# BESCHLUSS (EU, Euratom) 2015/444 DER KOMMISSION

## vom 13. März 2015

## über die Sicherheitsvorschriften für den Schutz von EU-Verschlusssachen

DIE EUROPÄISCHE KOMMISSION —

gestützt auf den Vertrag über die Arbeitsweise der Europäischen Union, insbesondere auf Artikel 249,

gestützt auf den Vertrag zur Gründung der Europäischen Atomgemeinschaft, insbesondere auf Artikel 106,

gestützt auf das den Verträgen beigefügte Protokoll Nr. 7 über die Vorrechte und Befreiungen der Europäischen Union, insbesondere auf Artikel 18,

in Erwägung nachstehender Gründe:

(1) Die Sicherheitsvorschriften der Kommission für den Schutz von Verschlusssachen der Europäischen Union (EU-VS) müssen unter Berücksichtigung institutioneller, organisatorischer, operativer und technologischer Entwicklungen überprüft und aktualisiert werden.

(2) Die Europäische Kommission hat mit den Regierungen von Belgien, Luxemburg und Italien für ihre Hauptstandorte Vereinbarungen zu Sicherheitsfragen abgeschlossen. ([1])

(3) Die Kommission, der Rat und der Europäische Auswärtige Dienst sind entschlossen, gleichwertige Sicherheitsstandards für den Schutz von EU-VS anzuwenden.

(4) Es ist wichtig, dass gegebenenfalls das Europäische Parlament und die anderen Organe, Einrichtungen, Ämter oder Agenturen der Union an den Grundsätzen, Standards und Vorschriften für den Schutz von Verschlusssachen, die erforderlich sind, um die Interessen der Union und ihrer Mitgliedstaaten zu schützen, beteiligt sind.

(5) 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 Grundsätzen und Mindeststandards dieses Beschlusses festzulegen und diese Maßnahmen entsprechend dem Konzept der mehrschichtigen Sicherheit anzuwenden. Die Wirksamkeit der betreffenden Maßnahmen wird fortlaufend bewertet.

(6) In der Kommission beinhaltet der materielle Geheimschutz von Verschlusssachen die Anwendung von physischen und technischen Schutzmaßnahmen, mit denen ein unbefugter Zugang zu EU-VS verhindert werden soll.

(7) Die Verwaltung von EU-VS 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 Kapiteln 2, 3 und 5 des vorliegenden Beschlusses zu ergänzen und dadurch dazu beizutragen, die beabsichtigte oder unbeabsichtigte Kompromittierung von Verschlusssachen sowie den Verlust von Verschlusssachen zu verhindern oder festzustellen und entsprechende Maßnahmen zur Wiederherstellung der Sicherheit zu treffen. Diese Maßnahmen beziehen sich insbesondere auf die Erstellung, die Speicherung beziehungsweise Aufbewahrung, die Registrierung, die Vervielfältigung, die Übersetzung, die Herabstufung, die Aufhebung des Geheimhaltungsgrads, die Beförderung und die Vernichtung von EU-VS und ergänzen die allgemeinen Bestimmungen zur Dokumentenverwaltung der Kommission (Beschluss 2002/47/EG, EGKS, Euratom ([2]) und Beschluss 2004/563/EG, Euratom ([3])).

([1]) Siehe „Arrangement entre le Gouvernement belge et le Parlement européen, le Conseil, la Commission, le Comité économique et social européen, le Comité des régions, la Banque européenne d'investissement en matière de sécurité" vom 31. Dezember 2004, „Accord de sécurité signé entre la Commission et le Gouvernement luxembourgeois" vom 20. Januar 2007 und „Accordo tra il Governo italiano e la Commissione europea dell'energia atomica (Euratom) per l'istituzione di un Centro comune di ricerche nucleari di competenza generale" vom 22. Juli 1959.

([2]) Beschluss 2002/47/EG, EGKS, Euratom der Kommission vom 23. Januar 2002 zur Änderung ihrer Geschäftsordnung (ABl. L 21 vom 24.1.2002, S. 23).

