►**B**

BESCHLUSS DES RATES

vom 23. September 2013

über die Sicherheitsvorschriften für den Schutz von EU-Verschlusssachen

(2013/488/EU)

(ABl. L 274 vom 15.10.2013, S. 1)

Geändert durch:

		Amtsblatt		
		Nr.	Seite	Datum
►**M1**	Beschluss 2014/233/EU des Rates vom 14. April 2014	L 125	72	26.4.2014
►**M2**	Beschluss (EU) 2019/2247 des Rates vom 19. Dezember 2019	L 336	291	30.12.2019
►**M3**	Beschluss (EU) 2021/1075 des Rates vom 21. Juni 2021	L 233	1	1.7.2021

Berichtigt durch:

►**C1**	Berichtigung, ABl. L 31 vom 7.2.2015, S. 33 (2013/488/EU)

▼B

BESCHLUSS DES RATES

vom 23. September 2013

über die Sicherheitsvorschriften für den Schutz von EU-Verschlusssachen

(2013/488/EU)

Artikel 1

Gegenstand, Anwendungsbereich und Begriffsbestimmungen

(1) Dieser Beschluss legt Grundprinzipien und Mindeststandards für die Sicherheit in Bezug auf den Schutz von EU-VS fest.

(2) Diese Grundprinzipien und Mindeststandards gelten für den Rat und das Generalsekretariat des Rates und werden von den Mitgliedstaaten nach Maßgabe ihrer jeweiligen innerstaatlichen Rechtsvorschriften beachtet, damit alle Seiten darauf vertrauen können, dass ein gleichwertiges Schutzniveau für EU-VS gewährleistet ist.

(3) Für die Zwecke dieses Beschlusses gelten die Begriffsbestimmungen in Anlage A.

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 Weitergabe 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 Weitergabe 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 Weitergabe 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 Weitergabe den wesentlichen Interessen der Europäischen Union oder eines oder mehrerer Mitgliedstaaten Schaden zufügen könnte;

d) RESTREINT UE/EU RESTRICTED: Informationen und Materialien, ►C1 deren unbefugte Weitergabe für die Interessen der Europäischen Union oder eines oder mehrerer Mitgliedstaaten nachteilig sein könnte. ◄

▼B

(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) Die zuständigen Behörden gewährleisten, dass EU-VS angemessen eingestuft werden, deutlich als Verschlusssache gekennzeichnet sind und den jeweiligen Geheimhaltungsgrad nur so lange behalten, wie es erforderlich ist.

(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) Der Rat billigt ein Sicherheitskonzept für die Erstellung von EU-VS, das auch einen praktischen Einstufungsleitfaden für Verschlusssachen umfasst.

Artikel 4

Schutz von Verschlusssachen

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

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

(3) Gibt ein Mitgliedstaat Verschlusssachen, die mit einem nationalen Geheimhaltungsgrad gekennzeichnet sind, in die Strukturen oder Netze der Union, so schützen der Rat und das Generalsekretariat des Rates diese Verschlusssachen nach den Anforderungen, die für EU-VS der entsprechenden Geheimhaltungsstufe gemäß der Entsprechungstabelle der Geheimhaltungsgrade in Anlage B gelten.

(4) Eine Gesamtheit von EU-VS kann ein Schutzniveau erfordern, das einem höheren Geheimhaltungsgrad als dem der einzelnen Bestandteile der Gesamtheit entspricht.

Artikel 5

Sicherheitsrisikomanagement

(1) Das Risikomanagement für EU-VS wird als Prozess angelegt. Ziel dieses Prozesses ist es, bekannte Sicherheitsrisiken zu bestimmen, Sicherheitsmaßnahmen zur Reduzierung dieser Risiken auf ein tragbares Maß gemäß den Grundprinzipien und Mindeststandards dieses Beschlusses festzulegen und diese Maßnahmen entsprechend dem Konzept der mehrschichtigen Sicherheit gemäß Anlage A anzuwenden. Die Wirksamkeit der betreffenden Maßnahmen wird fortlaufend bewertet.

▼B

(2) Die Sicherheitsmaßnahmen für den Schutz von EU-VS müssen während der gesamten Dauer ihrer Einstufung als EU-VS insbesondere dem Geheimhaltungsgrad, der Form und dem Umfang der Informationen und des Materials, der Lage und der Beschaffenheit der Anlagen, in denen EU-VS untergebracht sind, und der örtlichen Einschätzung der Bedrohung durch feindselige und/oder kriminelle Handlungen, einschließlich Spionage, Sabotage oder Terrorakte, entsprechen.

(3) In Notfallplänen wird berücksichtigt, dass EU-VS in Notsituationen geschützt werden müssen, damit der unbefugte Zugang, die unbefugte Weitergabe oder der Verlust der Integrität beziehungsweise der Verfügbarkeit verhindert werden.

(4) In Kontinuitätsplänen sind Präventions- und Wiederherstellungsmaßnahmen vorzusehen, damit die Auswirkungen größerer Störungen oder Zwischenfälle auf die Bearbeitung und Aufbewahrung von EU-VS so gering wie möglich gehalten werden.

Artikel 6

Anwendung dieses Beschlusses

(1) Soweit erforderlich, billigt der Rat auf Empfehlung des Sicherheitsausschusses Sicherheitskonzepte mit Maßnahmen zur Anwendung dieses Beschlusses.

(2) Der Sicherheitsausschuss kann auf seiner Ebene Sicherheitsleitlinien zur Ergänzung oder Untermauerung dieses Beschlusses und etwaiger vom Rat gebilligter Sicherheitskonzepte vereinbaren.

Artikel 7

Personeller Geheimschutz

(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,

— erforderlichenfalls einer Sicherheitsüberprüfung für die entsprechende Geheimhaltungsstufe unterzogen worden sind und

— über ihre Verantwortlichkeiten belehrt worden sind.

(2) Die Verfahren für die Sicherheitsüberprüfung des Personals dienen der Feststellung, ob eine Person unter Berücksichtigung ihrer Loyalität, Vertrauenswürdigkeit und Zuverlässigkeit zum Zugang zu EU-VS ermächtigt werden kann.

(3) Alle Personen im Generalsekretariat des Rates, für deren Aufgabenwahrnehmung der Zugang zu als „CONFIDENTIEL UE/EU CONFIDENTIAL“ oder höher eingestuften EU-VS oder deren Bearbeitung erforderlich ist, werden einer Sicherheitsüberprüfung für die entsprechende Geheimhaltungsstufe unterzogen, bevor ihnen Zugang zu diesen EU-VS gewährt wird. Diese Personen müssen von der Anstellungsbehörde des Generalsekretariats des Rates zum Zugang zu EU-VS bis zu einem bestimmten Geheimhaltungsgrad und bis zu einem bestimmten Zeitpunkt ermächtigt werden.

▼B

(4) Das Personal der Mitgliedstaaten nach Artikel 15 Absatz 3, das zur Wahrnehmung seiner Aufgaben gegebenenfalls Zugang zu als „CONFIDENTIEL UE/EU CONFIDENTIAL“ oder höher eingestuften EU-VS erhalten muss, wird nach Maßgabe der innerstaatlichen Rechtsvorschriften einer Sicherheitsüberprüfung für den entsprechenden Geheimhaltungsgrad unterzogen oder aufgrund seines Aufgabenbereichs auf andere Weise ordnungsgemäß ermächtigt, bevor ihm Zugang zu diesen EU-VS gewährt wird.

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

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

Artikel 8

Materieller Geheimschutz

(1) Der materielle Geheimschutz beinhaltet die Anwendung von materiellen und technischen Schutzmaßnahmen, damit ein unbefugter Zugang zu EU-VS verhindert wird.

(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 den Einsatz von Personal in Bezug auf den Zugang zu EU-VS 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 Gebäude, Büros, Räume und sonstigen Bereiche, in denen EU-VS bearbeitet bzw. aufbewahrt werden, getroffen, einschließlich Bereiche, in denen Kommunikations- und Informationssysteme gemäß Artikel 10 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 II eingerichtet und von der zuständigen Sicherheitsbehörde 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 II enthalten.

▼B

Artikel 9

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 7, 8 und 10 zu ergänzen und dadurch dazu beizutragen, die beabsichtigte oder unbeabsichtigte Kenntnisnahme von Verschlusssachen durch Unbefugte sowie den Verlust von Verschlusssachen zu verhindern und festzustellen. Diese Maßnahmen beziehen sich insbesondere auf die Erstellung, die Registrierung, die Vervielfältigung, die Übersetzung, die Herabstufung, die Aufhebung des Geheimhaltungsgrads, die Beförderung und die Vernichtung von EU-VS.

(2) Als „CONFIDENTIEL UE/EU CONFIDENTIAL“ oder höher eingestufte Verschlusssachen werden zu Sicherheitszwecken vor der Weiterleitung und bei Empfang registriert. Zu diesem Zweck richten die zuständigen Stellen im Generalsekretariat des Rates und in den Mitgliedstaaten ein Registratursystem ein. Als „TRÈS SECRET UE/EU TOP SECRET“ eingestufte Verschlusssachen werden in eigens dafür bestimmten Registraturen vereinnahmt.

(3) In Dienststellen und Räumlichkeiten, in denen EU-VS bearbeitet oder aufbewahrt werden, sind regelmäßig Inspektionen durch die zuständige Sicherheitsbehörde 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 gemäß Artikel 10 Absatz 6 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 10 Absatz 6 zugelassen wurden, oder

   ii) in allen anderen Fällen gemäß den Vorschriften der zuständigen Sicherheitsbehörde im Einklang mit den einschlägigen Schutzmaßnahmen des Anhangs III.

(5) Die Bestimmungen zur Anwendung dieses Artikels sind in den Anhängen III und IV enthalten.

Artikel 10

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

(1) Informationssicherung (Information Assurance, IA) im Bereich von Kommunikations- und Informationssystemen beinhaltet das 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.

▼B

(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 Voraussetzungen, einschließlich der Infrastruktur, der Organisation, des Personals und der Informationsressourcen. Dieser Beschluss gilt für Kommunikations- und Informationssysteme, mit denen EU-VS bearbeitet werden.

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

(4) Alle Kommunikations- und Informationssysteme 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 erreicht wird. In der Akkreditierungserklärung wird festgelegt, bis zu welchem Geheimhaltungsgrad und unter welchen Voraussetzungen Verschlusssachen in dem Kommunikations- und Informationssystem bearbeitet werden dürfen.

(5) Es werden Sicherungsmaßnahmen getroffen, um Kommunikations- und Informationssysteme, in denen als „CONFIDENTIEL UE/EU CONFIDENTIAL“ und höher eingestufte Verschlusssachen bearbeitet werden, so zu schützen, dass von den betreffenden Informationen nicht über unbeabsichtigte elektromagnetische Abstrahlung unbefugt Kenntnis genommen werden kann („TEMPEST-Sicherheitsvorkehrungen“). Diese Sicherheitsmaßnahmen müssen dem Risiko der Ausnutzung und dem Geheimhaltungsgrad der Informationen entsprechen.

(6) Wird der Schutz von EU-VS mit kryptografischen Produkten sichergestellt, so sind diese Produkte folgendermaßen zuzulassen:

a) Die Vertraulichkeit von als „SECRET UE/EU SECRET“ und höher eingestuften Verschlusssachen wird durch kryptografische Produkte geschützt, die vom Rat als Krypto-Zulassungsstelle (Crypto Approval Authority, CAA) auf Empfehlung des Sicherheitsausschusses zugelassen wurden;

b) die Vertraulichkeit von als „CONFIDENTIEL UE/EU CONFIDENTIAL“ oder „RESTREINT UE/EU RESTRICTED“ eingestuften Verschlusssachen wird durch kryptografische Produkte geschützt, die vom Generalsekretär des Rates (im Folgenden „Generalsekretär“) als CAA auf Empfehlung des Sicherheitsausschusses zugelassen wurden.

Ungeachtet des Buchstabens b kann die Vertraulichkeit von als „CONFIDENTIEL UE/EU CONFIDENTIAL“ oder „RESTREINT UE/EU RESTRICTED“ eingestuften EU-VS innerhalb der nationalen Systeme der Mitgliedstaaten durch kryptografische Produkte geschützt werden, die von der CAA eines Mitgliedstaats zugelassen wurden.

(7) Bei der Übermittlung von EU-VS auf elektronischem Wege werden zugelassene kryptografische Produkte verwendet. Ungeachtet dieser Anforderung können in Notsituationen spezielle Verfahren oder spezielle technische Konfigurationen nach Maßgabe des Anhangs IV angewendet werden.

▼B

(8) Die zuständigen Stellen des Generalsekretariats des Rates und der Mitgliedstaaten legen jeweils die folgenden Funktionen für Informationssicherung fest:

a) eine Stelle für Informationssicherung (IAA),

b) eine TEMPEST-Stelle (TA),

c) eine Krypto-Zulassungsstelle (CAA),

d) eine Krypto-Verteilungsstelle (CDA).

(9) Für jedes System legen die zuständigen Stellen des Generalsekretariats des Rates und der Mitgliedstaaten jeweils Folgendes fest:

a) eine Sicherheits-Akkreditierungsstelle (SAA),

b) eine für den Betrieb zuständige Stelle für Informationssicherung.

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

Artikel 11

Geheimschutz in der Wirtschaft

(1) Der Geheimschutz in der Wirtschaft beinhaltet die Anwendung von Maßnahmen, die darauf abzielen, den Schutz von EU-VS durch Auftragnehmer oder Subauftragnehmer während der Verhandlungen vor der Auftragsvergabe und während der gesamten Laufzeit des als Verschlusssache eingestuften Auftrags zu gewährleisten. Diese Aufträge beinhalten nicht den Zugang zu als „TRÈS SECRET UE/EU TOP SECRET“ eingestuften Verschlusssachen.

(2) Das Generalsekretariat des Rates kann industrielle oder andere Unternehmen, die in einem Mitgliedstaat oder in einem Drittstaat, der ein Abkommen oder eine Verwaltungsvereinbarung nach Artikel 13 Absatz 2 Buchstabe a oder b mit der EU geschlossen hat, eingetragen sind, vertraglich mit Aufträgen betrauen, die den Zugang zu oder die Bearbeitung oder Aufbewahrung von EU-VS beinhalten oder nach sich ziehen.

(3) Das Generalsekretariat des Rates 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.

(4) Die Nationale Sicherheitsbehörde (National Security Authority, NSA), die Beauftragte Sicherheitsbehörde (Designated Security Authority, DSA) oder eine andere zuständige Behörde jedes Mitgliedstaats stellt, soweit dies nach den innerstaatlichen Rechtsvorschriften möglich ist, sicher, dass in ihrem Hoheitsgebiet eingetragene Auftragnehmer und Subauftragnehmer alle geeigneten Maßnahmen zum Schutz von EU-VS bei den Verhandlungen vor der Auftragsvergabe oder bei der Ausführung eines als Verschlusssache eingestuften Auftrags treffen.

(5) Die Nationale Sicherheitsbehörde, die Beauftragte Sicherheitsbehörde oder eine sonstige zuständige Sicherheitsbehörde jedes Mitgliedstaats stellt gemäß den innerstaatlichen Rechtsvorschriften sicher, dass in dem jeweiligen Mitgliedstaat eingetragene Auftragnehmer und Subauftragnehmer, die an als Verschlusssache eingestuften Aufträgen oder Subaufträgen beteiligt sind, die den Zugang zu als „CONFIDENTIEL UE/EU CONFIDENTIAL“ oder „SECRET UE/EU SECRET“ eingestuften Verschlusssachen in ihren Räumlichkeiten erfordern, entweder bei der Ausführung dieser Aufträge oder bei den Verhandlungen vor der Auftragsvergabe im Besitz eines Sicherheitsbescheids für Unternehmen (Facility Security Clearance, FSC) der entsprechenden Geheimhaltungsstufe sind.

▼B

(6) Dem Personal des Auftragnehmers oder Subauftragnehmers, das zur Ausführung eines als Verschlusssache eingestuften Auftrags Zugang zu Informationen des Geheimhaltungsgrads „CONFIDENTIEL UE/EU CONFIDENTIAL“ oder „SECRET UE/EU SECRET“ erhalten muss, wird von der jeweiligen Nationalen Sicherheitsbehörde, der Beauftragten Sicherheitsbehörde oder einer sonstigen zuständigen Sicherheitsbehörde gemäß den innerstaatlichen Rechtsvorschriften und den Mindeststandards in Anhang I eine Sicherheitsermächtigung (Personnel Security Clearance, PSC) erteilt.

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

Artikel 12

Weitergabe von EU-VS

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

(2) 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 13

Austausch von Verschlusssachen mit Drittstaaten und internationalen Organisationen

(1) Entscheidet der Rat, dass EU-VS mit einem Drittstaat oder einer internationalen Organisation ausgetauscht werden müssen, so werden die hierfür erforderlichen rechtlichen Grundlagen geschaffen.

(2) Zur Festlegung dieser Grundlagen und der für beide Parteien geltenden Vorschriften für den Schutz von ausgetauschten Verschlusssachen

a) schließt die Union Abkommen mit Drittstaaten oder internationalen Organisationen über Sicherheitsverfahren für den Austausch und den Schutz von Verschlusssachen (im Folgenden „Geheimschutzabkommen“) oder

b) kann der Generalsekretär im Namen des Generalsekretariats des Rates Verwaltungsvereinbarungen gemäß Anhang VI Nummer 17 schließen, sofern die weiterzugebenden EU-VS in der Regel nicht höher als „RESTREINT UE/EU RESTRICTED“ eingestuft sind.

(3) Die Geheimschutzabkommen oder Verwaltungsvereinbarungen nach Absatz 2 enthalten Bestimmungen, mit denen sichergestellt wird, dass EU-VS nach Entgegennahme durch Drittstaaten oder internationale Organisationen in einer ihrem Geheimhaltungsgrad angemessenen Weise nach Maßgabe von Mindeststandards geschützt werden, die zumindest den in diesem Beschluss festgelegten Mindeststandards entsprechen.

▼B

(4) Der Beschluss, EU-VS des Rates an einen Drittstaat oder eine internationale Organisation weiterzugeben, wird vom Rat von Fall zu Fall nach Maßgabe von Art und Inhalt dieser Verschlusssachen, des Grundsatzes „Kenntnis nur, wenn nötig“ und der Vorteile für die Union gefasst. Sind die Verschlusssachen, um deren Weitergabe ersucht wird, nicht vom Rat herausgegeben worden, so holt das Generalsekretariat des Rates zunächst die schriftliche Zustimmung des Herausgebers zur Weitergabe der Verschlusssachen ein. Kann der Herausgeber nicht ermittelt werden, so trifft der Rat an seiner Stelle die Entscheidung.

(5) Zur Überprüfung der Wirksamkeit der Sicherheitsvorkehrungen, die Drittstaaten oder internationale Organisationen zum Schutz bereitgestellter oder ausgetauschter EU-VS getroffen haben, werden Bewertungsbesuche durchgeführt.

