c) zur Abwehr von terroristischen Anschlägen auf den EAD und sein Personal;

d) im Falle von Cybervorfällen;

e) bei sonstigen Vorfällen, die die allgemeine Sicherheit des EAD beeinträchtigen oder beeinträchtigen könnten, einschließlich vermuteter Straftaten.

(2) Die für Sicherheit zuständige Direktion des EAD wird gegebenenfalls mit Unterstützung von Sicherheitsexperten der Mitgliedstaaten und/oder anderer EU-Organe und — sofern erforderlich — mit Genehmigung der Sicherheitsbehörde des EAD alle aufgrund der Untersuchungen erforderlichen Abhilfemaßnahmen ergreifen, soweit dies angebracht erscheint.

Nur befugte Mitglieder des Personals, denen die Sicherheitsbehörde des EAD angesichts ihrer aktuellen Aufgaben einen entsprechenden, auf ihren Namen lautenden Auftrag erteilt hat, können ermächtigt werden, Sicherheitsuntersuchungen im EAD durchzuführen und zu koordinieren.

(3) Die Prüfer erhalten Zugang zu allen Informationen, die sie für die Durchführung der Untersuchungen benötigen und werden dabei von allen Dienststellen und dem Personal des EAD in vollem Umfang unterstützt.

Die Prüfer können geeignete Maßnahmen zur Sicherung des Nachweispfades ergreifen, die der Bedeutung der untersuchten Angelegenheit angemessen sind.

(4) Der Zugang zu personenbezogenen Daten, einschließlich solcher, die in den Kommunikations- und Informationssystemen erfasst sind, erfolgt nach Maßgabe der Verordnung (EG) Nr. 45/2001 ([2]).

(5) Ist für Untersuchungszwecke die Einrichtung einer Datenbank mit personenbezogenen Daten erforderlich, wird der Europäische Datenschutzbeauftragte gemäß der genannten Verordnung davon in Kenntnis gesetzt.

Artikel 11

Sicherheitsrisikomanagement

(1) Zur Bestimmung des Sicherheitsbedarfs wendet der EAD in enger Zusammenarbeit mit der Direktion Sicherheit der Kommission und gegebenenfalls mit dem Sicherheitsbüro des Generalsekretariats des Rates eine umfassende Methode zur Bewertung des Sicherheitsrisikos an.

(2) Das Risikomanagement für die Sicherheitsinteressen des EAD wird als Prozess angelegt. Ziel dieses Prozesses ist es, bekannte Sicherheitsrisiken zu bestimmen, Sicherheitsmaßnahmen zur Reduzierung dieser Risiken auf ein tragbares Maß festzulegen und Maßnahmen entsprechend dem Konzept der mehrschichtigen Sicherheit anzuwenden. Die Wirksamkeit der betreffenden Maßnahmen und das Risikoniveau werden fortlaufend bewertet.

([1]) Statut der Beamten der Europäischen Union und Beschäftigungsbedingungen für die sonstigen Bediensteten der Europäischen Union gemäß der Verordnung (EWG, Euratom, EGKS) Nr. 259/68 des Rates (ABl. L 56 vom 4.3.1968, S. 1), im Folgenden „Statut".

([2]) Verordnung (EG) Nr. 45/2001 des Europäischen Parlaments und des Rates vom 18. Dezember 2000 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft und zum freien Datenverkehr (ABl. L 8 vom 12.1.2001, S. 1).

(3) Die in diesem Beschluss festgelegten Funktionen, Verantwortlichkeiten und Aufgaben berühren nicht die Verantwortung eines jeden Mitglieds des dem EAD unterstehenden Personals; insbesondere EU-Personal, das an Missionen in Drittländern teilnimmt, muss mit gesundem Menschenverstand und Urteilsvermögen zur eigenen Sicherheit beitragen und alle Sicherheitsregeln, -vorschriften, -verfahren und -anweisungen einhalten.

(4) Um Sicherheitsrisiken vorzubeugen und diese zu beherrschen, kann beauftragtes Personal Zuverlässigkeitsüberprüfungen der in den Anwendungsbereich dieses Beschlusses fallenden Personen durchführen; dabei wird bestimmt, ob eine Sicherheitsbedrohung entsteht, falls diesen Personen Zugang zu Räumlichkeiten oder Informationen des EAD gewährt wird. Zu diesem Zweck und unter Einhaltung der Verordnung (EG) Nr. 45/2001 darf das beauftragte Personal a) jede dem EAD zur Verfügung stehende Informationsquelle nutzen, wobei die Zuverlässigkeit der Informationsquelle zu berücksichtigen ist; b) auf im Besitz des EAD befindliche Personalakten oder Daten über Personen zugreifen, die der EAD beschäftigt oder zu beschäftigen beabsichtigt; dies gilt auch für Personal von Auftragnehmern, sofern dies hinreichend begründet wird.

(5) Der EAD ergreift alle angemessenen Maßnahmen, um den Schutz seiner Sicherheitsinteressen zu gewährleisten und jeden nach vernünftigem Ermessen vorhersehbaren Schaden daran abzuwenden.

(6) Die Sicherheitsmaßnahmen im EAD für den Schutz von EU-VS während der gesamten Dauer ihrer Einstufung als Verschlusssache müssen insbesondere dem Geheimhaltungsgrad, der Form und dem Umfang der Informationen und Materialien, der Lage und der Beschaffenheit der Einrichtungen, in denen EU-VS aufbewahrt werden, und der Bedrohung, einschließlich der örtlichen Einschätzung der Bedrohung durch böswillige und/oder kriminelle Handlungen, einschließlich Spionage, Sabotage und Terrorismus, entsprechen.

Artikel 12

Sensibilisierung und Schulung in Sicherheitsfragen

(1) Die Sicherheitsbehörde des EAD stellt sicher, dass geeignete Programme zur Sensibilisierung und Schulung in Sicherheitsfragen ausgearbeitet und durchgeführt werden und dass das dem EAD unterstehende Personal sowie gegebenenfalls dessen Angehörige eine den Risiken an ihrem Wohnort angemessene Sicherheitsbelehrung und -schulung erhalten.

(2) Das Personal wird über seine Verantwortlichkeiten für den Schutz von EU-VS gemäß den Vorschriften nach Artikel 6 belehrt und erkennt sie an, bevor ihm Zugang zu EU-VS gewährt wird.

Artikel 13

Organisation der Sicherheit im EAD

Abschnitt 1

Allgemeine Bestimmungen

(1) Der Generalsekretär ist die Sicherheitsbehörde des EAD. In dieser Funktion gewährleistet er, dass

a) die Sicherheitsmaßnahmen, soweit erforderlich, mit den zuständigen Behörden der Mitgliedstaaten, dem Generalsekretariat des Rates und der Kommission und gegebenenfalls mit Drittstaaten oder internationalen Organisationen in Bezug auf alle für die Tätigkeiten des EAD relevanten Sicherheitsfragen, auch hinsichtlich der Art der Risiken für die Sicherheitsinteressen des EAD und der entsprechenden Schutzmaßnahmen, koordiniert werden;

b) die Sicherheitsaspekte bei sämtlichen Tätigkeiten des EAD von Beginn an vollständig berücksichtigt werden;

c) der Zugang zu Verschlusssachen nur Personen gewährt wird, die die Anforderungen gemäß Anhang A Artikel 5 erfüllen;

d) ein Registratursystem eingerichtet wird, um sicherzustellen, dass Verschlusssachen, die als „CONFIDENTIEL UE/EU CONFIDENTIAL“ oder höher eingestuft sind, innerhalb des EAD im Einklang mit diesem Beschluss bearbeitet werden; dies gilt auch für sämtliche an EU-Mitgliedstaaten, Organe, Einrichtungen und Agenturen der EU oder andere befugte Empfänger weitergegebenen Verschlusssachen. Alle vom EAD an Drittstaaten oder internationale Organisationen weitergegebenen EU-VS und alle von Drittstaaten und internationalen Organisationen erhaltenen Verschlusssachen werden in einem getrennten Verzeichnis erfasst;

e) Sicherheitsinspektionen nach Artikel 16 durchgeführt werden;

f) im Falle einer tatsächlichen oder vermuteten Verletzung der Sicherheit oder einer tatsächlichen oder vermuteten Kenntnisnahme von im EAD verwahrten oder herausgegebenen Verschlusssachen durch Unbefugte bzw. des Verlusts solcher Verschlusssachen Untersuchungen durchgeführt und die einschlägigen Sicherheitsbehörden um Unterstützung bei derartigen Untersuchungen ersucht werden;

g) angemessene Pläne und Mechanismen für das Vorfall- und Folgenmanagement entwickelt werden, um rechtzeitig und wirksam auf Sicherheitsvorfälle reagieren zu können;

h) angemessene Maßnahmen ergriffen werden, falls eine Person diesen Beschluss missachtet;

i) für den Schutz der Sicherheitsinteressen des EAD angemessene physische und organisatorische Maßnahmen getroffen werden.

Zu diesem Zweck wird die Sicherheitsbehörde des EAD

— die Sicherheitskategorie der Delegationen der Union in Abstimmung mit der Kommission festsetzen;

— gegebenenfalls nach Rücksprache mit dem Hohen Vertreter beschließen, wann aus Sicherheitsgründen eine Evakuierung des Personals einer Delegation der Union zu veranlassen ist;

— Maßnahmen beschließen, die zum Schutz von Angehörigen und unter Berücksichtigung der Vereinbarungen mit EU-Organen nach Artikel 3 Absatz 3 ergriffen werden;

— die Strategie für kryptografische Kommunikation, insbesondere das Programm für die Installation von kryptografischen Produkten und Mechanismen, genehmigen.

(2) Die Sicherheitsbehörde des EAD wird bei der Wahrnehmung dieser Aufgaben von dem Generaldirektor für Haushalt und Verwaltung, dem für Sicherheit zuständigen Direktor des EAD und gegebenenfalls dem stellvertretenden Generalsekretär für GSVP und Krisenreaktion unterstützt.

(3) Der Generalsekretär kann als Sicherheitsbehörde des EAD, falls erforderlich, entsprechende Aufgaben delegieren.

(4) Jeder Abteilungs-/Referatsleiter ist für die Anwendung der Vorschriften für den Schutz von EU-VS in seiner Abteilung/seinem Referat verantwortlich.

Jeder Abteilungs-/Referatsleiter benennt Mitglieder des Personals als Sicherheitskoordinatoren der Abteilung, wobei die Ressourcen dem Umfang der von der Abteilung/dem Referat bearbeiteten EU-VS angemessen sind; er trägt jedoch weiterhin die Verantwortung wie vorstehend ausgeführt.

Die Sicherheitskoordinatoren der Abteilung unterstützen gegebenenfalls ihren Abteilungs-/Referatsleiter bei der Wahrnehmung sicherheitsrelevanter Aufgaben, u. a. bei

a) der Ausarbeitung zusätzlicher Sicherheitsanforderungen, die dem spezifischen Bedarf der Abteilung/des Referats entsprechen;

b) regelmäßigen Sicherheitsbelehrungen der Mitglieder einer Abteilung/eines Referats;

c) der Gewährleistung, dass in ihrer Abteilung/ihrem Referat nach dem Grundsatz „Kenntnis nur wenn nötig“ verfahren wird;

d) der Führung einer aktuellen Liste sicherer Codes und Schlüssel;

e) der Aufrechterhaltung von Sicherheitsverfahren und Sicherheitsmaßnahmen;

f) der Berichterstattung über Verletzungen der Sicherheit und die Kenntnisnahme von EU-VS durch Unbefugte an ihre Direktoren und die für Sicherheit zuständige Direktion;

g) der Abschlussbesprechung mit Mitgliedern des Personals, deren Beschäftigungsverhältnis mit dem EAD endet;

h) der Bereitstellung regelmäßiger Berichte über sicherheitsrelevante Angelegenheiten in ihrer Abteilung/ihrem Referat durch ihre Vorgesetzten;

i) der Zusammenarbeit mit der für Sicherheit zuständigen Direktion des EAD in Sicherheitsfragen.

Die für Sicherheit zuständige Direktion des EAD wird rechtzeitig über jede Maßnahme oder Angelegenheit unterrichtet, die Auswirkungen auf die Sicherheit haben könnte.

(5) Jeder Delegationsleiter ist für die Durchführung sämtlicher Maßnahmen im Zusammenhang mit der Sicherheit der Delegation der Union verantwortlich.

Abschnitt 2

Die für Sicherheit zuständige Direktion des EAD

(1) Der EAD verfügt über eine für Sicherheit zuständige Direktion. Sie hat folgende Aufgaben:

a) Sie übernimmt Verwaltung, Koordinierung, Überwachung und/oder Umsetzung aller Sicherheitsmaßnahmen in allen der Verantwortung des EAD unterstehenden Räumlichkeiten in der Zentrale, innerhalb der EU und in Drittstaaten.

b) Sie gewährleistet die Kohärenz und Konsistenz mit diesem Beschluss und mit den Durchführungsbestimmungen bei allen Tätigkeiten, die sich auf den Schutz der Sicherheitsinteressen des EAD auswirken können.

c) Sie ist Hauptberater des Hohen Vertreters, der Sicherheitsbehörde des EAD und des stellvertretenden Generalsekretärs in allen sicherheitsrelevanten Fragen.

d) Sie wird von den zuständigen Dienststellen der Mitgliedstaaten nach Artikel 10 Absatz 3 des Beschlusses 2010/427/EU des Rates über die Organisation und die Arbeitsweise des EAD unterstützt.

e) Sie unterstützt durch Bewertungen des materiellen Geheimschutzes im Rahmen der allgemeinen Sicherheitsumgebung/lokalen Sicherheitsumgebung für Kommunikations- und Informationssysteme, mit denen EU-VS bearbeitet werden, und der Räumlichkeiten, die für die Bearbeitung und Aufbewahrung von EU-VS zugelassen sind, die Tätigkeiten der Sicherheitsakkreditierungsstelle des EAD.

(2) Der für Sicherheit zuständige Direktor des EAD hat folgende Aufgaben:

a) Gewährleistung eines umfassenden Schutzes der Sicherheitsinteressen des EAD;

b) Entwurf, Überprüfung und Aktualisierung der Sicherheitsvorschriften sowie Koordinierung der Sicherheitsmaßnahmen mit den zuständigen Behörden der Mitgliedstaaten und gegebenenfalls mit den zuständigen Behörden von Drittstaaten sowie mit internationalen Organisationen, die mit der EU Sicherheitsabkommen und/oder -vereinbarungen geschlossen haben;

c) Unterstützung der Arbeiten des Sicherheitsausschusses des EAD nach Artikel 15 Absatz 1 dieses Beschlusses;

d) gegebenenfalls Aufnahme von Kontakten zu anderen Partnern oder Behörden als den unter Buchstabe b aufgeführten im Zusammenhang mit sicherheitsrelevanten Angelegenheiten;

e) Schwerpunktsetzung und Unterbreitung von Vorschlägen für die Verwaltung der für die Sicherheit in der Zentrale und in den Delegationen der Union bereitgestellten Mittel.

(3) Der Leiter der für Sicherheit zuständigen Direktion des EAD hat folgende Aufgaben:

a) Gewährleistung der Aufzeichnung von Verletzungen der Sicherheit und der Kenntnisnahme von Verschlusssachen durch Unbefugte sowie der Einleitung und Durchführung von Untersuchungen, sofern erforderlich;

b) Organisation regelmäßiger Treffen und bei Bedarf von weiteren Treffen, um mit dem Sicherheitsdirektor des Generalsekretariats des Rates und dem Direktor der Direktion Sicherheit der Kommission Bereiche von gemeinsamem Interesse zu erörtern.

(4) Die für Sicherheit zuständige Direktion des EAD wird Kontakte knüpfen und eine enge Zusammenarbeit pflegen mit

— den für Sicherheit zuständigen Abteilungen der Außenministerien in den Mitgliedstaaten,

— den nationalen Sicherheitsbehörden und/oder sonstigen für Sicherheit zuständigen Sicherheitsbehörden der Mitgliedstaaten, um mit ihrer Unterstützung die Informationen zu erhalten, die sie für die Bewertung der Risiken und Bedrohungen benötigt, denen der EAD, sein Personal, seine Tätigkeiten, seine Werte und Ressourcen sowie seine Verschlusssachen möglicherweise an seinem üblichen Tätigkeitsort ausgesetzt sind,

— den zuständigen Sicherheitsbehörden der Mitgliedstaaten oder der Gastgeberländer, sofern der EAD in deren Gebiet seine Tätigkeit ausübt, im Zusammenhang mit allen Angelegenheiten, die den Schutz seines Personals, seiner Tätigkeiten, seiner Werte und Ressourcen sowie seiner Verschlusssachen betreffen,

— dem Sicherheitsbüro des Generalsekretariats des Rates und der Direktion Sicherheit der Generaldirektion Humanressourcen und Sicherheit der Kommission und gegebenenfalls mit den für Sicherheit zuständigen Abteilungen anderer Organe, Einrichtungen und Agenturen der EU,

— den für Sicherheit zuständigen Verwaltungsstellen von Drittstaaten und internationalen Organisationen im Hinblick auf eine nutzbringende Koordinierung und

— den nationalen Sicherheitsbehörden der Mitgliedstaaten bei allen Fragen, die den Schutz von EU-VS betreffen.

Abschnitt 3

Delegationen der Union

(1) Jeder Delegationsleiter ist vor Ort für die Durchführung und Organisation sämtlicher Maßnahmen zum Schutz der Sicherheitsinteressen des EAD innerhalb der Räumlichkeiten und Zuständigkeiten der Delegationen der Union verantwortlich.

Er unternimmt — wenn erforderlich in Abstimmung mit den zuständigen Behörden des Gastlandes — alle nach vernünftigem Ermessen zumutbaren Anstrengungen, um zu gewährleisten, dass zur Verwirklichung dieses Ziels angemessene physische und organisatorische Maßnahmen getroffen werden.

Der Delegationsleiter legt — gegebenenfalls unter Berücksichtigung etwaiger Verwaltungsvereinbarungen nach Artikel 3 Absatz 3 — Sicherheitsverfahren für den Schutz von Angehörigen im Sinne von Artikel 2 Buchstabe c fest. Der Delegationsleiter erstattet dem Leiter der für Sicherheit zuständigen Direktion des EAD Bericht über alle sicherheitsrelevanten Fragen, die in seinen Zuständigkeitsbereich fallen.

Er wird bei diesen Aufgaben durch die für Sicherheit zuständige Direktion des EAD, durch das Sicherheitsmanagement-Team der Delegation der Union, das aus mit Sicherheitsaufgaben und -funktionen betrautem Personal besteht, und durch Sicherheitspersonal, das erforderlichenfalls hierfür abgestellt wird, unterstützt.

Die Delegation der Union pflegt mit den diplomatischen Vertretungen der Mitgliedstaaten regelmäßige Kontakte und eine enge Zusammenarbeit in Sicherheitsfragen.

(2) Außerdem übernimmt der Delegationsleiter folgende Aufgaben:

— Aufstellung detaillierter Sicherheits- und Notfallpläne für die Delegation der Union anhand allgemeiner Standardverfahren;

— Betrieb eines rund um die Uhr einsatzbereiten Systems für das Management von Sicherheitsvorfällen und Notfällen im Rahmen des Tätigkeitsbereichs der Delegation der Union;

— Gewährleistung eines an die örtlichen Bedingungen angepassten Versicherungsschutzes des gesamten in der Delegation der Union eingesetzten Personals;

— Gewährleistung der Einbeziehung des Sicherheitsaspekts in die Einführungsschulung, die alle in der Delegation der Union eingesetzten Mitglieder des Personals bei Dienstantritt in der Delegation der Union erhalten, und

— Gewährleistung der Umsetzung aller Empfehlungen, die aus Sicherheitsbewertungen hervorgehen, und regelmäßige schriftliche Berichterstattung über die Umsetzung dieser Empfehlungen und andere Sicherheitsfragen an die Sicherheitsbehörde des EAD.

(3) Der Delegationsleiter, der weiterhin für die Gewährleistung des Sicherheitsmanagements sowie der Resilienz der Dienststelle verantwortlich und rechenschaftspflichtig bleibt, kann dem Sicherheitskoordinator der Delegation als stellvertretendem Delegationsleiter oder, wenn kein Koordinator ernannt wurde, einer geeigneten anderen Person, die Wahrnehmung seiner sicherheitsrelevanten Aufgaben übertragen.

Insbesondere folgende Aufgaben können dem Sicherheitskoordinator der Delegation übertragen werden:

— Koordinierung der Sicherheitsfunktionen in der Delegation der Union;

— Aufnahme von Kontakten in Sicherheitsfragen zu den zuständigen Behörden des Gaststaates und den entsprechenden Stellen in den Botschaften und diplomatischen Vertretungen der Mitgliedstaaten;

— Umsetzung geeigneter Verfahren für das Sicherheitsmanagement zum Schutz der Sicherheitsinteressen des EAD, einschließlich des Schutzes von EU-VS;

— Gewährleistung der Einhaltung der Sicherheitsvorschriften und -anweisungen;

— Belehrung des Personals über die für das Personal geltenden Sicherheitsvorschriften und im Gaststaat bestehende spezifische Risiken;

— Anträge an die für Fragen der Sicherheitsüberprüfung zuständige Direktion des EAD für Dienstposten, für die eine Erklärung über die Sicherheitsüberprüfung von Personal (Personnel Security Clearance — PSC) erforderlich ist; und

— regelmäßige Unterrichtung des Delegationsleiters, des regionalen Sicherheitsbeauftragten und der für Sicherheit zuständigen Direktion des EAD über Vorfälle oder Entwicklungen in dem Gebiet, die sich auf den Schutz der Sicherheitsinteressen des EAD auswirken können.

(4) Der Delegationsleiter kann administrative oder technische Sicherheitsaufgaben auf den Leiter der Verwaltung und andere Mitglieder des Personals der Delegation der Union übertragen.

(5) Die Delegation der Union wird von einem regionalen Sicherheitsbeauftragten unterstützt. Der regionale Sicherheitsbeauftragte erfüllt die nachstehend aufgeführten Aufgaben in einer Delegation der Union im Rahmen ihres jeweiligen geografischen Zuständigkeitsbereichs.

Wenn es die vorherrschende Sicherheitslage erfordert, kann unter bestimmten Umständen ein regionaler Sicherheitsbeauftragter auch dauerhaft auf Vollzeitbasis für eine spezifische Delegation der Union abgestellt werden.

Es kann erforderlich sein, dass ein regionaler Sicherheitsbeauftragter außerhalb seines jeweiligen Zuständigkeitsbereichs — einschließlich der Zentrale — versetzt wird oder auf Anweisung der für Sicherheit zuständigen Direktion des EAD nach Maßgabe der Sicherheitslage in einem Land dort seine Funktion dauerhaft ausübt.

(6) Der regionale Sicherheitsbeauftragte untersteht der direkten operativen Kontrolle der für Sicherheit im Einsatzgebiet zuständigen Dienststelle der Zentrale des EAD, jedoch der gemeinsamen administrativen Kontrolle des Leiters der Delegation am Ort der dienstlichen Verwendung und der für Sicherheit im Einsatzgebiet zuständigen Dienststelle der Zentrale. Der regionale Sicherheitsbeauftragte berät und unterstützt den Delegationsleiter und das Personal der Delegation der Union bei der Vorbereitung und Durchführung aller physischen, organisatorischen und verfahrenstechnischen Maßnahmen zur Gewährleistung der Sicherheit der Delegation der Union.

(7) Der regionale Sicherheitsbeauftragte berät und unterstützt den Delegationsleiter und das Personal der Delegation der Union. Gegebenenfalls und insbesondere, wenn ein regionaler Sicherheitsbeauftragter dauerhaft auf Vollzeitbasis tätig ist, sollte er eine Delegation der Union bei Sicherheitsmanagement und Sicherheitsimplementierung unterstützen, was auch die Vorbereitung von sicherheitsspezifischen Verträgen sowie die Verwaltung von Akkreditierungen und Sicherheitsüberprüfungen einschließt.

Artikel 14

GSVP-Operationen und EU-Sonderbeauftragte

In Ergänzung der spezifischen Vorgaben im Rahmen der vom Rat angenommenen einschlägigen Strategien berät die für Sicherheit zuständige Direktion des EAD den Direktor der Direktion Krisenbewältigung und Planung, den Generaldirektor des Militärstabs der EU, den Zivilen Operationskommandeur, der den Zivilen Planungs- und Durchführungsstab leitet, und die Kommandeure von militärischen Operationen der EU bei sicherheitsrelevanten Aspekten von GSVP-Operationen und die EU-Sonderbeauftragten bei sicherheitsrelevanten Aspekten ihrer Mandate.

Artikel 15

Sicherheitsausschuss des EAD

(1) Es wird ein Sicherheitsausschuss des EAD eingesetzt.

Den Vorsitz führt die Sicherheitsbehörde des EAD oder eine von ihr beauftragte Person; der Ausschuss tritt auf Anweisung des Vorsitzes oder auf Antrag eines seiner Mitglieder zusammen. Die für Sicherheit zuständige Direktion des EAD unterstützt den Vorsitz bei der Wahrnehmung seiner Aufgaben und leistet gegebenenfalls administrative Hilfe bei den Ausschussarbeiten.

(2) Der Sicherheitsausschuss des EAD setzt sich zusammen aus Vertretern

— jedes Mitgliedstaates,

— des Sicherheitsbüros des Generalsekretariats des Rates,

— der Direktion Sicherheit der Generaldirektion Humanressourcen und Sicherheit der Kommission.

Den Delegationen der Mitgliedstaaten für den Sicherheitsausschuss des EAD können als Mitglieder angehören

— Vertreter der nationalen Sicherheitsbehörden und/oder der beauftragten Sicherheitsbehörden,

— Vertreter der für Sicherheit zuständigen Abteilungen der Außenministerien.

(3) Die dem Ausschuss angehörenden Vertreter können sich von Experten begleiten und beraten lassen, wenn sie dies für notwendig erachten. Vertreter anderer Organe, Agenturen und Einrichtungen der EU können eingeladen werden, wenn Fragen erörtert werden, die ihre Sicherheit betreffen.