([3]) Beschluss 2004/563/EG, Euratom der Kommission vom 7. Juli 2004 zur Änderung ihrer Geschäftsordnung (ABl. L 251 vom 27.7.2004, S. 9).

(8) Dieser Beschluss gilt unbeschadet folgender Rechtsakte:

a) Verordnung (Euratom) Nr. 3 ([1]);

b) Verordnung (EG) Nr. 1049/2001 des Europäischen Parlaments und des Rates ([2]);

c) Verordnung (EG) Nr. 45/2001 des Europäischen Parlaments und des Rates ([3]);

d) Verordnung (EWG, Euratom) Nr. 354/83 des Rates ([4]) —

HAT FOLGENDEN BESCHLUSS ERLASSEN:

KAPITEL 1

**GRUNDSÄTZE UND MINDESTSTANDARDS**

*Artikel 1*

**Begriffsbestimmungen**

Für die Zwecke dieses Beschlusses gelten die folgenden Begriffsbestimmungen:

1. „Dienststelle der Kommission“: Generaldirektion oder Dienst der Kommission oder Kabinett eines Mitglieds der Kommission;

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

3. „Aufhebung des Geheimhaltungsgrades“: Löschung jeder Geheimhaltungskennzeichnung;

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

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

6. „Herabstufung“: Einstufung in einen niedrigeren Geheimhaltungsgrad;

7. „Bearbeitung“ von EU-VS: alle möglichen Handlungen, denen EU-VS während ihres gesamten Lebenszyklus unterliegen können. Sie umfasst die Erstellung, Registrierung, Verarbeitung, Beförderung, Herabstufung, Freigabe und Vernichtung. In Bezug auf Kommunikations- und Informationssysteme umfasst sie ferner die Sammlung, Darstellung, Übermittlung und Speicherung;

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

9. „Durchführungsbestimmungen“: sämtliche gemäß Kapitel 5 des Beschlusses (EU, Euratom) 2015/443 der Kommission ([5]) erlassenen Vorschriften oder Sicherheitshinweise;

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

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

12. „Räumlichkeiten“: unbewegliches Vermögen oder diesem gleichzustellendes Vermögen im Eigentum oder Besitz der Kommission;

---

([1]) Verordnung (Euratom) Nr. 3 vom 31. Juli 1958 zur Anwendung des Artikels 24 des Vertrags zur Gründung der Europäischen Atomgemeinschaft (ABl. 17 vom 6.10.1958, S. 406).

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

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

([4]) Verordnung (EWG, Euratom) Nr. 354/83 des Rates vom 1. Februar 1983 über die Freigabe der historischen Archive der Europäischen Wirtschaftsgemeinschaft und der Europäischen Atomgemeinschaft (ABl. L 43 vom 15.2.1983, S. 1).

([5]) Beschluss (EU, Euratom) 2015/443 der Kommission vom 13. März 2015 über die Sicherheit in der Kommission (siehe Seite 41 dieses Amtsblatts).

13. „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;

14. „Statut“: das in der Verordnung (EWG, Euratom, EGKS) Nr. 259/68 des Rates ([1]) festgelegte Statut der Beamten der Europäischen Gemeinschaften und die Beschäftigungsbedingungen für die sonstigen Bediensteten der Europäischen Gemeinschaften;

15. „Bedrohung“: potenzielle Ursache für einen unerwünschten Zwischenfall, der zu einem Schaden für eine Organisation oder ein von ihr benutztes System führen kann; solche Bedrohungen können unbeabsichtigt oder beabsichtigt (böswillig) sein und unterscheiden sich nach den Bedrohungselementen, potenziellen Zielen und Angriffsmethoden;

16. „Schwachstelle“: Anfälligkeit, die bei einer oder mehreren Bedrohungen ausgenutzt werden kann. Eine Schwachstelle kann durch ein Versäumnis entstehen oder sich auf eine Anfälligkeit durch nachlässige, unvollständige oder inkohärente Kontrollen beziehen und (verfahrens-)technischer, materieller, organisatorischer oder operativer Art sein.