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

Artikel 14

Verletzungen der Sicherheit und Kenntnisnahme von EU-VS durch Unbefugte

(1) Zu einer Verletzung der Sicherheit kommt es durch eine Handlung oder Unterlassung seitens einer Person, die den in diesem Beschluss festgelegten Sicherheitsvorschriften zuwiderläuft.

(2) Eine Kenntnisnahme von EU-VS durch Unbefugte liegt vor, wenn EU-VS infolge einer Verletzung der Sicherheit ganz oder teilweise an unbefugte Personen weitergegeben wurden.

(3) Verletzungen oder vermutete Verletzungen der Sicherheit werden der zuständigen Sicherheitsbehörde unverzüglich gemeldet.

(4) Wird bekannt oder besteht berechtigter Grund zu der Annahme, dass EU-VS Unbefugten zur Kenntnis gelangt oder verloren gegangen sind, trifft die Nationale Sicherheitsbehörde oder sonstige zuständige Behörde nach Maßgabe der einschlägigen Rechtsvorschriften alle geeigneten Maßnahmen, um

a) den Herausgeber zu verständigen;

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

c) den potenziellen Schaden für die Interessen der Union oder der Mitgliedstaaten einzuschätzen;

d) die geeigneten Maßnahmen zu treffen, damit ein solcher Vorfall sich nicht wiederholt, und

e) die zuständigen Stellen über die getroffenen Maßnahmen zu unterrichten.

(5) Gegen jede Person, die für eine Verletzung der Sicherheitsvorschriften dieses Beschlusses verantwortlich ist, können disziplinarische Maßnahmen gemäß den geltenden Vorschriften ergriffen werden. Gegen jede Person, die für die Kenntnisnahme von EU-VS durch Unbefugte oder deren Verlust verantwortlich ist, können gemäß den geltenden Rechtsvorschriften Disziplinarmaßnahmen ergriffen und/oder rechtliche Schritte unternommen werden.

▼B

Artikel 15

Verantwortung für die Durchführung

(1) Der Rat ergreift alle erforderlichen Maßnahmen, um die insgesamt übereinstimmende Anwendung dieses Beschlusses sicherzustellen.

(2) Der Generalsekretär trifft alle erforderlichen Maßnahmen, um sicherzustellen, dass die Bestimmungen dieses Beschlusses bei der Bearbeitung und Aufbewahrung von EU-VS oder anderen Verschlusssachen in den vom Rat genutzten Räumlichkeiten und im Generalsekretariat des Rates von den Beamten und sonstigen Bediensteten des Generalsekretariats des Rates, von zum Generalsekretariat des Rates abgeordnetem Personal und von Vertragspartnern des Generalsekretariats des Rates angewandt werden.

(3) Die Mitgliedstaaten treffen nach Maßgabe ihrer jeweiligen innerstaatlichen Rechtsvorschriften alle geeigneten Maßnahmen, um sicherzustellen, dass dieser Beschluss bei der Bearbeitung und Aufbewahrung von EU-VS von dem folgenden Personenkreis eingehalten wird:

a) dem Personal der Ständigen Vertretungen der Mitgliedstaaten bei der Europäischen Union sowie den nationalen Delegierten, die an Tagungen des Rates oder Sitzungen seiner Vorbereitungsgremien teilnehmen bzw. in sonstige Tätigkeiten des Rates einbezogen sind;

b) sonstigem Personal in den nationalen Verwaltungen der Mitgliedstaaten, einschließlich des zu diesen Verwaltungen abgeordneten Personals, unabhängig davon, ob es innerhalb oder außerhalb des Hoheitsgebiets der Mitgliedstaaten Dienst tut;

c) sonstigen Personen, die in den Mitgliedstaaten aufgrund ihrer Aufgaben förmlich zum Zugang zu EU-VS ermächtigt worden sind, und

d) Vertragspartnern der Mitgliedstaaten, unabhängig davon, ob sie innerhalb oder außerhalb des Hoheitsgebiets der Mitgliedstaaten tätig sind.

Artikel 16

Organisation der Sicherheit im Rat

(1) Im Rahmen seiner Funktion bei der Gewährleistung der insgesamt übereinstimmenden Anwendung dieses Beschlusses billigt der Rat

a) Abkommen gemäß Artikel 13 Absatz 2 Buchstabe a;

b) Beschlüsse zur Genehmigung oder Zustimmung zu der Weitergabe von vom Rat herausgegebenen oder in seinem Besitz befindlichen EU-VS an Drittstaaten und internationale Organisationen im Einklang mit dem Grundsatz der Zustimmung des Herausgebers;

c) ein jährliches Programm für Bewertungsbesuche, das vom Sicherheitsausschuss empfohlen wird, für Besuche zur Bewertung von Dienststellen und Räumlichkeiten der Mitgliedstaaten und von Einrichtungen, Agenturen und Stellen der EU, die diesen Beschluss oder die darin enthaltenen Grundsätze anwenden, und für Bewertungsbesuche in Drittstaaten und bei internationalen Organisationen zur Überprüfung der Wirksamkeit der zum Schutz von EU-VS durchgeführten Maßnahmen und

▼B

d) Sicherheitskonzepte gemäß Artikel 6 Absatz 1.

(2) Der Generalsekretär ist die Sicherheitsbehörde des Generalsekretariats des Rates. In dieser Funktion

a) führt er das Sicherheitskonzept des Rates durch und überprüft es fortlaufend;

b) stimmt er sich mit den Nationalen Sicherheitsbehörden der Mitgliedstaaten zu allen Sicherheitsfragen ab, die den Schutz von Verschlusssachen betreffen, die für die Tätigkeiten des Rates relevant sind;

c) erteilt er Beamten und sonstigen Bediensteten des Generalsekretariats des Rates sowie abgeordneten nationalen Experten die Genehmigung gemäß Artikel 7 Absatz 3 für den Zugang zu als „CONFIDENTIEL UE/EU CONFIDENTIAL“ oder höher eingestuften Verschlusssachen;

d) ordnet er gegebenenfalls eine Untersuchung an, wenn feststeht oder vermutet wird, dass im Besitz des Rates befindliche oder vom Rat herausgegebene Verschlusssachen Unbefugten zur Kenntnis gelangt oder verloren gegangen sind, und ersucht die einschlägigen Sicherheitsbehörden um Unterstützung bei derartigen Untersuchungen;

e) führt er regelmäßige Inspektionen der Sicherheitsvorkehrungen durch, die zum Schutz von Verschlusssachen in den Räumlichkeiten des Generalsekretariats des Rates getroffen wurden;

f) führt er regelmäßige Besuche zur Bewertung der Sicherheitsvorkehrungen durch, die zum Schutz von EU-VS in Einrichtungen, Agenturen und Stellen der Union, die diesen Beschluss oder die darin enthaltenen Grundsätze anwenden, getroffen wurden;

g) führt er gemeinsam und im Einvernehmen mit den betreffenden Nationalen Sicherheitsbehörden regelmäßige Bewertungen der Sicherheitsvorkehrungen durch, die zum Schutz von EU-VS in Dienststellen und Räumlichkeiten der Mitgliedstaaten getroffen wurden;

h) sorgt er dafür, dass Sicherheitsmaßnahmen bei Bedarf mit den für den Schutz von Verschlusssachen zuständigen Behörden der Mitgliedstaaten und gegebenenfalls mit Drittstaaten oder internationalen Organisationen — auch hinsichtlich der Art der Bedrohungen der Sicherheit von EU-VS und entsprechender Schutzmaßnahmen — abgestimmt werden, und

i) schließt er die Verwaltungsvereinbarungen nach Artikel 13 Absatz 2 Buchstabe b.

Das Sicherheitsbüro des Generalsekretariats des Rates steht dem Generalsekretär bei diesen Aufgaben unterstützend zur Verfügung.

(3) Zur Durchführung von Artikel 15 Absatz 3 sollten die Mitgliedstaaten wie folgt verfahren:

a) Sie benennen eine Nationale Sicherheitsbehörde, wie in Anlage C aufgeführt, die für die Sicherheitsvorkehrungen zum Schutz von EU-VS zuständig ist, damit

   i) EU-VS, die sich im Besitz einer öffentlichen oder privaten Stelle oder Einrichtung ihres Landes im In- oder Ausland befinden, gemäß diesem Beschluss geschützt werden;

   ii) die Sicherheitsvorkehrungen für den Schutz von EU-VS regelmäßig überprüft oder bewertet werden;

▼B

iii) alle in einer nationalen Verwaltung oder von einem Auftragnehmer beschäftigten Personen, denen Zugang zu als „CONFIDENTIEL UE/EU CONFIDENTIAL“ oder höher eingestuften Verschlusssachen gewährt werden kann, einer ordnungsgemäßen Sicherheitsüberprüfung unterzogen oder auf anderer Grundlage nach Maßgabe der innerstaatlichen Rechtsvorschriften aufgrund ihres Aufgabenbereichs ordnungsgemäß ermächtigt worden sind;

iv) die Sicherheitsprogramme erstellt werden, die erforderlich sind, um das Risiko einer Kenntnisnahme von EU-VS durch Unbefugte oder eines Verlusts von EU-VS so gering wie möglich zu halten;

v) Sicherheitsfragen im Zusammenhang mit dem Schutz von EU-VS mit anderen auf nationaler Ebene zuständigen Stellen koordiniert werden, einschließlich jener, die in diesem Beschluss genannt werden, und

vi) Ersuchen um geeignete Sicherheitsüberprüfung nachgekommen wird, die insbesondere von Einrichtungen, Agenturen und Stellen, bei Operationen der Union, die im Rahmen des Titels V Kapitel 2 EUV geschaffen bzw. eingeleitet wurden, sowie von EU-Sonderbeauftragten und ihrem Personal, die diesen Beschluss oder die darin enthaltenen Grundsätze anwenden, gestellt werden.

b) Sie gewährleisten, dass ihre zuständigen Stellen ihre Regierung und — über diese — den Rat über die Art der Bedrohungen der Sicherheit von EU-VS und entsprechende Schutzmaßnahmen informieren und beraten.

Artikel 17

Sicherheitsausschuss

(1) Es wird ein Sicherheitsausschuss eingesetzt. Er prüft und bewertet Sicherheitsfragen, die in den Anwendungsbereich dieses Beschlusses fallen, und legt dem Rat gegebenenfalls Empfehlungen vor.

(2) Der Sicherheitsausschuss setzt sich aus Vertretern der Nationalen Sicherheitsbehörden der Mitgliedstaaten zusammen; ein Vertreter der Kommission und des EAD nimmt an den Sitzungen des Ausschusses teil. Den Vorsitz im Ausschuss führt der Generalsekretär oder eine von ihm beauftragte Person. Der Sicherheitsausschuss tritt gemäß dem vom Rat erteilten Mandat oder auf Antrag des Generalsekretärs oder einer Nationalen Sicherheitsbehörde zusammen.

Vertreter von Einrichtungen, Agenturen und Stellen der Union, die diesen Beschluss oder die darin enthaltenen Grundsätze anwenden, können zur Teilnahme an den Sitzungen eingeladen werden, wenn Fragen erörtert werden, die sie betreffen.

(3) Der Sicherheitsausschuss organisiert seine Tätigkeit so, dass er Empfehlungen zu speziellen Sicherheitsfragen geben kann. Er setzt eine Fachuntergruppe für Fragen der Informationssicherung und bei Bedarf weitere Fachuntergruppen ein. Er legt das Mandat für diese Fachuntergruppen fest und erhält von diesen Berichte über ihre Tätigkeit, die gegebenenfalls Empfehlungen an den Rat enthalten.

▼B

Artikel 18

Ersetzung des bisherigen Beschlusses

(1) Der Beschluss 2011/292/EU des Rates ([1]) wird durch den vorliegenden Beschluss aufgehoben und ersetzt.

(2) Alle gemäß dem Beschluss 2001/264/EG des Rates ([2]) und dem Beschluss 2011/292/EU eingestuften EU-VS werden weiter gemäß den einschlägigen Bestimmungen dieses Beschlusses geschützt.

Artikel 19

Inkrafttreten

Dieser Beschluss tritt am Tag seiner Veröffentlichung im *Amtsblatt der Europäischen Union* in Kraft.

([1]) Beschluss 2011/292/EU des Rates vom 31. März 2011 über die Sicherheitsvorschriften für den Schutz von EU-Verschlusssachen (ABl. L 131 vom 27.5.2011, S. 17).

([2]) Beschluss 2001/264/EG des Rates vom 19. März 2001 über die Annahme der Sicherheitsvorschriften des Rates (ABl. L 101 vom 11.4.2001, S. 1).

▼B

ANHÄNGE

ANHANG I

Personeller Geheimschutz

ANHANG II

Materieller Geheimschutz

ANHANG III

Verwaltung von Verschlusssachen

ANHANG IV

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

ANHANG V

Geheimschutz in der Wirtschaft

ANHANG VI

Austausch von Verschlusssachen mit Drittstaaten und internationalen Organisationen

▼B

ANHANG I

PERSONELLER GEHEIMSCHUTZ

I. EINLEITUNG

1. Dieser Anhang enthält Bestimmungen zur Anwendung von Artikel 7. Er legt die Kriterien fest, anhand derer festgestellt wird, ob eine Person unter Berücksichtigung ihrer Loyalität, Vertrauenswürdigkeit und Zuverlässigkeit zum Zugang zu EU-VS ermächtigt werden kann, sowie die hierzu anzuwendenden Untersuchungs- und Verwaltungsverfahren.

II. GEWÄHRUNG DES ZUGANGS ZU EU-VS

2. Einer Person darf der Zugang zu Verschlusssachen nur gewährt werden, wenn

   a) festgestellt wurde, dass sie Kenntnis von Verschlusssachen haben muss;

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

   c) bei Verschlusssachen des Geheimhaltungsgrads „CONFIDENTIEL UE/EU CONFIDENTIAL“ und höher

      — sie über eine Sicherheitsermächtigung für den entsprechenden Geheimhaltungsgrad verfügt oder auf andere Weise aufgrund ihrer Tätigkeit nach Maßgabe der innerstaatlichen Rechtsvorschriften ordnungsgemäß befugt ist oder

      — ihr im Falle von Beamten und sonstigen Bediensteten des Generalsekretariats sowie abgeordneten nationalen Experten die Genehmigung für den Zugang zu EU-VS durch die Anstellungsbehörde des Generalsekretariats des Rates gemäß den Nummern 16 bis 25 bis zu einem bestimmten Geheimhaltungsgrad und bis zu einem bestimmten Zeitpunkt erteilt wurde.

3. Jeder Mitgliedstaat und das Generalsekretariat des Rates bestimmen innerhalb ihrer Strukturen die Dienstposten, für die ein Zugang zu als „CONFIDENTIEL UE/EU CONFIDENTIAL“ oder höher eingestuften Verschlusssachen und somit eine Verschlusssachenermächtigung für den entsprechenden Geheimhaltungsgrad erforderlich ist.

III. ANFORDERUNGEN AN DIE SICHERHEITSERMÄCHTIGUNG

4. Die Nationalen Sicherheitsbehörden oder andere zuständige nationale Behörden sind nach Erhalt eines entsprechenden Ersuchens dafür verantwortlich, sicherzustellen, dass Personen, die Staatsangehörige des betreffenden Staates sind und Zugang zu als „CONFIDENTIEL UE/EU CONFIDENTIAL“ oder höher eingestuften Verschlusssachen haben müssen, einer Sicherheitsüberprüfung unterzogen werden. Die Überprüfungsstandards müssen den innerstaatlichen Rechtsvorschriften im Hinblick auf die Ausstellung einer Sicherheitsermächtigung oder auf die Feststellung, dass die Person eine Genehmigung für den Zugang zu EU-VS erhalten kann, entsprechen.

5. Hat die betreffende Person ihren Wohnsitz im Hoheitsgebiet eines anderen Mitgliedstaats oder eines Drittstaats, so ersuchen die zuständigen nationalen Behörden die zuständige Behörde des Wohnsitzstaats gemäß den innerstaatlichen Rechtsvorschriften um Unterstützung. Die Mitgliedstaaten unterstützen sich gegenseitig bei der Durchführung von Sicherheitsüberprüfungen gemäß den innerstaatlichen Rechtsvorschriften.

6. Sofern die innerstaatlichen Rechtsvorschriften dies zulassen, können die Nationalen Sicherheitsbehörden oder andere zuständige nationale Behörden Überprüfungen von Personen anderer Staatsangehörigkeit durchführen, die Zugang zu als „CONFIDENTIEL UE/EU CONFIDENTIAL“ oder höher eingestuften Verschlusssachen haben müssen. Die Überprüfungsstandards müssen den innerstaatlichen Rechtsvorschriften entsprechen.

▼B

Kriterien für die Sicherheitsüberprüfung

7. Die Loyalität, Vertrauenswürdigkeit und Zuverlässigkeit einer Person zum Zwecke der Erteilung einer Verschlusssachenermächtigung im Hinblick auf den Zugang zu als „CONFIDENTIEL UE/EU CONFIDENTIAL“ oder höher eingestuften Verschlusssachen wird mit Hilfe einer Sicherheitsüberprüfung bestimmt. Ausgehend von den Ergebnissen der Sicherheitsüberprüfung nimmt die zuständige nationale Behörde eine Gesamtbewertung vor. Zu den Hauptkriterien, die zu diesem Zweck verwendet werden, gehört — soweit dies nach den innerstaatlichen Rechtsvorschriften möglich ist — eine Prüfung der Frage, ob die Person

a) Handlungen begangen oder zu begehen versucht hat, die mit Spionage, Terrorismus, Sabotage, Landesverrat oder Staatsgefährdung im Zusammenhang stehen, sich mit anderen Personen zur Begehung von derartigen Handlungen verabredet hat bzw. einer anderen Person bei der Begehung von derartigen Handlungen Beihilfe geleistet hat;

b) mit Spionen, Terroristen, Saboteuren oder mutmaßlichen Spionen, Terroristen oder Saboteuren oder mit Vertretern von Organisationen oder von ausländischen Staaten, einschließlich von ausländischen Nachrichtendiensten, die eine Bedrohung für die Sicherheit der Union und/oder ihrer Mitgliedstaaten darstellen, in Verbindung steht oder gestanden hat, es sei denn, diese Verbindung war im Rahmen der dienstlichen Tätigkeit der betreffenden Person gestattet;

c) Mitglied einer Organisation ist oder gewesen ist, die auf gewalttätige, subversive oder andere ungesetzliche Art und Weise unter anderem den Umsturz der Regierung eines Mitgliedstaats oder die Veränderung der verfassungsmäßigen Ordnung eines Mitgliedstaats bzw. seiner Regierungsform oder -politik anstrebt;

d) eine Organisation nach Buchstabe c unterstützt oder unterstützt hat oder in enger Verbindung mit Mitgliedern von derartigen Organisationen steht oder gestanden hat;

e) wichtige Informationen — insbesondere sicherheitsrelevante Informationen — wissentlich zurückgehalten, falsch wiedergegeben oder verfälscht hat oder beim Ausfüllen eines Sicherheitsfragebogens oder während einer Sicherheitsbefragung wissentlich Falschangaben gemacht hat;

f) wegen einer Straftat oder Straftaten rechtskräftig verurteilt wurde;

g) alkoholabhängig ist oder gewesen ist, illegale Drogen konsumiert oder konsumiert hat und/oder legale Drogen missbraucht oder missbraucht hat;

h) Verhaltensweisen an den Tag legt oder gelegt hat, die sie anfällig für Erpressung oder eine andere Form von Druck machen könnten;

i) sich durch Handlungen oder Äußerungen als unehrlich, unloyal, unzuverlässig oder nicht vertrauenswürdig erwiesen hat;

j) in schwerwiegender Weise oder wiederholt gegen Sicherheitsvorschriften verstoßen hat oder in unzulässiger Weise mit Kommunikations- und Informationssystemen umgegangen ist oder dies versucht hat und

k) unter Druck gesetzt werden könnte (z. B. aufgrund des Besitzes einer oder mehrerer Staatsangehörigkeiten von Nicht-EU-Ländern oder aufgrund von Verwandten oder nahestehenden Personen, die anfällig für Anbahnungsversuche fremder Nachrichtendienste, terroristischer Gruppen oder anderer subversiver Organisationen oder Personen sein könnten, deren Ziele eine Bedrohung der Sicherheitsinteressen der Union und/oder ihrer Mitgliedstaaten darstellen können).