(4) Unbeschadet des Absatzes 5 unterstützt der Sicherheitsausschuss des EAD den EAD im Rahmen von Konsultationen bei allen für die Tätigkeit des EAD, die Zentrale und die Delegationen der Union relevanten Sicherheitsfragen.

Unbeschadet des Absatzes 5 wird der Sicherheitsausschuss des EAD insbesondere

a) zu folgenden Fragen konsultiert:

— Sicherheitsstrategien, -leitlinien, -konzepte oder andere Dokumente über sicherheitsrelevante Methoden, insbesondere für den Schutz von Verschlusssachen und die Maßnahmen, die im Falle einer Missachtung der Sicherheitsvorschriften durch das Personal des EAD zur ergreifen sind;

— technische Sicherheitsaspekte, die den Beschluss des Hohen Vertreters, eine Empfehlung zur Aufnahme von Verhandlungen über Geheimschutzabkommen nach Anhang A Artikel 10 Absatz 1 Buchstabe a an den Rat zu richten, beeinflussen könnten;

— alle Änderungen dieses Beschlusses;

b) unbeschadet des Artikels 3 Absatz 3 zu Fragen, die die Sicherheit von Personal und Werten in der EAD-Zentrale und den Delegationen der Union betreffen, konsultiert oder darüber unterrichtet;

c) über alle Fälle von Kenntnisnahme durch Unbefugte oder den Verlust von EU-VS innerhalb des EAD unterrichtet.

(5) Für alle Änderungen der den Schutz von EU-VS betreffenden Vorschriften dieses Beschlusses und seines Anhangs A muss eine einhellig befürwortende Stellungnahme der im Sicherheitsausschuss des EAD vertretenen Mitgliedstaaten eingeholt werden. Eine solche einhellig befürwortende Stellungnahme ist auch erforderlich für

— die Aufnahme von Verhandlungen über Verwaltungsvereinbarungen nach Anhang A Artikel 10 Absatz 1 Buchstabe b;

— die Weitergabe von Verschlusssachen in den besonderen Ausnahmefällen nach Anhang A VI Nummern 9, 11 und 12;

— das Treffen der Entscheidung an der Stelle des Herausgebers der Verschlusssachen unter den in Anhang A Artikel 10 Absatz 6 letzter Satz genannten Umständen.

Eine einhellig befürwortende Stellungnahme gilt als erteilt, wenn während der Ausschussberatungen keine Einsprüche von den Delegationen der Mitgliedstaaten erhoben werden.

(6) Der Sicherheitsausschuss des EAD berücksichtigt in vollem Umfang die geltenden Sicherheitskonzepte und Leitlinien des Rates und der Kommission.

(7) Der Sicherheitsausschuss des EAD erhält jährlich eine Liste der EAD-Inspektionen sowie die endgültigen Inspektionsberichte.

(8) Organisation von Sitzungen:

— Der Sicherheitsausschuss des EAD tritt mindestens zweimal jährlich zusammen. Auf Initiative des Vorsitzes oder auf Antrag der Ausschussmitglieder können zusätzliche Sitzungen mit allen Mitgliedern oder mit den Vertretern der nationalen Sicherheitsbehörden/beauftragten Sicherheitsbehörden oder der für Sicherheit zuständigen Abteilungen der Außenministerien einberufen werden.

— Der Sicherheitsausschuss des EAD organisiert seine Tätigkeit so, dass er Empfehlungen zu spezifischen Sicherheitsfragen geben kann. Er kann bei Bedarf weitere Fachuntergruppen einrichten. Er legt das Mandat für diese Fachuntergruppen fest und erhält von diesen Berichte über ihre Tätigkeiten.

— Die für Sicherheit zuständige Direktion des EAD ist für die Vorbereitung der zu erörternden Themen zuständig. Der Vorsitz stellt für jede Sitzung eine vorläufige Tagesordnung auf. Die Mitglieder des Ausschusses können weitere Diskussionspunkte vorschlagen.

Artikel 16

Sicherheitsinspektionen

(1) Die Sicherheitsbehörde des EAD gewährleistet, dass in der Zentrale des EAD und in den Delegationen der Union regelmäßig Sicherheitsinspektionen durchgeführt werden, um zu überprüfen, ob die Sicherheitsmaßnahmen angemessen sind und mit diesem Beschluss im Einklang stehen. Die für Sicherheit zuständige Direktion des EAD kann gegebenenfalls Experten für die Beteiligung an Sicherheitsinspektionen in den nach Titel V Kapitel 2 EUV geschaffenen Agenturen und Einrichtungen der EU benennen.

(2) Die Sicherheitsinspektionen des EAD werden unter der Verantwortung der für Sicherheit zuständigen Direktion des EAD und gegebenenfalls mit Unterstützung von Sicherheitsexperten anderer Organe der EU oder der Mitgliedstaaten durchgeführt, insbesondere im Rahmen der Vereinbarungen nach Artikel 3 Absatz 3.

(3) Der EAD kann gegebenenfalls auf einschlägige Fachkenntnisse in den Mitgliedstaaten, dem Generalsekretariat des Rates und der Kommission zurückgreifen.

Sofern erforderlich, können Sicherheitsexperten, die sich im Rahmen von Missionen der Mitgliedstaaten in einem Drittland aufhalten und/oder Vertreter der diplomatischen Sicherheitsdienste der Mitgliedstaaten zur Teilnahme an der Sicherheitsinspektion einer Delegation der Union aufgefordert werden.

(4) Die Bestimmungen zur Anwendung dieses Artikels im Hinblick auf den Schutz von EU-VS sind in Anhang A III aufgeführt.

Artikel 17

Bewertungsbesuche

Bewertungsbesuche werden durchgeführt, um die Wirksamkeit der Sicherheitsvorkehrungen zu überprüfen, die zum Schutz von im Rahmen einer Verwaltungsvereinbarung nach Anhang A Artikel 10 Absatz 1 Buchstabe b ausgetauschten EU-VS in einem Drittstaat oder einer internationalen Organisation getroffen werden.

Die für Sicherheit zuständige Direktion des EAD kann Experten für die Beteiligung an Bewertungsbesuchen in Drittstaaten oder internationalen Organisationen benennen, mit denen die EU ein Geheimschutzabkommen nach Anhang A Artikel 10 Absatz 1 Buchstabe a geschlossen hat.

Artikel 18

Notfallplanung

Die für Sicherheit zuständige Direktion des EAD unterstützt die Sicherheitsbehörde des EAD beim Management der sicherheitsbezogenen Aspekte der allgemeinen Notfallplanung des EAD.

Artikel 19

Reisehinweise für Missionen außerhalb der EU

Die für Sicherheit zuständige Direktion des EAD gewährleistet, dass für Missionen, die das dem EAD unterstehende Personal außerhalb der EU auszuführen hat, Reisehinweise zur Verfügung stehen und greift dabei auf die Ressourcen aller zuständigen Dienste des EAD zurück, insbesondere des Lagezentrums, des INTCEN, der geografischen Abteilungen und der Delegationen der Union.

Die für Sicherheit zuständige Direktion des EAD stellt auf Antrag und unter Nutzung der genannten Ressourcen spezifische Reisehinweise für Missionen zur Verfügung, die das dem EAD unterstehende Personal in Drittstaaten mit hohem oder erhöhtem Sicherheitsrisiko auszuführen hat.

Artikel 20

Gesundheit und Sicherheit

Die EAD-Sicherheitsvorschriften ergänzen die vom Hohen Vertreter angenommenen Vorschriften des EAD für Gesundheitsschutz und Sicherheit.

Artikel 21

Umsetzung und Überprüfung

(1) In enger Zusammenarbeit mit den zuständigen Sicherheitsbehörden der Mitgliedstaaten und mit Unterstützung der einschlägigen Dienststellen der EU-Organe legt die Sicherheitsbehörde des EAD, gegebenenfalls nach Konsultation des Sicherheitsausschusses des EAD, Sicherheitsleitlinien mit allen erforderlichen Maßnahmen zur Anwendung dieser Vorschriften im EAD fest und schafft in Bezug auf alle Sicherheitsaspekte die erforderlichen Kapazitäten.

(2) Nach Artikel 4 Absatz 5 des Beschlusses 2010/427/EU des Rates vom 26. Juli 2010 über die Organisation und die Arbeitsweise des Europäischen Auswärtigen Dienstes können erforderlichenfalls Übergangsregelungen in Form von Dienstleistungsvereinbarungen mit den einschlägigen Dienststellen des Generalsekretariats des Rates und der Kommission zur Anwendung kommen.

(3) Der Hohe Vertreter stellt eine insgesamt kohärente Anwendung dieses Beschlusses sicher und überprüft regelmäßig die Sicherheitsvorschriften.

(4) Die EAD-Sicherheitsvorschriften werden in enger Zusammenarbeit mit den zuständigen Sicherheitsbehörden der Mitgliedstaaten umgesetzt.

(5) Der EAD gewährleistet, dass im Rahmen des Krisenreaktionssystems des EAD allen Aspekten des Sicherheitsprozesses Rechnung getragen wird.

(6) Der Generalsekretär als Sicherheitsbehörde und der Leiter der für Sicherheit zuständigen Direktion des EAD sorgen für die Durchführung dieses Beschlusses.

Artikel 22

Ersetzung bisheriger Beschlüsse

Der Beschluss der Hohen Vertreterin der Union für Außen- und Sicherheitspolitik vom 19. April 2013 über die Sicherheitsvorschriften für den Europäischen Auswärtigen Dienst ([1]) wird durch den vorliegenden Beschluss aufgehoben und ersetzt.

Artikel 23

Schlussbestimmungen

Dieser Beschluss tritt am Tag seiner Unterzeichnung in Kraft.

Er wird im Amtsblatt der Europäischen Union veröffentlicht.

Die zuständigen Stellen im EAD werden das gesamte Personal, das unter den Anwendungsbereich dieses Beschlusses und seiner Anhänge fällt, rechtzeitig und ordnungsgemäß über dessen Inhalt, Inkrafttreten und nachfolgende Änderungen unterrichten.

Geschehen zu Brüssel am 19. September 2017.

Federica MOGHERINI

Hohe Vertreterin der Union für Außen- und Sicherheitspolitik

([1]) ABl. C 190 vom 29.6.2013, S. 1.

ANHANG A

GRUNDPRINZIPIEN UND STANDARDS FÜR DEN SCHUTZ VON EU-VS

Artikel 1

Gegenstand, Anwendungsbereich und Begriffsbestimmungen

(1) In diesem Anhang sind die Grundprinzipien und Mindeststandards für die Sicherheit in Bezug auf den Schutz von EU-VS festgelegt.

(2) Diese Grundprinzipien und Mindeststandards gelten für den EAD und das dem EAD unterstehende, in den Artikeln 1 und 2 dieses Beschlusses aufgeführte und definierte Personal.

Artikel 2

Begriffsbestimmung für EU-VS, Geheimhaltungsgrade und Kennzeichnungen

(1) „EU-Verschlusssachen" (EU-VS) sind alle mit einem EU-Geheimhaltungsgrad gekennzeichneten Informationen oder Materialien, deren unbefugte Offenlegung den Interessen der Europäischen Union oder eines oder mehrerer ihrer Mitgliedstaaten in unterschiedlichem Maße schaden könnte.

(2) EU-VS werden in einen der folgenden Geheimhaltungsgrade eingestuft:

a) TRÈS SECRET UE/EU TOP SECRET: Informationen und Materialien, deren unbefugte Offenlegung den wesentlichen Interessen der Europäischen Union oder eines oder mehrerer Mitgliedstaaten äußerst schweren Schaden zufügen könnte.

b) SECRET UE/EU SECRET: Informationen und Materialien, deren unbefugte Offenlegung den wesentlichen Interessen der Europäischen Union oder eines oder mehrerer Mitgliedstaaten schweren Schaden zufügen könnte.

c) CONFIDENTIEL UE/EU CONFIDENTIAL: Informationen und Materialien, deren unbefugte Offenlegung den wesentlichen Interessen der Europäischen Union oder eines oder mehrerer Mitgliedstaaten Schaden zufügen könnte.

d) RESTREINT UE/EU RESTRICTED: Informationen und Materialien, deren unbefugte Offenlegung für die Interessen der Europäischen Union oder eines oder mehrerer Mitgliedstaaten nachteilig sein könnte.

(3) EU-VS werden mit einem Geheimhaltungsgrad gemäß Absatz 2 gekennzeichnet. Sie können zusätzliche Kennzeichnungen tragen, mit denen der Tätigkeitsbereich, auf den sie sich beziehen, angegeben, der Herausgeber benannt, die Verteilung begrenzt, die Verwendung eingeschränkt oder die Möglichkeit zur Weitergabe ausgewiesen wird.

Artikel 3

Regeln für die Einstufung als Verschlusssache

(1) Der EAD gewährleistet, dass EU-VS angemessen eingestuft werden, deutlich als Verschlusssache gekennzeichnet sind und ihren Geheimhaltungsgrad nur so lange wie erforderlich behalten.

(2) Der Geheimhaltungsgrad von EU-VS darf ohne vorherige schriftliche Zustimmung des Herausgebers weder herabgestuft noch aufgehoben werden; das Gleiche gilt für die Veränderung oder Entfernung der in Artikel 2 Absatz 3 genannten Kennzeichnungen.

(3) Die Sicherheitsbehörde des EAD legt nach Konsultation des Sicherheitsausschusses des EAD nach Artikel 15 Absatz 5 dieses Beschlusses Sicherheitsleitlinien für die Erstellung von EU-VS, einschließlich eines Einstufungsleitfadens für Verschlusssachen, fest.

Artikel 4

Schutz von Verschlusssachen

(1) EU-VS werden gemäß diesem Beschluss geschützt.

(2) Der Besitzer einer EU-VS ist dafür verantwortlich, diese gemäß diesem Beschluss zu schützen.

(3) Bringt ein Mitgliedstaat Verschlusssachen, die mit einem nationalen Geheimhaltungsgrad gekennzeichnet sind, in die Strukturen oder Netze des EAD ein, so schützt der EAD diese Verschlusssachen nach Maßgabe der Anforderungen, die für EU-VS mit gleichwertigem Geheimhaltungsgrad gemäß der Entsprechungstabelle in Anlage B gelten.

Der EAD legt geeignete Verfahren fest, um genaue Aufzeichnungen zu führen über den Herausgeber

— von Verschlusssachen, die der EAD erhält, und

— des Ausgangsmaterials, das in vom EAD stammenden Verschlusssachen enthalten ist.

Der Sicherheitsausschuss des EAD wird über diese Verfahren unterrichtet.

(4) Große Mengen oder eine Zusammenstellung von EU-VS können ein Schutzniveau erfordern, das einem höheren Geheimhaltungsgrad als dem der einzelnen Bestandteile entspricht.

Artikel 5

Personeller Geheimschutz bei der Bearbeitung von EU-Verschlusssachen

(1) Der personelle Geheimschutz beinhaltet die Anwendung von Maßnahmen, mit denen gewährleistet wird, dass nur Personen Zugang zu EU-VS erhalten, die

— Kenntnis von EU-VS haben müssen,

— für den Zugang zu als „CONFIDENTIEL UE/EU CONFIDENTIAL“ oder höher eingestuften Verschlusssachen für den entsprechenden Geheimhaltungsgrad sicherheitsüberprüft sind oder auf andere Weise aufgrund ihrer Tätigkeit nach Maßgabe der innerstaatlichen Rechtsvorschriften ordnungsgemäß ermächtigt sind und

— über ihre Verantwortlichkeiten belehrt worden sind.

(2) Das Verfahren zur Ausstellung von Erklärungen über die Sicherheitsüberprüfung von Personal (Personnel Security Clearance — PSC) dient der Feststellung, ob eine Person unter Berücksichtigung ihrer Loyalität, Vertrauenswürdigkeit und Zuverlässigkeit zum Zugang zu EU-VS ermächtigt werden kann.

(3) Jede Person wird über ihre Verantwortlichkeiten für den Schutz von EU-VS nach Maßgabe dieses Beschlusses belehrt und erkennt sie schriftlich an, bevor ihr Zugang zu EU-VS gewährt wird; eine solche Belehrung bzw. Anerkennung erfolgt auch später in regelmäßigen Abständen.

(4) Die Bestimmungen zur Anwendung dieses Artikels sind in Anhang A I enthalten.

Artikel 6

Materieller Geheimschutz für EU-Verschlusssachen

(1) Der materielle Geheimschutz beinhaltet die Anwendung von physischen und technischen Schutzmaßnahmen zur Verhinderung des unbefugten Zugangs zu EU-VS.

(2) Die Maßnahmen des materiellen Geheimschutzes zielen darauf ab, das heimliche oder gewaltsame Eindringen unbefugter Personen zu verhindern, von unbefugten Handlungen abzuschrecken bzw. diese zu verhindern und aufzudecken und beim Zugang von Personal zu EU-VS eine Differenzierung nach dem Grundsatz „Kenntnis nur, wenn nötig“ zu ermöglichen. Diese Maßnahmen werden auf der Grundlage eines Risikomanagementprozesses festgelegt.

(3) Die Maßnahmen des materiellen Geheimschutzes werden für alle Räumlichkeiten, Gebäude, Büros, Räume und sonstigen Bereiche, in denen EU-VS bearbeitet oder aufbewahrt werden, getroffen, einschließlich Bereichen, in denen Kommunikations- und Informationssysteme gemäß Anhang A Artikel 8 Absatz 2 untergebracht sind.

(4) Die Bereiche, in denen als „CONFIDENTIEL UE/EU CONFIDENTIAL“ oder höher eingestufte EU-VS aufbewahrt werden, werden als abgesicherte Bereiche nach Anhang A II eingerichtet und von der Sicherheitsbehörde des EAD genehmigt.

(5) Zum Schutz von als „CONFIDENTIEL UE/EU CONFIDENTIAL“ oder höher eingestuften EU-VS werden ausschließlich zugelassene Ausrüstungen oder Geräte verwendet.

(6) Die Bestimmungen zur Anwendung dieses Artikels sind in Anhang A II enthalten.

Artikel 7

Verwaltung von Verschlusssachen

(1) Die Verwaltung von Verschlusssachen beinhaltet die Anwendung administrativer Maßnahmen zur Kontrolle von EU-VS während der gesamten Dauer ihrer Einstufung als EU-VS mit dem Ziel, die Maßnahmen nach den Artikeln 5, 6 und 8 zu ergänzen und dadurch dazu beizutragen, die beabsichtigte oder unbeabsichtigte Kenntnisnahme von Verschlusssachen durch Unbefugte sowie den Verlust von Verschlusssachen zu verhindern oder aufzudecken und entsprechende Maßnahmen zur Wiederherstellung der Sicherheit zu treffen. Diese Maßnahmen beziehen sich insbesondere auf die Erstellung, die Registrierung, die Vervielfältigung, die Übersetzung, die Beförderung, die Bearbeitung, die Aufbewahrung und die Vernichtung von EU-VS.

(2) Als „CONFIDENTIEL UE/EU CONFIDENTIAL“ oder höher eingestufte Verschlusssachen werden zu Sicherheitszwecken bei Erhalt und vor ihrer Weiterleitung registriert. Zu diesem Zweck richten die zuständigen Stellen im EAD ein Registratursystem ein. Als „TRÈS SECRET UE/EU TOP SECRET“ eingestufte Verschlusssachen werden in eigens dafür bestimmten Registraturen registriert.

(3) In Dienststellen und Räumlichkeiten, in denen EU-VS bearbeitet oder aufbewahrt werden, sind regelmäßig Inspektionen durch die Sicherheitsbehörde des EAD durchzuführen.

(4) EU-VS werden zwischen Dienststellen und Räumlichkeiten außerhalb von physisch geschützten Bereichen wie folgt befördert:

a) In der Regel werden EU-VS elektronisch übermittelt und dabei durch kryptografische Produkte geschützt, die nach Artikel 7 Absatz 5 dieses Beschlusses und anhand klar definierter Sicherheitsbetriebsverfahren zugelassen wurden;

b) wenn die unter Buchstabe a genannten Mittel nicht verwendet werden, erfolgt die Beförderung von EU-VS entweder

   i) auf elektronischen Datenträgern (z. B. USB-Sticks, CDs, Festplattenlaufwerken), die durch kryptografische Produkte geschützt sind, die nach Artikel 8 Absatz 5 dieses Beschlusses zugelassen wurden, oder

   ii) in allen anderen Fällen gemäß den Vorschriften der Sicherheitsbehörde des EAD im Einklang mit den einschlägigen Schutzmaßnahmen von Anhang A III Abschnitt V.

(5) Die Bestimmungen zur Anwendung dieses Artikels sind in Anhang A III enthalten.

Artikel 8

Schutz von EU-VS, die in Kommunikations- und Informationssystemen bearbeitet werden

(1) Die Informationssicherung im Bereich von Kommunikations- und Informationssystemen beruht auf dem Vertrauen darauf, dass die in diesen Systemen bearbeiteten Informationen geschützt sind und dass diese Systeme unter der Kontrolle rechtmäßiger Nutzer jederzeit ordnungsgemäß funktionieren. Eine effektive Informationssicherung stellt ein angemessenes Niveau der Vertraulichkeit, Integrität, Verfügbarkeit, Beweisbarkeit und Authentizität sicher. Die Informationssicherung stützt sich auf einen Risikomanagementprozess.

(2) Ein „Kommunikations- und Informationssystem“ ist ein System, das die Bearbeitung von Informationen in elektronischer Form ermöglicht. Zu einem Kommunikations- und Informationssystem gehören sämtliche für seinen Betrieb benötigten Werte, einschließlich der Infrastruktur, der Organisation, des Personals und der Informationsressourcen. Dieser Anhang gilt für alle Kommunikations- und Informationssysteme des EAD, in denen EU-VS bearbeitet werden.

(3) In Kommunikations- und Informationssystemen werden EU-VS gemäß dem Konzept der Informationssicherung bearbeitet.

(4) Alle Kommunikations- und Informationssysteme, in denen EU-VS bearbeitet werden, werden einem Akkreditierungsverfahren unterzogen. Mit der Akkreditierung wird bezweckt, Gewissheit darüber zu erlangen, dass alle angemessenen Sicherheitsmaßnahmen durchgeführt worden sind und dass ein ausreichender Schutz der EU-VS und des Kommunikations- und Informationssystems gemäß diesem Beschluss gegeben ist. In der Akkreditierungserklärung wird festgelegt, bis zu welchem Geheimhaltungsgrad und unter welchen Voraussetzungen Verschlusssachen in dem Kommunikations- und Informationssystem bearbeitet werden dürfen.

(5) Kommunikations- und Informationssysteme, in denen als „CONFIDENTIEL UE/EU CONFIDENTIAL“ und höher eingestufte Verschlusssachen bearbeitet werden, werden so geschützt, dass von Informationen nicht über unbeabsichtigte elektromagnetische Abstrahlung unbefugt Kenntnis genommen werden kann („TEMPEST-Sicherheitsvorkehrungen“).

(6) Wird der Schutz von EU-VS mit kryptografischen Produkten sichergestellt, so sind diese Produkte nach Artikel 8 Absatz 5 dieses Beschlusses zuzulassen.

(7) Bei der elektronischen Übermittlung von EU-VS werden zugelassene kryptografische Produkte verwendet. Ungeachtet dieser Anforderung können in Notsituationen oder im Rahmen bestimmter technischer Konfigurationen spezielle Verfahren nach Maßgabe des Anhangs A IV angewandt werden.

(8) Nach Artikel 8 Absatz 6 dieses Beschlusses werden je nach Bedarf die nachstehenden Funktionen für Informationssicherung geschaffen:

a) eine Stelle für Informationssicherung,

b) eine TEMPEST-Stelle,

c) eine Krypto-Zulassungsstelle,

d) eine Krypto-Verteilungsstelle.

(9) Nach Artikel 8 Absatz 7 dieses Beschlusses wird für jedes System Folgendes eingerichtet:

a) eine Sicherheitsakkreditierungsstelle;

b) eine für den Betrieb zuständige Stelle für Informationssicherung.

(10) Die Bestimmungen zur Anwendung dieses Artikels sind in Anhang A IV enthalten.

Artikel 9

Geheimschutz in der Wirtschaft

(1) Der Geheimschutz in der Wirtschaft beinhaltet die Anwendung von Maßnahmen zum Schutz von EU-VS durch Auftragnehmer oder Unterauftragnehmer während der Verhandlungen vor der Auftragsvergabe und während der gesamten Laufzeit von als Verschlusssachen eingestuften Aufträgen. Grundsätzlich beinhalten derartige Aufträge nicht den Zugang zu als „TRÈS SECRET UE/EU TOP SECRET“ eingestuften Verschlusssachen.

(2) Der EAD kann industrielle oder andere Unternehmen, die in einem Mitgliedstaat oder in einem Drittstaat, mit dem ein Geheimschutzabkommen oder eine Verwaltungsvereinbarung nach Anhang A Artikel 10 Absatz 1 geschlossen wurde, eingetragen sind, vertraglich mit Aufträgen betrauen, die den Zugang zu oder die Bearbeitung oder Aufbewahrung von EU-VS beinhalten oder nach sich ziehen.

(3) Der EAD stellt als Vergabebehörde sicher, dass die in diesem Beschluss festgelegten und in dem Vertrag genannten Mindeststandards für den Geheimschutz in der Wirtschaft eingehalten werden, wenn als Verschlusssache eingestufte Aufträge von ihm an industrielle oder andere Unternehmen vergeben werden. Er sorgt für die Einhaltung dieser Mindeststandards durch die jeweilige nationale Sicherheitsbehörde/beauftragte Sicherheitsbehörde.

(4) In einem Mitgliedstaat eingetragene Auftragnehmer und Unterauftragnehmer, die an als Verschlusssache eingestuften Aufträgen oder Unteraufträgen beteiligt sind und entweder bei der Ausführung dieser Aufträge oder bei den Verhandlungen vor der Auftragsvergabe als „CONFIDENTIEL UE/EU CONFIDENTIAL“ oder „SECRET UE/EU SECRET“ eingestufte Verschlusssachen in ihren Räumlichkeiten bearbeiten und aufbewahren müssen, müssen im Besitz eines von der nationalen Sicherheitsbehörde, der beauftragten Sicherheitsbehörde oder einer sonstigen zuständigen Sicherheitsbehörde des betreffenden Mitgliedstaats erteilten Sicherheitsbescheids für Unternehmen des entsprechenden Geheimhaltungsgrads sein.