*Artikel 2*

**Gegenstand und Geltungsbereich**

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

(2) Dieser Beschluss findet auf alle Dienststellen und Gebäude der Kommission Anwendung.

(3) Ungeachtet spezifischer Anweisungen für bestimmte Gruppen von Mitarbeitern findet dieser Beschluss auf die Mitglieder der Kommission, auf die unter das Statut und die Beschäftigungsbedingungen für die sonstigen Bediensteten der Europäischen Gemeinschaften fallenden Bediensteten der Kommission, auf an die Kommission entsandte nationale Experten, auf Dienstleister und ihre Mitarbeiter, auf Praktikanten und auf sonstige Personen Anwendung, die Zugang zu den Gebäuden der Kommission, sonstigen Vermögenswerten oder von der Kommission bearbeiteten Information haben.

(4) Die Bestimmungen dieses Beschlusses gelten unbeschadet des Beschlusses 2002/47/EG, EGKS, Euratom und des Beschlusses 2004/563/EG, Euratom.

*Artikel 3*

**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, deren unbefugte Weitergabe für die wesentlichen Interessen der Europäischen Union oder eines oder mehrerer Mitgliedstaaten nachteilig sein könnte.

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

([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 (Beschäftigungsbedingungen für die sonstigen Bediensteten) (ABl. L 56 vom 4.3.1968, S. 1).

*Artikel 4*

**Regeln für die Einstufung als Verschlusssache**

(1) Jedes Mitglied der Kommission und jede Dienststelle der Kommission gewährleistet, dass die von ihm/ihr erstellten EU-VS angemessen eingestuft werden, deutlich als Verschlusssachen gekennzeichnet sind und ihren Geheimhaltungsgrad nur so lange wie erforderlich behalten.

(2) Unbeschadet des Artikels 26 darf der Geheimhaltungsgrad von EU-VS ohne vorherige schriftliche Zustimmung des Herausgebers weder herabgestuft noch aufgehoben werden; das Gleiche gilt für die Veränderung oder Entfernung der in Artikel 3 Absatz 2 genannten Kennzeichnungen.

(3) Erforderlichenfalls werden im Einklang mit Artikel 60 Durchführungsbestimmungen für den Umgang mit EU-VS erlassen, einschließlich eines Einstufungsleitfadens für Verschlusssachen.

*Artikel 5*

**Schutz von Verschlusssachen**

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

(2) Der Besitzer einer EU-VS ist dafür verantwortlich, diese in Einklang mit diesem Beschluss und seinen Durchführungsbestimmungen gemäß den Vorschriften nach Kapitel 4 zu schützen.

(3) Bringt ein Mitgliedstaat Verschlusssachen, die mit einem nationalen Geheimhaltungsgrad gekennzeichnet sind, in die Strukturen oder Netze der Kommission ein, so schützt die Kommission diese Verschlusssachen nach Maßgabe der Anforderungen, die für EU-VS des entsprechenden Geheimhaltungsgrades gemäß der Entsprechungstabelle in Anhang I gelten.

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

*Artikel 6*

**Sicherheitsrisikomanagement**

(1) Die Sicherheitsmaßnahmen für den Schutz von EU-VS während ihres gesamten Lebenszyklus müssen insbesondere dem Geheimhaltungsgrad, der Form und dem Umfang der Informationen und des Materials, der Lage und der Beschaffenheit der Einrichtungen, in denen EU-VS aufbewahrt werden, und der örtlichen Einschätzung der Bedrohung durch böswillige und/oder kriminelle Handlungen, einschließlich Spionage, Sabotage oder Terrorismus, entsprechen.

(2) In Notfallplänen wird berücksichtigt, dass EU-VS in Notsituationen geschützt werden müssen, damit der unbefugte Zugang sowie die unbefugte Weitergabe verhindert und die Unversehrtheit sowie die Verfügbarkeit sichergestellt werden.