▼B

8. Bei der Sicherheitsüberprüfung können nach den innerstaatlichen Rechtsvorschriften gegebenenfalls auch die Vermögensverhältnisse und der Gesundheitszustand einer Person als relevant angesehen werden.

9. Bei der Sicherheitsüberprüfung können nach den innerstaatlichen Rechtsvorschriften gegebenenfalls auch das Verhalten und die Lebensumstände des Ehegatten, Lebenspartners oder eines anderen engen Familienmitglieds als relevant angesehen werden.

Anforderungen an die Sicherheitsüberprüfung im Hinblick auf den Zugang zu EU-VS

Erstmalige Erteilung einer Verschlusssachenermächtigung

10. Die erstmalige Erteilung einer Verschlusssachenermächtigung für den Zugang zu Verschlusssachen der Geheimhaltungsgrade „CONFIDENTIEL UE/EU CONFIDENTIAL“ und „SECRET UE/EU SECRET“ erfolgt aufgrund einer Sicherheitsüberprüfung, die sich mindestens auf die letzten fünf Jahre oder, wenn dieser Zeitraum kürzer ist, auf die Zeit zwischen dem vollendeten 18. Lebensjahr und dem Zeitpunkt der Überprüfung erstreckt und Folgendes umfasst:

a) das Ausfüllen eines nationalen Sicherheitsfragebogens für den Geheimhaltungsgrad von EU-VS, zu denen die betreffende Person unter Umständen Zugang haben muss; dieser Fragebogen wird nach dem Ausfüllen an die zuständige Sicherheitsbehörde gesandt;

b) die Überprüfung der Identität/der Staatsbürgerschaft/der Staatsangehörigkeit — Geburtsdatum und -ort der Person werden geprüft und ihre Identität wird kontrolliert. Außerdem wird ihre frühere und derzeitige Staatsbürgerschaft und/oder Staatsangehörigkeit festgestellt; dazu gehört auch die Beurteilung der Frage, ob die betreffende Person von ausländischer Seite leicht unter Druck gesetzt werden kann — z. B. aufgrund eines früheren Wohnsitzes oder früherer Verbindungen —, und

c) die Einholung von Auskünften aus nationalen und lokalen Registern — aus nationalen Sicherheits- und zentralen Strafregistern, sofern solche vorhanden sind, und/oder aus anderen vergleichbaren staatlichen und polizeilichen Registern werden Auskünfte eingeholt. Ferner werden Auskünfte aus den Registern der Strafverfolgungsbehörden mit Zuständigkeit für den Ort eingeholt, an dem die Person ihren Wohnsitz gehabt hat oder einer Beschäftigung nachgegangen ist.

11. Die erstmalige Erteilung einer Verschlusssachenermächtigung für den Zugang zu Verschlusssachen des Geheimhaltungsgrads „TRÈS SECRET UE/EU TOP SECRET“ erfolgt aufgrund einer Sicherheitsüberprüfung, die sich mindestens auf die letzten zehn Jahre oder, wenn dieser Zeitraum kürzer ist, auf die Zeit zwischen dem vollendeten 18. Lebensjahr und dem Zeitpunkt der Überprüfung erstreckt. Werden Befragungen nach Buchstabe e durchgeführt, so erstreckt sich die Überprüfung mindestens auf die letzten sieben Jahre oder, wenn dieser Zeitraum kürzer ist, auf die Zeit zwischen dem vollendeten 18. Lebensjahr und dem Zeitpunkt der Überprüfung. Zusätzlich zu den Kriterien nach Nummer 7 wird vor Erteilung einer Sicherheitsermächtigung für den Zugang zu Verschlusssachen des Geheimhaltungsgrads „TRÈS SECRET UE/EU TOP SECRET“, soweit dies nach den innerstaatlichen Rechtsvorschriften möglich ist, eine Überprüfung in Bezug auf die nachstehenden Aspekte vorgenommen; sofern die innerstaatlichen Rechtsvorschriften dies erfordern, können diese Aspekte auch vor Erteilung einer Sicherheitsermächtigung für den Zugang zu Verschlusssachen der Geheimhaltungsgrade „CONFIDENTIEL UE/EU CONFIDENTIAL“ oder „SECRET UE/EU SECRET“ überprüft werden:

a) Vermögensverhältnisse — es werden Informationen zu den Vermögensverhältnissen der Person eingeholt, um festzustellen, ob sie aus dem Ausland oder von inländischer Seite wegen ernster finanzieller Schwierigkeiten unter Druck gesetzt werden könnte, oder um einen unerklärten Vermögenszuwachs aufzudecken;

▼B

b) Bildungsstand — es werden Informationen zur Überprüfung des Bildungswegs an Schulen, Universitäten und anderen Bildungseinrichtungen eingeholt, die von der Person seit Vollendung ihres 18. Lebensjahrs oder während eines anderen von der untersuchenden Stelle für angemessen erachteten Zeitraums besucht wurden;

c) Arbeitsverhältnisse — es werden Informationen zu derzeitigen und früheren Arbeitsverhältnissen eingeholt, wobei auf Quellen wie Beschäftigungsnachweise und Leistungsbeurteilungen sowie Arbeitgeber oder Vorgesetzte zurückgegriffen wird;

d) Wehrdienst — soweit zutreffend werden der Wehrdienst der Person und die Art der Entlassung überprüft, und

e) Befragungen — es werden, sofern nach dem nationalen Recht vorgesehen und zulässig, eine oder mehrere Befragungen mit der betreffenden Person durchgeführt. Befragungen werden auch mit anderen Personen durchgeführt, die in der Lage sind, eine unvoreingenommene Stellungnahme zu der Vorgeschichte, den Aktivitäten, der Loyalität, der Vertrauenswürdigkeit und der Zuverlässigkeit der Person abzugeben. Wenn es in einem Mitgliedstaat üblich ist, die zu überprüfende Person um die Nennung von Referenzpersonen zu bitten, so werden die entsprechenden Referenzpersonen befragt, sofern nicht gute Gründe dagegen sprechen.

12. Erforderlichenfalls und nach Maßgabe der innerstaatlichen Rechtsvorschriften können zusätzliche Überprüfungen durchgeführt werden, um die zu einer Person vorliegenden sicherheitsrelevanten Informationen zu vertiefen und um nachteilige Erkenntnisse zu erhärten oder zu widerlegen.

Erneuerung einer Verschlusssachenermächtigung

13. Nach der erstmaligen Erteilung einer Verschlusssachenermächtigung ist die Ermächtigung für den Geheimhaltungsgrad „TRÈS SECRET UE/EU TOP SECRET“ spätestens nach fünf Jahren und für die Geheimhaltungsgrade „SECRET UE/EU SECRET“ und „CONFIDENTIEL UE/EU CONFIDENTIAL“ spätestens nach zehn Jahren im Hinblick auf eine Erneuerung zu überprüfen, sofern die betreffende Person ununterbrochen bei einer nationalen Verwaltung oder dem Generalsekretariat des Rates tätig gewesen ist und weiterhin Zugang zu EU-VS benötigt; die genannten Zeiträume werden ab dem Tag der Mitteilung des Ergebnisses der letzten Sicherheitsüberprüfung berechnet, auf deren Grundlage die betreffende Verschlusssachenermächtigung erteilt wurde. Alle Sicherheitsüberprüfungen zur Erneuerung einer Verschlusssachenermächtigung erstrecken sich auf den seit der letzten Überprüfung vergangenen Zeitraum.

14. Im Falle der Erneuerung von Verschlusssachenermächtigungen werden die Aspekte gemäß den Nummern 10 und 11 überprüft.

15. Anträge auf Erneuerung sind rechtzeitig zu stellen, wobei die für Sicherheitsüberprüfungen erforderliche Zeitspanne zu berücksichtigen ist. Erhält die zuständige Nationale Sicherheitsbehörde oder eine sonstige zuständige nationale Behörde den betreffenden Erneuerungsantrag und den entsprechenden Sicherheitsfragebogen vor Ablauf der Gültigkeit einer Verschlusssachenermächtigung und ist die erforderliche Sicherheitsüberprüfung noch nicht abgeschlossen, so kann die zuständige nationale Behörde, sofern die innerstaatlichen Rechtsvorschriften dies zulassen, die Gültigkeit der bestehenden Verschlusssachenermächtigung um bis zu 12 Monate verlängern. Ist die Sicherheitsüberprüfung nach Ablauf dieses Zeitraums von 12 Monaten noch nicht abgeschlossen, so werden der betreffenden Person Aufgaben zugewiesen, für die eine Verschlusssachenermächtigung nicht erforderlich ist.

Verfahren zur Erteilung einer Genehmigung im Generalsekretariat des Rates

16. Für Beamte und sonstige Bedienstete des Generalsekretariats des Rates sendet die Sicherheitsbehörde des Generalsekretariats des Rates 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.

▼B

17. Werden dem Generalsekretariat des Rates sicherheitserhebliche Informationen zu einer Person bekannt, die eine Verschlusssachenermächtigung im Hinblick auf den Zugang zu EU-VS beantragt hat, so teilt es dies der zuständigen Nationalen Sicherheitsbehörde gemäß den einschlägigen Vorschriften mit.

18. Nach Abschluss der Sicherheitsüberprüfung teilt die betreffende Nationale Sicherheitsbehörde der Sicherheitsbehörde des Generalsekretariats des Rates das Ergebnis der Überprüfung unter Verwendung des vom Sicherheitsausschuss für den Schriftverkehr vorgeschriebenen Formblatts 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 in Frage stellen, kann die Anstellungsbehörde des Generalsekretariats des Rates der betreffenden Person die Genehmigung für den Zugang zu EU-VS bis zu dem entsprechenden Geheimhaltungsgrad bis zu einem bestimmten Zeitpunkt gewähren.

    b) Führt das Ergebnis der Sicherheitsüberprüfung nicht zu einer solchen Feststellung, so setzt die Anstellungsbehörde des Generalsekretariats des Rates die betreffende Person davon in Kenntnis; die betreffende Person kann beantragen, von der Anstellungsbehörde gehört zu werden. Die Anstellungsbehörde kann bei der zuständigen Nationalen Sicherheitsbehörde um weitere Auskünfte nachsuchen, die diese nach ihren innerstaatlichen Rechtsvorschriften geben darf. Bei Bestätigung des Ergebnisses der Sicherheitsüberprüfung wird die Genehmigung für den Zugang zu EU-VS nicht erteilt.

19. Für die Sicherheitsüberprüfung und deren Ergebnisse gelten die einschlägigen Rechtsvorschriften des betreffenden Mitgliedstaats, einschließlich der Rechtsvorschriften für etwaige Rechtsbehelfe. Gegen Entscheidungen der Anstellungsbehörde des Generalsekretariats des Rates können Rechtsbehelfe gemäß dem Statut der Beamten der Europäischen Union und der Beschäftigungsbedingungen für die sonstigen Bediensteten der Europäischen Union gemäß der Verordnung (EWG, Euratom, EGKS) Nr. 259/68 des Rates [1] (im Folgenden „Statut und Beschäftigungsbedingungen“) eingelegt werden.

20. Nationale Experten, die zum Generalsekretariat des Rates abgeordnet werden, um dort einen Dienstposten zu bekleiden, für den der Zugang zu als „CONFIDENTIEL UE/EU CONFIDENTIAL“ oder höher eingestuften EU-VS erforderlich ist, müssen der Sicherheitsbehörde des Generalsekretariats des Rates eine gültige Bescheinigung über die Sicherheitsermächtigung (Sicherheitsermächtigungsbescheinigung — Personnel Security Clearance Certificate, PSCC) für den Zugang zu EU-VS vorlegen, bevor sie ihren Dienst antreten, die Anstellungsbehörde erteilt auf dieser Grundlage eine Genehmigung für den Zugang zu EU-VS.

21. Das Generalsekretariat des Rates erkennt die von anderen Organen, Einrichtungen oder Agenturen der Union ausgestellten Genehmigungen für den Zugang zu EU-VS an, solange diese gültig sind. Die Genehmigung erstreckt sich auf alle Aufgaben, die die betreffende Person im Generalsekretariat des Rates übernimmt. Das Organ, die Einrichtung oder die Agentur der Union, bei dem bzw. der die betreffende Person ihre Beschäftigung aufnimmt, unterrichtet die zuständige Nationale Sicherheitsbehörde über den Wechsel des Arbeitgebers.

22. Nimmt eine Person innerhalb von 12 Monaten nach Mitteilung des Ergebnisses der Sicherheitsüberprüfung an die Anstellungsbehörde des Generalsekretariats des Rates ihren Dienst nicht auf oder unterbricht sie diesen für einen Zeitraum von 12 Monaten, in dem sie nicht beim Generalsekretariat des Rates oder bei einer nationalen Verwaltung eines Mitgliedstaats tätig ist, so wird die zuständige Nationale Sicherheitsbehörde mit diesem Ergebnis befasst, damit sie gegebenenfalls bestätigen kann, dass es weiterhin gültig und berechtigt ist.

23. Werden dem Generalsekretariat des Rates Informationen in Bezug auf ein Sicherheitsrisiko durch eine Person bekannt, die eine Genehmigung für den Zugang zu EU-VS besitzt, so teilt das Generalsekretariat des Rates dies der zuständigen Nationalen Sicherheitsbehörde gemäß den einschlägigen Vorschriften mit; es kann den Zugang zu EU-VS aussetzen oder die Genehmigung für den Zugang zu EU-VS zurücknehmen.

---

[1] Verordnung (EWG, Euratom, EGKS) Nr. 259/68 des Rates vom 29. Februar 1968 zur Festlegung des Statuts der Beamten der Europäischen Gemeinschaften und der Beschäftigungsbedingungen für die sonstigen Bediensteten dieser Gemeinschaften sowie zur Einführung von Sondermaßnahmen, die vorübergehend auf die Beamten der Kommission anwendbar sind (ABl. L 56 vom 4.3.1968, S. 1).

▼B

24. Teilt eine Nationale Sicherheitsbehörde dem Generalsekretariat des Rates mit, dass eine gemäß Nummer 18 Buchstabe a erfolgte Feststellung in Bezug auf eine Person, die im Besitz einer Genehmigung für den Zugang zu EU-VS ist, zurückgenommen wurde, kann die Anstellungsbehörde des Generalsekretariats des Rates bei der Nationalen Sicherheitsbehörde um alle weiteren Auskünfte nachsuchen, die diese nach ihren innerstaatlichen Rechtsvorschriften geben darf. Bei Bestätigung der nachteiligen Erkenntnisse wird die Genehmigung zurückgenommen und die betreffende Person vom Zugang zu EU-VS und von Dienstposten, auf denen sie sich Zugang zu EU-VS verschaffen kann oder auf denen sie ein Sicherheitsrisiko darstellen könnte, ausgeschlossen.

25. Jede Entscheidung über die Rücknahme oder die Aussetzung einer Genehmigung für den Zugang zu EU-VS für einen Beamten oder sonstigen Bediensteten des Generalsekretariats des Rates und gegebenenfalls die dafür maßgeblichen Gründe werden der betreffenden Person mitgeteilt; die betreffende Person kann beantragen, von der Anstellungsbehörde gehört zu werden. Für die von einer Nationalen Sicherheitsbehörde zur Verfügung gestellten Informationen gelten die einschlägigen Rechtsvorschriften des betreffenden Mitgliedstaats, einschließlich der Rechtsvorschriften für etwaige Rechtsbehelfe. Gegen Entscheidungen der Anstellungsbehörde des Generalsekretariats des Rates können Rechtsbehelfe gemäß dem Statut und den Beschäftigungsbedingungen eingelegt werden.

Verzeichnis der Verschlusssachenermächtigungen und Genehmigungen

26. Jeder Mitgliedstaat und das Generalsekretariat des Rates führen jeweils ein Verzeichnis der Sicherheitsermächtigungen bzw. der Genehmigungen, die im Hinblick auf den Zugang zu als „CONFIDENTIEL UE/EU CONFIDENTIAL“ oder höher eingestuften Verschlusssachen erteilt wurden. Diese Verzeichnisse enthalten mindestens Angaben zum Geheimhaltungsgrad der EU-VS, zu denen die betreffende Person Zugang haben darf, das Datum, an dem die Verschlusssachenermächtigung erteilt wurde, und deren Gültigkeitsdauer.

27. Die zuständige Sicherheitsbehörde kann eine PSCC ausstellen, die Angaben zum Geheimhaltungsgrad der EU-VS, zu denen die Person Zugang haben darf (als „CONFIDENTIEL UE/EU CONFIDENTIAL“ oder höher eingestufte Verschlusssachen), zur Gültigkeitsdauer der betreffenden Sicherheitsermächtigung für den Zugang zu EU-VS bzw. der Genehmigung für den Zugang zu EU-VS und zum Ende der Gültigkeitsdauer der Bescheinigung selbst enthält.

Ausnahmen vom Erfordernis einer Sicherheitsermächtigung

28. Für Personen, die in den Mitgliedstaaten aufgrund ihrer Aufgaben förmlich entsprechend befugt worden sind, wird der Zugang zu EU-VS gemäß den innerstaatlichen Rechtsvorschriften bestimmt; diese Personen werden über ihre Verpflichtungen aus den Sicherheitsvorschriften hinsichtlich des Schutzes von EU-VS belehrt.

IV. SCHULUNG UND SENSIBILISIERUNG IN BEZUG AUF SICHERHEIT

29. Alle Personen, denen eine Verschlusssachenermächtigung erteilt wurde, bestätigen schriftlich, dass sie sich ihrer Verpflichtungen in Bezug auf den Schutz von EU-VS und der Folgen einer Kenntnisnahme von EU-VS durch Unbefugte bewusst sind. Der Mitgliedstaat bzw. das Generalsekretariat des Rates verwahrt die Aufzeichnungen über derartige schriftliche Bestätigungen.