(5) Das Personal des Auftragnehmers oder Unterauftragnehmers, das zur Ausführung eines als Verschlusssache eingestuften Auftrags Zugang zu Informationen des Geheimhaltungsgrads „CONFIDENTIEL UE/EU CONFIDENTIAL“ oder „SECRET UE/EU SECRET“ erhalten muss, muss im Besitz eines von der jeweiligen nationalen Sicherheitsbehörde, der beauftragten Sicherheitsbehörde oder einer sonstigen zuständigen Sicherheitsbehörde gemäß den innerstaatlichen Rechtsvorschriften und den Mindeststandards in Anhang A I ausgestellten PSC sein.

(6) Die Bestimmungen zur Anwendung dieses Artikels sind in Anhang A V enthalten.

Artikel 10

Austausch von Verschlusssachen mit Drittstaaten und internationalen Organisationen

(1) Der EAD kann EU-VS nur mit einem Drittstaat oder einer internationalen Organisation austauschen, wenn

a) ein im Einklang mit Artikel 37 EUV und Artikel 218 AEUV geschlossenes Geheimschutzabkommen zwischen der EU und diesem Drittstaat oder dieser internationalen Organisation oder

b) eine nach dem Verfahren des Artikels 15 Absatz 5 dieses Beschlusses geschlossene Verwaltungsvereinbarung zwischen dem Hohen Vertreter und den zuständigen Sicherheitsstellen dieses Drittstaats oder dieser internationalen Organisation über den Austausch von Verschlusssachen, die grundsätzlich nicht höher als „RESTREINT UE/EU RESTRICTED“ eingestuft sind, oder

c) ein im Kontext einer GSVP-Krisenbewältigungsoperation zwischen der EU und diesem Drittstaat nach Artikel 37 EUV und Artikel 218 AEUV geschlossenes Rahmen- oder Ad-hoc-Abkommen über eine Beteiligung

in Kraft ist und die darin festgelegten Bedingungen erfüllt sind.

Ausnahmen zu dieser allgemeinen Regel sind in Anhang A VI Abschnitt V enthalten.

(2) Verwaltungsvereinbarungen nach Absatz 1 Buchstabe b enthalten Bestimmungen, mit denen sichergestellt wird, dass EU-VS nach ihrer Entgegennahme durch Drittstaaten oder internationale Organisationen in einer ihrem Geheimhaltungsgrad angemessenen Weise nach Mindeststandards geschützt werden, die nicht weniger streng als die in diesem Beschluss festgelegten Standards sind.

Informationen, die auf der Grundlage der in Absatz 1 Buchstabe c genannten Abkommen ausgetauscht werden, beschränken sich auf Informationen, die GSVP-Operationen betreffen, an denen sich der jeweilige Drittstaat auf der Grundlage dieser Abkommen und nach Maßgabe ihrer Bestimmungen beteiligt.

(3) Wird zwischen der Union und einem beteiligten Drittstaat oder einer beteiligten internationalen Organisation anschließend ein Geheimschutzabkommen geschlossen, so tritt das Geheimschutzabkommen, soweit der Austausch und die Bearbeitung von EU-VS betroffen sind, an die Stelle der Bestimmungen über den Austausch von Verschlusssachen in dem Rahmen- oder Ad-hoc-Beteiligungsabkommen oder der Ad-hoc-Verwaltungsvereinbarung.

(4) Für die Zwecke einer GSVP-Operation erstellte EU-VS können gemäß den Absätzen 1 bis 3 und Anhang A VI dem von Drittstaaten oder internationalen Organisationen für diese Operation abgeordneten Personal offengelegt werden. Wird diesem Personal Zugang zu EU-VS in Räumlichkeiten und/oder Kommunikations- und Informationssystemen einer GSVP-Operation gewährt, so müssen Maßnahmen (einschließlich der Aufzeichnung der offengelegten EU-VS) getroffen werden, um das Risiko des Verlusts oder der Kenntnisnahme durch Unbefugte gering zu halten. Entsprechende Maßnahmen sind in den einschlägigen Planungs- oder Missionsunterlagen festzulegen.

(5) Es werden nach Artikel 17 dieses Beschlusses Bewertungsbesuche in Drittstaaten bzw. bei internationalen Organisationen durchgeführt, um die Wirksamkeit der zum Schutz von EU-VS getroffenen Sicherheitsvorkehrungen zu überprüfen.

(6) Der Beschluss, EU-VS des EAD an einen Drittstaat oder eine internationale Organisation weiterzugeben, wird von Fall zu Fall nach Maßgabe von Art und Inhalt dieser Verschlusssachen, des Grundsatzes „Kenntnis nur, wenn nötig“ und der Vorteile für die EU gefasst.

Der EAD holt die schriftliche Zustimmung etwaiger Stellen ein, die Verschlusssachen als Ausgangsmaterial für vom EAD stammende EU-VS bereitgestellt haben, um sicherzustellen, dass keine Einwände gegen die Weitergabe bestehen.

Stammt eine Verschlusssache, um deren Weitergabe ersucht wird, nicht vom EAD, so holt der EAD zunächst die schriftliche Zustimmung des Herausgebers zur Weitergabe der Verschlusssache ein.

Kann der EAD den Herausgeber nicht ermitteln, so trifft der EAD an dessen Stelle die Entscheidung, nachdem er die einhellig befürwortende Stellungnahme der im Sicherheitsausschuss des EAD vertretenen Mitgliedstaaten eingeholt hat.

(7) Die Bestimmungen zur Anwendung dieses Artikels sind in Anhang A VI enthalten.

Artikel 11

Verletzung der Sicherheit und Kenntnisnahme von Verschlusssachen durch Unbefugte

(1) Eine tatsächliche oder vermutete Verletzung der Sicherheit oder die tatsächliche oder vermutete Kenntnisnahme von Verschlusssachen durch Unbefugte wird unverzüglich der für Sicherheit zuständigen Direktion des EAD gemeldet, die gegebenenfalls die betroffenen Mitgliedstaaten oder sonstige betroffene Stellen informiert.

(2) Wird bekannt oder besteht berechtigter Grund zu der Annahme, dass Verschlusssachen Unbefugten zur Kenntnis gelangt oder verloren gegangen sind, informiert die für Sicherheit zuständige Direktion des EAD die nationalen Sicherheitsbehörden der betroffenen Mitgliedstaaten und ergreift alle geeigneten Maßnahmen gemäß den einschlägigen Rechtsvorschriften, um

a) Beweise zu sichern,

b) sicherzustellen, dass der Fall zur Aufklärung des Sachverhalts von Personal untersucht wird, das von der Verletzung oder der Kenntnisnahme durch Unbefugte nicht unmittelbar betroffen ist,

c) unverzüglich den Herausgeber oder sonstige betroffene Stellen zu verständigen,

d) zu vermeiden, dass sich ein solcher Vorfall wiederholt,

e) den potenziellen Schaden für die Interessen der EU oder der Mitgliedstaaten einzuschätzen und

f) die zuständigen Stellen über die Auswirkungen der tatsächlichen oder vermuteten Kenntnisnahme durch Unbefugte und die getroffenen Maßnahmen zu unterrichten.

(3) Gegen jedes Mitglied des Personals, das dem EAD untersteht und für eine Verletzung der Sicherheitsvorschriften dieses Beschlusses verantwortlich ist, können disziplinarische Maßnahmen gemäß den geltenden Vorschriften ergriffen werden.

Gegen jede Person, die für die unbefugte Kenntnisnahme oder den Verlust von Verschlusssachen verantwortlich ist, können disziplinarische Maßnahmen gemäß den geltenden Rechts- und sonstigen Vorschriften ergriffen werden.

(4) Während der Untersuchung einer Verletzung der Sicherheit und/oder einer unbefugten Kenntnisnahme von Verschlusssachen kann der Leiter der für Sicherheit zuständigen Direktion des EAD den Zugang der betreffenden Person zu EU-VS und zu den Räumlichkeiten des EAD aussetzen. Die Direktion Sicherheit der Generaldirektion Humanressourcen und Sicherheit der Kommission, das Sicherheitsbüro des Generalsekretariats des Rates, die nationalen Sicherheitsbehörden der betroffenen Mitgliedstaaten oder sonstige betroffene Stellen werden von einem solchen Beschluss unverzüglich informiert.

ANHANG A I

PERSONELLER GEHEIMSCHUTZ

I. EINLEITUNG

1. Dieser Anhang enthält Vorschriften zur Anwendung von Anhang A Artikel 5. Er legt insbesondere die Kriterien fest, anhand deren der EAD feststellt, ob eine Person unter Berücksichtigung ihrer Loyalität, Vertrauenswürdigkeit und Zuverlässigkeit zum Zugang zu EU-VS ermächtigt werden kann, sowie die hierzu anzuwendenden Überprüfungs- und Verwaltungsverfahren.

2. Die „Erklärung über die Sicherheitsüberprüfung von Personal" (Personnel Security Clearance — PSC) mit Blick auf den Zugang zu EU-VS ist eine Erklärung einer zuständigen Behörde eines Mitgliedstaats, die nach Abschluss einer Sicherheitsüberprüfung durch die zuständigen Behörden eines Mitgliedstaats ausgestellt wird und mit der bescheinigt wird, dass einer Person, die nachweislich Kenntnis von Verschlusssachen haben muss, bis zu einem bestimmten Datum und bis zu einem bestimmten Geheimhaltungsgrad („CONFIDENTIEL UE/EU CONFIDENTIAL" oder höher) Zugang zu EU-VS gewährt werden kann; diese Person wird als „sicherheitsüberprüft" bezeichnet.

3. Die „Sicherheitsüberprüfungsbescheinigung" (Personnel Security Clearance Certificate — PSCC) ist eine von der Sicherheitsbehörde des EAD ausgestellte Bescheinigung, in der festgestellt wird, dass eine Person sicherheitsüberprüft ist, und aus der der Geheimhaltungsgrad, bis zu dem der Person Zugang zu EU-VS gewährt werden kann, die Gültigkeitsdauer der betreffenden PSC und das Ablaufdatum der Bescheinigung selbst hervorgehen.

4. Die „Ermächtigung zum Zugang zu EU-VS" ist eine Ermächtigung der Sicherheitsbehörde des EAD, die gemäß diesem Beschluss nach Ausstellung einer PSC durch die zuständigen Behörden eines Mitgliedstaats erteilt wird und mit der bescheinigt wird, dass einer Person, die nachweislich Kenntnis von Verschlusssachen haben muss, bis zu einem bestimmten Datum und bis zu einem bestimmten Geheimhaltungsgrad („CONFIDENTIEL UE/EU CONFIDENTIAL" oder höher) Zugang zu EU-VS gewährt werden kann; diese Person wird als „sicherheitsüberprüft" bezeichnet.

II. ERMÄCHTIGUNG ZUM ZUGANG ZU EU-VS

5. Der Zugang zu Verschlusssachen, die als „RESTREINT UE/EU RESTRICTED" eingestuft sind, erfordert keine Sicherheitsüberprüfung und wird gestattet, nachdem

   a) festgestellt wurde, dass die betreffende Person in einem arbeitsrechtlichen oder vertraglichen Verhältnis zum EAD steht,

   b) festgestellt wurde, dass sie Kenntnis von Verschlusssachen haben muss,

   c) die Person über die Sicherheitsvorschriften und -verfahren für den Schutz von EU-VS belehrt wurde und ihre Verantwortlichkeiten hinsichtlich des Schutzes von EU-VS nach Maßgabe dieses Beschlusses schriftlich anerkannt hat.

6. Einer Person darf der Zugang zu als „CONFIDENTIEL UE/EU CONFIDENTIAL" oder höher eingestuften Verschlusssachen der EU erst dann gestattet werden, wenn

   a) festgestellt wurde, dass die betreffende Person in einem arbeitsrechtlichen oder vertraglichen Verhältnis zum EAD steht,

   b) festgestellt wurde, dass sie Kenntnis von Verschlusssachen haben muss,

   c) ihr eine PSC für den entsprechenden Geheimhaltungsgrad ausgestellt wurde oder sie auf andere Weise aufgrund ihrer Tätigkeit nach Maßgabe der innerstaatlichen Rechtsvorschriften ordnungsgemäß ermächtigt ist und

   d) sie über die Sicherheitsvorschriften und -verfahren für den Schutz von EU-VS belehrt wurde und ihre Verantwortlichkeiten hinsichtlich des Schutzes solcher Informationen schriftlich anerkannt hat.

7. Der EAD bestimmt innerhalb seiner Strukturen die Dienstposten, für die ein Zugang zu als „CONFIDENTIEL UE/EU CONFIDENTIAL" oder höher eingestuften Verschlusssachen und somit eine PSC für den entsprechenden Geheimhaltungsgrad gemäß Nummer 4 erforderlich ist.

8. Die Mitglieder des Personals des EAD geben eine Erklärung darüber ab, ob sie die Staatsangehörigkeit mehrerer Länder besitzen.

Verfahren des EAD zur Beantragung einer PSC

9. Für Mitglieder des Personals des EAD sendet die Sicherheitsbehörde des EAD den ausgefüllten Sicherheitsfragebogen an die nationale Sicherheitsbehörde des Mitgliedstaats, dessen Staatsangehörigkeit die betreffende Person besitzt, und beantragt die Durchführung einer Sicherheitsüberprüfung für den Geheimhaltungsgrad von EU-VS, zu denen die betreffende Person Zugang haben muss.

10. Besitzt eine Person die Staatsangehörigkeit mehrerer Länder, wird die Sicherheitsüberprüfung bei der nationalen Sicherheitsbehörde des Landes beantragt, unter dessen Staatsangehörigkeit die Person eingestellt wurde.

11. Werden dem EAD sicherheitserhebliche Informationen zu einer Person bekannt, die eine PSC beantragt hat, so teilt er dies der zuständigen nationalen Sicherheitsbehörde gemäß den einschlägigen Vorschriften mit.

12. Nach Abschluss der Sicherheitsüberprüfung teilt die betreffende nationale Sicherheitsbehörde der für Sicherheit zuständigen Direktion des EAD das Ergebnis der Überprüfung mit.

    a) Führt das Ergebnis der Sicherheitsüberprüfung zu der Feststellung, dass über die betreffende Person keine nachteiligen Erkenntnisse vorliegen, die ihre Loyalität, Vertrauenswürdigkeit und Zuverlässigkeit infrage stellen, kann die Sicherheitsbehörde des EAD der betreffenden Person eine bis zu einem bestimmten Datum gültige Ermächtigung zum Zugang zu EU-VS bis zu dem entsprechenden Geheimhaltungsgrad erteilen.

    b) Der EAD trifft sämtliche geeigneten Maßnahmen, um sicherzustellen, dass die von der nationalen Sicherheitsbehörde festgelegten Bedingungen oder Beschränkungen ordnungsgemäß angewendet werden. Die nationale Sicherheitsbehörde wird über das Ergebnis unterrichtet.

    c) Führt das Ergebnis der Sicherheitsüberprüfung nicht zu einer solchen Feststellung, so setzt die Sicherheitsbehörde des EAD die betreffende Person davon in Kenntnis, die beantragen kann, von der Sicherheitsbehörde des EAD gehört zu werden. Die Sicherheitsbehörde des EAD kann die zuständige nationale Sicherheitsbehörde um weitere Auskünfte ersuchen, die diese nach ihren innerstaatlichen Rechtsvorschriften geben darf. Wird das Ergebnis der Sicherheitsüberprüfung bestätigt, darf keine Ermächtigung zum Zugang zu EU-VS erteilt werden. In diesem Fall trifft der EAD sämtliche geeigneten Maßnahmen, um sicherzustellen, dass der Antragsteller keinen Zugang zu EU-VS erhält.

13. Für die Sicherheitsüberprüfung und deren Ergebnisse, auf die sich der EAD bei seiner Entscheidung über die Erteilung einer Ermächtigung zum Zugang zu EU-VS stützt, gelten die einschlägigen Rechtsvorschriften des betreffenden Mitgliedstaats, einschließlich der Rechtsvorschriften für etwaige Rechtsbehelfe. Gegen Entscheidungen der Sicherheitsbehörde des EAD können Rechtsbehelfe gemäß dem Statut eingelegt werden.

14. Die Feststellung, auf die sich eine PSC stützt, erstreckt sich — solange diese gültig ist — auf alle Aufgaben, die die betreffende Person im EAD, im Generalsekretariat des Rates oder in der Kommission übernimmt.

15. Der EAD erkennt die von anderen Organen, Einrichtungen oder Agenturen der Europäischen Union ausgestellten Ermächtigungen zum Zugang zu EU-VS an, solange diese gültig sind. Die Ermächtigungen erstrecken sich auf alle Aufgaben, die der betreffenden Person innerhalb des EAD zugewiesen werden. Das Organ, die Einrichtung oder die Agentur der Europäischen Union, bei dem bzw. bei der die betreffende Person ihre Beschäftigung aufnimmt, unterrichtet die zuständige nationale Sicherheitsbehörde über den Wechsel des Arbeitgebers.

16. Nimmt eine Person innerhalb von 12 Monaten nach Mitteilung des Ergebnisses der Sicherheitsüberprüfung an die Sicherheitsbehörde des EAD ihren Dienst nicht auf oder unterbricht sie diesen für einen Zeitraum von 12 oder mehr Monaten, in dem sie nicht beim EAD, bei einem anderen Organ, einer anderen Agentur oder Einrichtung der EU oder bei einer nationalen Verwaltung eines Mitgliedstaats auf einem Dienstposten tätig ist, der den Zugang zu Verschlusssachen erfordert, so wird die zuständige nationale Sicherheitsbehörde mit diesem Ergebnis befasst, damit sie gegebenenfalls bestätigen kann, dass es weiterhin gültig und berechtigt ist.

17. Werden dem EAD Informationen bekannt, nach denen eine Person, die eine gültige PSC besitzt, ein Sicherheitsrisiko darstellt, so teilt der EAD dies der zuständigen nationalen Sicherheitsbehörde gemäß den einschlägigen Vorschriften mit; er kann den Zugang zu EU-VS aussetzen oder die Ermächtigung zum Zugang zu EU-VS zurücknehmen. Teilt eine nationale Sicherheitsbehörde dem EAD mit, dass eine gemäß Nummer 12 Buchstabe a erfolgte Feststellung in Bezug auf eine Person, die im Besitz einer gültigen Ermächtigung zum Zugang zu EU-VS ist, zurückgenommen wurde, kann die Sicherheitsbehörde des EAD die nationale Sicherheitsbehörde um alle weiteren Auskünfte ersuchen, die diese nach ihren innerstaatlichen Rechtsvorschriften geben darf. Bei Bestätigung der nachteiligen Erkenntnisse wird die vorgenannte Ermächtigung zurückgenommen und die betreffende Person vom Zugang zu EU-VS und von Dienstposten, auf denen sie auf EU-VS zugreifen oder ein Sicherheitsrisiko darstellen könnte, ausgeschlossen.

18. Jede Entscheidung über die Rücknahme einer Ermächtigung zum Zugang zu EU-VS für ein Mitglied des Personals des EAD und gegebenenfalls die dafür maßgeblichen Gründe werden der betreffenden Person mitgeteilt, die beantragen kann, von der Sicherheitsbehörde des EAD gehört zu werden. Für die von einer nationalen Sicherheitsbehörde zur Verfügung gestellten Informationen gelten die einschlägigen Rechtsvorschriften des betreffenden Mitgliedstaats, einschließlich der Rechtsvorschriften über etwaige Rechtsbehelfe. Gegen Entscheidungen der Sicherheitsbehörde des EAD können Rechtsbehelfe gemäß dem Statut eingelegt werden.

19. Nationale Sachverständige, die zum EAD abgeordnet werden, um dort einen Dienstposten zu bekleiden, für den der Zugang zu als „CONFIDENTIEL UE/EU CONFIDENTIAL“ oder höher eingestuften Verschlusssachen erforderlich ist, müssen der Sicherheitsbehörde des EAD eine gültige PSC für den Zugang zu EU-VS für den entsprechenden Geheimhaltungsgrad vorlegen, bevor sie ihren Dienst antreten. Dieser Vorgang wird von dem abordnenden Mitgliedstaat abgewickelt.

Verzeichnisse der PSC

20. Der EAD unterhält eine Datenbank, in der der Sicherheitsstatus des gesamten dem EAD unterstehenden Personals und des Personals der Auftragnehmer des EAD erfasst ist. Diese Verzeichnisse enthalten Angaben zum Geheimhaltungsgrad („CONFIDENTIEL UE/EU CONFIDENTIAL“ oder höher) der EU-VS, zu denen der betreffenden Person Zugang gewährt werden darf, das Datum, an dem die PSC ausgestellt wurde, und deren Gültigkeitsdauer.

21. Es werden geeignete Verfahren für die Koordinierung mit den Mitgliedstaaten und anderen Organen, Agenturen und Einrichtungen der EU eingeführt, um sicherzustellen, dass der EAD ein genaues und umfassendes Verzeichnis des Sicherheitsstatus des gesamten dem EAD unterstehenden Personals und des Personals der Auftragnehmer des EAD führt.

22. Die Sicherheitsbehörde des EAD kann eine Sicherheitsüberprüfungsbescheinigung (PSCC) ausstellen, die Angaben zum Geheimhaltungsgrad („CONFIDENTIEL UE/EU CONFIDENTIAL“ oder höher) der EU-VS, zu denen der Person Zugang gewährt werden darf, zur Gültigkeitsdauer der betreffenden PSC bzw. Ermächtigung und zum Ablaufdatum der Bescheinigung selbst enthält.

Ausnahmen vom Erfordernis einer PSC

23. Personen, die aufgrund ihrer Aufgaben nach den innerstaatlichen Rechtsvorschriften zum Zugang zu EU-VS ordnungsgemäß ermächtigt worden sind, werden von der für Sicherheit zuständigen Direktion des EAD entsprechend über ihre Sicherheitspflichten im Hinblick auf den Schutz von EU-VS belehrt.

III. SCHULUNG UND SENSIBILISIERUNG IN SICHERHEITSFRAGEN

24. Vor der Ermächtigung zum Zugang zu EU-VS bestätigen alle betreffenden Personen schriftlich, dass sie sich ihrer Pflichten in Bezug auf den Schutz von EU-VS und der Folgen einer Kenntnisnahme von EU-VS durch Unbefugte bewusst sind. Der EAD verwahrt die Aufzeichnungen über derartige schriftliche Bestätigungen.

25. Alle Personen, die zum Zugang zu EU-VS ermächtigt sind oder EU-VS bearbeiten müssen, werden in einer ersten Phase für Bedrohungen der Sicherheit sensibilisiert und später in regelmäßigen Abständen darüber belehrt; sie müssen alle von ihnen als verdächtig oder ungewöhnlich erachteten Anbahnungsversuche oder sonstigen Tätigkeiten unverzüglich den zuständigen Sicherheitsbehörden melden.

26. Sämtliche Personen, denen der Zugang zu EU-VS gestattet wird, sind während des Zeitraums, in dem sie EU-VS bearbeiten, laufenden Maßnahmen des personellen Geheimschutzes zu unterziehen (d. h. laufende Betreuung). Für den laufenden personellen Geheimschutz verantwortlich sind

a) Personen, denen der Zugang zu EU-VS gestattet ist: Diese Personen sind persönlich für ihr eigenes Sicherheitsverhalten verantwortlich und müssen den zuständigen Sicherheitsbehörden alle von ihnen als verdächtig oder ungewöhnlich erachteten Anbahnungsversuche oder sonstigen Tätigkeiten sowie jegliche Änderung ihrer persönlichen Verhältnisse, die sich auf ihre PSC oder ihre Ermächtigung zum Zugang zu EU-VS auswirken könnte, unverzüglich melden.

b) Führungskräfte: Sie sind dafür verantwortlich, zu gewährleisten, dass ihr Personal die Sicherheitsmaßnahmen und die Verantwortlichkeiten für den Schutz von EU-VS kennt, das Sicherheitsverhalten ihres Personals zu überwachen und problematische Sicherheitsfragen selbst zu klären und die zuständigen Sicherheitsbehörden über etwaige nachteilige Erkenntnisse zu unterrichten, die sich auf die PSC ihres Personals oder dessen Ermächtigung zum Zugang zu EU-VS auswirken könnten.

c) Sicherheitsakteure im Rahmen der Organisation der Sicherheit im EAD im Sinne von Artikel 12 dieses Beschlusses: Sie sind verantwortlich für die Durchführung von Sicherheitsbelehrungen, um zu gewährleisten, dass das Personal in ihrem Bereich regelmäßig entsprechend unterwiesen wird, für die Förderung einer gefestigten Sicherheitskultur in ihrem Zuständigkeitsbereich, für die Einführung von Maßnahmen zur Überwachung des Sicherheitsverhaltens des Personals und für die Unterrichtung der zuständigen Sicherheitsbehörden über etwaige nachteilige Erkenntnisse, die sich auf die PSC einer Person auswirken könnten.

d) EAD und Mitgliedstaaten: Sie sorgen für die Schaffung der notwendigen Kanäle für die Weiterleitung von Informationen, die sich auf die PSC einer Person oder ihre Ermächtigung zum Zugang zu EU-VS auswirken können.

27. Alle Personen, die nicht mehr mit Aufgaben betraut sind, die einen Zugang zu EU-VS erfordern, werden über ihre Pflichten in Bezug auf den fortgesetzten Schutz von EU-VS belehrt und haben diese gegebenenfalls schriftlich zu bestätigen.

IV. AUßERGEWÖHNLICHE UMSTÄNDE

28. Aus Gründen der Dringlichkeit kann die Sicherheitsbehörde des EAD in Erwartung des Abschlusses einer umfassenden Sicherheitsüberprüfung nach Konsultation der nationalen Sicherheitsbehörde des Mitgliedstaats, dessen Staatsangehörigkeit die betreffende Person besitzt, und vorbehaltlich der Ergebnisse einer ersten Prüfung, mit der festgestellt werden soll, ob keine nachteiligen Erkenntnisse vorliegen, Beamten und sonstigen Bediensteten des EAD eine vorläufige Ermächtigung zum Zugang zu EU-VS für eine bestimmte Tätigkeit erteilen, wenn dies im dienstlichen Interesse gerechtfertigt ist. Eine umfassende Sicherheitsüberprüfung sollte so bald wie möglich durchgeführt werden. Solche vorläufigen Ermächtigungen gelten für höchstens sechs Monate und berechtigen nicht zum Zugang zu Verschlusssachen, die als „TRÈS SECRET UE/EU TOP SECRET“ eingestuft sind. Alle Personen, denen eine vorläufige Ermächtigung erteilt wurde, bestätigen schriftlich, dass sie sich ihrer Pflichten in Bezug auf den Schutz von EU-VS und der Folgen einer Kenntnisnahme von EU-VS durch Unbefugte bewusst sind. Der EAD verwahrt die Aufzeichnungen über derartige schriftliche Bestätigungen.