(3) In den Kontinuitätsplänen aller Dienststellen werden Präventions- und Wiederherstellungsmaßnahmen vorgesehen, damit die Auswirkungen größerer Störungen oder Zwischenfälle auf die Bearbeitung und Speicherung beziehungsweise Aufbewahrung von EU-VS so gering wie möglich gehalten werden.

*Artikel 7*

**Anwendung des Beschlusses**

(1) Erforderlichenfalls werden zur Ergänzung oder Untermauerung dieses Beschlusses im Einklang mit Artikel 60 Durchführungsbestimmungen erlassen.

(2) Die Dienststellen der Kommission treffen alle in ihre Zuständigkeit fallenden Maßnahmen, um zu gewährleisten, dass bei der Bearbeitung und Speicherung beziehungsweise Aufbewahrung von EU-VS oder anderen Verschlusssachen dieser Beschluss und die einschlägigen Durchführungsbestimmungen Anwendung finden.

(3) Die zur Durchführung dieses Beschlusses getroffenen Sicherheitsmaßnahmen müssen im Einklang mit den in Artikel 3 des Beschlusses (EU, Euratom) 2015/443 festgelegten Grundsätzen für die Sicherheit in der Kommission stehen.

(4) Der Generaldirektor für Humanressourcen und Sicherheit richtet innerhalb seiner Generaldirektion die Sicherheitsstelle der Kommission ein. Die Sicherheitsstelle der Kommission nimmt die ihr mit dem vorliegenden Beschluss und seinen Durchführungsbestimmungen übertragenen Zuständigkeiten wahr.

(5) In jeder Dienststelle der Kommission nimmt der lokale Sicherheitsbeauftragte gemäß Artikel 20 des Beschlusses (EU, Euratom) 2015/443 in enger Zusammenarbeit mit der Generaldirektion Humanressourcen und Sicherheit und im Einklang mit diesem Beschluss folgende Aufgaben zum Schutz von EU-VS wahr:

a) Bearbeitung von Anträgen auf Sicherheitsermächtigungen für das Personal;

b) Beiträge zu Fortbildungs- und Sensibilisierungsmaßnahmen zum Thema Sicherheit;

c) Beaufsichtigung des Registraturkontrollbeauftragten der Dienststelle;

d) Berichterstattung über etwaige Sicherheitsverletzungen und Kompromittierungen von EU-VS;

e) Aufbewahrung von Ersatzschlüsseln und schriftlichen Aufzeichnungen der einzelnen Kombinationen;

f) sonstige Aufgaben, die mit dem Schutz von EU-VS zusammenhängen oder in den Durchführungsbestimmungen vorgesehen sind.

*Artikel 8*

**Sicherheitsverletzungen und Kompromittierungen von EU-VS**

(1) Zu einer Sicherheitsverletzung kommt es durch eine Handlung oder Unterlassung einer Person, die den in diesem Beschluss und den Durchführungsbestimmungen festgelegten Sicherheitsvorschriften zuwiderläuft.

(2) Eine Kompromittierung von EU-VS liegt vor, wenn EU-VS infolge einer Sicherheitsverletzung ganz oder teilweise unbefugten Personen zur Kenntnis gelangt sind.

(3) Erfolgte oder vermutete Verletzungen der Sicherheit werden der Sicherheitsstelle der Kommission unverzüglich gemeldet.

(4) Wird bekannt oder besteht berechtigter Grund zu der Annahme, dass EU-VS kompromittiert oder verloren gegangen sind, wird im Einklang mit Artikel 13 des Beschlusses (EU, Euratom) 2015/443 eine Sicherheitsuntersuchung durchgeführt.