30. 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 unterrichtet; sie müssen alle von ihnen als verdächtig oder ungewöhnlich erachteten Anbahnungsversuche oder sonstigen Tätigkeiten unverzüglich den für Sicherheit zuständigen Stellen melden.

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

V. AUSSERGEWÖHNLICHE UMSTÄNDE

32. Soweit die innerstaatlichen Rechtsvorschriften dies zulassen, kann eine von einer zuständigen nationalen Behörde eines Mitgliedstaats für den Zugang

▼B

zu nationalen Verschlusssachen erteilte Verschlusssachenermächtigung während eines befristeten Zeitraums bis zur Erteilung einer Sicherheitsermächtigung für den Zugang zu EU-VS nationale Bedienstete zum Zugang zu EU-VS bis zu der entsprechenden Geheimhaltungsstufe gemäß der Entsprechungstabelle in Anlage B berechtigen, wenn ein solcher befristeter Zugang im Interesse der Union erforderlich ist. Die Nationalen Sicherheitsbehörden unterrichten den Sicherheitsausschuss, sofern die innerstaatlichen Rechtsvorschriften einen befristeten Zugang zu EU-VS nicht zulassen.

33. Aus Gründen der Dringlichkeit kann die Anstellungsbehörde des Generalsekretariats des Rates 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, die dazu dient, festzustellen, ob keine nachteiligen Erkenntnisse vorliegen, Beamten und sonstigen Bediensteten des Generalsekretariats des Rates eine vorläufige Ermächtigung zum Zugang zu EU-VS für eine bestimmte Tätigkeit erteilen, wenn dies im dienstlichen Interesse gerechtfertigt ist. 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. Das Generalsekretariat des Rates verwahrt die Aufzeichnungen über derartige schriftliche Bestätigungen.

34. Wird einer Person eine Tätigkeit zugewiesen, die eine Verschlusssachenermächtigung erfordert, die für Verschlusssachen gilt, die einen eine Stufe höheren Geheimhaltungsgrad aufweisen als die Verschlusssachen, für die sie eine Ermächtigung besitzt, 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 Sicherheitsermächtigung bzw. einer gültigen Genehmigung für den Zugang zu EU-VS ist;

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

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

    f) die zuständige Behörde der Zuweisung der Tätigkeit an die Person zustimmt und

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

35. 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 ermächtigt wurde. Auf dieses Verfahren darf nicht regelmäßig zurückgegriffen werden.

36. 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 die Mitgliedstaaten und der Generalsekretär Personen, die nicht die erforderliche Verschlusssachenermächtigung besitzen, 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 und keine begründeten Zweifel an der Loyalität, Vertrauenswürdigkeit und Zuverlässigkeit der betreffenden Person bestehen. Von dieser Erlaubnis wird eine Aufzeichnung aufbewahrt, in der die Verschlusssachen beschrieben werden, zu denen der Zugang genehmigt wurde.

▼B

37. Im Falle von Verschlusssachen, die als „TRÈS SECRET UE/EU TOP SECRET“ eingestuft sind, wird diese Art des Zugangs in Ausnahmefällen auf Staatsangehörige der Mitgliedstaaten der Union 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.

38. Der Sicherheitsausschuss wird über die Fälle unterrichtet, in denen auf das Verfahren nach den Nummern 36 und 37 zurückgegriffen wird.

39. Sehen die innerstaatlichen Rechtsvorschriften eines Mitgliedstaats strengere Vorschriften in Bezug auf befristete Ermächtigungen, die vorläufige Zuweisung von Tätigkeiten, den einmaligen Zugang oder den Zugang im Notfall von Personen zu Verschlusssachen vor, so werden die in diesem Abschnitt vorgesehenen Verfahren nur innerhalb der von den einschlägigen innerstaatlichen Rechtsvorschriften gesetzten Grenzen angewandt.

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

VI. TEILNAHME AN SITZUNGEN IM RAT

41. Vorbehaltlich der Nummer 28 darf Personen, die an Tagungen des Rates oder an Sitzungen seiner Vorbereitungsgremien teilnehmen sollen, in deren Rahmen als „CONFIDENTIEL UE/EU CONFIDENTIAL“ und höher eingestufte Informationen erörtert werden, die Teilnahme nur dann gestattet werden, wenn die Verschlusssachenermächtigung der betreffenden Person bestätigt wurde. Im Falle von Delegierten wird eine Sicherheitsermächtigungsbescheinigung (PSCC) oder ein anderer Nachweis für eine Verschlusssachenermächtigung dem Sicherheitsbüro des Generalsekretariats des Rates von den zuständigen Behörden übermittelt oder ausnahmsweise von dem betreffenden Delegierten vorgelegt. Gegebenenfalls kann eine konsolidierte Namensliste verwendet werden, die den einschlägigen Nachweis einer Verschlusssachenermächtigung enthält.

42. Wird einer Person, die im Rahmen ihrer Aufgaben an Tagungen des Rates oder an Sitzungen seiner Vorbereitungsgremien teilnehmen muss, die Sicherheitsermächtigung für den Zugang zu EU-VS aus Sicherheitsgründen entzogen, so setzt die zuständige Behörde das Generalsekretariat des Rates davon in Kenntnis.

VII. MÖGLICHER ZUGANG ZU EU-VERSCHLUSSSACHEN

43. Boten, Sicherheitsbedienstete und Begleitpersonen werden einer Sicherheitsüberprüfung der erforderlichen Geheimhaltungsstufe unterzogen oder auf andere Weise gemäß den innerstaatlichen Rechtsvorschriften angemessen überprüft und über die Sicherheitsverfahren zum Schutz von EU-VS sowie über ihre Pflichten zum Schutz der ihnen anvertrauten Verschlusssachen belehrt.

▼B

ANHANG II

MATERIELLER GEHEIMSCHUTZ

I. EINLEITUNG

1. Dieser Anhang enthält Bestimmungen zur Anwendung von Artikel 8. 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 Zugang unbefugter Personen 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. Die Auswahl der Maßnahmen des materiellen Geheimschutzes erfolgt auf der Grundlage einer Einschätzung der Bedrohungslage durch die zuständigen Behörden. Das Generalsekretariat des Rates wie auch die Mitgliedstaaten wenden in ihren Gebäuden einen Risikomanagementprozess für den Schutz von EU-VS an, um dafür zu sorgen, dass der Umfang des materiellen Schutzes dem festgestellten Risiko entspricht. Bei dem Risikomanagementprozess wird allen relevanten Faktoren Rechnung getragen, 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, und

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

4. Die zuständige Sicherheitsbehörde legt unter Anwendung des Konzepts der mehrschichtigen Sicherheit die angemessene Kombination von Maßnahmen des materiellen Geheimschutzes fest, die durchgeführt werden müssen. Dies kann eine oder mehrere der folgenden Maßnahmen umfassen:

   a) Absperrung: ein materielles 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 an Stelle von Sicherheitspersonal oder zu dessen Unterstützung verwendet werden;

▼B

c) Zugangskontrolle: Die Zugangskontrollen können einen Standort, ein oder mehrere Gebäude an einem Standort 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 (CCTV): Videoüberwachungssysteme können vom Sicherheitspersonal zur Überprüfung von Störfällen 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, und

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

5. Die zuständige Behörde kann befugt werden, Durchsuchungen an den Ein- und Ausgängen vorzunehmen, um damit vom Verbringen unzulässigen Materials in Räumlichkeiten oder Gebäude oder von der nicht genehmigten 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 physischen Schutz von EU-VS stellt die zuständige Sicherheitsbehörde sicher, dass die Ausrüstung den genehmigten technischen Standards und Mindestanforderungen entspricht.

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

10. Die Sicherheitssysteme müssen in regelmäßigen Abständen überprüft werden; die Ausrüstung muss regelmäßig gewartet werden. Bei den Wartungsarbeiten ist dem Ergebnis der Überprüfungen 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 physischen Schutz von EU-VS werden zwei Arten von durch Maßnahmen des materiellen Geheimschutzes geschützten Bereichen oder entsprechende Bereiche auf nationaler Ebene eingerichtet:

▼B

a) Verwaltungsbereiche und

b) besonders geschützte Bereiche (einschließlich technisch abgesicherter Bereiche).

In diesem Beschluss gelten alle Bezugnahmen auf Verwaltungsbereiche und besonders geschützte Bereiche, einschließlich technisch abgesicherter Bereiche, auch als Bezugnahmen auf die entsprechenden Bereiche auf nationaler Ebene.

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

14. Für Verwaltungsbereiche:

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

b) nur Personen, die von der zuständigen Behörde entsprechend ermächtigt wurden, dürfen diesen Bereich unbegleitet betreten, und

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

15. Für besonders geschützte Bereiche:

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

b) nur sicherheitsüberprüfte und speziell ermächtigte Personen dürfen diesen Bereich auf der Grundlage der Tatsache, dass sie Zugang zu Verschlusssachen haben müssen, unbegleitet betreten, und

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

16. Wenn das Betreten eines besonders geschützten Bereichs de facto den unmittelbaren Zugang zu 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 Genehmigung, 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.

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

a) Diese Bereiche werden mit Einbruchsmeldeanlagen ausgerüstet, 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;

b) alle Personen, die diese Bereiche betreten, und alles Material, das dorthin verbracht wird, sind zu kontrollieren;

▼B

c) diese Bereiche sind gemäß den Vorschriften der zuständigen Sicherheitsbehörde 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, und

d) in diesen Bereichen sind nicht zugelassene Kommunikationsverbindungen, nicht zugelassene Telefone und andere nicht zugelassene Kommunikationsgeräte und 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 zu 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 zuständigen Sicherheitsbehörde 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. Die abgesicherten 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 Sicherheitsbetriebsverfahren 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) die Personen, die aufgrund dessen, dass sie Kenntnis von Verschlusssachen haben müssen, und aufgrund ihrer Sicherheitsermächtigung unbegleiteten Zugang zu diesem Bereich erhalten;

d) gegebenenfalls die Verfahren für die Begleitung anderer Personen, denen Zugang zu diesem Bereich gewährt wird, bzw. die Verfahren zum Schutz von EU-VS in einem solchen Fall und

e) sonstige einschlägige Maßnahmen und Verfahren.

22. Tresorräume werden in abgesicherte Bereiche eingebaut. Wände, Böden, Decken, Fenster und verschließbare Türen müssen von der zuständigen Sicherheitsbehörde zugelassen werden und einen Schutz bieten, der dem eines Sicherheitsbehältnisses entspricht, das für die Aufbewahrung von EU-VS desselben Geheimhaltungsgrads zugelassen ist.

V. MATERIELLE 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 besonders geschützten Bereich;

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

▼B

c) außerhalb eines besonders geschützten Bereichs oder eines Verwaltungsbereichs, sofern der Besitzer die EU-VS gemäß Anhang III Nummern 28 bis 41 befördert und sich verpflichtet hat, besondere Maßnahmen einzuhalten, die in den Sicherheitsanweisungen der zuständigen Sicherheitsbehörde festgelegt 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 besonders geschützten Bereich aufzubewahren. Sie können zeitweilig außerhalb eines besonders geschützten Bereichs oder eines Verwaltungsbereichs aufbewahrt werden, sofern der Besitzer sich verpflichtet hat, besondere Maßnahmen einzuhalten, die in den Sicherheitsanweisungen der zuständigen Sicherheitsbehörde festgelegt sind.

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

a) in einem besonders geschützten 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 III Nummern 28 bis 41 befördert;

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

iii) die EU-VS jederzeit unter persönlicher Kontrolle hält und

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 besonders geschützten Bereich entweder in einem Sicherheitsbehältnis oder in einem Tresorraum aufbewahrt.

27. EU-VS des Geheimhaltungsgrads „TRÈS SECRET UE/EU TOP SECRET“ werden in einem besonders geschützten Bereich bearbeitet.

28. EU-VS des Geheimhaltungsgrads „TRÈS SECRET UE/EU TOP SECRET“ sind in einem besonders geschützten Bereich unter einer der folgenden Bedingungen aufzubewahren:

a) in einem VS-Verwahrgelass entsprechend Nummer 8 mit mindestens einer der folgenden zusätzlichen Kontrollen:

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

ii) zugelassene Einbruchsmeldeanlage in Verbindung mit Bereitschaftspersonal im Sicherheitsdienst;

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

▼B

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

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

30. Die zuständige Sicherheitsbehörde 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 für Tresorräume, in denen EU-VS aufbewahrt werden, sind zu ändern

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.

▼B

ANHANG III

VERWALTUNG VON VERSCHLUSSSACHEN

I. EINLEITUNG

1. Dieser Anhang enthält Bestimmungen zur Anwendung von Artikel 9. In ihm sind die Verwaltungsmaßnahmen zur Überwachung von EU-VS während der gesamten Dauer ihrer Einstufung als EU-VS festgelegt; diese sollen dazu dienen, die beabsichtigte oder unbeabsichtigte Kenntnisnahme dieser Verschlusssachen durch Unbefugte bzw. den Verlust dieser Verschlusssachen zu verhindern und festzustellen.

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 ursprünglichen Empfängerkreis der Informationen zu bestimmen.

4. Der Geheimhaltungsgrad einer EU-VS ist nach Artikel 2 Absatz 2 und unter Bezugnahme auf das gemäß Artikel 3 Absatz 3 zu billigende Sicherheitskonzept festzulegen.

5. Der Geheimhaltungsgrad ist eindeutig und richtig anzugeben, unabhängig davon, ob die EU-VS im Papierformat, in mündlicher, elektronischer oder anderer Form vorliegt.

6. 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.

7. Der Geheimhaltungsgrad des Gesamtdokuments oder der Datei entspricht mindestens dem Geheimhaltungsgrad seines/ihres am höchsten eingestuften Teils. Werden Informationen aus verschiedenen Quellen in einem Dokument 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.

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. 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

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

a) eine 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 oder

▼B

d) gegebenenfalls der Angabe des Zeitpunkts oder des speziellen Ereignisses, nach dem der Geheimhaltungsgrad herabgestuft oder aufgehoben werden kann.

Abgekürzte Einstufungskennzeichnungen

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

12. 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

13. Bei der Erstellung einer EU-Verschlusssache

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 und

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

14. Ist eine Anwendung der Nummer 13 auf EU-VS nicht möglich, so sind im Einklang mit nach Artikel 6 Absatz 2 festzulegenden Sicherheitsleitlinien andere geeignete Maßnahmen anzuwenden.

Herabstufung und Aufhebung des Geheimhaltungsgrads von EU-VS

15. 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 Zeitpunkt oder im Anschluss an ein bestimmtes Ereignis herabgestuft oder aufgehoben werden kann.

16. Das Generalsekretariat des Rates überprüft regelmäßig die in seinem Besitz befindlichen EU-VS daraufhin, ob ihr Geheimhaltungsgrad weiterhin zutreffend ist. Das Generalsekretariat des Rates legt ein System fest, mit dem der Geheimhaltungsgrad der von ihm stammenden EU-VS mindestens alle fünf Jahre überprüft wird. Eine solche Überprüfung ist nicht erforderlich, wenn der Herausgeber bereits von vornherein mitgeteilt hat, dass der Geheimhaltungsgrad der Informationen automatisch herabgestuft oder aufgehoben wird, und die Informationen entsprechend gekennzeichnet wurden.

III. REGISTRIERUNG VON EU-VS ZU SICHERHEITSZWECKEN

17. Für jede Stelle im Generalsekretariat des Rates und in den nationalen Verwaltungen der Mitgliedstaaten, in denen EU-VS bearbeitet werden, wird eine zuständige Registratur bestimmt, damit bei der Bearbeitung von EU-VS die Einhaltung dieses Beschlusses gewährleistet wird. Die Registraturen werden als besonders geschützte Bereiche im Sinne des Anhangs II eingerichtet.

▼B

18. Im Sinne dieses Beschlusses bezeichnet der Ausdruck „Registrierung zu Sicherheitszwecken“ (im Folgenden „Registrierung“) die Durchführung von Verfahren, bei denen jede Phase des Umlaufs der Materialien, auch deren Weitergabe und Vernichtung, aufgezeichnet wird.

19. Alle als „CONFIDENTIEL UE/EU CONFIDENTIAL“ und höher eingestuften Materialien sind in den benannten Registraturen zu registrieren, wenn sie in einer Verwaltungseinheit eingehen oder diese verlassen.

20. Die Zentralregistratur im Generalsekretariat des Rates verwahrt die Aufzeichnungen über alle Verschlusssachen, die vom Rat und vom Generalsekretariat des Rates an Drittstaaten und internationale Organisationen weitergegeben werden, und über alle Verschlusssachen, die von Drittstaaten oder internationalen Organisationen eingehen.

21. Im Falle eines Kommunikations- und Informationssystems können die Registrierungsverfahren durch Prozesse im Kommunikations- und Informationssystem selbst vorgenommen werden.

22. Der Rat billigt ein Sicherheitskonzept in Bezug auf die Registrierung von EU-VS zu Sicherheitszwecken.

„TRÈS SECRET UE/EU TOP SECRET“-Registraturen

23. In den Mitgliedstaaten und im Generalsekretariat des Rates wird eine Registratur benannt, die als zentrale Eingangs- und Ausgangsstelle für als „TRÈS SECRET UE/EU TOP SECRET“ eingestufte Verschlusssachen fungiert. Sofern erforderlich, können nachgeordnete Registraturen zur Bearbeitung dieser Verschlusssachen zu Registrierungszwecken bestimmt werden.

24. 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

25. Als „TRÈS SECRET UE/EU TOP SECRET“ eingestufte Dokumente dürfen ohne vorherige schriftliche Zustimmung des Herausgebers weder kopiert noch übersetzt werden.

26. 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.

27. Die für das Originaldokument geltenden Sicherheitsmaßnahmen finden auf Kopien und Übersetzungen dieses Dokuments Anwendung.

V. BEFÖRDERUNG VON EU-VS

28. Für die Beförderung von EU-VS gelten die Schutzmaßnahmen nach den Nummern 30 bis 41. Bei der Beförderung von EU-VS auf elektronischen Datenträgern können ungeachtet des Artikels 9 Absatz 4 die nachstehend beschriebenen Schutzmaßnahmen entsprechend den Weisungen der zuständigen Sicherheitsbehörde durch geeignete technische Abwehrmaßnahmen ergänzt werden, damit das Risiko eines Verlusts oder der Kenntnisnahme durch Unbefugte so gering wie möglich gehalten wird.

29. Die zuständigen Sicherheitsbehörden des Generalsekretariats des Rates und der Mitgliedstaaten erlassen ergänzende Weisungen für die Beförderung von EU-VS nach Maßgabe dieses Beschlusses.

Innerhalb eines Gebäudes oder einer geschlossenen Gebäudegruppe

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

▼B

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

Innerhalb der Union

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

33. Die Beförderung von Verschlusssachen mit den Geheimhaltungsgraden „CONFIDENTIEL UE/EU CONFIDENTIAL“ oder „SECRET UE/EU SECRET“ innerhalb der Union 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 II aufbewahrt wird;

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

iii) die betreffenden Personen über ihre Verantwortlichkeiten für die Sicherheit belehrt werden und

iv) die betreffenden Personen erforderlichenfalls einen Kurierausweis erhalten;

c) durch Postdienste oder private Kurierdienste, sofern

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

ii) sie entsprechend den gemäß Artikel 6 Absatz 2 festzulegenden Mindestanforderungen geeignete Schutzmaßnahmen anwenden.