29. Wird einer Person eine Tätigkeit zugewiesen, die eine PSC für Verschlusssachen erfordert, die einen eine Stufe höheren Geheimhaltungsgrad als denjenigen aufweisen, für den der Person die PSC ausgestellt wurde, so kann die Zuweisung dieser Tätigkeit vorläufig erfolgen, sofern

a) der Vorgesetzte der Person schriftlich begründet, dass der Zugang zu EU-VS eines höheren Geheimhaltungsgrads zwingend erforderlich ist,

b) der Zugang auf bestimmte EU-VS beschränkt ist, die für die zugewiesene Aufgabe erforderlich sind,

c) die betreffende Person im Besitz einer gültigen PSC ist,

d) Schritte eingeleitet wurden, um die Zugangsermächtigung für den für die Tätigkeit erforderlichen Geheimhaltungsgrad zu erwirken,

e) von der zuständigen Behörde hinreichend überprüft worden ist, ob die betreffende Person nicht in gravierender Weise oder wiederholt gegen die Sicherheitsvorschriften verstoßen hat,

f) die zuständige Stelle des EAD der Zuweisung zustimmt,

g) die zuständige nationale Sicherheitsbehörde/beauftragte Sicherheitsbehörde, die die PSC ausgestellt hat, konsultiert wurde und keine Einwände erhoben hat und

h) in der zuständigen Registratur oder untergeordneten Registratur eine Aufzeichnung der Ausnahmegenehmigung, einschließlich einer Beschreibung der Verschlusssache, zu der der Zugang genehmigt wurde, aufbewahrt wird.

30. Das vorstehend beschriebene Verfahren gilt für den einmaligen Zugang zu EU-VS, die einen eine Stufe höheren Geheimhaltungsgrad aufweisen als derjenige, für den die betreffende Person sicherheitsüberprüft wurde. Auf dieses Verfahren darf nicht regelmäßig zurückgegriffen werden.

31. In besonderen Ausnahmefällen, wie bei Missionen in feindlicher Umgebung oder in Zeiten zunehmender internationaler Spannungen, wenn Sofortmaßnahmen ergriffen werden müssen, insbesondere zur Rettung von Menschenleben, können der Hohe Vertreter, die Sicherheitsbehörde des EAD oder die Generaldirektion Haushalt und Verwaltung Personen, die nicht über die erforderliche PSC verfügen, nach Möglichkeit schriftlich Zugang zu als „CONFIDENTIEL UE/EU CONFIDENTIAL“ oder „SECRET UE/EU SECRET“ eingestuften Verschlusssachen gewähren, sofern eine derartige Erlaubnis absolut notwendig ist. Von dieser Erlaubnis wird eine Aufzeichnung aufbewahrt, in der die Verschlusssachen beschrieben werden, zu denen der Zugang genehmigt wurde.

32. Im Falle von Verschlusssachen, die als „TRÈS SECRET UE/EU TOP SECRET“ eingestuft sind, wird diese Art des Zugangs in Ausnahmefällen auf Staatsangehörige der EU-Mitgliedstaaten beschränkt, die zum Zugang entweder zu nationalen Verschlusssachen, die dem Geheimhaltungsgrad „TRÈS SECRET UE/EU TOP SECRET“ entsprechen, oder zu Verschlusssachen des Geheimhaltungsgrads „SECRET UE/EU SECRET“ ermächtigt wurden.

33. Der Sicherheitsausschuss des EAD wird über die Fälle unterrichtet, in denen auf das Verfahren nach den Nummern 31 und 32 zurückgegriffen wird.

34. Der Sicherheitsausschuss des EAD erhält einen jährlichen Bericht über die Inanspruchnahme der in diesem Abschnitt beschriebenen Verfahren.

V. TEILNAHME AN SITZUNGEN IN DER ZENTRALE DES EAD UND DEN DELEGATIONEN DER UNION

35. Personen, die an Sitzungen in der Zentrale des EAD und den Delegationen der Union teilnehmen sollen, in deren Rahmen als „CONFIDENTIEL UE/EU CONFIDENTIAL“ oder höher eingestufte Verschlusssachen erörtert werden, darf die Teilnahme nur dann gestattet werden, wenn bestätigt wurde, dass sie angemessen sicherheitsüberprüft sind. Im Falle von Vertretern der Mitgliedstaaten, Beamten des Generalsekretariats des Rates und der Kommission wird eine Sicherheitsüberprüfungsbescheinigung oder ein anderer Nachweis einer PSC der für Sicherheit zuständigen Direktion des EAD bzw. dem Sicherheitskoordinator der Delegation der Union von den zuständigen Behörden übermittelt oder ausnahmsweise von der betreffenden Person vorgelegt. Gegebenenfalls kann eine konsolidierte Namensliste verwendet werden, die den einschlägigen Nachweis der PSC enthält.

36. Wird einer Person, deren Aufgaben die Teilnahme an Sitzungen in der Zentrale des EAD oder Delegationen der Union erfordern, in deren Rahmen als „CONFIDENTIEL UE/EU CONFIDENTIAL“ und höher eingestufte Verschlusssachen erörtert werden, die PSC für den Zugang zu EU-VS entzogen, so setzt die zuständige Behörde den EAD davon in Kenntnis.

VI. MÖGLICHER ZUGANG ZU EU-VS

37. Werden Personen unter Umständen beschäftigt, unter denen sie möglicherweise Zugang zu Verschlusssachen des Geheimhaltungsgrads „CONFIDENTIEL UE/EU CONFIDENTIAL“ oder höher haben könnten, müssen sie angemessen sicherheitsüberprüft sein oder jederzeit begleitet werden.

38. Boten, Sicherheitsbedienstete und Begleitpersonen müssen für den entsprechenden Geheimhaltungsgrad sicherheitsüberprüft oder auf andere Weise gemäß den innerstaatlichen Rechtsvorschriften angemessen überprüft sein und regelmäßig über die Sicherheitsverfahren zum Schutz von EU-VS sowie über ihre Pflichten zum Schutz der ihnen anvertrauten oder ihnen unbeabsichtigt zugänglich gewordenen Verschlusssachen belehrt werden.

ANHANG A II

MATERIELLER GEHEIMSCHUTZ FÜR EU-VERSCHLUSSSACHEN

I. EINLEITUNG

1. Dieser Anhang enthält die Bestimmungen zur Anwendung von Anhang A Artikel 6. Er legt Mindestanforderungen an den materiellen Schutz von Gebäuden, Büros, Räumen und sonstigen Bereichen fest, in denen EU-VS bearbeitet und aufbewahrt werden, einschließlich Bereichen, in denen Kommunikations- und Informationssysteme untergebracht sind.

2. Die Maßnahmen des materiellen Geheimschutzes zielen darauf ab, den unbefugten Zugang zu EU-VS zu verhindern, indem

   a) gewährleistet wird, dass EU-VS auf geeignete Weise bearbeitet und aufbewahrt werden,

   b) die Einteilung des Personals in Bezug auf den Zugang zu EU-VS nach dem Grundsatz „Kenntnis nur, wenn nötig" und gegebenenfalls anhand der Sicherheitsermächtigung der betreffenden Bediensteten ermöglicht wird,

   c) von unbefugten Handlungen abgeschreckt wird bzw. diese verhindert und aufgedeckt werden und

   d) das heimliche oder gewaltsame Eindringen unbefugter Personen von außen verhindert oder aufgehalten wird.

II ANFORDERUNGEN UND MAßNAHMEN BEZÜGLICH DES MATERIELLEN GEHEIMSCHUTZES

3. Der EAD wendet einen Risikomanagementprozess zum Schutz von EU-VS in den betreffenden Räumlichkeiten, um dafür zu sorgen, dass der Umfang des materiellen Schutzes dem festgestellten Risiko entspricht. Der Risikomanagementprozess trägt allen relevanten Faktoren Rechnung, insbesondere:

   a) dem Geheimhaltungsgrad der EU-VS;

   b) der Form und dem Umfang der EU-VS, wobei zu berücksichtigen ist, dass bei großen Mengen oder einer Zusammenstellung von EU-VS unter Umständen strengere Schutzmaßnahmen zu ergreifen sind;

   c) der Umgebung und der Struktur der Gebäude oder Bereiche, in denen EU-VS verwahrt werden;

   d) der vom INTCEN insbesondere anhand der Berichte der EU-Delegationen vorgenommenen Einschätzung der in Drittländern vorhandenen Bedrohungen;

   e) der Einschätzung der nachrichtendienstlichen Bedrohung, die gegen die EU oder die Mitgliedstaaten gerichtet ist, sowie der Bedrohung durch Sabotage, Terrorismus und andere subversive oder kriminelle Handlungen.

4. Die Sicherheitsbehörde des EAD legt unter Anwendung des Konzepts der mehrschichtigen Sicherheit eine angemessene Kombination erforderlicher Maßnahmen des materiellen Geheimschutzes fest. Dies kann eine oder mehrere der folgenden Maßnahmen umfassen:

   a) Absperrung: ein physisches Hindernis, dass einen zu schützenden Bereich abgrenzt;

   b) Einbruchsmeldeanlagen: Eine Einbruchsmeldeanlage kann zur Erhöhung des durch eine Zutrittssperre gewährten Sicherheitsniveaus oder in Räumen und Gebäuden anstelle von Sicherheitspersonal oder zu dessen Unterstützung verwendet werden;

   c) Zugangskontrolle: Die Zugangskontrollen können einen Standort, ein oder mehrere Gebäude an einem Standort oder Bereiche oder Räumlichkeiten innerhalb eines Gebäudes betreffen. Die Kontrollen können elektronisch oder elektromechanisch, durch Sicherheits- und/oder Empfangspersonal oder im Wege anderer physischer Maßnahmen erfolgen;

   d) Sicherheitspersonal: Unter anderem zur Abschreckung von Personen, die ein unbemerktes Eindringen planen, kann Sicherheitspersonal beschäftigt werden, das ausgebildet und überwacht und erforderlichenfalls angemessen sicherheitsüberprüft sein muss;

   e) Videoüberwachung: Videoüberwachungssysteme können vom Sicherheitspersonal zur Überprüfung von Vorfällen und bei Alarmierung durch die Einbruchsmeldeanlagen an größeren Standorten oder an den äußeren Abgrenzungen genutzt werden;

f) Sicherheitsbeleuchtung: Sicherheitsbeleuchtungen können eingesetzt werden, um potenzielle Eindringlinge abzuschrecken und für die Beleuchtung zu sorgen, die für eine wirksame Überwachung entweder unmittelbar durch das Sicherheitspersonal oder mittelbar durch ein Videoüberwachungssystem erforderlich ist;

g) alle sonstigen geeigneten physischen Maßnahmen zur Abschreckung oder Aufdeckung unbefugter Zugangsversuche oder zur Verhinderung von Verlust und Beschädigung von EU-VS.

5. Die für Sicherheit zuständige Direktion des EAD kann Durchsuchungen an den Ein- und Ausgängen vornehmen, um damit vom unbefugten Verbringen von Material in Räumlichkeiten oder Gebäude oder von der unbefugten Mitnahme von EU-VS aus Räumlichkeiten oder Gebäuden abzuschrecken.

6. Besteht die Gefahr einer — auch versehentlichen — unzulässigen Einsicht in EU-VS, so werden geeignete Maßnahmen ergriffen, um dieser Gefahr entgegenzuwirken.

7. Bei neuen Anlagen müssen die Anforderungen hinsichtlich des materiellen Geheimschutzes und deren funktionale Spezifikationen bei der Planung und Konzeption der Anlagen festgelegt werden. Bei bestehenden Anlagen müssen die Anforderungen hinsichtlich des materiellen Geheimschutzes möglichst weitgehend umgesetzt werden.

III. AUSRÜSTUNG FÜR DEN MATERIELLEN SCHUTZ VON EU-VS

8. Bei der Beschaffung von Ausrüstung (wie Sicherheitsbehältnissen, Aktenvernichtern, Türschlössern, elektronischen Zugangskontrollsystemen, Einbruchsmeldeanlagen, Alarmsystemen) für den materiellen Schutz von EU-VS stellt die Sicherheitsbehörde des EAD sicher, dass die Ausrüstung den genehmigten technischen Standards und Mindestanforderungen entspricht.

9. Die technischen Spezifikationen der Ausrüstung, die zum materiellen Schutz von EU-VS eingesetzt werden soll, werden in Sicherheitsleitlinien festgehalten, die vom Sicherheitsausschuss des EAD gebilligt werden.

10. Die Sicherheitssysteme müssen in regelmäßigen Abständen inspiziert werden; die Ausrüstung muss regelmäßig gewartet werden. Bei den Wartungsarbeiten ist dem Ergebnis der Inspizierungen Rechnung zu tragen, damit ein optimales Funktionieren der betreffenden Ausrüstung weiterhin gewährleistet ist.

11. Die Wirksamkeit der einzelnen Sicherheitsmaßnahmen und des gesamten Sicherheitssystems ist bei jeder Inspektion zu überprüfen.

IV. DURCH MAßNAHMEN DES MATERIELLEN GEHEIMSCHUTZES GESCHÜTZTE BEREICHE

12. Zum materiellen Schutz von EU-VS werden zwei Arten von durch Maßnahmen des materiellen Geheimschutzes geschützten Bereichen bzw. entsprechenden Bereichen auf nationaler Ebene eingerichtet:

a) Verwaltungsbereiche und

b) abgesicherte Bereiche (einschließlich technisch abgesicherter Bereiche).

13. Die Sicherheitsbehörde des EAD legt fest, ob ein bestimmter Bereich die Anforderungen für eine Ausweisung als Verwaltungsbereich, als abgesicherter Bereich oder als technisch abgesicherter Bereich erfüllt.

14. Für Verwaltungsbereiche gilt Folgendes:

a) Es wird eine sichtbare äußere Abgrenzung eingerichtet, die die Kontrolle von Personen und gegebenenfalls von Fahrzeugen ermöglicht;

b) nur Personen, die von der für Sicherheit zuständigen Direktion des EAD ordnungsgemäß ermächtigt wurden, dürfen diesen Bereich unbegleitet betreten;

c) bei allen anderen Personen ist eine ständige Begleitung oder eine gleichwertige Kontrolle sicherzustellen.

15. Für abgesicherte Bereiche gilt Folgendes:

a) Es wird eine sichtbare und geschützte äußere Abgrenzung mit vollständiger Eingangs- und Ausgangskontrolle eingerichtet, die mittels eines Berechtigungsausweises oder eines Systems zur persönlichen Identifizierung erfolgt;

b) nur Personen, die für den entsprechenden Geheimhaltungsgrad sicherheitsüberprüft sind und aufgrund der Tatsache, dass sie Kenntnis von den Verschlusssachen haben müssen, speziell zum Zutritt ermächtigt wurden, dürfen diesen Bereich unbegleitet betreten;

c) bei allen anderen Personen ist eine ständige Begleitung oder eine gleichwertige Kontrolle sicherzustellen.

16. Wenn das Betreten eines abgesicherten Bereichs de facto den unmittelbaren Zugang zu den darin enthaltenen Verschlusssachen ermöglicht, sind außerdem folgende Anforderungen zu erfüllen:

a) Der höchste Geheimhaltungsgrad der Verschlusssachen, die in der Regel in dem Bereich verwahrt werden, ist eindeutig anzugeben;

b) alle Besucher benötigen eine spezielle Ermächtigung, um den Bereich betreten zu dürfen, müssen jederzeit begleitet werden und müssen entsprechend sicherheitsüberprüft sein, es sei denn, es werden Maßnahmen getroffen, um sicherzustellen, dass kein Zugang zu EU-VS möglich ist;

c) elektronische Geräte müssen außerhalb des Bereichs verbleiben.

17. Abgesicherte Bereiche mit Abhörschutz sind als technisch abgesicherte Bereiche auszuweisen. Es gelten die folgenden zusätzlichen Anforderungen:

a) Diese Bereiche werden mit Einbruchsmeldeanlagen ausgerüstet und sind dann, wenn sie nicht besetzt sind, verschlossen zu halten, und dann, wenn sie besetzt sind, zu bewachen. Die Kontrolle der Schlüssel erfolgt nach Maßgabe des Abschnitts VI dieses Anhangs;

b) alle Personen, die diese Bereiche betreten, und alle Materialien, die dorthin verbracht werden, sind zu kontrollieren;

c) diese Bereiche sind gemäß den Vorschriften der Sicherheitsbehörde des EAD regelmäßig zu inspizieren und/oder technisch zu überprüfen. Diese Inspektionen bzw. Überprüfungen sind auch dann vorzunehmen, wenn die Bereiche nachweislich oder vermutlich unbefugt betreten wurden;

d) in diesen Bereichen sind nicht zugelassene Kommunikationsverbindungen, nicht zugelassene Telefone und andere nicht zugelassene Kommunikationsgeräte sowie nicht zugelassene elektrische oder elektronische Ausrüstung verboten.

18. Ungeachtet der Nummer 17 Buchstabe d müssen alle Kommunikationsgeräte und elektrischen oder elektronischen Geräte vor ihrer Nutzung in Bereichen, in denen Sitzungen oder Arbeiten im Zusammenhang mit Verschlusssachen des Geheimhaltungsgrads „SECRET UE/EU SECRET“ und höher stattfinden, sowie in Fällen, in denen die Gefährdung von EU-VS als hoch eingeschätzt wird, vorab von der Sicherheitsbehörde des EAD untersucht werden, um sicherzustellen, dass mit diesen Geräten keine verständlichen Informationen auf unbeabsichtigte oder unzulässige Weise aus dem betreffenden abgesicherten Bereich nach außen übermittelt werden können.

19. Abgesicherte Bereiche, die nicht rund um die Uhr von Dienst tuendem Personal besetzt sind, sind gegebenenfalls unmittelbar nach den üblichen Arbeitszeiten und in unregelmäßigen Abständen außerhalb der üblichen Arbeitszeiten zu inspizieren, es sei denn, es wird eine Einbruchsmeldeanlage verwendet.

20. Innerhalb eines Verwaltungsbereichs können zeitweilig abgesicherte Bereiche oder technisch abgesicherte Bereiche im Hinblick auf eine geheimhaltungsbedürftige Sitzung oder einen anderen ähnlichen Zweck eingerichtet werden.

21. Für jeden abgesicherten Bereich werden sicherheitsbezogene Betriebsverfahren aufgestellt, die Folgendes regeln:

a) den Geheimhaltungsgrad der EU-VS, die in diesem Bereich bearbeitet oder aufbewahrt werden dürfen;

b) die einzuhaltenden Überwachungs- und Schutzmaßnahmen;

c) welchen Personen aufgrund der Tatsache, dass sie Kenntnis von Verschlusssachen haben müssen und sicherheitsüberprüft sind, unbegleiteter Zugang zu diesem Bereich gewährt werden kann;

d) wie gegebenenfalls in Bezug auf die Begleitung anderer Personen, denen Zugang zu diesem Bereich gewährt wird, beziehungsweise in Bezug auf den Schutz von EU-VS in einem solchen Fall zu verfahren ist;

e) sonstige einschlägige Maßnahmen und Verfahren.

22. In abgesicherten Bereichen werden Tresorräume eingebaut. Wände, Böden, Decken, Fenster und verschließbare Türen müssen von der Sicherheitsbehörde des EAD zugelassen werden und einen Schutz bieten, der dem eines Sicherheitsbehältnisses entspricht, das für die Aufbewahrung von EU-VS desselben Geheimhaltungsgrads zugelassen ist.

V. PHYSISCHE SCHUTZMAßNAHMEN FÜR DIE BEARBEITUNG UND AUFBEWAHRUNG VON EU-VS

23. EU-VS des Geheimhaltungsgrads „RESTREINT UE/EU RESTRICTED“ dürfen in folgenden Bereichen bearbeitet werden:

    a) in einem abgesicherten Bereich;

    b) in einem Verwaltungsbereich, sofern die EU-VS vor dem Zugang unbefugter Personen geschützt werden; oder

    c) außerhalb eines abgesicherten Bereichs oder eines Verwaltungsbereichs, sofern der Besitzer die EU-VS gemäß Anhang A III Nummern 30 bis 42 befördert und sich verpflichtet hat, besondere Maßnahmen einzuhalten, die in den Sicherheitsanweisungen der Sicherheitsbehörde des EAD niedergelegt sind, um sicherzustellen, dass die EU-VS vor dem Zugang durch unbefugte Personen geschützt sind.

24. EU-VS des Geheimhaltungsgrads „RESTREINT UE/EU RESTRICTED“ sind in geeigneten, verschließbaren Büromöbeln in einem Verwaltungsbereich oder einem abgesicherten Bereich aufzubewahren. Sie können zeitweilig außerhalb eines abgesicherten Bereichs oder eines Verwaltungsbereichs aufbewahrt werden, sofern der Besitzer sich verpflichtet hat, besondere Maßnahmen einzuhalten, die in den Sicherheitsanweisungen der Sicherheitsbehörde des EAD niedergelegt sind.

25. EU-VS der Geheimhaltungsgrade „CONFIDENTIEL UE/EU CONFIDENTIAL“ oder „SECRET UE/EU SECRET“ dürfen in folgenden Bereichen bearbeitet werden:

    a) in einem abgesicherten Bereich;

    b) in einem Verwaltungsbereich, sofern die EU-VS vor dem Zugang Unbefugter geschützt werden; oder

    c) außerhalb eines abgesicherten Bereichs oder eines Verwaltungsbereichs, sofern der Besitzer

        i) die EU-VS gemäß Anhang A III Nummern 30 bis 42 befördert;

        ii) sich verpflichtet hat, besondere Maßnahmen einzuhalten, die in den Sicherheitsanweisungen der Sicherheitsbehörde des EAD niedergelegt sind, um sicherzustellen, dass die EU-VS vor dem Zugang unbefugter Personen geschützt sind;

        iii) die EU-VS jederzeit unter seiner persönlichen Kontrolle hält;

        iv) im Falle von Dokumenten in Papierform die einschlägige Registratur davon in Kenntnis gesetzt hat.

26. EU-VS der Geheimhaltungsgrade „CONFIDENTIEL UE/EU CONFIDENTIAL“ und „SECRET UE/EU SECRET“ werden in einem abgesicherten Bereich in einem Sicherheitsbehältnis oder in einem Tresorraum aufbewahrt.

27. EU-VS des Geheimhaltungsgrads „TRES SECRET UE/EU TOP SECRET“ werden in einem abgesicherten Bereich bearbeitet.

28. EU-VS des Geheimhaltungsgrads „TRES SECRET UE/EU TOP SECRET“ sind in der Zentrale des EAD in einem abgesicherten Bereich unter einer der folgenden Bedingungen aufzubewahren:

    a) in einem Sicherheitsbehältnis entsprechend Nummer 8 mit einer oder mehreren der folgenden zusätzlichen Kontrollen:

        i) ständige Bewachung oder Kontrolle durch überprüftes Sicherheitspersonal oder Dienst tuendes Personal;

        ii) zugelassenes Einbruchmeldesystem in Verbindung mit Bereitschaftspersonal im Sicherheitsdienst;

        oder

    b) in einem mit einem Einbruchmeldesystem ausgestatteten Tresorraum in Verbindung mit Bereitschaftspersonal im Sicherheitsdienst.

29. Die Vorschriften über die Beförderung von EU-VS außerhalb von materiell geschützten Bereichen sind in Anhang A III enthalten.

VI. KONTROLLE DER SCHLÜSSEL UND KOMBINATIONEN ZUM SCHUTZ VON EU-VS

30. Die Sicherheitsbehörde des EAD legt Verfahren für die Verwaltung der Schlüssel und Kombinationen für Büros, Räume, Tresorräume und Sicherheitsbehältnisse fest. Diese Verfahren müssen Schutz vor unbefugtem Zugang gewähren.

31. Der Kreis der Personen, denen die Kombinationen zur Kenntnis gegeben werden, ist so weit wie möglich zu begrenzen. Die Kombinationen für Sicherheitsbehältnisse und Tresorräume, in denen EU-VS aufbewahrt werden, werden geändert

    a) bei Entgegennahme eines neuen Behälters,

    b) bei Wechsel des Personals, das die Kombination kennt,

    c) bei tatsächlicher oder vermuteter Kenntnisnahme durch Unbefugte,

    d) bei Wartung oder Reparatur eines Schlosses und

    e) mindestens alle 12 Monate.

ANHANG A III

VERWALTUNG VON VERSCHLUSSSACHEN

I. EINLEITUNG

1. Dieser Anhang enthält die Bestimmungen zur Anwendung von Anhang A Artikel 7.Darin werden die Verwaltungsmaßnahmen zur Überwachung von EU-VS während der gesamten Dauer ihrer Einstufung als EU-VS mit dem Ziel festgelegt, die beabsichtigte oder unbeabsichtigte Kenntnisnahme dieser Verschlusssachen durch Unbefugte bzw. den Verlust dieser Verschlusssachen zu verhindern oder aufzudecken oder Maßnahmen zur Wiederherstellung der Sicherheit zu treffen.

II. REGELN FÜR DIE EINSTUFUNG ALS VERSCHLUSSSACHE

Geheimhaltungsgrade und Kennzeichnungen

2. Informationen werden als Verschlusssache eingestuft, wenn sie hinsichtlich ihrer Vertraulichkeit zu schützen sind.

3. Der Herausgeber einer EU-VS ist dafür zuständig, nach Maßgabe der einschlägigen Einstufungsleitlinien den Geheimhaltungsgrad und den Empfängerkreis der Informationen zu bestimmen.

4. Der Geheimhaltungsgrad einer EU-VS ist nach Anhang A Artikel 2 Absatz 2 und unter Bezugnahme auf die gemäß Anhang A Artikel 3 Absatz 3 zu billigenden Sicherheitsleitlinien festzulegen.