(5) Es werden alle geeigneten Maßnahmen getroffen, 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) zu vermeiden, dass sich ein solcher Vorfall wiederholt und

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

(6) Gegen jede Person, die für eine Verletzung der Sicherheitsvorschriften dieses Beschlusses verantwortlich ist, können im Einklang mit dem Statut Disziplinarmaßnahmen ergriffen werden. Gegen jede Person, die für die Kompromittierung oder den Verlust von EU-VS verantwortlich ist, können gemäß den geltenden Rechtsvorschriften, Regelungen und sonstigen Vorschriften Disziplinarmaßnahmen ergriffen und/oder rechtliche Schritte unternommen werden.

KAPITEL 2

**PERSONELLER GEHEIMSCHUTZ**

*Artikel 9*

**Begriffsbestimmungen**

Für die Zwecke dieses Kapitels gelten folgende Begriffsbestimmungen:

1. „Ermächtigung für den Zugang zu EU-VS“: Beschluss der Sicherheitsstelle der Kommission auf Grundlage der von einer zuständigen Behörde eines Mitgliedstaats getroffenen Feststellung, dass einem Beamten der Kommission, einem sonstigen Bediensteten oder einem abgeordneten nationalen Sachverständigen 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; diese Person wird als „sicherheitsermächtigt“ bezeichnet.

2. „Sicherheitsermächtigung für Personal“: Anwendung von Maßnahmen, mit denen gewährleistet wird, dass nur Personen Zugang zu EU-VS erhalten, die

   a) Kenntnis von EU-VS haben müssen;

   b) erforderlichenfalls für den entsprechenden Geheimhaltungsgrad sicherheitsermächtigt sind und

   c) über ihre Verantwortlichkeiten belehrt worden sind.

3. „Erklärung über die Sicherheitsüberprüfung von Personal“ (Personnel Security Clearance, PSC): Erklärung einer zuständigen Behörde eines Mitgliedstaats, die nach Abschluss einer Sicherheitsüberprüfung durch die zuständigen Behörden eines Mitgliedstaats abgegeben und mit der bescheinigt wird, dass einer Person, die nachweislich Kenntnis von Verschlusssachen haben muss und die über ihre Verantwortlichkeiten angemessen belehrt worden ist, bis zu einem bestimmten Datum und bis zu einem bestimmten Geheimhaltungsgrad („CONFIDENTIEL UE/EU CONFIDENTIAL“ oder höher) Zugang zu EU-VS gewährt werden kann;

4. „Sicherheitsüberprüfungsbescheinigung“ (Personnel Security Clearance Certificate, PSCC): von einer zuständigen Behörde ausgestellte Bescheinigung, in der festgestellt wird, dass eine Person sicherheitsüberprüft ist oder eine von der Sicherheitsstelle der Kommission ausgestellte gültige Sicherheitsermächtigung besitzt, 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 Sicherheitsüberprüfung oder -ermächtigung und das Ablaufdatum der Bescheinigung selbst hervorgehen.

5. „Sicherheitsüberprüfung“: Überprüfung, die von der zuständigen Behörde eines Mitgliedstaats nach den innerstaatlichen Rechtsvorschriften und Regelungen durchgeführt wird, um Gewissheit darüber zu erlangen, dass über die betreffende Person keine nachteiligen Erkenntnisse vorliegen, die dem Zugang zu Verschlusssachen bis zu einem bestimmten Geheimhaltungsgrad („CONFIDENTIEL UE/EU CONFIDENTIAL“ oder höher) entgegenstehen würden.

*Artikel 10*

**Grundsätze**

(1) Einer Person darf der Zugang zu EU-VS nur gewährt werden, wenn

1. festgestellt wurde, dass sie Kenntnis von Verschlusssachen haben muss;

2. sie über die Sicherheitsvorschriften für den Schutz von EU-VS und die einschlägigen Sicherheitsnormen und -richtlinien belehrt wurde und ihre Verantwortlichkeiten hinsichtlich des Schutzes solcher Informationen anerkannt hat;

3. sie für den Zugang zu als „CONFIDENTIEL UE/EU CONFIDENTIAL“ oder höher eingestuften Verschlusssachen über eine Sicherheitsermächtigung für den entsprechenden Geheimhaltungsgrad verfügt oder auf andere Weise aufgrund ihrer Tätigkeit nach Maßgabe der innerstaatlichen Rechtsvorschriften ordnungsgemäß ermächtigt ist.