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

34. Informationen des Geheimhaltungsgrads „RESTREINT UE/EU RESTRICTED“ dürfen auch durch Postdienste oder private Kurierdienste befördert werden. Ein Kurierausweis ist für die Beförderung solcher Informationen nicht erforderlich.

35. Als „CONFIDENTIEL UE/EU CONFIDENTIAL“ oder „SECRET UE/EU SECRET“ eingestufte Materialien (beispielsweise Geräte oder Maschinen), die nicht mit den unter Nummer 33 aufgeführten Beförderungsmitteln befördert werden können, werden nach Maßgabe des Anhangs V von gewerblichen Beförderungsunternehmen als Fracht befördert.

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

Aus der Union in das Hoheitsgebiet eines Drittstaats

37. EU-VS, die aus der Union in das Hoheitsgebiet eines Drittstaats befördert werden, sind so zu verpacken, dass sie vor unbefugter Kenntnisnahme geschützt sind.

▼B

38. Die Beförderung von Verschlusssachen der Geheimhaltungsgrade „CONFIDENTIEL UE/EU CONFIDENTIAL“ oder „SECRET UE/EU SECRET“ aus der Union in das Hoheitsgebiet eines Drittstaats erfolgt

    a) durch militärischen oder diplomatischen Kurier;

    b) 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 II aufbewahrt wird;

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

        v) die betreffenden Personen über ihre Verantwortlichkeiten für die Sicherheit belehrt werden.

39. Die Beförderung von Verschlusssachen der Geheimhaltungsgrade „CONFIDENTIEL UE/EU CONFIDENTIAL“ oder „SECRET UE/EU SECRET“ aus der Union in einen Drittstaat oder zu einer internationalen Organisation erfolgt nach den einschlägigen Bestimmungen eines Geheimschutzabkommens oder einer Verwaltungsvereinbarung nach Artikel 13 Absatz 2 Buchstabe a oder b.

40. Informationen des Geheimhaltungsgrads „RESTREINT UE/EU RESTRICTED“ dürfen auch durch Postdienste oder private Kurierdienste befördert werden.

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

VI. VERNICHTUNG VON EU-VS

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

43. Registrierungspflichtige Dokumente nach Artikel 9 Absatz 2 werden von der zuständigen Registratur auf Anweisung des Besitzers oder einer zuständigen Behörde vernichtet. Die Dienstbücher und sonstigen Registrierungsinformationen werden entsprechend aktualisiert.

44. Bei Dokumenten des Geheimhaltungsgrads „SECRET UE/EU SECRET“ oder „TRÈS SECRET UE/EU TOP SECRET“ erfolgt die Vernichtung im Beisein eines Zeugen, der mindestens zum Zugang zu Verschlusssachen mit dem Geheimhaltungsgrad des zu vernichtenden Dokuments ermächtigt ist.

45. 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.

46. Verschlusssachen, auch Verschlusssachen des Geheimhaltungsgrads „RESTREINT UE/EU RESTRICTED“, werden nach Verfahren vernichtet, die die einschlägigen Unionsnormen oder gleichwertige Normen erfüllen oder

▼B

die gemäß nationalen technischen Normen von den Mitgliedstaaten zugelassen worden sind, damit so einer vollständigen oder teilweisen Wiederherstellung vorgebeugt wird.

47. Die Vernichtung elektronischer Datenträger, die für EU-VS verwendet wurden, erfolgt gemäß Anhang IV Nummer 37.

48. Wenn in Notfällen das unmittelbare Risiko einer unbefugten Weitergabe besteht, sind die EU-VS durch den Besitzer so zu vernichten, dass eine vollständige oder teilweise Wiederherstellung ausgeschlossen ist. Der Herausgeber und die herausgebende Registratur sind von der als Notfallmaßnahme durchgeführten Vernichtung der registrierten EU-VS in Kenntnis zu setzen.

VII. BEWERTUNGSBESUCHE

49. Der Ausdruck „Bewertungsbesuch“ bezeichnet im Folgenden

a) jede Inspektion oder jeden Bewertungsbesuch nach Artikel 9 Absatz 3 und Artikel 16 Absatz 2 Buchstaben e, f und g oder

b) jeden Bewertungsbesuch gemäß Artikel 13 Absatz 5

zur Evaluierung der Wirksamkeit der Maßnahmen, die zum Schutz von EU-VS getroffen wurden.

50. Bewertungsbesuche werden unter anderem durchgeführt, um

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

b) der Bedeutung der Sicherheitsaspekte und eines wirksamen Risikomanagements in den inspizierten Stellen Nachdruck zu verleihen;

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

d) die laufenden Programme der Sicherheitsbehörden zur Sicherheitsschulung und zur Vermittlung von Sicherheitsbewusstsein zu unterstützen.

51. Der Rat stimmt vor Ablauf eines jeden Kalenderjahrs dem Programm für Bewertungsbesuche nach Artikel 16 Absatz 1 Buchstabe c für das Folgejahr zu. Der genaue Terminplan für die einzelnen Bewertungsbesuche wird im Benehmen mit den betreffenden Einrichtungen oder Agenturen der EU, Mitgliedstaaten, Drittstaaten oder internationalen Organisationen festgelegt.

Durchführung von Bewertungsbesuchen

52. Es werden Bewertungsbesuche durchgeführt, um die einschlägigen Vorschriften, Regelungen und Verfahren der besuchten Stelle zu überprüfen und um nachzuprüfen, ob die Verfahrensweisen der Stelle den in diesem Beschluss festgelegten Grundprinzipien und Mindeststandards und den Bestimmungen für den Austausch von Verschlusssachen mit dieser Einrichtung entsprechen.

53. Bewertungsbesuche werden in zwei Phasen durchgeführt. Vor dem eigentlichen Besuch findet gegebenenfalls mit der betreffenden Stelle eine Vorbereitungssitzung statt. Daraufhin erstellt das Bewertungsteam im Benehmen mit der betreffenden Stelle ein detailliertes Bewertungsbesuchsprogramm für alle Sicherheitsbereiche. Das Bewertungsteam sollte Zugang zu jedem Ort erhalten, an dem EU-VS bearbeitet werden, insbesondere Registraturen und Zugangspunkte (PoP) der Kommunikations- und Informationssysteme.

54. Bewertungsbesuche bei den nationalen Verwaltungen der Mitgliedstaaten, in Drittstaaten und bei internationalen Organisationen werden in uneingeschränkter Zusammenarbeit mit den Bediensteten der besuchten Stelle bzw. des besuchten Drittstaates bzw. der besuchten internationalen Organisation durchgeführt.

▼B

55. Bewertungsbesuche bei den Einrichtungen, Agenturen und sonstigen Stellen der EU, die diesen Beschluss oder die darin enthaltenen Grundsätze anwenden, werden mit Unterstützung von Experten der Nationalen Sicherheitsbehörde, in deren Gebiet Einrichtung oder Agentur ihren Sitz hat, durchgeführt.

56. Im Falle von Bewertungsbesuchen bei Einrichtungen, Agenturen und Stellen der EU, die diesen Beschluss oder die darin enthaltenen Grundsätze anwenden, sowie in Drittstaaten und bei internationalen Organisationen kann im Einklang mit den vom Sicherheitsausschuss zu vereinbarenden ausführlichen Regelungen Unterstützung und Mitwirkung von Experten der Nationalen Sicherheitsbehörden angefordert werden.

Berichte

57. Am Ende der Bewertungsbesuche werden der besuchten Stelle die wichtigsten Schlussfolgerungen und Empfehlungen vorgelegt. Anschließend wird ein Bericht über den Bewertungsbesuch erstellt. Wurden Abhilfemaßnahmen und Empfehlungen vorgeschlagen, so muss der Bericht hinreichende Einzelheiten zur Untermauerung der erzielten Schlussfolgerungen enthalten. Der Bericht wird der zuständigen Behörde der besuchten Stelle übermittelt.

58. Für Bewertungsbesuche in den nationalen Verwaltungen der Mitgliedstaaten gilt Folgendes:

    a) Der Entwurf des Bewertungsberichts wird der betreffenden Nationalen Sicherheitsbehörde übermittelt, damit diese überprüfen kann, ob er inhaltlich korrekt ist und keine Informationen enthält, die höher als „RESTREINT UE/EU RESTRICTED“ eingestuft sind und

    b) sofern die Nationale Sicherheitsbehörde des betreffenden Mitgliedstaats nicht darum ersucht, von einer allgemeinen Verteilung abzusehen, werden die Bewertungsberichte an den Sicherheitsausschuss verteilt. Der Bericht wird in den Geheimhaltungsgrad „RESTREINT UE/EU RESTRICTED“ eingestuft.

    Unter der Verantwortung der Sicherheitsbehörde des Generalsekretariats des Rates (Sicherheitsbüro) wird regelmäßig ein Bericht erstellt, in dem die Erfahrungswerte, die sich aus den während eines bestimmten Zeitraums in den Mitgliedstaaten durchgeführten Bewertungsbesuchen ergeben, dargelegt werden; dieser Bericht wird vom Sicherheitsausschuss geprüft.

59. Bei Bewertungsbesuchen in Drittstaaten und bei internationalen Organisationen wird der Bericht an den Sicherheitsausschuss verteilt. Der Bericht wird zumindest in den Geheimhaltungsgrad „RESTREINT UE/EU RESTRICTED“ eingestuft. Etwaige Abhilfemaßnahmen werden bei einem Folgebesuch verifiziert und dem Sicherheitsausschuss gemeldet.

60. Bei Bewertungsbesuchen von Einrichtungen, Agenturen und Stellen der EU, die diesen Beschluss oder die darin enthaltenen Grundsätze anwenden, werden die Berichte über Bewertungsbesuche an den Sicherheitsausschuss verteilt. Der Entwurf des Berichts über den Bewertungsbesuch wird der betreffenden Agentur oder Einrichtung übermittelt, damit diese überprüfen kann, ob er inhaltlich korrekt ist und keine Informationen enthält, die höher als „RESTREINT UE/EU RESTRICTED“ eingestuft sind. Etwaige Abhilfemaßnahmen werden bei einem Folgebesuch verifiziert und dem Sicherheitsausschuss gemeldet.

61. Die Sicherheitsbehörde des Generalsekretariats des Rates führt regelmäßig Inspektionen in den Verwaltungseinheiten des Generalsekretariats des Rates für die unter Nummer 50 festgelegten Zwecke durch.

Prüfliste

62. Die Sicherheitsbehörde des Generalsekretariats des Rates (Sicherheitsbüro) erstellt eine Prüfliste für die bei einem Bewertungsbesuch zu überprüfenden Aspekte und aktualisiert diese Liste. Diese Prüfliste wird dem Sicherheitsausschuss übermittelt.

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

▼B

ANHANG IV

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

I. EINLEITUNG

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

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 Garantie, 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 Sicherheitskonzepten und Sicherheitsleitlinien für 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 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 bei der Sicherheitsrisikobehandlung muss darin bestehen, ein Paket von Sicherheitsmaßnahmen anzuwenden, die zu einer zufriedenstellenden Ausgewogenheit zwischen den Anforderungen der Nutzer, den Kosten und dem Sicherheitsrestrisiko führen.

7. Die spezifischen Anforderungen, der Maßstab und Grad der Detaillierung, die von der einschlägigen 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.

▼B

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 Kommunikations- und Informationssystem einschließlich seiner technischen und nicht technischen Sicherheitsmaßnahmen wird während des Akkreditierungsverfahrens Sicherheitsprüfungen unterzogen, damit gewährleistet ist, dass das erforderliche Sicherheitsniveau erreicht wird, und geprüft wird, dass es korrekt implementiert, integriert und konfiguriert wird.

11. Sicherheitsbewertungen, -inspektionen und -überprüfungen 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 weiterentwickelt als integraler Bestandteil des Prozesses eines Änderungs- und Konfigurationsmanagements.

Optimale Vorgehensweisen

13. Das Generalsekretariat des Rates und die Mitgliedstaaten arbeiten 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, physischer 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 Union, 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 Generalsekretariat des Rates und von den Mitgliedstaaten betriebenen Kommunikations- und Informationssystemen erreicht wird, die EU-VS bearbeiten.

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 Angriffs auf möglichst wenige Informationen oder Werte des Kommunikations- und Informationssystemen zu begrenzen und weiteren Schaden zu verhindern, und

    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, wird durch eine Risikobewertung bestimmt.

17. Die Nationale Sicherheitsbehörde oder eine andere zuständige Behörde trägt dafür Sorge, dass

    a) Cyberabwehrfähigkeiten implementiert werden, damit auf Bedrohungen, die die Grenzen einer Organisation oder eines Staates überschreiten können, reagiert werden kann, und

▼B

b) die Reaktionen koordiniert und Informationen über diese Bedrohungen, Zwischenfälle und damit zusammenhängende Risikokonstellationen 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 Genehmigungen, 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 Informationssicherung

21. 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 erheblich schaden;

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

c) sie 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, müssen Schulung und Sensibilisierung in Bezug auf Informationssicherung für das gesamte beteiligte Personal, einschließlich des Führungspersonals, und die Nutzer von Kommunikations- und Informationssystemen obligatorisch sein.

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 (CAA) eines Mitgliedstaats evaluiert und zugelassen.

26. Bevor kryptografische Produkte dem Rat oder dem Generalsekretär gemäß Artikel 10 Absatz 6 zur Zulassung empfohlen werden, müssen sie eine Zweitevaluierung durch eine entsprechend 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. Der Rat billigt ein Sicherheitskonzept in Bezug auf die Evaluierung und Zulassung von kryptografischen Produkten.

27. Wenn dies aus spezifischen operativen Gründen gerechtfertigt ist, kann der Rat oder gegebenenfalls der Generalsekretär auf Empfehlung des Sicherheitsausschusses auf die Anforderungen nach Nummer 25 oder 26 dieses Anhangs verzichten und eine vorläufige Zulassung für einen spezifischen Zeitraum gemäß dem Verfahren nach Artikel 10 Absatz 6 erteilen.

▼B

28. Der Rat kann auf Empfehlung des Sicherheitsausschusses den Bewertungs-, Auswahl- und Zulassungsprozess eines Drittstaats oder einer internationalen Organisation für kryptografische Produkte anerkennen und dementsprechend diese kryptografischen Produkte als für den Schutz von an den betreffenden Drittstaat oder die betreffende internationale Organisation weitergegebenen EU-VS zugelassen ansehen.

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

30. Der Rat billigt ein Sicherheitskonzept in Bezug auf die Eignung und Zulassung von nichtkryptografischen IT-Sicherheitsprodukten.

Übermittlung innerhalb abgesicherter Bereiche und innerhalb von Verwaltungsbereichen

31. 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

32. 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.

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

34. 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 durch die zuständigen SAA, und

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

35. 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 Dienste für den Schutz von Systemübergängen verfügt, die zu diesem Zweck zwischen dem Kommunikations- und Informationssystem und dem ungeschützten oder öffentlichen Netz installiert wurden. Die Sicherheitsmaßnahmen für eine derartige Zusammenschaltung werden von der zuständigen Stelle für Informationssicherung 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 10 zugelassenes kryptografisches Produkt verschlüsselt werden, gilt eine derartige Verbindung nicht als Zusammenschaltung.

36. 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

37. Die Vernichtung elektronischer Datenträger erfolgt nach Verfahren, die von der zuständigen Sicherheitsbehörde genehmigt wurden.

▼B

38. Elektronische Datenträger werden nach gemäß Artikel 6 Absatz 2 festzulegenden Sicherheitsleitlinien wiederverwendet, herabgestuft oder freigegeben.

Notsituationen

39. Unbeschadet der Bestimmungen dieses Beschlusses können in einer Notsituation wie beispielsweise drohenden oder bereits eingetretenen Krisen, Konflikten, Kriegssituationen oder im Fall besonderer operativer Umstände die nachstehend beschriebenen besonderen Verfahren angewandt werden.

40. EU-VS können mit Hilfe 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 Preisgabe 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.

41. 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.

42. Wird gemäß Nummer 39 vorgegangen, ist der zuständigen Behörde und dem Sicherheitsausschuss anschließend Bericht zu erstatten.

III FUNKTIONEN UND STELLEN FÜR INFORMATIONSSICHERUNG

43. In den Mitgliedstaaten und beim Generalsekretariat des Rates werden die nachstehenden Funktionen für Informationssicherung geschaffen. 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.

Information Assurance Authority (Stelle für Informationssicherung)

44. Die Stelle für Informationssicherung (IAA) ist für Folgendes zuständig:

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

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

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

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

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

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

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

▼B

TEMPEST Authority (TEMPEST-Stelle)

45. Die TEMPEST-Stelle (TA) 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.

Crypto Approval Authority (Krypto-Zulassungsstelle)

46. Die Krypto-Zulassungsstelle (CAA) hat sicherzustellen, dass kryptografische Produkte den nationalen Kryptografiekonzepten bzw. dem Kryptografiekonzept des Rates entsprechen. Sie erteilt für ein kryptografisches Produkt die Zulassung, EU-VS bis zu einem bestimmten Geheimhaltungsgrad in dem betreffenden Betriebsumfeld zu schützen. Was die Mitgliedstaaten anbelangt, so ist die CAA ferner dafür zuständig, kryptografische Produkte zu evaluieren.

Crypto Distribution Authority (Krypto-Verteilungsstelle)

47. Die Krypto-Verteilungsstelle (CDA) ist für Folgendes zuständig:

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

b) Gewährleistung, dass für das gesamte EU-Kryptomaterial in Bezug auf Rechenschaftspflicht, sichere Bearbeitung, Speicherung und Verteilung geeignete Verfahren durchgesetzt und Kanäle eingerichtet werden, und

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

Security Accreditation Authority (Sicherheits-Akkreditierungsstelle)

48. Die Sicherheits-Akkreditierungsstelle (SAA) für das jeweilige System ist für Folgendes zuständig:

a) Gewährleistung, dass die Kommunikations- und Informationssysteme den einschlägigen Sicherheitskonzepten und 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 Konzepten 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 (im Folgenden „SSRS“), der Dokumentation über die Überprüfung der Sicherheitsimplementierung und der sicherheitsbezogenen Betriebsverfahren (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, -kontrollen oder -überprüfungen;

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;

▼B

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

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.

49. Die SAA des Generalsekretariats des Rates ist für die Akkreditierung aller Kommunikations- und Informationssysteme zuständig, die im Zuständigkeitsbereich des Generalsekretariats des Rates betrieben werden.

50. Die einschlägige SAA eines Mitgliedstaats ist für die Akkreditierung von Kommunikations- und Informationssystemen und deren Komponenten zuständig, die im Zuständigkeitsbereich eines Mitgliedstaats betrieben werden.