5. Für Verschlusssachen der Mitgliedstaaten, die mit dem EAD ausgetauscht werden, wird dasselbe Schutzniveau gewährt wie für EU-VS des entsprechenden Geheimhaltungsgrads. Eine Entsprechungstabelle findet sich in Anlage B dieses Beschlusses.

6. Der Geheimhaltungsgrad und gegebenenfalls das Datum oder das spezielle Ereignis, nach dem der Geheimhaltungsgrad herabgestuft oder aufgehoben werden kann, sind eindeutig und richtig anzugeben, unabhängig davon, ob die EU-VS in Papierformat oder in mündlicher, elektronischer oder anderer Form vorliegt.

7. Einzelne Teile eines bestimmten Dokuments (d. h. Seiten, Absätze, Abschnitte, Anhänge oder sonstige Anlagen) können eine unterschiedliche Einstufung erforderlich machen und sind entsprechend zu kennzeichnen, auch bei Aufbewahrung in elektronischer Form.

8. Dokumente, die Teile mit unterschiedlichen Geheimhaltungsgraden umfassen, sollten möglichst so untergliedert werden, dass Teile mit verschiedenen Geheimhaltungsgraden leicht zu erkennen sind und gegebenenfalls abgetrennt werden können.

9. Der Geheimhaltungsgrad des Gesamtdokuments oder der Datei entspricht mindestens dem Geheimhaltungsgrad seines/ihres am höchsten eingestuften Teils. Werden Informationen aus verschiedenen Quellen zusammengestellt, so wird die endgültige Fassung durchgesehen, um den grundsätzlichen Geheimhaltungsgrad zu bestimmen, da sie einen höheren Geheimhaltungsgrad als für die einzelnen Bestandteile nötig erfordern kann.

10. Ein Begleitschreiben oder ein Übermittlungsvermerk samt Anlagen ist so hoch einzustufen wie die am höchsten eingestufte Anlage. Der Herausgeber muss anhand einer entsprechenden Kennzeichnung klar angeben, welcher Geheimhaltungsgrad für das Begleitschreiben bzw. den Übermittlungsvermerk gilt, wenn diesem die Anlagen nicht beigefügt sind, z. B.:

CONFIDENTIEL UE/EU CONFIDENTIAL

Ohne Anlage(n) RESTREINT UE/EU RESTRICTED

Kennzeichnungen

11. Zusätzlich zu einer der Kennzeichnungen nach Anhang A Artikel 2 Absatz 2 können EU-VS mit zusätzlichen Kennzeichnungen versehen sein, wie z. B.:

a) einer Kennzeichnung, die den Herausgeber identifiziert;

b) Warnhinweisen, Codewörtern oder Akronymen, mit denen der Tätigkeitsbereich, auf den sich das Dokument bezieht, eine besondere Verteilung gemäß dem Grundsatz „Kenntnis nur, wenn nötig“ oder Verwendungsbeschränkungen angegeben werden;

c) Weitergabekennzeichnungen.

12. Im Anschluss an die Entscheidung über die Weitergabe von EU-VS an einen Drittstaat oder eine internationale Organisation übermittelt die für Sicherheit zuständige Direktion des EAD das betreffende Dokument, auf dem durch eine Weitergabekennzeichnung angegeben wird, an welchen Drittstaat oder welche internationale Organisation es weiterzugeben ist.

13. Die Sicherheitsbehörde des EAD verabschiedet die Liste der zugelassenen Kennzeichnungen.

Abgekürzte Einstufungskennzeichnungen

14. Standardmäßig abgekürzte Einstufungskennzeichnungen können verwendet werden, um den Geheimhaltungsgrad einzelner Absätze eines Textes auszuweisen. Die Abkürzungen ersetzen nicht die vollständigen Einstufungskennzeichnungen.

15. In EU-VS können folgende Standardabkürzungen verwendet werden, um den Geheimhaltungsgrad von Textabschnitten oder Textteilen von weniger als einer Seite anzugeben:

TRÈS SECRET UE/EU TOP SECRET	TS-UE/EU-TS
SECRET UE/EU SECRET,	S-UE/EU-S
CONFIDENTIEL UE/EU CONFIDENTIAL	C-UE/EU-C
RESTREINT UE/EU RESTRICTED:	R-UE/EU-R

Erstellung von EU-VS

16. Bei der Erstellung einer EU-VS

a) wird auf jeder Seite der Geheimhaltungsgrad eindeutig vermerkt,

b) wird jede Seite nummeriert,

c) wird dem Dokument ein Aktenzeichen und ein Betreff zugeordnet, der selbst keinen Geheimhaltungsgrad führt, wenn er nicht entsprechend gekennzeichnet ist,

d) wird das Dokument datiert,

e) erhalten Dokumente des Geheimhaltungsgrads „CONFIDENTIEL UE/EU CONFIDENTIAL“ oder höher auf jeder Seite eine eigene Exemplarnummer, wenn sie in mehreren Exemplaren verteilt werden sollen.

17. Ist eine Anwendung der Nummer 16 auf EU-VS nicht möglich, so sind im Einklang mit nach diesem Beschluss festzulegenden Sicherheitsleitlinien andere geeignete Maßnahmen anzuwenden.

Herabstufung und Aufhebung des Geheimhaltungsgrads von EU-VS

18. Der Herausgeber teilt, sofern möglich und insbesondere bei Verschlusssachen mit dem Geheimhaltungsgrad „RESTREINT UE/EU RESTRICTED“, zum Zeitpunkt der Erstellung einer EU-VS mit, ob deren Geheimhaltungsgrad zu einem bestimmten Datum oder im Anschluss an ein bestimmtes Ereignis herabgestuft oder aufgehoben werden kann.

19. Der EAD überprüft regelmäßig die in seinem Besitz befindlichen EU-VS daraufhin, ob ihr Geheimhaltungsgrad weiterhin zutreffend ist. Der EAD legt ein System fest, mit dem der Geheimhaltungsgrad der von ihm herausgegebenen registrierten EU-VS mindestens alle fünf Jahre überprüft wird. Eine solche Überprüfung ist nicht erforderlich, wenn der Herausgeber bereits von vorneherein einen Zeitpunkt mitgeteilt hat, zu dem der Geheimhaltungsgrad der Informationen automatisch herabgestuft oder aufgehoben wird, und die Informationen entsprechend gekennzeichnet wurden.

III. REGISTRIERUNG VON EU-VS ZU SICHERHEITSZWECKEN

20. In der Zentrale des EAD wird eine Zentralregistratur eingerichtet. Für jede Stelle im EAD, in der EU-VS bearbeitet werden, wird eine der Zentralregistratur untergeordnete zuständige Registratur eingerichtet, damit bei der Bearbeitung von EU-VS die Einhaltung dieses Beschlusses gewährleistet wird. Die Registraturen werden als abgesicherte Bereiche im Sinne des Anhangs A eingerichtet.

Jede Delegation der Union richtet ihre eigene EU-VS-Registratur ein.

Die Sicherheitsbehörde des EAD ernennt einen Chief Registry Officer für diese Registraturen.

21. Im Sinne dieses Beschlusses bezeichnet der Ausdruck „Registrierung zu Sicherheitszwecken“ (im Folgenden „Registrierung“) die Durchführung von Verfahren, bei denen jede Phase des Lebenszyklus der Informationen, auch deren Verbreitung und Vernichtung, aufgezeichnet wird. Im Falle eines Kommunikations- und Informationssystems können die Registrierungsverfahren durch Prozesse im Kommunikations- und Informationssystem selbst vorgenommen werden.

22. Alle als „CONFIDENTIEL UE/EU CONFIDENTIAL“ und höher eingestuften Materialien sind zu registrieren, wenn sie in einer Verwaltungseinheit (einschließlich Delegationen der Union) eingehen oder diese verlassen. Als „TRÈS SECRET UE/EU TOP SECRET“ eingestufte Verschlusssachen werden in den benannten Registraturen registriert.

23. Die Zentralregistratur in der EAD-Zentrale ist Haupteingangs- und Ausgangsstelle für den Austausch von Verschlusssachen mit Drittstaaten und internationalen Organisationen. Sie verwahrt Aufzeichnungen über jeden Austausch.

24. Die Sicherheitsbehörde des EAD billigt im Einklang mit Artikel 14 dieses Beschlusses Sicherheitsleitlinien in Bezug auf die Registrierung von EU-VS zu Sicherheitszwecken.

„TRÈS SECRET UE/EU TOP SECRET“-Registraturen

25. Die Zentralregistratur in der EAD-Zentrale wird als zentrale Eingangs- und Ausgangsstelle für als „TRÈS SECRET UE/EU TOP SECRET“ eingestufte Verschlusssachen benannt. Sofern erforderlich, können nachgeordnete Registraturen zur Bearbeitung dieser Verschlusssachen zu Registrierungszwecken bestimmt werden.

26. Diese nachgeordneten Registraturen dürfen als „TRÈS SECRET UE/EU TOP SECRET“ eingestufte Dokumente nicht unmittelbar an andere nachgeordnete Registraturen derselben zentralen „TRÈS SECRET UE/EU TOP SECRET“-Registratur oder anderweitig übermitteln, ohne dass diese ihre ausdrückliche schriftliche Zustimmung erteilt hat.

IV. KOPIEREN UND ÜBERSETZEN VON EU-VERSCHLUSSSACHEN

27. Ohne vorherige schriftliche Zustimmung des Herausgebers dürfen als „TRÈS SECRET UE/EU TOP SECRET“ eingestufte Dokumente weder kopiert noch übersetzt werden.

28. Hat der Herausgeber von als „SECRET UE/EU SECRET“ und niedriger eingestuften Dokumenten keine Einschränkungen hinsichtlich der Anfertigung von Kopien oder Übersetzungen auferlegt, so können diese Dokumente auf Anweisung des Besitzers kopiert bzw. übersetzt werden.

29. Die für das Originaldokument geltenden Sicherheitsmaßnahmen finden auf Kopien und Übersetzungen dieses Dokuments Anwendung. Die Kopien von als „CONFIDENTIEL UE/EU CONFIDENTIAL“ eingestuften Dokumenten dürfen nur von einer zuständigen (nachgeordneten) Registratur auf einem gesicherten Kopiergerät erstellt werden. Die Kopien müssen registriert werden.

V. BEFÖRDERUNG VON EU-VS

30. Für die Beförderung von EU-VS gelten die Schutzmaßnahmen nach den Nummern 32 bis 42. Bei der Beförderung von EU-VS auf elektronischen Datenträgern können ungeachtet Anhang A Artikel 7 Absatz 4 die nachstehend beschriebenen Schutzmaßnahmen entsprechend den Weisungen der Sicherheitsbehörde des EAD durch geeignete technische Abwehrmaßnahmen ergänzt werden, damit das Risiko eines Verlusts oder der Kenntnisnahme durch Unbefugte so gering wie möglich gehalten wird.

31. Die Sicherheitsbehörde des EAD erlässt Weisungen für die Beförderung von EU-VS nach Maßgabe dieses Beschlusses.

Beförderung innerhalb eines Gebäudes oder einer geschlossenen Gebäudegruppe

32. EU-VS, die innerhalb eines Gebäudes oder einer geschlossenen Gebäudegruppe befördert werden, sind zu verpacken, damit keine Rückschlüsse auf ihren Inhalt möglich sind.

33. Innerhalb eines Gebäudes oder einer geschlossenen Gebäudegruppe werden Verschlusssachen des Geheimhaltungsgrads „TRÈS SECRET UE/EU TOP SECRET“ von angemessen sicherheitsüberprüften Personen in einem gesicherten Umschlag befördert, auf dem lediglich der Name des Empfängers angegeben ist.

Beförderung innerhalb der EU

34. EU-VS, die zwischen Gebäuden oder Räumlichkeiten innerhalb der EU befördert werden, sind so zu verpacken, dass sie vor unbefugter Offenlegung geschützt sind.

35. Die Beförderung von Verschlusssachen bis zum Geheimhaltungsgrad „SECRET UE/EU SECRET“ innerhalb der EU erfolgt

    a) je nach Sachlage durch militärischen, diplomatischen oder Regierungskurier,

    b) als Handgepäck mit der Maßgabe, dass

        i) die EU-VS ununterbrochen im Besitz des Überbringers verbleibt, es sei denn, dass sie entsprechend den Anforderungen des Anhangs A II aufbewahrt wird,

        ii) die EU-VS nicht während der Beförderung geöffnet oder an öffentlich zugänglichen Orten gelesen wird,

        iii) die betreffenden Personen für den entsprechenden Geheimhaltungsgrad sicherheitsüberprüft sind und über ihre Verantwortlichkeiten für die Sicherheit belehrt wurden,

        iv) die betreffenden Personen erforderlichenfalls einen Kurierausweis erhalten,

    c) oder durch Postdienste oder private Kurierdienste, sofern

        i) sie von der zuständigen nationalen Sicherheitsbehörde nach Maßgabe der innerstaatlichen Rechtsvorschriften zugelassen worden sind und

        ii) sie geeignete Schutzmaßnahmen entsprechend den gemäß Artikel 21 Absatz 1 dieses Beschlusses in Sicherheitsleitlinien festzulegenden Mindestanforderungen anwenden.

    Bei der Beförderung von einem Mitgliedstaat in einen anderen wird Buchstabe c lediglich auf Verschlusssachen bis zum Geheimhaltungsgrad „CONFIDENTIEL UE/EU CONFIDENTIAL“ angewendet.

36. Als „CONFIDENTIEL UE/EU CONFIDENTIAL“ oder „SECRET UE/EU SECRET“ eingestufte Materialien (beispielsweise Geräte oder Maschinen), die nicht mit den unter Nummer 34 aufgeführten Beförderungsmitteln befördert werden können, werden nach Maßgabe des Anhangs A V von gewerblichen Beförderungsunternehmen als Fracht befördert.

37. Die Beförderung von als „TRES SECRET UE/EU TOP SECRET“ eingestuften Verschlusssachen zwischen Gebäuden oder Räumlichkeiten innerhalb der EU erfolgt je nach Sachlage durch militärischen, diplomatischen oder Regierungskurier.

Beförderung aus der EU in das Hoheitsgebiet eines Drittstaats oder zwischen EU-Einrichtungen in Drittstaaten

38. EU-VS, die aus der EU in das Hoheitsgebiet eines Drittstaats oder zwischen EU-Einrichtungen in Drittstaaten befördert werden, sind so zu verpacken, dass sie vor unbefugter Offenlegung geschützt sind.

39. Die Beförderung von Verschlusssachen der Geheimhaltungsgrade „CONFIDENTIEL UE/EU CONFIDENTIAL“ oder „SECRET UE/EU SECRET“ aus der EU in das Hoheitsgebiet eines Drittstaats und die Beförderung von EU-VS bis zum Geheimhaltungsgrad „SECRET UE/EU SECRET“ zwischen EU-Einrichtungen in Drittstaaten erfolgt

    a) durch militärischen oder diplomatischen Kurier

    b) oder als Handgepäck mit der Maßgabe, dass

        i) das Paket ein amtliches Siegel trägt oder so gestaltet ist, dass deutlich wird, dass es sich um eine amtliche Sendung handelt, die keiner Überprüfung durch Zoll- und Sicherheitsbehörden unterzogen werden darf,

        ii) die betreffenden Personen einen Kurierausweis mit sich führen, in dem das Paket verzeichnet ist und die betreffenden Personen zur Beförderung des Pakets ermächtigt werden,

        iii) die EU-VS ununterbrochen im Besitz des Überbringers verbleibt, es sei denn, dass sie entsprechend den Anforderungen des Anhangs A II aufbewahrt wird,

        iv) die EU-VS nicht während der Beförderung geöffnet oder an öffentlich zugänglichen Orten gelesen wird und

        v) die betreffenden Personen für den entsprechenden Geheimhaltungsgrad sicherheitsüberprüft sind und über ihre Verantwortlichkeiten für die Sicherheit belehrt wurden.

40. Die Beförderung von Verschlusssachen der Geheimhaltungsgrade „CONFIDENTIEL UE/EU CONFIDENTIAL“ oder „SECRET UE/EU SECRET“ aus der EU in einen Drittstaat oder zu einer internationalen Organisation erfolgt nach den einschlägigen Bestimmungen eines Geheimschutzabkommens oder einer Verwaltungsvereinbarung nach Anhang A Artikel 10 Absatz 2.

41. Verschlusssachen des Geheimhaltungsgrads „RESTREINT UE/EU RESTRICTED“ dürfen auch aus der EU in das Hoheitsgebiet eines Drittstaats durch Postdienste oder private Kurierdienste befördert werden.

42. Die Beförderung von Verschlusssachen des Geheimhaltungsgrads „TRÈS SECRET UE/EU TOP SECRET“ aus der EU in das Hoheitsgebiet eines Drittstaats oder zwischen EU-Einrichtungen in Drittstaaten erfolgt durch militärischen oder diplomatischen Kurier.

VI. VERNICHTUNG VON EU-VS

43. Nicht mehr benötigte EU-Verschlusssachen können unbeschadet der einschlägigen Vorschriften über die Archivierung vernichtet werden.

44. Registrierungspflichtige Dokumente nach Anhang A Artikel 7 Absatz 2 werden von der zuständigen Registratur auf Anweisung des Besitzers oder einer zuständigen Behörde vernichtet. Die Dienstbücher und sonstigen Registrierungsinformationen werden entsprechend aktualisiert.

45. Bei Dokumenten des Geheimhaltungsgrads „SECRET UE/EU SECRET“ oder „TRÈS SECRET UE/EU TOP SECRET“ erfolgt die Vernichtung im Beisein eines Zeugen, der mindestens für den Geheimhaltungsgrad des zu vernichtenden Dokuments sicherheitsüberprüft ist.

46. Der Registerführer und der Zeuge — falls dessen Anwesenheit erforderlich ist — unterschreiben eine Vernichtungsbescheinigung, die in der Registratur abgelegt wird. Die Registratur bewahrt die Vernichtungsbescheinigungen von Dokumenten des Geheimhaltungsgrads „TRÈS SECRET UE/EU TOP SECRET“ mindestens zehn Jahre lang und von Dokumenten der Geheimhaltungsgrade „CONFIDENTIEL UE/EU CONFIDENTIAL“ und „SECRET UE/EU SECRET“ mindestens fünf Jahre lang auf.

47. Verschlusssachen, auch Verschlusssachen des Geheimhaltungsgrads „RESTREINT UE/EU RESTRICTED“, werden nach Verfahren vernichtet, die die einschlägigen EU-Standards oder gleichwertige Standards erfüllen oder die gemäß nationalen technischen Normen von den Mitgliedstaaten zugelassen worden sind, damit so einer vollständigen oder teilweisen Wiederherstellung vorgebeugt wird.

48. Die Vernichtung elektronischer Datenträger, die für EU-VS verwendet wurden, erfolgt gemäß den von der Sicherheitsbehörde des EAD gebilligten Verfahren.

VII. SICHERHEITSINSPEKTIONEN

Sicherheitsinspektionen des EAD

49. Im Einklang mit Artikel 16 dieses Beschlusses umfassen Sicherheitsinspektionen des EAD

a) allgemeine Sicherheitsinspektionen mit dem Ziel einer Beurteilung der allgemeinen Sicherheit in der EAD-Zentrale, den Delegationen der Union und sämtlichen zugehörigen Räumlichkeiten, um vor allem die Wirksamkeit der zum Schutz der Sicherheitsinteressen des EAD getroffenen Sicherheitsmaßnahmen zu bewerten, und

b) EU-VS-Sicherheitsinspektionen mit dem Ziel, die Wirksamkeit der zum Schutz von EU-VS getroffenen Maßnahmen in der EAD-Zentrale und den Delegationen der Union zu bewerten, in der Regel mit Blick auf eine Akkreditierung.

Derartige Inspektionen werden unter anderem durchgeführt, um

i) sicherzustellen, dass die für den Schutz von EU-VS erforderlichen Mindeststandards, die in diesem Beschluss festgelegt sind, eingehalten werden,

ii) der Bedeutung der Sicherheitsaspekte und eines wirksamen Risikomanagements in den inspizierten Einrichtungen Nachdruck zu verleihen,

iii) Abwehrmaßnahmen zu empfehlen, um die spezifischen Auswirkungen des Verlusts der Vertraulichkeit, der Integrität oder der Verfügbarkeit von Verschlusssachen begrenzen zu können, und

iv) die laufenden Programme der Sicherheitsbehörden zur Schulung und Sensibilisierung in Sicherheitsfragen zu unterstützen.

Durchführung von Sicherheitsinspektionen des EAD und anschließende Berichterstattung

50. Sicherheitsinspektionen des EAD werden von einem Inspektionsteam der für Sicherheit zuständigen Direktion des EAD durchgeführt, das gegebenenfalls von Sicherheitsexperten anderer EU-Organe oder der Mitgliedstaaten unterstützt wird.

Das Inspektionsteam hat Zugang zu jedem Ort, an dem EU-VS bearbeitet werden, insbesondere Registraturen und Zugangspunkten der Kommunikations- und Informationssysteme.

51. Sicherheitsinspektionen des EAD in Delegationen der Union können erforderlichenfalls mit Unterstützung der Sicherheitsbeauftragten der Botschaften der Mitgliedstaaten in den betreffenden Drittstaaten durchgeführt werden.

52. Die Sicherheitsbehörde des EAD nimmt vor Ablauf eines jeden Kalenderjahrs das Sicherheitsinspektionsprogramm des EAD für das Folgejahr an.

53. Erforderlichenfalls kann die Sicherheitsbehörde des EAD Sicherheitsinspektionen veranlassen, die nicht in diesem Programm vorgesehen sind.

54. Am Ende der Sicherheitsinspektion werden der inspizierten Einrichtung die wichtigsten Schlussfolgerungen und Empfehlungen vorgelegt. Anschließend erstellt das Inspektionsteam einen Inspektionsbericht. Wurden Abhilfemaßnahmen und Empfehlungen vorgeschlagen, so muss der Bericht hinreichende Einzelheiten zur Untermauerung der betreffenden Schlussfolgerungen enthalten. Der Bericht wird der Sicherheitsbehörde des EAD und dem Leiter der inspizierten Einrichtung übermittelt.

    Unter der Verantwortung der für Sicherheit zuständigen Direktion des EAD wird regelmäßig ein Bericht erstellt, in dem die Erfahrungswerte, die sich aus den während eines bestimmten Zeitraums durchgeführten Inspektionen ergeben, dargelegt werden; dieser Bericht wird vom Sicherheitsausschuss des EAD geprüft.

Durchführung von Sicherheitsinspektionen in den nach Titel V Kapitel 2 EUV geschaffenen Agenturen und Einrichtungen der EU sowie anschließende Berichterstattung

55. Die für Sicherheit zuständige Direktion des EAD kann gegebenenfalls Experten für die Beteiligung an gemeinsamen EU-Inspektionsteams benennen, die Sicherheitsinspektionen in den nach Titel V Kapitel 2 EUV geschaffenen Agenturen und Einrichtungen der EU durchführen.

Prüfliste für Sicherheitsinspektionen des EAD

56. Die für Sicherheit zuständige Direktion des EAD erstellt eine Prüfliste für die Sicherheitsinspektionen des EAD und aktualisiert diese Liste. Diese Prüfliste wird dem Sicherheitsausschuss des EAD übermittelt.

57. Die Informationen zum Ausfüllen der Prüfliste werden insbesondere während der Inspektion vom Sicherheitsmanagement der inspizierten Einrichtung eingeholt. Nachdem sie mit den ausführlichen Antworten ausgefüllt wurde, wird die Prüfliste im Benehmen mit der inspizierten Einrichtung als Verschlusssache eingestuft. Sie ist nicht Teil des Inspektionsberichts.

ANHANG A IV

SCHUTZ VON EU-VS, DIE IN KOMMUNIKATIONS- UND INFORMATIONSSYSTEMEN BEARBEITET WERDEN

I. EINLEITUNG

1. Dieser Anhang enthält die Bestimmungen zur Anwendung von Anhang A Artikel 8.

2. Die folgenden Eigenschaften und Konzepte der Informationssicherung sind für die Sicherheit und die ordnungsgemäße Durchführung von Operationen in Kommunikations- und Informationssystemen unerlässlich:

Authentizität:	die Gewährleistung, dass die Informationen echt sind und aus Bona-fide Quellen stammen;
Verfügbarkeit:	der Umstand, dass die Informationen auf Anfrage einer befugten Stelle verfügbar und nutzbar sind;
Vertraulichkeit:	der Umstand, dass die Informationen nicht gegenüber unbefugten Personen, Stellen oder Verarbeitungsprozessen offengelegt werden;
Integrität:	der Umstand, dass die Genauigkeit und die Vollständigkeit der Informationen und Werte gewährleistet sind;
Beweisbarkeit:	die Möglichkeit des Nachweises, dass ein Vorgang oder ein Ereignis stattgefunden hat, so dass dieser Vorgang oder dieses Ereignis nicht nachträglich abgestritten werden kann.

II. GRUNDSÄTZE DER INFORMATIONSSICHERUNG

3. Die nachstehenden Bestimmungen sind Ausgangsbasis für die Sicherheit eines jeden Kommunikations- und Informationssystems, in dem EU-VS bearbeitet werden. Detaillierte Anforderungen zur Durchführung dieser Bestimmungen werden in Sicherheitsleitlinien für die Informationssicherung festgelegt.

Sicherheitsrisikomanagement

4. Sicherheitsrisikomanagement ist ein integraler Bestandteil der Konzeption, der Entwicklung, des Betriebs und der Wartung von Kommunikations- und Informationssystemen. Das Risikomanagement (Bewertung, Behandlung, Akzeptanz und Kommunikation) wird als fortlaufender Prozess gemeinsam von Vertretern der Systemeigner, den für ein Projekt zuständigen Stellen, den für den Betrieb zuständigen Stellen und den Sicherheits-Zulassungsstellen durchgeführt; dabei wird ein bewährtes, transparentes und vollkommen verständliches Risikobewertungsverfahren durchgeführt. Der Umfang des Kommunikations- und Informationssystems und seine Werte müssen gleich zu Beginn des Risikomanagementprozesses klar umrissen sein.