51. Wenn Kommunikations- und Informationssysteme in die Zuständigkeit sowohl der SAA des Generalsekretariats des Rates als auch der SAA der Mitgliedstaaten fallen, so nimmt ein gemeinsames Sicherheits-Akkreditierungsgremium (Security Accreditation Board, SAB) die Akkreditierung des betreffenden Systems vor. Es setzt sich aus einem SAA-Vertreter jedes Mitgliedstaats zusammen, und ein SAA-Vertreter der Kommission nimmt 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 Generalsekretariats des Rates. 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 regelmäßig Berichte über seine Tätigkeit und übermittelt ihm alle Akkreditierungserklärungen.

Für den Betrieb zuständige Stelle für Informationssicherung

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

a) Ausarbeitung der Sicherheitsdokumentation im Einklang mit den Sicherheitskonzepten und 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 übernehmen 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 TA 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 und

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

▼B

ANHANG V

GEHEIMSCHUTZ IN DER WIRTSCHAFT

I. EINLEITUNG

1. Dieser Anhang enthält Bestimmungen zur Anwendung von Artikel 11. Er legt allgemeine Sicherheitsvorschriften für industrielle oder andere Unternehmen fest, die während der Verhandlungen vor der Auftragsvergabe und während der Laufzeit von vom Rat vergebenen und als Verschlusssache eingestuften Aufträgen gelten.

2. Der Rat billigt Leitlinien für den Geheimschutz in der Wirtschaft, mit denen insbesondere ausführliche Anforderungen in Bezug auf Sicherheitsbescheide für Unternehmen (FSC), Geheimschutzklauseln (SAL), Besuche sowie die Übermittlung und Beförderung von EU-VS aufgestellt werden.

II. SICHERHEITSBESTIMMUNGEN BEI ALS VERSCHLUSSSACHE EINGESTUFTEN AUFTRÄGEN

VS-Einstufungsliste (SCG)

3. Vor der Ausschreibung oder der Vergabe eines als Verschlusssache eingestuften Auftrags bestimmt das Generalsekretariat des Rates 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 das Generalsekretariat des Rates 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 VS-Einstufungsliste berücksichtigt das Generalsekretariat des Rates 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 globale Geheimhaltungsgrad des Auftrags darf nicht niedriger sein als der höchste Geheimhaltungsgrad eines einzelnen Teilauftrags, und

   c) gegebenenfalls setzt sich das Generalsekretariat des Rates 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 (SAL)

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

6. Die Geheimschutzklausel enthält die Bestimmungen, mit denen der Auftragnehmer und/oder Subauftragnehmer 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 (PSI)

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 PSI von der mit der Verwaltung des Programms oder Projekts beauftragten Vergabebehörde ausgearbeitet werden. Die Sicherheitsanweisung bedarf der Genehmigung durch die Nationalen

▼B

Sicherheitsbehörden/Beauftragten Sicherheitsbehörden der Mitgliedstaaten oder durch eine andere zuständige Sicherheitsbehörde, die an dem Programm/Projekt beteiligt ist, und kann zusätzliche Sicherheitserfordernisse beinhalten.

III. SICHERHEITSBESCHEID FÜR UNTERNEHMEN (FSC)

8. Ein Sicherheitsbescheid für Unternehmen wird von der Nationalen Sicherheitsbehörde oder der Beauftragten Sicherheitsbehörde oder einer anderen zuständigen Behörde eines Mitgliedstaats ausgestellt und gibt gemäß den innerstaatlichen Rechtsvorschriften Auskunft darüber, 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. Der Bescheid ist dem Generalsekretariat des Rates als der Vergabebehörde vorzulegen, bevor einem Auftragnehmer oder Subauftragnehmer bzw. einem möglichen Auftragnehmer oder Subauftragnehmer EU-VS zur Verfügung gestellt werden können oder ihm Zugang zu diesen gewährt werden kann.

9. Bei der Erteilung eines Sicherheitsbescheids für Unternehmen hat die zuständige Nationale Sicherheitsbehörde oder Beauftragte Sicherheitsbehörde zumindest Folgendes zu beachten:

a) Sie bewertet die Integrität des industriellen oder anderen Unternehmens;

b) sie bewertet die Eigentums- und Kontrollverhältnisse bzw. die Möglichkeit einer unzulässigen Einflussnahme unter dem Aspekt eines eventuellen Sicherheitsrisikos;

c) sie überprüft, ob das industrielle oder andere Unternehmen ein Sicherheitssystem eingeführt hat, das alle geeigneten Geheimschutzmaßnahmen umfasst, die nach den in diesem Beschluss niedergelegten Anforderungen zum Schutz von als „CONFIDENTIEL UE/EU CONFIDENTIAL“ oder „SECRET UE/EU SECRET“ eingestuften Informationen oder Materialien erforderlich sind;

d) sie überprüft, ob die Sicherheitsermächtigungen der Geschäftsführung, der Eigentümer und der Mitarbeiter, die Zugang zu als „CONFIDENTIEL UE/EU CONFIDENTIAL“ oder „SECRET UE/EU SECRET“ eingestuften Verschlusssachen benötigen, gemäß den Anforderungen dieses Beschlusses vorliegen, und

e) sie überprüft, ob das industrielle oder andere Unternehmen einen Sicherheitsbevollmächtigten benannt hat, der gegenüber seiner Geschäftsführung für die Durchsetzung der Geheimschutzmaßnahmen in diesem Unternehmen verantwortlich ist.

10. Das Generalsekretariat des Rates als Vergabebehörde teilt der zuständigen Nationalen Sicherheitsbehörde/Beauftragten Sicherheitsbehörde oder einer anderen zuständigen Sicherheitsbehörde gegebenenfalls mit, dass ein Sicherheitsbescheid für Unternehmen in der Phase vor der Auftragsvergabe oder für die Ausführung des Auftrags erforderlich ist. Ein Sicherheitsbescheid für Unternehmen oder eine Sicherheitsermächtigung 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.

11. Die Vergabebehörde vergibt keinen als Verschlusssache eingestuften Auftrag an einen bevorzugten Bieter, bevor sie von der Nationalen Sicherheitsbehörde/Beauftragten Sicherheitsbehörde oder einer anderen zuständigen Sicherheitsbehörde des Mitgliedstaats, in dem der betreffende Auftragnehmer oder Subauftragnehmer eingetragen ist, die Bestätigung erhalten hat, dass erforderlichenfalls ein entsprechender Sicherheitsbescheid für das Unternehmen erteilt wurde.

12. Die Nationale Sicherheitsbehörde/Beauftragte Sicherheitsbehörde oder eine sonstige zuständige Sicherheitsbehörde, die einen Sicherheitsbescheid erteilt hat, teilt dem Generalsekretariat des Rates als Vergabebehörde alle

▼B

Änderungen mit, die diesen Sicherheitsbescheid betreffen. Bei Subaufträgen ist die Nationale Sicherheitsbehörde/Beauftragte Sicherheitsbehörde oder eine sonstige zuständige Sicherheitsbehörde entsprechend zu informieren.

13. Die Aufhebung eines Sicherheitsbescheids für Unternehmen durch die jeweilige Nationale Sicherheitsbehörde/Beauftragte Sicherheitsbehörde oder eine sonstige zuständige Sicherheitsbehörde stellt für das Generalsekretariat des Rates als Vergabebehörde einen ausreichenden Grund dar, den als Verschlusssache eingestuften Auftrag zu kündigen oder einen Bieter vom Vergabeverfahren auszuschließen.

IV. ALS VERSCHLUSSSACHE EINGESTUFTE AUFTRÄGE UND SUBAUFTRÄGE

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

15. Sobald der Zuschlag für einen als Verschlusssache eingestuften Auftrag oder Subauftrag erteilt wurde, teilt das Generalsekretariat des Rates als Vergabebehörde der Nationalen Sicherheitsbehörde/Beauftragten Sicherheitsbehörde des Auftragnehmers oder Subauftragnehmers oder einer sonstigen zuständigen Sicherheitsbehörde die Sicherheitsvorschriften für den als Verschlusssache eingestuften Auftrag mit.

16. Werden diese Aufträge gekündigt, so informiert das Generalsekretariat des Rates als Vergabebehörde (und/oder gegebenenfalls die Nationale Sicherheitsbehörde/Beauftragte Sicherheitsbehörde oder eine sonstige zuständige Sicherheitsbehörde bei Subaufträgen) unverzüglich die Nationale Sicherheitsbehörde/Beauftrage Sicherheitsbehörde oder eine sonstige zuständige Sicherheitsbehörde des Mitgliedstaats, in dem der Auftragnehmer oder Subauftragnehmer eingetragen ist.

17. Generell ist der Auftragnehmer oder Subauftragnehmer verpflichtet, bei der Kündigung eines als Verschlusssache eingestuften Auftrags oder Subauftrags in seinem Besitz befindliche EU-VS an die Vergabebehörde zurückzugeben.

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

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

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

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

22. 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 Subauftragnehmer EU-VS nicht ohne die vorherige schriftliche Einwilligung der Vergabebehörde zur Verfügung.

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

▼B

V. BESUCHE IM ZUSAMMENHANG MIT ALS VERSCHLUSSSACHE EINGESTUFTEN AUFTRÄGEN

24. Benötigt Personal des Generalsekretariats des Rates, der Auftragnehmer oder der Subauftragnehmer 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. Im Zusammenhang mit speziellen Projekten können die Nationalen Sicherheitsbehörden/Beauftragten Sicherheitsbehörden jedoch ein Verfahren vereinbaren, nach dem Besuche unmittelbar verabredet werden können.

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

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

VI. ÜBERMITTLUNG UND BEFÖRDERUNG VON EU-VS

27. Für die Übermittlung von EU-VS auf elektronischem Wege gelten die einschlägigen Bestimmungen des Artikels 10 und des Anhangs IV.

28. Für die Beförderung von EU-VS gelten die einschlägigen Bestimmungen des Anhangs III im Einklang mit den innerstaatlichen Rechtsvorschriften.

29. 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 Sicherheitsbescheid für Unternehmen des entsprechenden Geheimhaltungsgrads. In solchen Fällen müssen die Personen, die einen VS-Transport durchführen, eine Sicherheitsüberprüfung gemäß Anhang I durchlaufen haben;

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 von den betreffenden Nationalen Sicherheitsbehörden/Beauftragten Sicherheitsbehörden oder einer sonstigen zuständigen Sicherheitsbehörde genehmigt werden muss;

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

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 von der Nationalen Sicherheitsbehörde/Beauftragten Sicherheitsbehörde oder einer sonstigen zuständigen Sicherheitsbehörde sowohl des Staates des Absenders als auch des Staates des Empfängers genehmigt worden ist.

VII. WEITERGABE VON EU-VS AN AUFTRAGNEHMER IN DRITTSTAATEN

30. EU-VS werden an Auftragnehmer und Subauftragnehmer in Drittstaaten nach Maßgabe der Geheimschutzmaßnahmen weitergegeben, die zwischen dem Generalsekretariat des Rates als Vergabebehörde und der Nationalen Sicherheitsbehörde/Beauftragten Sicherheitsbehörde des betreffenden Drittstaats, in dem der Auftragnehmer eingetragen ist, vereinbart wurden.

▼B

VIII. ALS „RESTREINT UE/EU RESTRICTED“ EINGESTUFTE VERSCHLUSSSACHEN

31. Gegebenenfalls im Benehmen mit der Nationalen Sicherheitsbehörde/Beauftragten Sicherheitsbehörde des Mitgliedstaats ist das Generalsekretariat des Rates als Vergabebehörde berechtigt, Inspektionen der Anlagen von Auftragnehmern/Subauftragnehmern auf der Grundlage vertraglicher Bestimmungen durchzuführen, um zu überprüfen, dass die nach dem Vertrag erforderlichen einschlägigen Geheimschutzmaßnahmen zum Schutz von EU-VS des Geheimhaltungsgrads „RESTREINT UE/EU RESTRICTED“ getroffen wurden.

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

33. Bei Aufträgen des Generalsekretariats des Rates mit Informationen des Geheimhaltungsgrads „RESTREINT UE/EU RESTRICTED“ ist ein Sicherheitsbescheid für Unternehmen oder eine Sicherheitsermächtigung für Auftragnehmer und Subauftragnehmer und deren Personal nicht erforderlich.

34. Das Generalsekretariat des Rates 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 Sicherheitsbescheid für Unternehmen oder eine Sicherheitsermächtigung, die nach Maßgabe der innerstaatlichen Rechtsvorschriften gegebenenfalls bestehen.

35. Die Bedingungen für die Vergabe von Subaufträgen durch den Auftragnehmer stehen im Einklang mit Nummer 21.

36. Ist mit einem Auftrag die Bearbeitung von Verschlusssachen des Geheimhaltungsgrads „RESTREINT UE/EU RESTRICTED“ in einem Kommunikations- und Informationssystem verbunden, das vom Auftragnehmer betrieben wird, so stellt das Generalsekretariat des Rates als Vergabebehörde sicher, dass in dem Auftrag und etwaigen Subaufträgen die notwendigen technischen und organisatorischen 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.

▼B

ANHANG VI

AUSTAUSCH VON VERSCHLUSSSACHEN MIT DRITTSTAATEN UND INTERNATIONALEN ORGANISATIONEN

I. EINLEITUNG

1. Dieser Anhang enthält Bestimmungen zur Anwendung von Artikel 13.

II. VEREINBARUNGEN FÜR DEN AUSTAUSCH VON VERSCHLUSSSACHEN

2. Wenn der Rat feststellt, dass über einen längeren Zeitraum Verschlusssachen ausgetauscht werden müssen, wird

— ein Geheimschutzabkommen oder

— eine Verwaltungsvereinbarung

gemäß Artikel 13 Absatz 2 und den Abschnitten III und IV und auf der Grundlage einer Empfehlung des Sicherheitsausschusses geschlossen.

3. Werden EU-VS, die für die Zwecke einer GSVP-Operation erstellt wurden, Drittstaaten oder internationalen Organisationen, die an dieser Operation teilnehmen, zur Verfügung gestellt, ohne dass eine Vereinbarung im Sinne der Nummer 2 besteht, so richtet sich der Austausch von EU-VS mit dem beteiligten Drittstaat oder der beteiligten internationalen Organisation nach Maßgabe des Abschnitts V nach

— einem Rahmenabkommen über die Beteiligung,

— einem Ad-hoc-Abkommen über die Beteiligung oder

— einer Ad-hoc-Verwaltungsvereinbarung in Ermangelung eines der beiden vorgenannten Abkommen.

4. Besteht keine Vereinbarung im Sinne der Nummern 2 und 3 und wird beschlossen, EU-VS an einen Drittstaat oder eine internationale Organisation ausnahmsweise auf Ad-hoc-Basis gemäß Abschnitt VI weiterzugeben, so wird der betreffende Drittstaat bzw. die betreffende internationale Organisation um schriftliche Zusagen ersucht, um sicherzustellen, dass EU-VS, die an den Drittstaat/die internationale Organisation weitergegeben werden, im Einklang mit den in diesem Beschluss festgelegten Grundprinzipien und Mindeststandards geschützt werden.

III GEHEIMSCHUTZABKOMMEN

5. In Geheimschutzabkommen werden die Grundprinzipien und Mindeststandards für den Austausch von Verschlusssachen zwischen der Union und einem Drittstaat oder einer internationalen Organisation niedergelegt.

6. In Geheimschutzabkommen werden die technischen Durchführungsbestimmungen geregelt, die zwischen den zuständigen Sicherheitsbehörden der betreffenden Organe und Einrichtungen der Union und der zuständigen Sicherheitsbehörde des betreffenden Drittstaats bzw. der betreffenden internationalen Organisation zu vereinbaren sind. In den Durchführungsvereinbarungen ist das Schutzniveau, das die in dem betreffenden Drittstaat oder bei der betreffenden internationalen Organisation bestehenden Sicherheitsvorschriften, -strukturen und -verfahren gewährleisten, zu berücksichtigen. Sie werden vom Sicherheitsausschuss gebilligt.

7. EU-VS werden im Rahmen eines Geheimschutzabkommens nicht auf elektronischem Wege ausgetauscht, es sei denn, dies ist in dem Abkommen und/oder den entsprechenden technischen Durchführungsvereinbarungen ausdrücklich vorgesehen.

8. Schließt der Rat ein Geheimschutzabkommen mit Dritten, so wird bei jeder Vertragspartei eine Registratur als Haupteingangs- bzw. -ausgangsstelle für den Austausch von Verschlusssachen bestimmt.

▼B

9. Zur Bewertung der Wirksamkeit der Sicherheitsvorschriften, -strukturen und -verfahren des betreffenden Drittstaats bzw. der betreffenden internationalen Organisation werden im gegenseitigen Einvernehmen mit dem betreffenden Drittstaat bzw. der betreffenden internationalen Organisation Bewertungsbesuche durchgeführt. Diese Bewertungsbesuche werden gemäß den einschlägigen Bestimmungen des Anhangs III durchgeführt; dabei wird Folgendes bewertet:

   a) der für den Schutz von Verschlusssachen geltende Rechtsrahmen;

   b) alle spezifischen Merkmale des Sicherheitskonzepts und die Art und Weise der Organisation der Sicherheit in dem betreffenden Drittstaat oder bei der betreffenden internationalen Organisation, soweit sich dies darauf auswirken kann, welchen Geheimhaltungsgrad die auszutauschenden Verschlusssachen haben dürfen;

   c) die tatsächlich bestehenden Sicherheitsmaßnahmen und -verfahren und

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

10. Das Team, das Bewertungsbesuche im Namen der Union durchführt, bewertet die Frage, ob die Sicherheitsregelungen und -verfahren in dem betreffenden Drittstaat oder in der betreffenden internationalen Organisation für den Schutz von EU-VS einer bestimmten Geheimhaltungsstufe angemessen sind.

11. Die Ergebnisse dieser Besuche werden in einem Bericht festgehalten, auf dessen Grundlage der Sicherheitsausschuss festlegt, welches der höchste Geheimhaltungsgrad ist, bis zu dem EU-VS in Papierform und gegebenenfalls elektronisch mit dem betreffenden Dritten ausgetauscht werden dürfen, und welche speziellen Voraussetzungen hierfür gelten.

12. Es müssen alle Anstrengungen unternommen werden, die Besuche zur umfassenden Bewertung der Sicherheit in dem betreffenden Drittstaat oder bei der betreffenden internationalen Organisation vor Billigung der Durchführungsvereinbarungen durch den Sicherheitsausschuss durchzuführen, damit Art und Wirksamkeit des bestehenden Sicherheitssystems festgestellt werden können. Ist dies nicht möglich, erhält der Sicherheitsausschuss jedoch einen möglichst umfassenden Bericht des Sicherheitsbüros des Generalsekretariats des Rates auf der Grundlage der dem Büro vorliegenden Informationen, mit dem der Sicherheitsausschuss darüber unterrichtet wird, welche Sicherheitsvorschriften in dem betreffenden Drittstaat oder bei der betreffenden internationalen Organisation gelten und wie dort die Organisation der Sicherheit gehandhabt wird.