5. Die zuständigen Stellen des EAD müssen die potenziellen Bedrohungen für Kommunikations- und Informationssysteme überprüfen und über stets aktuelle und genaue Risikobewertungen entsprechend dem jeweiligen betrieblichen Umfeld verfügen. Sie halten ihre Kenntnisse über potenzielle Schwachstellen stets auf dem neuesten Stand und überprüfen regelmäßig die Bewertung der Schwachstellen, um den sich ändernden IT-Gegebenheiten Rechnung zu tragen.

6. Das Ziel des Sicherheitsrisikomanagements muss darin bestehen, ein Paket von Sicherheitsmaßnahmen anzuwenden, die zu einer zufriedenstellenden Ausgewogenheit zwischen den Anforderungen der Nutzer und dem Sicherheitsrestrisiko führen.

7. Die spezifischen Anforderungen, der Maßstab und Grad der Detaillierung, die von der einschlägigen Sicherheitsakkreditierungsstelle (Security Accreditation Authority — SAA) zur Akkreditierung eines Kommunikations- und Informationssystems festgelegt werden, müssen dem festgestellten Risiko entsprechen; dabei ist allen relevanten Faktoren Rechnung zu tragen, darunter dem Geheimhaltungsgrad der EU-VS, die in dem Kommunikations- und Informationssystem bearbeitet werden. Zur Akkreditierung gehören eine förmliche Erklärung zum Restrisiko und die Akzeptanz des Restrisikos durch eine zuständige Stelle.

Sicherheit während des gesamten Lebenszyklus eines Kommunikations- und Informationssystems

8. Die Gewährleistung der Sicherheit ist während des gesamten Lebenszyklus eines Kommunikations- und Informationssystems ab der Einführung bis zur Außerbetriebstellung erforderlich.

9. Die Rolle aller an einem Kommunikations- und Informationssystem Beteiligten und deren Interaktion hinsichtlich der Sicherheit des Systems werden für jede Phase des Lebenszyklus definiert.

10. Jegliches CIS einschließlich seiner technischen und nicht technischen Sicherheitsmaßnahmen wird während des Akkreditierungsprozesses Sicherheitsprüfungen unterzogen, damit gewährleistet ist, dass bei den implementierten Sicherheitsmaßnahmen das entsprechende Sicherheitsniveau erreicht wird, und überprüft wird, ob sie korrekt implementiert, integriert und konfiguriert werden.

11. Sicherheitsbewertungen, -inspektionen und -prüfungen werden während des Betriebs eines Kommunikations- und Informationssystems und während Wartungsarbeiten in regelmäßigen Abständen sowie im Falle außergewöhnlicher Umstände durchgeführt.

12. Die Sicherheitsdokumentation für ein Kommunikations- und Informationssystem wird während dessen Lebenszyklus als integraler Bestandteil des Prozesses eines Änderungs- und Konfigurationsmanagements weiterentwickelt.

Optimale Vorgehensweisen

13. Der EAD arbeitet mit dem Generalsekretariat des Rates, der Kommission und den Mitgliedstaaten zusammen, um optimale Vorgehensweisen für den Schutz von EU-VS, die in Kommunikations- und Informationssystemen bearbeitet werden, zu entwickeln. Leitlinien zu optimalen Vorgehensweisen enthalten Sicherheitsmaßnahmen in den Bereichen Technik, materieller Schutz, Organisation und Verfahren für Kommunikations- und Informationssysteme, deren Effizienz bei der Abwehr von Bedrohungen und der Behebung von Schwachstellen belegt ist.

14. Für den Schutz von EU-VS, die in Kommunikations- und Informationssystemen bearbeitet werden, sind die Erfahrungen derjenigen Stellen innerhalb und außerhalb der EU, die im Bereich Informationssicherung tätig sind, heranzuziehen.

15. Die Verbreitung und anschließende Anwendung optimaler Vorgehensweisen soll dazu beitragen, dass ein gleichwertiges Sicherheitsniveau für die verschiedenen, vom EAD betriebenen Kommunikations- und Informationssysteme erreicht wird, in denen EU-VS bearbeitet werden.

Mehrschichtige Sicherheit

16. Um das Risiko bei Kommunikations- und Informationssystemen zu verringern, wird eine Reihe von technischen und nicht technischen Sicherheitsmaßnahmen in Form eines mehrschichtigen Abwehrsystems durchgeführt. Dazu gehören

    a) *Abschreckung*: Sicherheitsmaßnahmen, mit denen darauf abgezielt wird, Gegner von einer Planung von Angriffen auf das Kommunikations- und Informationssystem abzuhalten;

    b) *Prävention*: Sicherheitsmaßnahmen, mit denen darauf abgezielt wird, einen Angriff auf das Kommunikations- und Informationssystem zu verhindern oder abzublocken;

    c) *Erkennung*: Sicherheitsmaßnahmen, mit denen darauf abgezielt wird, einen Angriff auf das Kommunikations- und Informationssystem zu erkennen;

    d) *Widerstandsfähigkeit*: Sicherheitsmaßnahmen, mit denen darauf abgezielt wird, die Auswirkungen eines Angriffes auf möglichst wenige Informationen oder Komponenten des CIS zu begrenzen und weiteren Schaden zu verhindern;

    e) *Wiederherstellung*: Sicherheitsmaßnahmen, mit denen darauf abgezielt wird, für das Kommunikations- und Informationssystem eine Situation der Sicherheit wiederherzustellen.

    Wie streng diese Sicherheitsmaßnahmen zu sein haben und in welchen Fällen sie zur Anwendung kommen, wird durch eine Risikobewertung bestimmt.

17. Die zuständigen Stellen des EAD tragen dafür Sorge, dass sie auf Zwischenfälle, die die Grenzen einer Organisation oder eines Staates überschreiten können, reagieren können, damit die Reaktionen koordiniert und Informationen über diese Zwischenfälle und damit zusammenhängende Risiken ausgetauscht werden (Computer-Notfall-Reaktionsfähigkeit).

Minimalitätsprinzip und Prinzip der minimalen Zugriffsrechte

18. Nur die für die operativen Anforderungen unbedingt notwendigen Funktionen, Geräte und Dienste werden implementiert, damit unnötige Risiken vermieden werden.

19. Nutzer von Kommunikations- und Informationssystemen und automatisierten Verfahrensabläufen erhalten nur den Zugang, die Berechtigung oder die Ermächtigungen, die für die Erfüllung ihrer Aufgaben erforderlich sind, damit der Schaden, der durch Zwischenfälle, Fehler oder die unbefugte Nutzung von Ressourcen des Kommunikations- und Informationssystems entstehen kann, begrenzt wird.

20. Die von einem Kommunikations- und Informationssystem durchgeführten Registrierungsverfahren werden, soweit erforderlich, als Teil des Akkreditierungsverfahrens überprüft.

Sensibilisierung in Bezug auf die Informationssicherung

21. Die Sensibilisierung für die Risiken und die zur Verfügung stehenden Sicherheitsmaßnahmen ist die erste Verteidigungslinie in Bezug auf die Sicherheit von Kommunikations- und Informationssystemen. Insbesondere sollte sich das gesamte Personal, das mit einem Kommunikations- und Informationssystem während dessen Lebenszyklus befasst ist, einschließlich der Nutzer, über Folgendes bewusst sein:

    a) Sicherheitslücken können den Kommunikations- und Informationssystemen und der gesamten Organisation erheblich schaden;

    b) aus einer Vernetzung und Verflechtung kann sich potenzieller Schaden für andere ergeben;

    c) die Nutzer sind persönlich für die Sicherheit eines Kommunikations- und Informationssystems entsprechend ihrer konkreten Aufgabe innerhalb des Systems und bei den Prozessen verantwortlich und dafür rechenschaftspflichtig.

22. Damit sichergestellt ist, dass die Verantwortlichkeiten für die Sicherheit bekannt sind, sind die Schulung und Sensibilisierung in Bezug auf Informationssicherung für das gesamte beteiligte Personal, einschließlich des Führungspersonals und der Nutzer von Kommunikations- und Informationssystemen, obligatorisch.

Evaluierung und Zulassung von IT-Sicherheitsprodukten

23. Das erforderliche Maß an Vertrauen in die Sicherheitsmaßnahmen, das als Niveau der Vertrauenswürdigkeit definiert wird, wird aufgrund der Ergebnisse des Risikomanagementprozesses und entsprechend den einschlägigen Sicherheitskonzepten und Sicherheitsleitlinien bestimmt.

24. Das Vertrauenswürdigkeitsniveau wird geprüft, indem international anerkannte oder national genehmigte Verfahren und Methoden angewandt werden. Dazu gehören in erster Linie Evaluierung, Kontrollen und Betriebsanalysen.

25. Kryptografische Produkte zum Schutz von EU-VS werden von einer nationalen Krypto-Zulassungsstelle (Crypto Approval Authority — CAA) eines Mitgliedstaats bewertet und zugelassen.

26. Bevor kryptografische Produkte der CAA des EAD gemäß Artikel 8 Absatz 5 dieses Beschlusses zur Zulassung empfohlen werden, müssen sie eine Bewertung durch eine zweite Stelle, und zwar eine qualifizierte Behörde (Appropriately Qualified Authority — AQUA) eines Mitgliedstaats, die nicht an der Konzeption oder Herstellung der Ausrüstung beteiligt ist, erfolgreich durchlaufen. Wie detailliert bei einer Zweitevaluierung zu prüfen ist, hängt von dem angestrebten höchsten Geheimhaltungsgrad der EU-VS ab, die mit diesen Produkten geschützt werden sollen.

27. Wenn dies aus spezifischen operativen Gründen gerechtfertigt ist, kann die CAA des EAD auf Empfehlung des Sicherheitsausschusses des Rates auf die Anforderungen nach den Nummern 25 oder 26 verzichten und eine vorläufige Zulassung für einen bestimmten Zeitraum gemäß dem Verfahren nach Artikel 8 Absatz 5 dieses Beschlusses erteilen.

28. Eine AQUA ist eine CAA eines Mitgliedstaats, die auf der Grundlage vom Rat festgelegter Kriterien dafür akkreditiert wurde, die Zweitevaluierung von kryptografischen Produkten zum Schutz von EU-VS vorzunehmen.

29. Der Hohe Vertreter billigt ein Sicherheitskonzept in Bezug auf die Eignung und Zulassung von nichtkryptografischen IT-Sicherheitsprodukten.

Übermittlung innerhalb abgesicherter Bereiche

30. Ungeachtet der Bestimmungen dieses Beschlusses kann, wenn EU-VS innerhalb abgesicherter Bereiche oder Verwaltungsbereiche übermittelt werden, eine nicht verschlüsselte Übermittlung oder eine Verschlüsselung auf einer niedrigeren Stufe unter Zugrundelegung der Ergebnisse eines Risikomanagementprozesses und vorbehaltlich der Zustimmung der SAA erfolgen.

Sichere Zusammenschaltung von Kommunikations- und Informationssystemen

31. Im Sinne dieses Beschlusses ist eine Systemzusammenschaltung die direkte Verbindung von zwei oder mehr IT-Systemen für die gemeinsame Nutzung von Daten und anderen Informationsressourcen (beispielsweise Kommunikation); die Verbindung kann unidirektional oder multidirektional sein.

32. Ein Kommunikations- und Informationssystem muss jedes angeschlossene IT-System zunächst als nicht vertrauenswürdig behandeln und Schutzmaßnahmen durchführen, um den Austausch von Verschlusssachen zu kontrollieren.

33. Bei der Zusammenschaltung eines Kommunikations- und Informationssystems mit einem anderen IT-System müssen stets die folgenden grundlegenden Anforderungen erfüllt sein:

    a) Die betrieblichen und operativen Anforderungen für solche Zusammenschaltungen müssen von den zuständigen Stellen bekannt gegeben und genehmigt werden;

    b) die Zusammenschaltung ist einem Risikomanagement- und Akkreditierungsverfahren zu unterziehen und bedarf der Genehmigung der zuständigen SAA;

    c) Dienste für den Schutz von Systemübergängen (Boundary Protection Services — BPS) werden an der Peripherie aller Kommunikations- und Informationssysteme implementiert.

34. Es darf keine Zusammenschaltung zwischen einem akkreditierten Kommunikations- und Informationssystem und einem ungeschützten oder öffentlichen Netz geben, außer wenn das Kommunikations- und Informationssystem über zugelassene BPS verfügt, die zu diesem Zweck zwischen dem Kommunikations- und Informationssystem und dem ungeschützten oder öffentlichen Netz installiert wurden. Die Sicherheitsmaßnahmen für einen derartigen Verbund werden von der zuständigen Stelle für Informationssicherung (Information Assurance Authority — IAA) überprüft und von der zuständigen SAA genehmigt.

    Wenn das ungeschützte oder öffentliche Netz lediglich als Träger verwendet wird und die Daten durch ein gemäß Artikel 8 Absatz 5 dieses Beschlusses zugelassenes kryptografisches Produkt verschlüsselt werden, gilt eine derartige Verbindung nicht als Zusammenschaltung.

35. Die direkte oder kaskadierte Zusammenschaltung eines Kommunikations- und Informationssystems, das für die Bearbeitung von Verschlusssachen des Geheimhaltungsgrads „TRÈS SECRET UE/EU TOP SECRET“ akkreditiert ist, mit einem ungeschützten oder öffentlichen Netz ist untersagt.

Elektronische Datenträger

36. Die Vernichtung elektronischer Datenträger erfolgt nach Verfahren, die von der Sicherheitsbehörde des EAD genehmigt wurden.

37. Für die Wiederverwendung elektronischer Datenträger und für die Herabstufung oder Aufhebung ihres Geheimhaltungsgrads gelten die nach Artikel 8 Absatz 2 dieses Beschlusses festzulegenden Sicherheitsleitlinien.

Notsituationen

38. Unbeschadet der Bestimmungen dieses Beschlusses können in Notsituationen wie beispielsweise drohenden oder bereits eingetretenen Krisen, Konflikten, Kriegssituationen oder im Fall besonderer operativer Umstände die nachstehend beschriebenen besonderen Verfahren für einen befristeten Zeitraum angewandt werden.

39. EU-VS können mithilfe kryptografischer Produkte, die für einen niedrigeren Geheimhaltungsgrad zugelassen sind, oder mit Zustimmung der zuständigen Behörde unverschlüsselt übermittelt werden, wenn eine Verzögerung einen Schaden verursachen würde, der deutlich größer wäre als der Schaden, der durch eine Offenlegung des als Verschlusssache eingestuften Materials entstehen würde, und wenn

    a) Absender und Empfänger nicht die erforderliche Verschlüsselungseinrichtung oder gar keine Verschlüsselungseinrichtung haben und

    b) das als Verschlusssache eingestufte Material nicht rechtzeitig auf anderem Wege übermittelt werden kann.

40. Verschlusssachen, die unter den unter Nummer 39 erläuterten Umständen übermittelt werden, sind nicht mit Kennzeichnungen oder Angaben zu versehen, die sie von nicht als Verschlusssache eingestuften Informationen oder solchen unterscheiden, die mit einem zur Verfügung stehenden kryptografischen Produkt geschützt werden können. Die Empfänger werden auf anderem Weg unverzüglich über den Geheimhaltungsgrad unterrichtet.

41. Wird gemäß Nummer 39 vorgegangen, ist der Direktion Sicherheit des EAD anschließend Bericht zu erstatten, die wiederum den Sicherheitsausschuss des EAD unterrichtet. In diesem Bericht werden mindestens der Absender, der Empfänger und der Herausgeber jeder EU-VS angegeben.

III. FUNKTIONEN UND STELLEN FÜR INFORMATIONSSICHERUNG

42. Folgende Funktionen im Bereich der Informationssicherung werden im EAD eingerichtet. Hierfür sind keine zentralen organisatorischen Einheiten erforderlich. Für die einzelnen Funktionen werden gesonderte Mandate erteilt. Diese Funktionen und die damit einhergehenden Verantwortlichkeiten können jedoch zusammengefasst oder der gleichen organisatorischen Einheit zugewiesen oder auf verschiedene organisatorische Einheiten aufgeteilt werden, sofern interne Interessen- oder Aufgabenkonflikte vermieden werden.

Stelle für Informationssicherung

43. Die Stelle für Informationssicherung (Information Aussurance Authority — IAA) ist für Folgendes zuständig:

a) Ausarbeitung von Sicherheitsleitlinien für Informationssicherung sowie Überwachung ihrer Wirksamkeit und Relevanz;

b) Schutz und Verwaltung der technischen Informationen über kryptografische Produkte;

c) Gewährleistung, dass die für den Schutz von EU-VS gewählten Informationssicherungsmaßnahmen den einschlägigen Leitlinien für ihre Eignung und Auswahl entsprechen;

d) Gewährleistung, dass die kryptografischen Produkte unter Einhaltung der Leitlinien für ihre Eignung und Auswahl gewählt werden;

e) Koordinierung von Schulung und Sensibilisierung in Bezug auf Informationssicherung;

f) Konsultation des Systembetreibers, der Sicherheitsakteure und der Vertreter der Nutzer in Bezug auf die Sicherheitsleitlinien für Informationssicherung;

g) Gewährleistung, dass in der für Fragen der Informationssicherung zuständigen Fachuntergruppe des Sicherheitsausschusses des EAD das geeignete Fachwissen vorhanden ist.

TEMPEST-Stelle

44. Die TEMPEST-Stelle hat sicherzustellen, dass die Kommunikations- und Informationssysteme den TEMPEST-Konzepten und -Leitlinien entsprechen. Sie genehmigt TEMPEST-Schutzmaßnahmen für Installationen und Produkte, damit EU-VS bis zu einem bestimmten Geheimhaltungsgrad in dem betreffenden Betriebsumfeld geschützt sind.

Krypto-Zulassungsstelle

45. Die Krypto-Zulassungsstelle (Crypto Approval Authority — CAA) hat sicherzustellen, dass kryptografische Produkte den jeweiligen Kryptografieleitlinien entsprechen. Sie erteilt für ein kryptografisches Produkt die Zulassung, EU-VS bis zu einem bestimmten Geheimhaltungsgrad in dem betreffenden Betriebsumfeld zu schützen.

Krypto-Verteilungsstelle

46. Die Krypto-Verteilungsstelle (Crypto Distribution Authority — CDA) ist für Folgendes zuständig:

a) Verwaltung und Rechenschaftslegung in Bezug auf EU-Kryptomaterial;

b) Gewährleistung, dass für das gesamte EU-Kryptomaterial in Bezug auf Rechenschaftslegung, sicheren Umgang, Speicherung und Verteilung geeignete Verfahren durchgesetzt und Kanäle eingerichtet werden;

c) Sicherstellung des Transfers von EU-Kryptomaterial zu den oder von den Einzelpersonen oder Dienststellen, die es verwenden.

Sicherheits-Akkreditierungsstelle

47. Die Sicherheit-Akkreditierungsstelle (Security Accreditation Authority — SAA) für das jeweilige System ist für Folgendes zuständig:

a) Gewährleistung, dass die Kommunikations- und Informationssysteme den einschlägigen Sicherheitsleitlinien entsprechen, Ausstellung einer Zulassungserklärung für Kommunikations- und Informationssysteme zur Bearbeitung von EU-VS bis zu einem bestimmten Geheimhaltungsgrad in dem betreffenden Betriebsumfeld, wobei die Akkreditierungsvoraussetzungen sowie die Kriterien angegeben werden, aufgrund deren eine erneute Zulassung erforderlich wird;

b) Festlegung eines Verfahrens für die Sicherheitsakkreditierung im Einklang mit den einschlägigen Leitlinien unter genauer Angabe der Voraussetzungen für die Zulassung von Kommunikations- und Informationssystemen unter der Leitung der SAA;

c) Festlegung einer Strategie für die Sicherheitsakkreditierung, in der dargelegt wird, wie detailliert das Akkreditierungsverfahren entsprechend der geforderten Vertraulichkeit angelegt sein muss;

d) Prüfung und Zulassung der sicherheitsbezogenen Dokumentation — einschließlich der Erklärung zum Risikomanagement und der Erklärung zum Restrisiko, der Aufstellung der systemspezifischen Sicherheitsanforderungen (System-specific Security Requirement Statements — im Folgenden „SSRS"), der Dokumentation über die Überprüfung der Sicherheitsimplementierung und der sicherheitsbezogenen Betriebsverfahren (Security Operating Procedures — im Folgenden „SecOPs") — und Gewährleistung, dass sie mit den Sicherheitsvorschriften und -konzepten des Rates übereinstimmt;

e) Kontrolle der Implementierung der Sicherheitsmaßnahmen in Bezug auf das Kommunikations- und Informationssystem im Wege der Durchführung oder Förderung von Sicherheitsbewertungen, -inspektionen oder -prüfungen;

f) Festlegung von Sicherheitsanforderungen (z. B. Sicherheitsstufen für die Sicherheitsüberprüfung des Personals) für die Besetzung der für das Kommunikations- und Informationssystem sicherheitskritischen Stellen;

g) Förderung der Auswahl von zugelassenen kryptografischen und TEMPEST-Produkten, die zur Gewährleistung der Sicherheit eines Kommunikations- und Informationssystems verwendet werden;

h) Genehmigung — oder gegebenenfalls Mitwirkung an der gemeinsamen Genehmigung — der Zusammenschaltung eines Kommunikations- und Informationssystems mit anderen Kommunikations- und Informationssystemen;

i) Konsultation des Systembetreibers, der Sicherheitsakteure und der Vertreter der Nutzer in Bezug auf das Sicherheitsrisikomanagement — insbesondere hinsichtlich des Restrisikos — und auf die Voraussetzungen für die Erklärung über die Zulassung.

48. Die SAA des EAD ist für die Akkreditierung aller CIS zuständig, die im Zuständigkeitsbereich des EAD betrieben werden.

Sicherheits-Akkreditierungsgremium

49. Wenn CIS in die Zuständigkeit sowohl der SAA des EAD als auch der SAA der Mitgliedstaaten fallen, so nimmt ein gemeinsames Akkreditierungsgremium (Security Accreditation Board — SAB) die Akkreditierung des betreffenden Systems vor. Es setzt sich aus einem SAA-Vertreter jedes Mitgliedstaats zusammen, und je ein SAA-Vertreter des Generalsekretariats des Rates und der Kommission nehmen an den Sitzungen teil. Andere Stellen, die an ein Kommunikations- und Informationssystem angeschlossen sind, werden zu Beratungen über das betreffende System eingeladen.

Den Vorsitz des SAB führt ein Vertreter der SAA des EAD. Im SAB beschließen die SAA-Vertreter der Organe, Mitgliedstaaten und sonstigen Stellen, die an das Kommunikations- und Informationssystem angeschlossen sind, einvernehmlich. Das SAB erstellt für den Sicherheitsausschuss des EAD regelmäßig Berichte über seine Tätigkeit und übermittelt ihm alle Akkreditierungserklärungen.

Für den Betrieb zuständige Stelle für Informationssicherung

50. Die für den Betrieb des jeweiligen Systems zuständige Stelle für Informationssicherung ist für Folgendes zuständig:

a) Ausarbeitung der Sicherheitsdokumentation im Einklang mit den Sicherheitsleitlinien; dies betrifft insbesondere die SSRS einschließlich der Erklärung zum Restrisiko, die SecOPs und das Kryptokonzept im Rahmen des Akkreditierungsverfahrens für Kommunikations- und Informationssysteme;

b) Mitwirkung bei Auswahl und Prüfung der systemspezifischen technischen Sicherheitsmaßnahmen, -vorrichtungen und -software mit dem Ziel, deren Implementierung zu überwachen und zu gewährleisten, dass sie im Einklang mit der einschlägigen Sicherheitsdokumentation sicher installiert, konfiguriert und gewartet werden;

c) Mitwirkung bei der Auswahl der TEMPEST-Sicherheitsmaßnahmen und -vorrichtungen, sofern dies in den SSRS verlangt wird, und Gewährleistung, dass sie in Zusammenarbeit mit der TEMPEST-Stelle sicher installiert und gewartet werden;

d) Überwachung der Implementierung und Anwendung der SecOPs und gegebenenfalls Übertragung der Verantwortung für die Betriebssicherheit an den Systemeigner;

e) Management und Handhabung von kryptografischen Produkten, Gewährleistung der Aufbewahrung von verschlüsseltem und der Kontrolle unterliegendem Material sowie erforderlichenfalls Gewährleistung der Generierung kryptografischer Variablen;

f) Durchführung von Sicherheitsanalysen, -überprüfungen und -tests, insbesondere im Hinblick auf die Erstellung der von der SAA verlangten einschlägigen Risikoberichte;

g) Durchführung von für das Kommunikations- und Informationssystem spezifischen Schulungen in Bezug auf Informationssicherung;

h) Implementierung und Durchführung von für das Kommunikations- und Informationssystem spezifischen Sicherheitsmaßnahmen.

ANHANG A V

GEHEIMSCHUTZ IN DER WIRTSCHAFT

I. EINLEITUNG

1. Dieser Anhang enthält die Bestimmungen zur Anwendung von Anhang A Artikel 9. Er legt allgemeine Sicherheitsvorschriften für industrielle oder andere Unternehmen fest, die während der Verhandlungen vor der Auftragsvergabe und während der Laufzeit der als Verschlusssache eingestuften Aufträge, die vom EAD vergeben werden, gelten.

2. Die Sicherheitsbehörde des EAD billigt Leitlinien für den Geheimschutz in der Wirtschaft, mit deren insbesondere ausführliche Anforderungen in Bezug auf Sicherheitsbescheide für Unternehmen (Facility Security Clearances — FSC), Geheimschutzklauseln (Security Aspects Letters — SAL), Besuche sowie die Übermittlung und Beförderung von EU-VS aufgestellt werden.

II. SICHERHEITSBESTIMMUNGEN BEI ALS VERSCHLUSSSACHE EINGESTUFTEN AUFTRÄGEN

VS-Einstufungsliste

3. Vor der Ausschreibung oder der Vergabe eines als Verschlusssache eingestuften Auftrags bestimmt der EAD als Vergabebehörde den Geheimhaltungsgrad für Informationen, die Bietern oder Auftragnehmern zur Verfügung gestellt werden, sowie den Geheimhaltungsgrad für Informationen, die vom Auftragnehmer herauszugeben sind. Zu diesem Zweck erstellt der EAD die bei der Ausführung des Auftrags zu verwendende VS-Einstufungsliste (Security Classification Guide — SCG).