13. Der Bericht über den Bewertungsbesuch oder der Bericht nach Nummer 12, falls ein Bericht über den Bewertungsbesuch nicht vorliegt, muss dem Sicherheitsausschuss zugeleitet und von diesem als zufriedenstellend bewertet werden, bevor die EU-VS tatsächlich an den betreffenden Drittstaat oder die betreffende internationale Organisation weitergegeben werden.

14. Die zuständigen Sicherheitsbehörden der Organe und Einrichtungen der Union teilen dem betreffenden Drittstaat oder der betreffenden internationalen Organisation den Zeitpunkt, ab dem die Union in der Lage ist, EU-VS im Rahmen des Abkommens weiterzugeben, sowie den höchsten Geheimhaltungsgrad mit, bis zu dem EU-VS in Papierform oder elektronisch ausgetauscht werden dürfen.

15. Erforderlichenfalls werden Folgebesuche zu den Bewertungsbesuchen durchgeführt, insbesondere wenn

   a) der höchste Geheimhaltungsgrad, bis zu dem EU-VS weitergegeben werden dürfen, geändert werden muss,

   b) der Union grundlegende Änderungen der Sicherheitsvorkehrungen des betreffenden Drittstaats oder der betreffenden internationalen Organisation mitgeteilt werden, die sich auf die Art und Weise auswirken könnten, wie der Dritte EU-VS schützt, oder

   c) es zu einem schwerwiegenden Sicherheitsvorfall mit unbefugter Weitergabe von EU-VS gekommen ist.

▼B

16. Sobald das Geheimschutzabkommen in Kraft getreten ist und Verschlusssachen mit dem betreffenden Drittstaat oder der betreffenden internationalen Organisation ausgetauscht werden, kann der Sicherheitsausschuss insbesondere im Lichte der weiteren Bewertungsbesuche beschließen, den höchsten Geheimhaltungsgrad, bis zu dem EU-VS in Papierform oder elektronisch ausgetauscht werden dürfen, zu ändern.

IV. VERWALTUNGSVEREINBARUNGEN

17. Wenn langfristig die Notwendigkeit besteht, mit einem Drittstaat oder einer internationalen Organisation Verschlusssachen, die in der Regel höchstens in den Geheimhaltungsgrad „RESTREINT UE/EU RESTRICTED“ eingestuft sind, auszutauschen, und wenn der Sicherheitsausschuss festgestellt hat, dass die betreffende Vertragspartei nicht über ein ausreichend entwickeltes Sicherheitssystem verfügt, um ein Geheimschutzabkommen abschließen zu können, kann der Generalsekretär vorbehaltlich der Zustimmung des Rates im Namen des Generalsekretariats des Rates eine Verwaltungsvereinbarung mit den zuständigen Stellen des betreffenden Drittstaats oder mit der betreffenden internationalen Organisation schließen.

18. Wenn aus dringenden operativen Gründen rasch ein rechtlicher Rahmen für den Austausch von Verschlusssachen geschaffen werden muss, kann der Rat ausnahmsweise beschließen, dass eine Verwaltungsvereinbarung für den Austausch von Informationen eines höheren Geheimhaltungsgrads geschlossen wird.

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

20. Es wird ein Bewertungsbesuch gemäß Nummer 9 durchgeführt und der Bericht oder der Bericht nach Nummer 12, falls ein Bericht über den Bewertungsbesuch nicht vorliegt, dem Sicherheitsausschuss zugeleitet, der den Bericht als zufriedenstellend bewerten muss, bevor die EU-VS tatsächlich an den betreffenden Drittstaat oder die betreffende internationale Organisation weitergegeben werden.

21. EU-VS werden nicht im Rahmen einer Verwaltungsvereinbarung auf elektronischem Wege ausgetauscht, es sei denn, dies ist in der Vereinbarung ausdrücklich vorgesehen.

V. AUSTAUSCH VON VERSCHLUSSSACHEN IM RAHMEN VON GSVP-OPERATIONEN

22. Die Beteiligung von Drittstaaten oder internationalen Organisationen an GSVP-Operationen wird in Rahmenabkommen über die Beteiligung geregelt. Diese Abkommen enthalten Bestimmungen über die Weitergabe von für die Zwecke der GSVP-Operationen erstellten EU-VS an die beteiligten Drittstaaten oder internationalen Organisationen. Der höchstzulässige Geheimhaltungsgrad von EU-VS, die ausgetauscht werden können, ist der Geheimhaltungsgrad „RESTREINT UE/EU RESTRICTED“ für zivile GSVP-Operationen und „CONFIDENTIEL UE/EU CONFIDENTIAL“ für militärische GSVP-Operationen, es sei denn, dass im Beschluss zur Einrichtung der jeweiligen GSVP-Operation etwas anderes festgelegt ist.

23. Ad-hoc-Abkommen über die Beteiligung, die für eine spezielle GSVP-Operation geschlossen werden, enthalten Bestimmungen über die Weitergabe von für die Zwecke dieser Operation erstellten EU-VS an den beteiligten Drittstaat oder die beteiligte internationale Organisation. Der höchstzulässige Geheimhaltungsgrad von EU-VS, die ausgetauscht werden können, ist der Geheimhaltungsgrad „RESTREINT UE/EU RESTRICTED“ für zivile GSVP-Operationen und „CONFIDENTIEL UE/EU CONFIDENTIAL“ für militärische GSVP-Operationen, es sei denn, dass im Beschluss zur Einrichtung der jeweiligen GSVP-Operation etwas anderes festgelegt ist.

▼B

24. Besteht kein Geheimschutzabkommen, so wird bis zum Abschluss eines Abkommens über die Beteiligung die Weitergabe von für die Zwecke dieser Operation erstellten EU-VS an einen an der Operation beteiligten Drittstaat oder an eine an der Operation beteiligte internationale Organisation durch eine vom Hohen Vertreter einzugehende Verwaltungsvereinbarung geregelt oder unterliegt einem Beschluss über die Ad-hoc-Weitergabe nach Abschnitt VI. EU-VS können im Rahmen einer solchen Vereinbarung nur so lange ausgetauscht werden, wie die Beteiligung des Drittstaats oder der internationalen Organisation immer noch geplant ist. Der höchstzulässige Geheimhaltungsgrad von EU-VS, die ausgetauscht werden können, ist der Geheimhaltungsgrad „RESTREINT UE/EU RESTRICTED“ für zivile GSVP-Operationen und „CONFIDENTIEL UE/EU CONFIDENTIAL“ für militärische GSVP-Operationen, es sei denn, dass im Beschluss zur Einrichtung der jeweiligen GSVP-Operation etwas anderes festgelegt ist.

25. In den in die Rahmenabkommen für eine Beteiligung, die Ad-hoc-Abkommen über eine Beteiligung und die unter den Nummern 22 bis 24 genannten Ad-hoc-Verwaltungsvereinbarungen aufzunehmenden Bestimmungen über Verschlusssachen wird festgelegt, dass der betreffende Drittstaat oder die betreffende internationale Organisation dafür zu sorgen hat, dass sein/ihr für eine Operation abgeordnetes Personal EU-VS im Einklang mit den Sicherheitsvorschriften des Rates und den von den zuständigen Stellen — einschließlich der Befehlskette der Operation — erteilten sonstigen Weisungen schützt.

26. 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 Rahmenabkommen über eine Beteiligung, des Ad-hoc-Abkommens über eine Beteiligung oder der Ad-hoc-Verwaltungsvereinbarung.

27. Der Austausch von EU-VS auf elektronischem Wege im Rahmen eines Rahmenabkommens über eine Beteiligung, eines Ad-hoc-Abkommens über eine Beteiligung oder einer Ad-hoc-Verwaltungsvereinbarung mit einem Drittstaat oder einer internationalen Organisation ist nicht zulässig, es sei denn, dies ist in dem betreffenden Abkommen oder der betreffenden Vereinbarung ausdrücklich vorgesehen.

28. Für die Zwecke einer GSVP-Operation erstellte EU-VS können gemäß den Nummern 22 bis 27 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.

29. Besteht kein Geheimschutzabkommen, so kann im Falle eines speziellen und dringenden operativen Bedarfs die Weitergabe von EU-VS an den Aufnahmestaat, in dessen Hoheitsgebiet die GSVP-Operation durchgeführt wird, durch eine vom Hohen Vertreter einzugehende Verwaltungsvereinbarung geregelt werden. Diese Möglichkeit ist im Beschluss zur Einrichtung der GSVP-Operation vorzusehen. Unter diesen Umständen dürfen nur EU-VS weitergegeben werden, die für die Zwecke der GSVP-Operation erstellt wurden und keinen höheren Geheimhaltungsgrad als „RESTREINT UE/EU RESTRICTED“ aufweisen, es sei denn, in dem Beschluss zur Einrichtung der GSVP-Operation ist ein höherer Geheimhaltungsgrad festgelegt. Im Rahmen einer derartigen Verwaltungsvereinbarung ist der Aufnahmestaat verpflichtet, die EU-VS gemäß Mindeststandards zu schützen, die nicht weniger streng als die in dem vorliegenden Beschluss festgelegten Mindeststandards sind.

▼B

30. Besteht kein Geheimschutzabkommen, so kann die Weitergabe von EU-VS an einschlägige Drittstaaten und internationale Organisationen, die nicht an einer GSVP-Operation beteiligt sind, durch eine vom Hohen Vertreter einzugehende Verwaltungsvereinbarung geregelt werden. Gegebenenfalls wird diese Möglichkeit — sowie alle damit verbundenen Bedingungen — in dem Beschluss zur Einrichtung der GSVP-Operation vorgesehen. Unter diesen Umständen dürfen nur EU-VS weitergegeben werden, die für die Zwecke der GSVP-Operation erstellt wurden und keinen höheren Geheimhaltungsgrad als „RESTREINT UE/EU RESTRICTED“ aufweisen, es sei denn, in dem Beschluss zur Einrichtung der GSVP-Operation ist ein höherer Geheimhaltungsgrad festgelegt. Im Rahmen einer derartigen Verwaltungsvereinbarung wird der betreffende Drittstaat oder die betreffende internationale Organisation verpflichtet, die EU-VS gemäß Mindeststandards zu schützen, die nicht weniger streng als die in dem vorliegenden Beschluss festgelegten Mindeststandards sind.

31. Vor der Durchführung der Bestimmungen über die Weitergabe von EU-VS entsprechend den Nummern 22, 23 und 24 sind keine Durchführungsvereinbarungen oder Bewertungsbesuche erforderlich.

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

32. Wenn kein rechtlicher Rahmen gemäß den Abschnitten III bis V besteht und der Rat oder eines seiner Vorbereitungsgremien beschließt, dass es in einem Ausnahmefall notwendig ist, an einen Drittstaat oder eine internationale Organisation EU-VS weiterzugeben, verfährt das Generalsekretariat des Rates wie folgt:

a) Es 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, und

b) es ersucht den Sicherheitsausschuss um eine Empfehlung, in der dieser anhand der verfügbaren Informationen zu der Frage Stellung nimmt, wie vertrauenswürdig die Sicherheitsvorschriften, -strukturen und -verfahren in dem Drittstaat oder bei der internationalen Organisation sind, an den/die die EU-VS weitergegeben werden sollen.

33. Spricht sich der Sicherheitsausschuss in seiner Empfehlung für die Weitergabe der EU-VS aus, so wird die Angelegenheit an den Ausschuss der Ständigen Vertreter (AStV) verwiesen, der über die Weitergabe der Verschlusssachen entscheidet.

34. Spricht sich der Sicherheitsausschuss in seiner Empfehlung gegen die Weitergabe der EU-VS aus, so erfolgt

a) bei Angelegenheiten, die unter die GASP/GSVP fallen, eine Erörterung der Frage durch das Politische und Sicherheitspolitische Komitee, das eine Empfehlung für eine Entscheidung des AStV formuliert;

b) bei allen anderen Angelegenheiten eine Erörterung der Frage durch den AStV, der eine Entscheidung trifft.

35. Falls es für sinnvoll erachtet wird, kann der AStV — vorbehaltlich der vorherigen schriftlichen Zustimmung des Herausgebers — entscheiden, dass die Verschlusssachen nur teilweise oder nur nach einer Herabstufung oder Aufhebung ihres Geheimhaltungsgrads weitergegeben werden dürfen oder dass die weiterzugebenden Informationen ohne Bezug auf die Quelle oder den ursprünglichen EU-Geheimhaltungsgrad erstellt werden.

36. Im Anschluss an die Entscheidung über die Weitergabe der EU-VS übermittelt das Generalsekretariat des Rates das betreffende Dokument, auf dem durch eine Weitergabekennzeichnung angegeben wird, an welchen Drittstaat oder welche internationale Organisation es weitergegeben wurde. Vor oder bei der tatsächlichen Weitergabe muss der betreffende Dritte sich schriftlich verpflichten, die empfangenen EU-VS gemäß den Grundprinzipien und Mindeststandards dieses Beschlusses zu schützen.

▼B

VII. ERMÄCHTIGUNG ZUR WEITERGABE VON EU-VS AN DRITTSTAATEN ODER INTERNATIONALE ORGANISATIONEN

37. Besteht eine Vereinbarung gemäß Nummer 2 für den Austausch von Verschlusssachen mit einem Drittstaat oder einer internationalen Organisation, so beschließt der Rat, dass der Generalsekretär ermächtigt wird, EU-VS an den betreffenden Drittstaat oder die betreffende internationale Organisation im Einklang mit dem Grundsatz der Zustimmung des Herausgebers weiterzugeben. Der Generalsekretär kann eine solche Ermächtigung an leitende Beamte des Generalsekretariats des Rates delegieren.

38. Besteht ein Geheimschutzabkommen gemäß Nummer 2 erster Gedankenstrich, so kann der Rat beschließen, dass der Hohe Vertreter ermächtigt wird, vom Rat im Bereich der Gemeinsamen Außen und Sicherheitspolitik herausgegebene EU-VS an den betreffenden Drittstaat oder an die betreffende internationale Organisation weiterzugeben, nachdem die Zustimmung des Herausgebers von darin enthaltenem Quellenmaterial eingeholt wurde. Der Hohe Vertreter kann eine solche Ermächtigung an leitende Beamte des EAD oder an EU-Sonderbeauftragte delegieren.

39. Besteht eine Vereinbarung gemäß Nummer 2 oder 3 für den Austausch von Verschlusssachen mit einem Drittstaat oder einer internationalen Organisation, so ist der Hohe Vertreter ermächtigt, EU-VS im Einklang mit dem Beschluss zur Einrichtung der GSVP-Operation und nach dem Grundsatz der Zustimmung des Herausgebers weiterzugeben. Der Hohe Vertreter kann eine solche Ermächtigung an leitende Beamte des EAD, an Befehlshaber von Operationen, Einsatzkräften oder Missionen der EU oder an EU-Missionsleiter delegieren.

▼B

Anlagen

Anlage A

Begriffsbestimmungen

Anlage B

Entsprechungstabelle der Geheimhaltungsgrade

Anlage C

Liste der Nationalen Sicherheitsbehörden

Anlage D

Abkürzungsverzeichnis

▼B

Anlage A

BEGRIFFSBESTIMMUNGEN

Für die Zwecke dieses Beschlusses gelten folgende Begriffsbestimmungen:

„Akkreditierung“: das Verfahren, das zu einer förmlichen Erklärung der Sicherheits-Akkreditierungsstelle (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 anerkanntes Bündel von Sicherheitsmaßnahmen in den Bereichen Technik, physischer Schutz, Organisation und Verfahren durchgeführt wird;

„als Verschlusssache eingestufter Auftrag“: ein Vertrag zwischen dem Generalsekretariat des Rates 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 Subauftrag“: ein Vertrag zwischen einem Auftragnehmer des Generalsekretariats des Rates und einem anderen Auftragnehmer (d. h. dem Subauftragnehmer) 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;

„Aufhebung des Geheimhaltungsgrades“: Löschung jeder Geheimhaltungskennzeichnung;

„Auftragnehmer“: eine Einzelperson oder Rechtsperson, die geschäftsfähig ist;

„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, Freigabe und Zerstörung. In Bezug auf Kommunikations- und Informationssysteme umfasst sie ferner die Sammlung, Darstellung, Übermittlung und Speicherung;

„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 dazu qualifizierten Behörde wahrgenommen werden;

„Bedrohung“: eine potenzielle Ursache für einen unerwünschten Zwischenfall, 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;

„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 ist;

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

▼B

„EU-Verschlusssachen“ (EU-VS) — siehe Artikel 2 Absatz 1;

„Geheimschutz in der Wirtschaft“ — siehe Artikel 11 Absatz 1;

„Geheimschutzklausel“ (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;

„Genehmigung für den Zugang zu EU-VS“: einen Beschluss der Anstellungsbehörde des Generalsekretariats des Rates aufgrund der von einer zuständigen Behörde eines Mitgliedstaats getroffenen Feststellung, dass einem Beamten des Generalsekretariats, einem anderen Bediensteten oder einem abgeordneten nationalen Experten bis zu einem bestimmten Zeitpunkt und bis zu einem bestimmten Geheimhaltungsgrad („CONFIDENTIEL UE/EU CONFIDENTIAL“ oder höher) Zugang zu EU-VS gewährt werden kann, sofern die betreffende Person nachweislich Kenntnis von Verschlusssachen haben muss und sie über ihre Verantwortlichkeiten angemessen belehrt worden ist;

„GSVP-Operation“: militärische oder zivile Krisenbewältigungsoperationen nach Titel V Kapitel 2 EUV;

„Herabstufung“: die Einstufung in einen niedrigeren Geheimhaltungsgrad;

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

„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 selbständige Tätigkeit ausüben, handeln;

„Informationssicherung“ — siehe Artikel 10 Absatz 1;

„Kommunikations- und Informationssystem“ — siehe Artikel 10 Absatz 2;

„kryptografisches Material (Kryptomaterial)“: kryptografische Algorithmen, kryptografische Hardware- und Softwaremodule und Produkte, die Implementierungsdetails enthalten, sowie die dazugehörige Dokumentation und das Verschlüsselungsmaterial;

„kryptografisches Produkt“: ein Erzeugnis, dessen erste und wichtigste Funktion es ist, durch einen oder mehrere kryptografische Mechanismen Sicherheitsdienste (Vertraulichkeit, Integrität, Verfügbarkeit, Authentizität, Beweisbarkeit) bereitzustellen;

„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;

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

▼B

„materieller Geheimschutz“ — siehe Artikel 8 Absatz 1;

„mehrschichtige Sicherheit“ (defence in depth): die Anwendung einer Reihe von Sicherheitsmaßnahmen in Form eines mehrschichtigen Abwehrsystems;

„personeller Geheimschutz“ — siehe Artikel 7 Absatz 1;

„Registrierung“ — siehe Anhang III Nummer 18;

„Restrisiko“: das Risiko, das nach dem Ergreifen von Sicherheitsmaßnahmen verbleibt, da 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 Entscheidung, hinzunehmen, dass nach der Risikobehandlung ein Restrisiko fortbesteht;

— „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;

— „Risikobehandlung“: die Abschwächung, Beseitigung oder Verringerung des Risikos (durch geeignete Maßnahmen in Bezug auf Technik, materielle Aspekte, Verwaltung oder Verfahren), der Risikotransfer oder die Überwachung des Risikos;

„Schwachstelle“: Vorliegen einer Schwäche, die bei einer oder mehreren Bedrohungen ausgenutzt werden kann. Eine Schwachstelle kann durch ein Versäumnis entstehen oder sie kann sich auf eine Schwäche infolge nachlässiger, unvollständiger oder inkohärenter Kontrollen beziehen; sie kann die Technik, die Verfahren, die materiellen Eigenschaften, die Organisation oder den Betrieb betreffen.