4. Für die Bestimmung des Geheimhaltungsgrads der verschiedenen Bestandteile eines als Verschlusssache eingestuften Auftrags gelten die folgenden Grundsätze:

   a) bei der Erstellung einer SCG berücksichtigt der EAD alle relevanten Sicherheitsaspekte, unter anderem den Geheimhaltungsgrad, den der Herausgeber der Information, deren Nutzung für den Auftrag er gebilligt hat, dieser zugewiesen hat;

   b) der Geheimhaltungsgrad des Gesamtauftrags darf nicht niedriger sein als der höchste Grad der einzelnen Auftragskomponenten;

   c) gegebenenfalls setzt sich der EAD mit den nationalen Sicherheitsbehörden/beauftragten Sicherheitsbehörden der Mitgliedstaaten oder mit der betreffenden sonstigen zuständigen Sicherheitsbehörde in Verbindung, wenn es den Geheimhaltungsgrad von Informationen, die bei der Ausführung eines Auftrags von den Auftragnehmern erstellt oder diesen zur Verfügung gestellt werden, ändert und wenn es nachfolgende Änderungen in der VS-Einstufungsliste vornimmt.

Geheimschutzklausel

5. Die auftragsspezifischen Sicherheitsanforderungen werden in einer Geheimschutzklausel (Security Aspects Letter — SAL) beschrieben. Die SAL enthält gegebenenfalls die SCG und ist fester Bestandteil eines als Verschlusssache eingestuften Auftrags oder Unterauftrags.

6. Die SAL enthält die Bestimmungen, mit denen der Auftragnehmer und/oder Unterauftragnehmer verpflichtet wird, die Mindeststandards dieses Beschlusses einzuhalten. Die Nichteinhaltung dieser Mindeststandards kann einen ausreichenden Grund dafür darstellen, dass der Auftrag gekündigt wird.

Sicherheitsanweisung für ein Programm/Projekt

7. Abhängig vom Umfang von Programmen oder Projekten, die mit dem Zugang zu oder der Bearbeitung oder Aufbewahrung von EU-VS verbunden sind, kann eine spezifische Sicherheitsanweisung für ein Programm/Projekt (Programme/Project Security Instructions — PSI) von der mit der Verwaltung des Programms oder Projekts beauftragten Vergabebehörde ausgearbeitet werden. Die Sicherheitsanweisung bedarf der Genehmigung durch die nationalen Sicherheitsbehörden/beauftragten Sicherheitsbehörden der Mitgliedstaaten oder durch eine andere zuständige Sicherheitsbehörde, die an dem Programm/Projekt beteiligt ist, und kann zusätzliche Sicherheitsanforderungen beinhalten.

III. SICHERHEITSBESCHEID FÜR UNTERNEHMEN

8. Die für Sicherheit zuständige Direktion des EAD ersucht die nationale Sicherheitsbehörde/beauftragte Sicherheitsbehörde oder eine andere zuständige Behörde des betreffenden Mitgliedstaats um Ausstellung eines Sicherheitsbescheids für Unternehmen (Facility Security Clearance — FSC), der gemäß den innerstaatlichen Rechtsvorschriften Auskunft darüber gibt, dass ein industrielles oder anderes Unternehmen in der Lage ist, EU-VS bis zu dem entsprechenden Geheimhaltungsgrad („CONFIDENTIEL UE/EU CONFIDENTIAL“ oder „SECRET UE/EU SECRET“) in seinen Anlagen zu schützen. Ein Nachweis über die Ausstellung des FSC ist dem EAD vorzulegen, bevor einem Auftragnehmer oder Unterauftragnehmer bzw. einem möglichen Auftragnehmer oder Unterauftragnehmer EU-VS zur Verfügung gestellt werden können oder ihm Zugang zu diesen gewährt werden kann.

9. Der EAD als Vergabebehörde teilt der zuständigen nationalen Sicherheitsbehörde/beauftragten Sicherheitsbehörde oder einer anderen zuständigen Sicherheitsbehörde gegebenenfalls mit, dass ein FSC in der Phase vor der Auftragsvergabe oder für die Ausführung des Auftrags erforderlich ist. Ein FSC oder eine Erklärung über die Sicherheitsüberprüfung von Personal (PSC) ist in der Phase vor der Auftragsvergabe erforderlich, wenn EU-VS mit dem Geheimhaltungsgrad „CONFIDENTIEL UE/EU CONFIDENTIAL“ oder „SECRET UE/EU SECRET“ während des Bietverfahrens zur Verfügung gestellt werden müssen.

10. Der EAD als Vergabebehörde vergibt keinen als Verschlusssache eingestuften Auftrag an einen bevorzugten Bieter, bevor er von der nationalen Sicherheitsbehörde/beauftragten Sicherheitsbehörde oder einer anderen zuständigen Sicherheitsbehörde des Mitgliedstaats, in dem der betreffende Auftragnehmer oder Unterauftragnehmer eingetragen ist, die Bestätigung erhalten hat, dass erforderlichenfalls ein entsprechender FSC erteilt wurde.

11. Der EAD als Vergabebehörde ersucht die nationale Sicherheitsbehörde/beauftragte Sicherheitsbehörde oder die sonstige zuständige Sicherheitsbehörde, die einen FSC erteilt hat, ihn über etwaige nachteilige Erkenntnisse zu unterrichten, die diesen FSC betreffen. Bei Unteraufträgen ist die Nationale Sicherheitsbehörde/Beauftragte Sicherheitsbehörde oder eine sonstige zuständige Sicherheitsbehörde entsprechend zu informieren.

12. Die Aufhebung eines FSC durch die jeweilige nationale Sicherheitsbehörde/beauftragte Sicherheitsbehörde oder eine sonstige zuständige Sicherheitsbehörde stellt für den EAD als Vergabebehörde einen ausreichenden Grund dar, den als Verschlusssache eingestuften Auftrag zu kündigen oder einen Bieter vom Vergabeverfahren auszuschließen.

IV. ERKLÄRUNGEN ÜBER DIE SICHERHEITSÜBERPRÜFUNG VON PERSONAL (PSC) BEI AUFTRAGNEHMERN

13. Das gesamte Personal eines Auftragnehmers, das Zugang zu als „CONFIDENTIEL UE/EU CONFIDENTIAL“ oder höher eingestuften EU-VS haben muss, wird ordnungsgemäß sicherheitsüberprüft und erhält Zugang zu Informationen nach dem Grundsatz „Kenntnis nur, wenn nötig“ („need-to-know“). Obwohl für den Zugang zu als „RESTREINT UE/EU RESTRICTED“ eingestuften EU-VS keine PSC erforderlich ist, wird dieser Zugang nur nach dem Prinzip „Kenntnis nur, wenn nötig“ gewährt.

14. Die PSC für das Personal von Auftragnehmern sind bei der für das betreffende Unternehmen zuständigen nationalen Sicherheitsbehörde/beauftragten Sicherheitsbehörde zu beantragen.

15. Der EAD macht Auftraggeber, die einen Drittstaatsangehörigen für eine Tätigkeit beschäftigen wollen, für die der Zugang zu EU-VS erforderlich ist, darauf aufmerksam, dass die nationale Sicherheitsbehörde/beauftragte Sicherheitsbehörde in dem Mitgliedstaat, in dem das einstellende Unternehmen seinen Sitz hat und eingetragen ist, dafür zuständig ist, zu entscheiden, ob der betreffenden Person der Zugang zu solchen Informationen nach Maßgabe dieses Beschlusses gewährt werden kann, und zu bestätigen, dass der Herausgeber vor Gewährung des Zugangs zu Informationen seine Zustimmung erteilt hat.

V. ALS VERSCHLUSSSACHE EINGESTUFTE AUFTRÄGE UND UNTERAUFTRÄGE

16. Werden EU-VS einem Bieter in der Phase vor der Auftragsvergabe zur Verfügung gestellt, so enthält die Ausschreibung eine Geheimschutzklausel, wonach ein Bieter, der kein Angebot abgibt oder der nicht ausgewählt wird, verpflichtet ist, alle Verschlusssachen innerhalb einer vorgegebenen Frist zurückzugeben.

17. Sobald der Zuschlag für einen als Verschlusssache eingestuften Auftrag oder Unterauftrag erteilt wurde, teilt der EAD als Vergabebehörde der für den Auftragnehmer oder Unterauftragnehmer zuständigen nationalen Sicherheitsbehörde/beauftragten Sicherheitsbehörde oder einer sonstigen zuständigen Sicherheitsbehörde die Sicherheitsvorschriften für den als Verschlusssache eingestuften Auftrag mit.

18. Bei Kündigung oder Ablauf eines solchen Auftrags informiert der EAD als Vergabebehörde (und/oder gegebenenfalls die nationale Sicherheitsbehörde/beauftragte Sicherheitsbehörde oder eine sonstige zuständige Sicherheitsbehörde bei Unteraufträgen) unverzüglich die nationale Sicherheitsbehörde/beauftrage Sicherheitsbehörde oder eine sonstige zuständige Sicherheitsbehörde des Mitgliedstaats, in dem der Auftragnehmer oder Unterauftragnehmer eingetragen ist.

19. Generell ist der Auftragnehmer oder Unterauftragnehmer verpflichtet, bei der Kündigung oder Ablauf eines als Verschlusssache eingestuften Auftrags oder Unterauftrags in seinem Besitz befindliche EU-VS an die Vergabebehörde zurückzugeben.

20. Die besonderen Bestimmungen für die Vernichtung von EU-VS während der Ausführung des Auftrags oder bei dessen Kündigung oder Ablauf werden in der Geheimschutzklausel festgelegt.

21. Wird dem Auftragnehmer oder Unterauftragnehmer gestattet, EU-VS nach Kündigung oder Ablauf eines Auftrags zu behalten, so müssen die in diesem Beschluss niedergelegten Mindeststandards weiterhin eingehalten und die Geheimhaltung von EU-VS von dem Auftragnehmer oder Unterauftragnehmer geschützt werden.

22. Die Bedingungen, zu denen der Auftragnehmer Unteraufträge vergeben darf, sind in der Ausschreibung und im Auftrag festgelegt.

23. Der Auftragnehmer holt die Erlaubnis des EAD als Vergabebehörde ein, bevor er für Teile eines als Verschlusssache eingestuften Auftrags Unteraufträge vergibt. Unteraufträge dürfen nicht an industrielle oder andere Unternehmen vergeben werden, die in einem Nicht-EU-Mitgliedstaat eingetragen sind, der mit der EU kein Geheimschutzabkommen geschlossen hat.

24. Der Auftragnehmer ist dafür verantwortlich, sicherzustellen, dass alle im Rahmen von Unteraufträgen vergebenen Tätigkeiten im Einklang mit den Mindeststandards dieses Beschlusses ausgeführt werden; er stellt einem Unterauftragnehmer EU-VS nicht ohne die vorherige schriftliche Einwilligung der Vergabebehörde zur Verfügung.

25. Für EU-VS, die von einem Auftragnehmer oder Unterauftragnehmer herausgegeben oder bearbeitet werden, werden die dem Herausgeber obliegenden Rechte von der Vergabebehörde ausgeübt.

VI. BESUCHE IM ZUSAMMENHANG MIT ALS VERSCHLUSSSACHE EINGESTUFTEN AUFTRÄGEN

26. Benötigen der EAD, die Auftragnehmer oder die Unterauftragnehmer zur Ausführung eines als Verschlusssache eingestuften Auftrags Zugang zu Informationen des Geheimhaltungsgrads „CONFIDENTIEL UE/EU CONFIDENTIAL“ oder „SECRET UE/EU SECRET“ in den Räumlichkeiten des jeweils anderen, werden im Benehmen mit der jeweiligen nationalen Sicherheitsbehörde/beauftragten Sicherheitsbehörde oder einer sonstigen zuständigen Sicherheitsbehörde Besuche vereinbart. Dies lässt die Befugnis der Nationalen Sicherheitsbehörden/Beauftragten Sicherheitsbehörden unberührt, im Zusammenhang mit spezifischen Projekten ein Verfahren zu vereinbaren, nach dem Besuche unmittelbar verabredet werden können.

27. Alle Besucher müssen über eine entsprechende PSC verfügen und im Hinblick auf den Zugang zu EU-VS in Verbindung mit dem Auftrag des EAD dem Erfordernis „Kenntnis nur, wenn nötig“ genügen.

28. Die Besucher erhalten nur Zugang zu EU-VS, die mit dem Zweck des Besuchs in Beziehung stehen.

VII. ÜBERMITTLUNG UND BEFÖRDERUNG VON EU-VS

29. Für die Übermittlung von EU-VS auf elektronischem Wege gelten die einschlägigen Bestimmungen von Anhang A Artikel 8 sowie von Anhang A IV.

30. Für die Beförderung von EU-VS gelten die einschlägigen Bestimmungen von Anhang A III im Einklang mit den innerstaatlichen Rechtsvorschriften.

31. Für die Beförderung von Verschlusssachen als Fracht gelten folgende Grundsätze bei der Festlegung der Sicherheitsvorkehrungen:

    a) Die Sicherheit muss vom Ausgangsort bis zum endgültigen Bestimmungsort in allen Phasen der Beförderung gewährleistet sein;

    b) das Schutzniveau für eine Sendung richtet sich nach dem höchsten Geheimhaltungsgrad des in der Sendung enthaltenen Materials;

    c) die Transportunternehmen benötigen einen FSC des entsprechenden Geheimhaltungsgrads, wenn sie in ihren Anlagen Verschlusssachen aufbewahren sollen. In solchen Fällen muss das Personal, das einen VS-Transport durchführt, gemäß Anhang A I entsprechend sicherheitsüberprüft sein;

d) vor jeder grenzüberschreitenden Verbringung von als „CONFIDENTIEL UE/EU CONFIDENTIAL“ oder „SECRET UE/EU SECRET“ eingestuftem Material stellt der Absender einen Transportplan auf, der vom EAD — ggf. im Benehmen mit den nationalen Sicherheitsbehörde/beauftragten Sicherheitsbehörden in den Mitgliedstaaten, in denen der Absender und der Empfänger ihren Sitz haben, oder einer sonstigen zuständigen Sicherheitsbehörde — genehmigt wird;

e) die Beförderung erfolgt nach Möglichkeit ohne Umwege und wird so rasch abgeschlossen, wie es die Umstände erlauben;

f) nach Möglichkeit werden nur Transportrouten gewählt, die durch die Mitgliedstaaten führen. Transportrouten, die durch andere Staaten als Mitgliedstaaten führen, werden nur gewählt, wenn dies vom EAD oder von einer sonstigen zuständigen Sicherheitsbehörde sowohl des Staates des Absenders als auch des Staates des Empfängers genehmigt worden ist.

VIII. WEITERLEITUNG VON EU-VS AN AUFTRAGNEHMER IN DRITTSTAATEN

32. EU-VS werden an Auftragnehmer und Unterauftragnehmer in Drittstaaten, die über ein gültiges Gemeinschutzabkommen mit der EU verfügen, nach Maßgabe der Geheimschutzmaßnahmen weitergeleitet, die zwischen dem EAD als Vergabebehörde und der Nationalen Sicherheitsbehörde/Beauftragten Sicherheitsbehörde des betreffenden Drittstaats, in dem der Auftragnehmer eingetragen ist, vereinbart wurden.

IX. BEARBEITUNG UND AUFBEWAHRUNG VON ALS „RESTREINT UE/EU RESTRICTED“ EINGESTUFTEN VERSCHLUSSSACHEN

33. Gegebenenfalls im Benehmen mit der Nationalen Sicherheitsbehörde/Beauftragten Sicherheitsbehörde des Mitgliedstaats ist der EAD als Vergabebehörde berechtigt, Besuche in den Anlagen von Auftragnehmern/Unterauftragnehmern auf der Grundlage vertraglicher Bestimmungen durchzuführen, um zu überprüfen, ob die nach dem Vertrag erforderlichen einschlägigen Geheimschutzmaßnahmen zum Schutz von EU-VS des Geheimhaltungsgrads „RESTREINT UE/EU RESTRICTED“ getroffen wurden.

34. Soweit dies nach den innerstaatlichen Rechtsvorschriften erforderlich ist, werden die Nationalen Sicherheitsbehörden/Beauftragten Sicherheitsbehörden oder eine andere zuständige Sicherheitsbehörde vom EAD als Vergabebehörde über Aufträge oder Unteraufträge, die als „RESTREINT UE/EU RESTRICTED“ eingestufte Informationen enthalten, unterrichtet.

35. Bei Aufträgen des EAD mit Informationen des Geheimhaltungsgrads „RESTREINT UE/EU RESTRICTED“ ist ein FSC oder eine PSC für Auftragnehmer und Unterauftragnehmer und deren Personal nicht erforderlich.

36. Der EAD als Vergabebehörde prüft die Antworten auf Ausschreibungen bei Aufträgen, die Zugang zu Informationen des Geheimhaltungsgrads „RESTREINT EU/EU RESTRICTED“ erfordern, ungeachtet etwaiger Anforderungen in Bezug auf einen FSC oder eine PSC, die nach Maßgabe der innerstaatlichen Rechtsvorschriften gegebenenfalls bestehen.

37. Die Bedingungen für die Vergabe von Unteraufträgen durch den Auftragnehmer stehen im Einklang mit den Nummern 22-24.

38. Ist mit einem Auftrag die Bearbeitung von Verschlusssachen des Geheimhaltungsgrads „RESTREINT UE/EU RESTRICTED“ in einem Kommunikations- und Informationssystem verbunden, das von einem Auftragnehmer betrieben wird, so stellt der EAD als Vergabebehörde sicher, dass in dem Auftrag und etwaigen Unteraufträgen die notwendigen technischen und administrativen Anforderungen in Bezug auf die Akkreditierung des Kommunikations- und Informationssystems angegeben werden, die dem festgestellten Risiko entsprechen, wobei allen relevanten Faktoren Rechnung zu tragen ist. Der Umfang der Akkreditierung eines solchen Kommunikations- und Informationssystems ist von der Vergabebehörde mit der betreffenden nationalen Sicherheitsbehörde/beauftragten Sicherheitsbehörde zu vereinbaren.

ANHANG A VI

AUSTAUSCH VON VERSCHLUSSSACHEN MIT DRITTSTAATEN UND INTERNATIONALEN ORGANISATIONEN

I. EINLEITUNG

1. Dieser Anhang enthält die Bestimmungen zur Anwendung von Anhang A Artikel 10.

II. VEREINBARUNGEN FÜR DEN AUSTAUSCH VON VERSCHLUSSSACHEN

2. Der EAD kann gemäß Anhang A Artikel 10 Absatz 1 EU-VS mit Drittstaaten oder internationalen Organisationen austauschen.

   Bei der Wahrnehmung der Aufgaben nach Artikel 218 AEUV wird der Hohe Vertreter wie folgt unterstützt:

   a) Die zuständige geografische oder thematische Abteilung des EAD ermittelt in Rücksprache mit der für Sicherheit zuständigen Direktion des EAD den Bedarf an einem langfristigen Austausch von EU-VS mit dem betreffenden Drittstaat bzw. der betreffenden internationalen Organisation;

   b) die für Sicherheit zuständige Direktion des EAD legt — in Rücksprache mit der zuständigen geografischen Abteilung des EAD — dem Hohen Vertreter die Textentwürfe vor, die dem Rat im Einklang mit Artikel 218 Absätze 3, 5 und 6 AEUV vorgelegt werden sollen;

   c) die für Sicherheit zuständige Direktion des EAD unterstützt den Hohen Vertreter bei der Führung von Verhandlungen in Abstimmung mit den zuständigen Dienststellen der Kommission und des Generalsekretariats des Rates;

   d) in Bezug auf Abkommen oder Vereinbarungen mit Drittstaaten über deren Beteiligung an GSVP-Krisenbewältigungsoperationen nach Anhang A Artikel 10 Absatz 1 Buchstabe c Anhangs A legt die Direktion Krisenbewältigung und Planung des EAD in Rücksprache mit den zuständigen Dienststellen des EAD dem Hohen Vertreter die Textentwürfe vor, die dem Rat nach Artikel 218 Absätze 3, 5 und 6 AEUV vorgelegt werden sollen, und unterstützt den Hohen Vertreter bei der Führung von Verhandlungen in Abstimmung mit den zuständigen Dienststellen des EAD und des Generalsekretariats des Rates.

3. Sehen Geheimschutzabkommen die Vereinbarung von technischen Durchführungsbestimmungen zwischen der für Sicherheit zuständigen Direktion des EAD — in Rücksprache mit der Direktion Sicherheit der Generaldirektion Humanressourcen und Sicherheit der Kommission und dem Sicherheitsbüro des Generalsekretariats des Rates — und der zuständigen Sicherheitsbehörde des betreffenden Drittstaates oder der betreffenden internationalen Organisation vor, so tragen diese Durchführungsbestimmungen dem durch die Sicherheitsbestimmungen, -strukturen und -verfahren des Drittstaates bzw. der internationalen Organisation gewährleisteten Schutzniveau Rechnung.

4. Wenn langfristig die Notwendigkeit besteht, dass der EAD mit einem Drittstaat oder einer internationalen Organisation Verschlusssachen, die grundsätzlich höchstens in den Geheimhaltungsgrad „RESTREINT UE/EU RESTRICTED“ eingestuft sind, austauscht, und wenn festgestellt wird, dass die betreffende Vertragspartei nicht über ein ausreichend entwickeltes Sicherheitssystem verfügt, um ein Geheimschutzabkommen abschließen zu können, kann der Hohe Vertreter nach einstimmiger befürwortender Stellungnahme des Sicherheitsausschusses des EAD nach Artikel 15 Absatz 5 dieses Beschlusses eine Verwaltungsvereinbarung mit den zuständigen Sicherheitsbehörden des betreffenden Drittstaats oder der betreffenden internationalen Organisation schließen.

5. EU-VS werden nicht auf elektronischem Wege mit einem Drittstaat oder einer internationalen Organisation ausgetauscht, es sei denn, dies ist in dem Geheimschutzabkommen oder der Verwaltungsvereinbarung ausdrücklich vorgesehen.

6. Nach Maßgabe einer Verwaltungsvereinbarung über den Austausch von Verschlusssachen benennen der EAD und der betreffende Drittstaat bzw. die betreffende internationale Organisation ein Register, das als zentrale Stelle für den Ein- und Ausgang der austauschten Verschlusssachen dient. Für den EAD ist dies das EAD-Zentralregister.

7. Verwaltungsvereinbarungen werden in der Regel in Form eines Briefwechsels geschlossen.

III. BEWERTUNGSBESUCHE

8. Bewertungsbesuche gemäß Artikel 17 dieses Beschlusses werden im gegenseitigen Einvernehmen mit dem betreffenden Drittstaat bzw. der betreffenden internationalen Organisation durchgeführt und dienen zur Bewertung

   a) des für den Schutz von Verschlusssachen geltenden Rechtsrahmens,

   b) etwaiger besonderer Merkmale der Sicherheitsgesetze, -vorschriften, -strategien oder -verfahren des Drittstaates bzw. der internationalen Organisationen, die sich auf den höchsten Geheimhaltungsgrad der Verschlusssachen, die ausgetauscht werden dürfen, auswirken könnten,

   c) der derzeit zum Schutz von Verschlusssachen geltenden Sicherheitsmaßnahmen und -verfahren und

   d) der Verfahren für die Sicherheitsüberprüfung von Personal für den Geheimhaltungsgrad der EU-VS, die weitergegeben werden sollen.

9. Keine EU-Verschlusssachen werden ausgetauscht, bevor ein Bewertungsbesuch durchgeführt und die Ebene, auf der Verschlusssachen zwischen den Vertragsparteien ausgetauscht werden dürfen, auf der Grundlage der Gleichwertigkeit des gewährten Schutzniveaus bestimmt wurde.

   Sollte noch vor einem solchen Bewertungsbesuch der Hohe Vertreter auf außergewöhnliche oder dringende Gründe für den Austausch von Verschlusssachen aufmerksam gemacht werden, so

   a) holt der EAD die schriftliche Zustimmung des Herausgebers ein, um auszuschließen, dass es Gründe für die Nichtweitergabe der Verschlusssachen gibt, und

   b) verweist der EAD den Fall an die Sicherheitsbehörde des EAD, die die Weitergabe der Verschlusssachen beschließen kann, vorausgesetzt, dass die im Sicherheitsausschuss des EAD vertretenen Mitgliedstaaten einstimmig eine befürwortende Stellungnahme abgegeben haben.

   Kann der EAD den Herausgeber nicht ermitteln, so übernimmt die Sicherheitsbehörde des EAD die Verantwortung des Herausgebers, nachdem sie die einstimmige befürwortende Stellungnahme des Sicherheitsausschusses des EAD eingeholt hat.

IV. BEFUGNIS ZUR WEITERGABE VON EU-VS AN DRITTSTAATEN ODER INTERNATIONALE ORGANISATIONEN

10. Besteht bereits ein Rahmen für den Austausch von Verschlusssachen mit einem Drittstaat oder einer internationalen Organisation gemäß Anhang A Artikel 10 Absatz 1, so wird die Entscheidung zur Weitergabe von EU-VS an einen Drittstaat oder eine internationale Organisation durch den EAD von der Sicherheitsbehörde des EAD getroffen, die diese Befugnis an leitende EAD-Beamte oder andere ihr unterstehende Personen übertragen kann.

11. Handelt es sich beim Herausgeber der weiterzugebenden Verschlusssachen, einschließlich der Herausgeber des möglicherweise darin enthaltenen Quellenmaterials, nicht um den EAD, so holt der EAD zunächst die schriftliche Zustimmung des Herausgebers ein, um auszuschließen, dass Gründe für die Nichtweitergabe der Verschlusssachen bestehen. Kann der EAD den Herausgeber nicht ermitteln, so übernimmt die Sicherheitsbehörde des EAD die Verantwortung des Herausgebers, nachdem sie die einstimmige befürwortende Stellungnahme der im Sicherheitsausschuss des EAD vertretenen Mitgliedstaaten eingeholt hat.