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

▼B

„Sicherheitsbescheid für Unternehmen“ (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;

„Sicherheitsermächtigung“ (PSC): eine Erklärung einer zuständigen Behörde eines Mitgliedstaats, die im Anschluss an den Abschluss einer Sicherheitsüberprüfung durch die zuständigen Behörden eines Mitgliedstaats abgegeben wird und bescheinigt, dass einer Person bis zu einem bestimmten Zeitpunkt und bis zu einem bestimmten Geheimhaltungsgrad („CONFIDENTIEL UE/EU CONFIDENTIAL“ oder höher) Zugang zu EU-VS gewährt werden kann;

„Sicherheitsermächtigungsbescheinigung“ (PSCC): eine von einer zuständigen Behörde ausgestellte Bescheinigung, in der festgestellt wird, dass eine Person sicherheitsüberprüft ist und eine gültige Sicherheitsermächtigungsbescheinigung oder Genehmigung der Anstellungsbehörde 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, das Gültigkeitsdatum der betreffenden Sicherheitsermächtigung und das Ablaufdatum der Bescheinigung selbst hervorgehen;

„Sicherheitsmodus des Betriebs“: Definition der Bedingungen, unter denen ein Kommunikations- und Informationssystem arbeitet, auf der Grundlage des Geheimhaltungsgrads der bearbeiteten Informationen und der Überprüfungsniveaus, der formellen Zugangsgenehmigungen und des berechtigten Informationsbedarfs seiner Nutzer. Für die Bearbeitung von Verschlusssachen und deren Übermittlung gibt es vier Betriebsmodi: Dedicated, System-high, Compartmented und Multilevel:

— „Modus ‚Dedicated‘“: Betriebsart, bei der alle Personen, die Zugang zum Kommunikations- und Informationssystem haben, für den Zugriff bis zum höchsten im Kommunikations- und Informationssystem bearbeiteten Geheimhaltungsgrad sicherheitsüberprüft sind und generell einen berechtigten Informationsbedarf in Bezug auf alle im Kommunikations- und Informationssystem bearbeiteten Informationen haben;

— „Modus ‚System-high‘“: Betriebsart, bei der alle Personen, die Zugang zum Kommunikations- und Informationssystem haben, für den Zugriff bis zum höchsten im Kommunikations- und Informationssystem bearbeiteten Geheimhaltungsgrad sicherheitsüberprüft sind, bei der aber nicht alle Personen, die Zugang zum Kommunikations- und Informationssystem haben, generell einen berechtigten Informationsbedarf in Bezug auf die im Kommunikations- und Informationssystem bearbeiteten Informationen haben; der Zugang zu Informationen kann von einer Einzelperson genehmigt werden;

— „Modus ‚Compartmented‘“: Betriebsart, bei der alle Personen, die Zugang zum Kommunikations- und Informationssystem haben, für den Zugriff bis zum höchsten im Kommunikations- und Informationssystem bearbeiteten Geheimhaltungsgrad sicherheitsüberprüft sind, bei der aber nicht alle Personen, die Zugang zum Kommunikations- und Informationssystem haben, über eine förmliche Ermächtigung zum Zugang zu allen im Kommunikations- und Informationssystem bearbeiteten Informationen verfügen; eine förmliche Ermächtigung setzt — im Gegensatz zur Ermessensentscheidung einer Einzelperson, Zugang zu gewähren — eine förmliche zentrale Verwaltung der Zugangskontrolle voraus;

▼B

— „Modus ‚Multi-level'": Betriebsart, bei der nicht alle Personen, die Zugang zum Kommunikations- und Informationssystem haben, für den Zugriff bis zum höchsten im Kommunikations- und Informationssystem bearbeiteten Geheimhaltungsgrad sicherheitsüberprüft sind und nicht alle Personen, die Zugang zum Kommunikations- und Informationssystem haben, generell einen berechtigten Informationsbedarf in Bezug auf die im Kommunikations- und Informationssystem bearbeiteten Informationen haben;

„Sicherheitsrisikomanagement-Prozess": der gesamte 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;

„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 Erteilung einer Sicherheitsermächtigung oder einer Genehmigung für den Zugang zu EU-VS bis zu einem bestimmten Geheimhaltungsgrad („CONFIDENTIEL UE/EU CONFIDENTIAL" oder höher) entgegenstehen würden;

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

„Verwaltung von Verschlusssachen" — siehe Artikel 9 Absatz 1;

„VS-Einstufungsliste" (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;

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

„Zusammenschaltung" — siehe Anhang IV Nummer 32.

▼M3

ANLAGE B

ENTSPRECHUNGSTABELLE DER GEHEIMHALTUNGSGRADE

EU	TRÈS SECRET UE/EU TOP SECRET	SECRET UE/EU SECRET	CONFIDENTIEL UE/EU CONFIDENTIAL	RESTREINT UE/EU 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 (Wet 11.12.1998)	siehe Fußnote ([1])
Bulgarien	Строго секретно	Секретно	Поверително	За служебно ползване
Tschechien	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 Abr: ΑΑΠ	Απόρρητο Abr: (ΑΠ)	Εμπιστευτικό Abr: (ΕΜ)	Περιορισμένης Χρήσης Abr: (ΠΧ)
Spanien	SECRETO	RESERVADO	CONFIDENCIAL	DIFUSIÓN LIMITADA
Frankreich	TRÈS SECRET TRÈS SECRET DÉFENSE ([3])	SECRET SECRET DÉFENSE ([3])	CONFIDENTIEL DÉFENSE ([3]), ([4])	siehe Fußnote ([5])
Kroatien	VRLO TAJNO	TAJNO	POVJERLJIVO	OGRANIČENO
Italien	Segretissimo	Segreto	Riservatissimo	Riservato
Zypern	Άκρως Απόρρητο Abr: (ΑΑΠ)	Απόρρητο Abr: (ΑΠ)	Εμπιστευτικό Abr: (ΕΜ)	Περιορισμένης Χρήσης Abr: (ΠΧ)
Lettland	Sevišķi slepeni	Slepeni	Konfidenciāli	Dienesta vajadzībām

▼M3

EU	TRÈS SECRET UE/EU TOP SECRET	SECRET UE/EU SECRET	CONFIDENTIEL UE/EU CONFIDENTIAL	RESTREINT UE/EU RESTRICTED
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 Top Secret	Sigriet Secret	Kunfidenzjali Confidential	Ristrett Restricted ([6])
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
Rumänien	Strict secret de importanţă 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	Kvalificerat hemlig	Hemlig	Konfidentiell	Begränsat hemlig

([1]) „Diffusion restreinte/Beperkte Verspreiding“ ist kein in Belgien verwendeter Geheimhaltungsgrad. Belgien behandelt 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]) Informationen, die Frankreich vor dem 1. Juli 2021 erstellt hat und die als „TRÈS SECRET DÉFENSE“, „SECRET DÉFENSE“ oder „CONFIDENTIEL DÉFENSE“ eingestuft sind, werden weiterhin auf dem gleichwertigen Schutzniveau von „TRÈS SECRET UE/EU TOP SECRET“, „SECRET UE/EU SECRET“ bzw. „CONFIDENTIEL UE/EU CONFIDENTIAL“ behandelt und geschützt.

([4]) Frankreich behandelt und schützt die als „CONFIDENTIEL UE/EU CONFIDENTIAL“ eingestuften Informationen gemäß den französischen Sicherheitsmaßnahmen für den Schutz von als „SECRET“ eingestuften Informationen.

([5]) Frankreich verwendet in seinem nationalen System nicht den Geheimhaltungsgrad „RESTREINT“. Frankreich behandelt 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.

([6]) Für Malta sind die maltesischen und englischen Kennzeichnungen austauschbar.

▼M3

ANLAGE C

LISTE DER NATIONALEN SICHERHEITSBEHÖRDEN

BELGIEN Autorité nationale de Sécurité SPF Affaires étrangères, Commerce extérieur et Coopération au Développement 15, rue des Petits Carmes 1000 Bruxelles Tel. Secretariat: +32 25014542 Fax +32 25014596 E-mail: nvo-ans@diplobel.fed.be	DÄNEMARK Politiets Efterretningstjeneste (Danish Security Intelligence Service) Klausdalsbrovej 1 2860 Søborg Tel. +45 45 15 90 07 Fax +45 45 15 01 90 Forsvarets Efterretningstjeneste (Danish Defence Intelligence Service) Kastellet 30 2100 Copenhagen Ø Tel. +45 33325566 Fax +45 33931320
BULGARIEN State Commission on Information Security 4 Kozloduy Str. 1202 Sofia Tel. +359 29333600 Fax +359 29873750 E-mail: dksi@government.bg Website: www.dksi.bg	DEUTSCHLAND Bundesministerium des Innern, für Bau und Heimat Section ATS II 5 Alt-Moabit 140 D-10557 Berlin Tel. +49 30186810 Fax +49 30186811441 E-mail 1: OESII5@bmi.bund.de E-mail 2: PersGS@bmi.bund.de
TSCHECHIEN Národní bezpečnostní úřad (National Security Authority) Na Popelce 2/16 150 06 Praha 56 Tel. +420 257283335 Fax +420 257283110 E-mail: oms@nbu.cz Website: www.nbu.cz	ESTLAND National Security Authority Department Estonian Foreign Intelligence Service Rahumäe tee 4B 11316 Tallinn Tel. +372 693 9211 Fax +372 693 5001 E-mail: nsa@fis.gov.ee
IRLAND National Security Authority Department of Foreign Affairs and Trade 76-78 Harcourt Street Dublin 2 D02 DX45 Ireland Tel. 1: +353 1 4082842 Tel. 2: +353 1 4082724 E-mail: nsa@dfa.ie	FRANKREICH Secrétariat général de la défense et de la sécurité nationale Sous-direction Protection du secret (SGDSN/PSD) 51 Boulevard de la Tour-Maubourg 75700 Paris 07 SP Tel. +33 171758177 Fax +33 171758200
GRIECHENLAND Γενικό Επιτελείο Εθνικής Άμυνας (ΓΕΕΘΑ) Διεύθυνση Ασφαλείας και Αντιπληροφοριών ΣΤΓ 1020 -Χολαργός (Αθήνα) Ελλάδα Τηλ.: +30 2106572045 (ώρες γραφείου) +30 2106572009 (ώρες γραφείου) Φαξ: +30 2106536279 +30 2106577612 Hellenic National Defence General Staff (HNDGS) Counter Intelligence and Security Directorate (NSA) 227-231 HOLARGOS STG 1020 ATHENS Tel. +30 2106572045 +30 2106572009 Fax +30 2106536279 +30 2106577612	KROATIEN Office of the National Security Council Croatian NSA Jurjevska 34 10000 Zagreb Croatia Tel. +385 14681222 Fax +385 14686049 E-mail: NSACroatia@uvns.hr Website: www.uvns.hr

▼**M3**

SPANIEN Autoridad Nacional de Seguridad Oficina Nacional de Seguridad Calle Argentona, 30 28023 Madrid Tel. +34 913725000 Fax +34 913725808 E-mail: nsa-sp@areatec.com	ITALIEN Presidenza del Consiglio dei Ministri Dipartimento Informazioni per la Sicurezza (DIS) Ufficio Centrale per la Segretezza (UCSe) Via Galilei, 32 00185 Roma Tel. +39 06478601 Fax +39 064885273 E-mail: nsa.ita@alfa.gov.it
ZYPERN ΥΠΟΥΡΓΕΙΟ ΑΜΥΝΑΣ ΣΤΡΑΤΙΩΤΙΚΟ ΕΠΙΤΕΛΕΙΟ ΤΟΥ ΥΠΟΥΡΓΟΥ ΑΜΥΝΑΣ ΕΘΝΙΚΗ ΑΡΧΗ ΑΣΦΑΛΕΙΑΣ (ΕΑΑ) Υπουργείο Άμυνας Λεωφόρος Στροβόλου 172-174, 1432 Λευκωσία Ταχυδρομικός Κώδικας: 2048 Τηλεφωνα: +357 22807569, +357 22807643, +357 22807764 Τηλεομοιότυπ: +357 22302351 Ηλεκτρονικό Ταχυδρομείο: cynsa@mod.gov.cy Ministry of Defence Minister's Military Staff National Security Authority (NSA) 172-174 Strovolou Avenue, 1432 Nicosia Postal code: 2048 Tel. +357 22807569, +357 22807643, +357 22807764 Fax +357 22302351 E-mail: cynsa@mod.gov.cy	LITAUEN Lietuvos Respublikos paslapčių apsaugos koordinavimo komisija (The Commission for Secrets Protection Coordination of the Republic of Lithuania National Security Authority) Pilaitės ave. 19 LT-06264 Vilnius Tel. +370 5 706 66128 Fax +370 706 66700 E-mail: nsa@vsd.lt
LETTLAND National Security Authority Constitution Protection Bureau of the Republic of Latvia P.O.Box 286 LV-1001 Riga Tel. +371 67025418 E-mail: ndi@sab.gov.lv	LUXEMBURG Autorité nationale de Sécurité Boîte postale 2379 1023 Luxembourg Tel. +352 24782210 central Tel. +352 24782253 direct Fax +352 24782243
UNGARN Nemzeti Biztonsági Felügyelet (National Security Authority of Hungary) 1024 Budapest, Szilágyi Erzsébet fasor 11/B Postal address: 1399 Budapest, Pf. 710/50 Tel. +36-1/391-1862 Fax +36-1/391-1889 E-mail: nbf@nbf.hu Website: www.nbf.hu	ÖSTERREICH Informationssicherheitskommission Bundeskanzleramt Ballhausplatz 2 1010 Wien Tel. +43 1 53115 202594 Fax +43 1 53109 202594 E-mail: isk@bka.gv.at
MALTA Ministry for Home Affairs and National Security P.O. Box 146 MT-Valletta Tel. +356 21249844 Fax +356 25695321	POLEN Agencja Bezpieczeństwa Wewnętrznego — ABW (Internal Security Agency) 2A Rakowiecka St. 00-993 Warszawa Tel. +48 225857663 Fax +48 225858509 E-mail: nsa@abw.gov.pl Website: www.abw.gov.pl

▼**M3**

NIEDERLANDE Ministerie van Binnenlandse Zaken en Koninkrijksrelaties Postbus 20010 2500 EA Den Haag Tel. +31 703204400 Fax +31 703200733 Ministerie van Defensie Beveiligingsautoriteit Postbus 20701 2500 ES Den Haag Tel. +31 703187060 Fax +31 703187522	PORTUGAL Presidência do Conselho de Ministros Autoridade Nacional de Segurança Rua da Junqueira, 69 1300-342 Lisboa Tel. +351 213031710 Fax +351 213031711
RUMÄNIEN Oficiul Registrului Naţional al Informaţiilor Secrete de Stat – Romanian NSA — ORNISS National Registry Office for Classified Information Strada Mureş nr. 4 012275 Bucharest Tel. +40 212075114 Fax +40 212240714 E-mail: nsa.romania@nsa.ro Website: www.orniss.ro	FINNLAND National Security Authority Ministry for Foreign Affairs P.O. Box 453 FI-00023 Government Tel. +358 9 16055890 E-mail: NSA@formin.fi
SLOWENIEN Urad Vlade RS za varovanje tajnih podatkov Šmartinska 152 1000 Ljubljana Tel. +386 147817570 Fax +386 14781399 E-mail: gp.uvtp@gov.si	SCHWEDEN Ministry for Foreign Affairs Swedish National Security Authority 103 39 Stockholm Tel. +46 8 405 10 00 E-mail: ud-nsa@gov.se
SLOWAKEI Národný bezpečnostný úrad (National Security Authority) Budatínska 30 851 06 Bratislava Tel. +421 2 6869 1111 Fax +421 2 6869 1700 E-mail: podatelna@nbu.gov.sk Website: www.nbu.gov.sk	

▼B

Anlage D

LISTE DER ABKÜRZUNGEN

Abkürzung	Bedeutung
AQUA	Appropriately Qualified Authority (entsprechend qualifizierte Behörde)
BPS	Boundary Protection Services (Dienste für den Schutz von Systemübergängen)
CAA	Crypto Approval Authority (Krypto-Zulassungsstelle)
CCTV	Closed Circuit Television (Videoüberwachung)
CDA	Crypto Distribution Authority (Krypto-Verteilungsstelle)
CFSP	Common Foreign and Security Policy (Gemeinsame Außen- und Sicherheitspolitik, GASP)
CIS	Communication and Information Systems handling EUCI (Kommunikations- und Informationssysteme, in denen EU-VS bearbeitet werden)
Coreper	Committee of Permanent Representatives (Ausschuss der Ständigen Vertreter, AStV)
CSDP	Common Security and Defence Policy (Gemeinsame Sicherheits- und Verteidigungspolitik, GSVP)
DSA	Designated Security Authority (Beauftragte Sicherheitsbehörde)
ECSD	European Commission Security Directorate (Direktion Sicherheit der Europäischen Kommission)
EUCI	EU Classified Information (EU-Verschlusssachen, EU-VS)
EUSR	EU Special Representative (EU-Sonderbeauftragter)
FSC	Facility Security Clearance (Sicherheitsbescheid für Unternehmen)
GSC	General Secretariat of the Council (Generalsekretariat des Rates)
IA	Information Assurance (Informationssicherung)
IAA	Information Assurance Authority (Stelle für Informationssicherung)
IDS	Intrusion Detection System (Einbruchsmeldeanlage)
IT	Information Technology (Informationstechnologie)
NSA	National Security Authority (Nationale Sicherheitsbehörde)
PSC	Personnel Security Clearance (Sicherheitsermächtigung)
PSCC	Personnel Security Clearance Certificate (Sicherheitsermächtigungsbescheinigung)
PSI	Programme/Project Security Instructions (Sicherheitsanweisung für ein Programm/Projekt)
SAA	Security Accreditation Authority (Sicherheits-Akreditierungsstelle)
SAB	Security Accreditation Board (Sicherheits-Akkreditierungsgremium)
SAL	Security Aspects Letter (Geheimschutzklausel)
SecOPs	Security Operating Procedures (sicherheitsbezogene Betriebsverfahren)
SCG	Security Classification Guide (VS-Einstufungsliste)
SSRS	System-Specific Security Requirement Statement (Aufstellung der systemspezifischen Sicherheitsanforderungen)
TA	TEMPEST Authority (TEMPEST-Stelle)