V. AD-HOC-WEITERGABE VON EU-VERSCHLUSSSACHEN IN AUSNAHMEFÄLLEN

12. Ist kein Rahmen gemäß Anhang A Artikel 10 Absatz 1 vorhanden und ist die Weitergabe von EU-VS aus politischen, operativen oder dringenden Gründen im Interesse der EU oder eines oder mehrerer ihrer Mitgliedstaaten, so können EU-VS unter folgenden Voraussetzungen ausnahmsweise an einen Drittstaat oder eine internationale Organisation weitergegeben werden.

   Nachdem die für Sicherheit zuständige Direktion des EAD sichergestellt hat, dass die Bedingungen nach Nummer 11 erfüllt sind, ergreift sie folgende Maßnahmen:

   a) Sie vergewissert sich, soweit es möglich ist, zusammen mit den Sicherheitsbehörden des betreffenden Drittstaats oder der betreffenden internationalen Organisation, dass dessen bzw. deren Sicherheitsvorschriften, -strukturen und -verfahren so beschaffen sind, dass sie die Gewähr dafür bieten, dass die an ihn bzw. sie weitergegebenen EU-VS nach Maßgabe von Standards geschützt sind, die nicht weniger streng als die in diesem Beschluss festgelegten Standards sind;

b) sie ersucht den Sicherheitsausschuss des EAD, anhand der verfügbaren Informationen eine Stellungnahme im Hinblick auf die Vertrauenswürdigkeit der Sicherheitsvorschriften, -strukturen und -verfahren des Drittstaats bzw. der internationalen Organisation, an den/die die EU-VS weitergegeben werden sollen, zu formulieren;

c) sie verweist den Fall an die Sicherheitsbehörde des EAD, die die Weitergabe der Verschlusssachen beschließen kann, vorausgesetzt, dass die im Sicherheitsausschuss des EAD vertretenen Mitgliedstaaten einstimmig eine befürwortende Stellungnahme abgegeben haben.

13. Ist kein Rahmen gemäß Anhang A Artikel 10 Absatz 1 vorhanden, so verpflichtet sich der betreffende Dritte schriftlich zum angemessenen Schutz von EU-VS.

Anlage A

Begriffsbestimmungen

Für die Zwecke dieses Beschlusses bezeichnet der Ausdruck

„Akkreditierung" das Verfahren, das zu einer förmlichen Erklärung der Sicherheits-Akkreditierungsstelle (Security Accreditation Authority — SAA) führt, wonach ein System für den Betrieb mit einem definierten Geheimhaltungsgrad, in einem bestimmten Sicherheitsmodus in seiner Betriebsumgebung und bei einem akzeptablen Risikoniveau unter der Voraussetzung zugelassen wird, dass ein zugelassenes Bündel von Sicherheitsmaßnahmen in den Bereichen Technik, materieller Schutz, Organisation und Verfahren durchgeführt wird;

„Wert" alles, was für eine Organisation, ihre Tätigkeiten und deren Kontinuität von Nutzen ist, einschließlich der Informationsressourcen, auf die sich die Organisation bei der Wahrnehmung ihrer Aufgaben stützt;

„Ermächtigung zum Zugang zu EU-VS" eine Ermächtigung der Sicherheitsbehörde des EAD, die gemäß diesem Beschluss nach Ausstellung einer PSC durch die zuständigen Behörden eines Mitgliedstaats erteilt wird und mit der bescheinigt wird, dass einer Person, die nachweislich Kenntnis von Verschlusssachen haben muss, bis zu einem bestimmten Datum Zugang zu EU-VS bis zu einem bestimmten Geheimhaltungsgrad „CONFIDENTIEL UE/EU CONFIDENTIAL" oder höher) gewährt werden kann — siehe Anhang A I Artikel 2;

„Verletzung" eine Handlung oder Unterlassung seitens einer Person, die den in diesem Beschluss festgelegten Sicherheitsvorschriften und/oder den zu seiner Umsetzung notwendigen Sicherheitskonzepten oder -leitlinien zuwiderläuft;

„Lebenszyklus eines Kommunikations- und Informationssystems" die gesamte Lebensdauer eines Kommunikations- und Informationssystems, die Initiierung, Konzeption, Planung, Anforderungsanalyse, Entwurf, Entwicklung, Erprobung, Implementierung, Betrieb, Wartung und Außerbetriebnahme umfasst;

„als Verschlusssache eingestufter Auftrag" einen Vertrag zwischen dem EAD und einem Auftragnehmer über die Lieferung von Waren, die Durchführung von Arbeiten oder die Erbringung von Dienstleistungen, dessen Ausführung den Zugang zu oder die Erstellung von EU-VS erfordert oder mit sich bringt;

„als Verschlusssache eingestufter Unterauftrag" einen Vertrag zwischen einem Auftragnehmer des EAD und einem anderen Auftragnehmer (d. h. dem Unterauftragnehmer) über die Lieferung von Waren, die Durchführung von Arbeiten oder die Erbringung von Dienstleistungen, dessen Ausführung den Zugang zu oder die Erstellung von EU-VS erfordert oder mit sich bringt;

„Kommunikations- und Informationssystem" (Communication and Information System — CIS) ein System, das die Bearbeitung von Informationen in elektronischer Form ermöglicht. Zu einem Kommunikations- und Informationssystem gehören sämtliche für seinen Betrieb benötigten Werte, einschließlich der Infrastruktur, der Organisation, des Personals und der Informationsressourcen — siehe Anhang A Artikel 8 Absatz 2;

„Kenntnisnahme von EU-VS durch Unbefugte" die vollständige oder teilweise Offenlegung von EU-VS gegenüber nicht ermächtigten Personen oder Stellen — siehe Artikel 9 Absatz 2;

„Auftragnehmer" eine Einzelperson oder Rechtsperson, die geschäftsfähig ist;

„kryptografische Produkte" kryptografische Algorithmen, kryptografische Hardware- und Softwaremodule und Produkte, die Implementierungsdetails enthalten, sowie die dazugehörige Dokumentation und das Verschlüsselungsmaterial;

„GSVP-Operation" eine militärische oder zivile Krisenbewältigungsoperation nach Titel V Kapitel 2 EUV;

„Aufhebung der Geheimhaltungsgrads" die Löschung jeder Geheimhaltungskennzeichnung;

„mehrschichtige Sicherheit" die Anwendung einer Reihe von Sicherheitsmaßnahmen in Form eines mehrschichtigen Abwehrsystems;

„beauftragte Sicherheitsbehörde" eine Behörde, die gegenüber der nationalen Sicherheitsbehörde eines Mitgliedstaats für die Unterrichtung industrieller oder anderer Unternehmen über die nationale Politik in allen Fragen des Geheimschutzes in der Wirtschaft und für Weisungen und Unterstützung bei seiner Umsetzung verantwortlich ist. Die Funktion der beauftragten Sicherheitsbehörde kann von der nationalen Sicherheitsbehörde oder einer anderen zuständigen Behörde wahrgenommen werden;

„Dokument" jede aufgezeichnete Information, unabhängig von ihrer materiellen Form oder ihren Merkmalen;

„Herabstufung“ die Einstufung in einen niedrigeren Geheimhaltungsgrad;

„EU-Verschlusssachen“ (EU-VS) alle mit einem EU-Geheimhaltungsgrad gekennzeichneten Informationen oder Materialien, deren unbefugte Offenlegung den Interessen der Europäischen Union oder eines oder mehrerer ihrer Mitgliedstaaten in unterschiedlichem Maße schaden könnte — siehe Artikel 2 Buchstabe f;

„Sicherheitsbescheid für Unternehmen“ (Facility Security Clearance — FSC) die verwaltungsrechtliche Feststellung durch eine nationale Sicherheitsbehörde oder beauftragte Sicherheitsbehörde, dass ein Unternehmen unter dem Gesichtspunkt der Sicherheit ausreichenden Schutz für EU-VS eines bestimmten Geheimhaltungsgrads bietet und dass sein Personal, das Zugang zu EU-VS haben muss, ordnungsgemäß sicherheitsüberprüft ist und über die für den Zugang zu und den Schutz von EU-VS erforderlichen einschlägigen Sicherheitsanforderungen belehrt wurde;

„Bearbeitung“ von EU-VS alle möglichen Handlungen, denen EU-VS während der gesamten Dauer ihrer Einstufung als EU-VS unterliegen können. Sie umfasst die Erstellung, Verarbeitung, Beförderung, Herabstufung, Aufhebung des Geheimhaltungsgrads und Zerstörung. In Bezug auf Kommunikations- und Informationssysteme umfasst sie ferner die Sammlung, Darstellung, Übermittlung und Speicherung;

„Besitzer“ eine ordnungsgemäß ermächtigte Person, die nachweislich Kenntnis von Verschlusssachen haben muss und die im Besitz einer EU-VS ist und dementsprechend für deren Schutz verantwortlich zeichnet;

„industrielles oder anderes Unternehmen“ ein Unternehmen, das an der Lieferung von Waren, der Durchführung von Arbeiten oder der Erbringung von Dienstleistungen beteiligt ist; dabei kann es sich um Industrie-, Handels-, Dienstleistungs-, Wissenschafts-, Forschungs-, Bildungs- oder Entwicklungsunternehmen oder um Personen, die eine selbstständige Tätigkeit ausüben, handeln;

„gewerblicher Geheimschutz“ die Anwendung von Maßnahmen, die darauf abzielen, den Schutz von EU-VS durch Auftragnehmer oder Unterauftragnehmer während der Verhandlungen vor der Auftragsvergabe und während der Laufzeit des als Verschlusssache eingestuften Auftrags zu gewährleisten — siehe Anhang A Artikel 9 Absatz 1;

„Informationssicherung“ im Bereich von Kommunikations- und Informationssystemen das Vertrauen darauf, dass die in diesen Systemen bearbeiteten Informationen geschützt sind und dass diese Systeme jederzeit ordnungsgemäß funktionieren und von rechtmäßigen Nutzern kontrolliert werden. Eine effektive Informationssicherung stellt ein angemessenes Niveau der Vertraulichkeit, Integrität, Verfügbarkeit, Beweisbarkeit und Authentizität sicher. Die Informationssicherung stützt sich auf einen Prozess des Risikomanagements — siehe Anhang A Artikel 8 Absatz 1;

„Zusammenschaltung“ die direkte Verbindung von zwei oder mehr IT-Systemen zum Zweck der gemeinsamen Nutzung von Daten und anderen Informationsressourcen (beispielsweise Kommunikation); die Verbindung kann unidirektional oder multidirektional sein — siehe Anhang A IV Nummer 31;

„Verwaltung von Verschlusssachen“ die Anwendung administrativer Maßnahmen zur Kontrolle von EU-VS während der gesamten Dauer ihrer Einstufung als EU-VS mit dem Ziel, die Maßnahmen nach den Artikeln 5, 6 und 8 zu ergänzen und dadurch dazu beizutragen, die beabsichtigte oder unbeabsichtigte Kenntnisnahme von Verschlusssachen durch Unbefugte sowie den Verlust von Verschlusssachen zu verhindern oder aufzudecken und entsprechende Maßnahmen zur Wiederherstellung der Sicherheit zu treffen. Diese Maßnahmen beziehen sich insbesondere auf die Erstellung, die Registrierung, die Vervielfältigung, die Übersetzung, die Beförderung, die Bearbeitung, die Aufbewahrung und die Vernichtung von EU-VS — siehe Anhang A Artikel 7 Absatz 1;

„Material“ Dokumente, Geräte oder Ausrüstungsgegenstände jeder Art, die bereits hergestellt oder noch in der Herstellung befindlich sind;

„Herausgeber“ das Organ, die Agentur oder die Einrichtung der EU, der Mitgliedstaat, der Drittstaat oder die internationale Organisation, unter dessen/deren Aufsicht Verschlusssachen erstellt und/oder in die Strukturen der EU eingebracht wurden;

„personeller Geheimschutz“ die Anwendung von Maßnahmen, mit denen gewährleistet wird, dass nur Personen Zugang zu EU-VS erhalten, die

— Kenntnis von EU-VS haben müssen,

— für den Zugang zu als „CONFIDENTIEL UE/EU CONFIDENTIAL“ oder höher eingestuften Verschlusssachen sicherheitsüberprüft oder auf andere Weise aufgrund ihrer Tätigkeit nach Maßgabe der innerstaatlichen Rechtsvorschriften ordnungsgemäß ermächtigt sind und

— über ihre Verantwortlichkeiten belehrt worden sind —

siehe Anhang A Artikel 5 Absatz 1;

„Erklärung über die Sicherheitsüberprüfung von Personal“ (Personnel Security Clearance — PSC) mit Blick auf den Zugang zu EU-VS eine Erklärung einer zuständigen Behörde eines Mitgliedstaats, die nach Abschluss einer Sicherheitsüberprüfung durch die zuständigen Behörden eines Mitgliedstaats abgegeben wird und mit der bescheinigt wird, dass einer Person, die nachweislich Kenntnis von Verschlusssachen haben muss, bis zu einem bestimmten Datum und bis zu einem bestimmten Geheimhaltungsgrad („CONFIDENTIEL UE/EU CONFIDENTIAL“ oder höher) Zugang zu EU-VS gewährt werden kann; diese Person wird als „sicherheitsüberprüft“ bezeichnet;

„Sicherheitsüberprüfungsbescheinigung“ (Personnel Security Clearance Certificate — PSCC) eine von einer zuständigen Behörde ausgestellte Bescheinigung, in der festgestellt wird, dass eine Person sicherheitsüberprüft ist und eine gültige PSC oder gültige Ermächtigung des Leiters der für Sicherheit zuständigen Direktion für den Zugang zu EU-VS besitzt, und aus der der Geheimhaltungsgrad („CONFIDENTIEL UE/EU CONFIDENTIAL“ oder höher), bis zu dem der Person Zugang zu EU-VS gewährt werden kann, die Gültigkeitsdauer der betreffenden PSC und das Ablaufdatum der Bescheinigung selbst hervorgehen;

„materieller Geheimschutz“ die Anwendung von physischen und technischen Schutzmaßnahmen zur Verhinderung des unbefugten Zugangs zu EU-VS - siehe Anhang A Artikel 6;

„Sicherheitsanweisung für das Programm/Projekt“ eine Liste von Sicherheitsverfahren, die für ein spezifisches Programm/Projekt verwendet werden, um die Sicherheitsverfahren zu vereinheitlichen. Sie kann im Verlauf des Programms/Projekts überarbeitet werden;

„Registrierung“ die Durchführung von Verfahren, bei denen jede Phase des Lebenszyklus der Informationen, auch deren Verbreitung und Vernichtung, aufgezeichnet wird — siehe Anhang A III Nummer 21;

„Restrisiko“ das nach dem Ergreifen von Sicherheitsmaßnahmen verbleibende Risiko, falls nicht alle Bedrohungen erfasst werden und nicht alle Schwachstellen beseitigt werden können;

„Risiko“ die Möglichkeit, dass bei einer bestimmten Bedrohung die internen und externen Schwachstellen einer Organisation oder eines der von ihr verwendeten Systeme ausgenutzt und dadurch die Organisation und ihre materiellen und immateriellen Werte geschädigt werden. Gemessen wird das Risiko als die Kombination der Wahrscheinlichkeit des Eintretens von Bedrohungen und ihrer Auswirkungen;

„Risikoakzeptanz“ die Hinnahme der Möglichkeit, dass nach der Risikobehandlung ein Restrisiko bleibt;

„Risikobewertung“ die Ermittlung von Bedrohungen und Schwachstellen und die Durchführung diesbezüglicher Risikoanalysen, d. h. die Analyse der Eintrittswahrscheinlichkeit und der Auswirkungen;

„Risikokommunikation“ die Sensibilisierung der Nutzer eines Kommunikations- und Informationssystems für Risiken, die Unterrichtung von Zulassungsstellen über Risiken und die entsprechende Berichterstattung an die für den Betrieb zuständigen Stellen;

„Risikomanagementprozess“ den gesamten Prozess der Ermittlung, Kontrolle und Minimierung möglicher Zwischenfälle, die die Sicherheit einer Organisation oder eines der von ihr benutzten Systeme beeinträchtigen könnten. Darunter fallen sämtliche risikobezogenen Tätigkeiten, einschließlich der Risikobewertung, -behandlung, -akzeptanz und -kommunikation;

„Risikobehandlung“ die Minderung, Beseitigung, Verringerung (durch eine geeignete Kombination von technischen, physischen, organisatorischen oder verfahrenstechnischen Maßnahmen), Übertragung oder Überwachung des Risikos;

„Geheimschutzklausel“ (Security Aspects Letter — SAL) besondere Auftragsbedingungen der Vergabebehörde, die fester Bestandteil eines als Verschlusssache eingestuften und mit dem Zugang zu oder der Erstellung von EU-VS verbundenen Auftrags sind und in denen die Sicherheitsanforderungen oder die sicherheitsschutzbedürftigen Teile des Auftrags festgelegt sind — siehe Anhang A V Abschnitt II;

„VS-Einstufungsliste“ (Security Classification Guide — SCG) ein Dokument, das die als Verschlusssache eingestuften Teile eines Programms oder Auftrags beschreibt und in dem die anzuwendenden Geheimhaltungsgrade angegeben sind. Die VS-Einstufungsliste kann während der Laufzeit des Programms oder Auftrags erweitert werden, und Teile der Informationen können neu eingestuft oder herabgestuft werden; sofern eine VS-Einstufungsliste besteht, bildet sie Teil der Geheimschutzklausel — siehe Anhang A V Abschnitt II;

„Sicherheitsüberprüfung“ ein Untersuchungsverfahren, das von der zuständigen Behörde eines Mitgliedstaats nach den innerstaatlichen Rechtsvorschriften durchgeführt wird, um Gewissheit darüber zu erlangen, dass über die betreffende Person keine nachteiligen Erkenntnisse vorliegen, die der Ausstellung einer nationalen oder einer EU-PSC für den Zugang zu EU-VS bis zu einem bestimmten Geheimhaltungsgrad („CONFIDENTIEL UE/EU CONFIDENTIAL“ oder höher) entgegenstehen würden;

„sicherheitsbezogene Betriebsverfahren“ (Security Operating Procedures — SecOPs) Beschreibung des geplanten Sicherheitskonzepts, der Betriebsverfahren und der Zuständigkeit des Personals;

„nicht als VS eingestufte vertrauliche Informationen“ Materialien oder Informationen, die der EAD aufgrund rechtlicher Verpflichtungen aus den Verträgen oder aus zu deren Durchführung erlassenen Rechtsakten und/oder wegen ihrer Vertraulichkeit schützen muss. Zu vertraulichen Informationen, die nicht zu den Verschlusssachen zählen, gehören unter anderem Materialien oder Informationen, die unter das Berufsgeheimnis gemäß Artikel 339 AEUV fallen, die zu den nach Artikel 4 der Verordnung (EG) Nr. 1049/2001 des Europäischen Parlaments und des Rates [1] in Verbindung mit der einschlägigen Rechtsprechung des Gerichtshofs der Europäischen Union geschützten Interessen zu rechnen sind oder die zu den personenbezogenen Daten zählen, die unter die Verordnung (EG) Nr. 45/2001 fallen;

„Aufstellung der systemspezifischen Sicherheitsanforderungen“ verbindliche Sicherheitsgrundsätze und detaillierte Sicherheitsanforderungen, die als Grundlage für die Zertifizierung und Akkreditierung von Kommunikations- und Informationssystemen dienen;

„TEMPEST“ die Ermittlung, Analyse und Kontrolle kompromittierender elektromagnetischer Abstrahlung und die Vorkehrungen, um diese zu unterdrücken;

„Bedrohung“ eine potenzielle Ursache für einen unerwünschten Vorfall, der zu einem Schaden für eine Organisation oder eines der von ihr benutzten Systeme führen kann; solche Bedrohungen können unbeabsichtigt oder beabsichtigt (böswillig) sein und unterscheiden sich nach den Bedrohungselementen, potenziellen Zielen und Angriffsmethoden;

„Schwachstelle“ das Vorliegen einer beliebigen, die bei einer oder mehreren Bedrohungen ausgenutzt werden kann. Eine Schwachstelle kann durch ein Versäumnis entstehen oder sie kann sich auf eine Schwäche durch nachlässige, unvollständige oder inkohärente Kontrollen beziehen und kann die Technik, die Verfahren, die materiellen Eigenschaften, die Organisation oder den Betrieb betreffen.

---

[1] Verordnung (EG) Nr. 1049/2001 des Europäischen Parlaments und des Rates vom 30. Mai 2001 über den Zugang der Öffentlichkeit zu Dokumenten des Europäischen Parlaments, des Rates und der Kommission (ABl. L 145 vom 31.5.2001, S. 43).

Anlage B

Gleichwertigkeit der Geheimhaltungsgrade

EU	TRÈS SECRET UE/EU TOP SECRET	TRÈS SECRET UE/EU TOP SECRET,	CONFIDENTIEL UE/EU CONFIDENTIAL	RESTREINT UE/EU REST-RICTED:
EURATOM	EURA TOP SECRET	EURA SECRET	EURA CONFIDENTIAL	EURA RESTRICTED
Belgien	Très Secret (Loi 11.12.1998) Zeer Geheim (Wet 11.12.1998)	Secret (Loi 11.12.1998) Geheim (Wet 11.12.1998)	Confidentiel (Loi 11.12.1998) Vertrouwelijk (Gesetz vom 11.12.1998)	siehe Fußnote (1)
Bulgarien	Строго секретно	Секретно	Поверително	За служебно ползване
Tschechische Republik	Přísně tajné	Tajné	Důvěrné	Vyhrazené
Dänemark	Yderst hemmeligt	Hemmeligt	Fortroligt	Til tjenestebrug
Deutschland	STRENG GEHEIM	GEHEIM	VS (2) — VERTRAULICH	VS — NUR FÜR DEN DIENSTGEBRAUCH
Estland	Täiesti salajane	Salajane	Konfidentsiaalne	Piiratud
Irland	Top Secret	Secret	Confidential	Restricted
Griechenland	Άκρως Απόρρητο Abk.: ΑΑΠ	Απόρρητο Abk.: (ΑΠ)	Εμπιστευτικό Abk.: (ΕΜ)	Περιορισμένης Χρήσης Abk.: (ΠΧ)
Spanien	SECRETO	RESERVADO	CONFIDENCIAL	DIFUSIÓN LIMITADA
Frankreich	Très Secret Défense	Secret Défense	Confidentiel Défense	siehe Fußnote (3)
Kroatien	VRLO TAJNO	TAJNO	POVJERLJIVO	OGRANIČENO
Italien	Segretissimo	Segreto	Riservatissimo	Riservato
Zypern	Άκρως ΑπόρρητοAbk.: (ΑΑΠ)	ΑπόρρητοAbk.: (ΑΠ)	ΕμπιστευτικόAbk.: (ΕΜ)	Περιορισμένης ΧρήσηςAbk.: (ΠΧ)
Lettland	Sevišķi slepeni	Slepeni	Konfidenciāli	Dienesta vajadzībām
Litauen	Visiškai slaptai	Slaptai	Konfidencialiai	Riboto naudojimo
Luxemburg	Très Secret Lux	Secret Lux	Confidentiel Lux	Restreint Lux
Ungarn	„Szigorúan titkos!“	„Titkos!“	„Bizalmas!“	„Korlátozott terjesztésű!“
Malta	L-Ogħla Segretezza	Sigriet	Kunfidenzjali	Ristrett
Niederlande	Stg. ZEER GEHEIM	Stg. GEHEIM	Stg. CONFIDENTIEEL	Dep. VERTROUWELIJK
Österreich	Streng Geheim	Geheim	Vertraulich	Eingeschränkt
Polen	Ściśle Tajne	Tajne	Poufne	Zastrzeżone
Portugal	Muito Secreto	Secreto	Confidencial	Reservado

EU	TRÈS SECRET UE/EU TOP SECRET	TRÈS SECRET UE/EU TOP SECRET,	CONFIDENTIEL UE/EU CONFIDENTIAL	RESTREINT UE/EU REST-RICTED:
Rumänien	Strict secret de importanță deosebită	Strict secret	Secret	Secret de serviciu
Slowenien	Strogo tajno	Tajno	Zaupno	Interno
Slowakei	Prísne tajné	Tajné	Dôverné	Vyhradené
Finnland	ERITTÄIN SALAINEN YTTERST HEMLIG	SALAINEN HEMLIG	LUOTTAMUKSELLINEN KONFIDENTIELL	KÄYTTÖ RAJOITETTU BEGRÄNSAD TILLGÅNG
Schweden (4)	HEMLIG/TOP SECRET HEMLIG AV SYNNERLIG BETYDELSE FÖR RIKETS SÄKERHET	HEMLIG/SECRET HEMLIG	HEMLIG/CONFIDENTIAL HEMLIG	HEMLIG/RESTRICTED HEMLIG
Vereinigtes Königreich	UK TOP SECRET	UK SECRET	Keine Entsprechung (5)	UK OFFICIAL - SENSITIVE

(1) „Diffusion Restreinte/Beperkte Verspreiding“ ist kein in Belgien verwendeter Geheimhaltungsgrad. Belgien bearbeitet und schützt die als „RESTREINT UE/EU RESTRICTED“ eingestuften Informationen in einer Weise, bei der die in den Sicherheitsvorschriften des Rates der Europäischen Union beschriebenen Standards und Verfahren nicht unterschritten werden.

(2) Deutschland: VS = Verschlusssache.

(3) Frankreich verwendet in seinem nationalen System nicht den Geheimhaltungsgrad „RESTREINT“. Frankreich bearbeitet und schützt die als „RESTREINT UE/EU RESTRICTED“ eingestuften Informationen in einer Weise, bei der die in den Sicherheitsvorschriften des Rates der Europäischen Union beschriebenen Standards und Verfahren nicht unterschritten werden.

(4) Schweden: Die in der oberen Reihe aufgeführten Geheimhaltungsgrade werden von den Verteidigungsbehörden verwendet, die in der unteren Reihe aufgeführten Geheimhaltungsgrade von den anderen Behörden.

(5) Das Vereinigte Königreich bearbeitet und schützt die als „CONFIDENTIEL UE/EU CONFIDENTIAL“ eingestuften EU-VS gemäß den Anforderungen der Sicherheitsvorschriften für den Geheimhaltungsgrad „UK SECRET“.

ISSN 1977-088X (elektronische Ausgabe)
ISSN 1725-2407 (Papierausgabe)

Amt für Veröffentlichungen der Europäischen Union
2985 Luxemburg
LUXEMBURG

DE