(2) Alle Personen, die zur Wahrnehmung ihrer Aufgaben auf als „CONFIDENTIEL UE/EU CONFIDENTIAL“ oder höher eingestufte EU-VS zugreifen können müssen, müssen über eine Sicherheitsermächtigung für den entsprechenden Geheimhaltungsgrad verfügen, bevor ihnen Zugang zu diesen EU-VS gewährt wird. Die betreffende Person erklärt sich schriftlich damit einverstanden, dass sie der Sicherheitsüberprüfung unterzogen wird. Andernfalls kann ihr keine Stelle, Funktion oder Aufgabe zugewiesen werden, die den Zugang zu als „CONFIDENTIEL UE/EU CONFIDENTIAL“ oder höher eingestuften Verschlusssachen umfasst.

(3) Die Verfahren für die Sicherheitsüberprüfung von Personal dienen der Feststellung, ob einer Person unter Berücksichtigung ihrer Loyalität, Vertrauenswürdigkeit und Zuverlässigkeit der Zugang zu EU-VS gewährt werden kann.

(4) Mit Hilfe einer von den zuständigen Behörden eines Mitgliedstaats im Einklang mit den innerstaatlichen Rechtsvorschriften und Regelungen durchgeführten Sicherheitsüberprüfung wird festgestellt, ob bei einer Person die nötige Loyalität, Vertrauenswürdigkeit und Zuverlässigkeit für den Zugang zu als „CONFIDENTIEL UE/EU CONFIDENTIAL“ oder höher eingestuften Verschlusssachen gegeben ist.

(5) Für den Kontakt zu den nationalen Sicherheitsbehörden oder anderen zuständigen nationalen Behörden im Rahmen der Sicherheitsüberprüfung ist ausschließlich die Sicherheitsstelle der Kommission zuständig. Der gesamte Austausch zwischen den Dienststellen der Kommission und ihrem Personal sowie den nationalen Sicherheitsbehörden und anderen zuständigen Behörden erfolgt über die Sicherheitsstelle der Kommission.

*Artikel 11*

**Sicherheitsermächtigungsverfahren**

(1) Jeder Generaldirektor oder Dienststellenleiter der Kommission bestimmt innerhalb seiner Dienststelle die Dienstposten, deren Inhaber zur Wahrnehmung ihrer Aufgaben Zugang zu als „CONFIDENTIEL UE/EU CONFIDENTIAL“ oder höher eingestuften Verschlusssachen und eine entsprechende Sicherheitsermächtigung benötigen.

(2) Sobald feststeht, dass eine Person auf einen Dienstposten berufen wird, der den Zugang zu als „CONFIDENTIEL UE/EU CONFIDENTIAL“ oder höher eingestuften Verschlusssachen erfordert, unterrichtet der lokale Sicherheitsbeauftragte der betreffenden Kommissionsdienststelle die Sicherheitsstelle der Kommission hierüber. Letztere übermittelt der betreffenden Person den Fragebogen für die Sicherheitsüberprüfung der nationalen Sicherheitsbehörde des Mitgliedstaats, unter dessen Staatsangehörigkeit die Person bei den EU-Organen oder -Einrichtungen eingestellt wurde. Die betreffende Person erklärt sich schriftlich damit einverstanden, dass sie der Sicherheitsüberprüfung unterzogen wird, und sendet der Sicherheitsstelle der Kommission den ausgefüllten Fragebogen innerhalb kürzester Frist zurück.

(3) Die Sicherheitsstelle der Kommission übermittelt der nationalen Sicherheitsbehörde des Mitgliedstaats, unter dessen Staatsangehörigkeit die betreffende Person bei den EU-Organen oder -Einrichtungen eingestellt wurde, den ausgefüllten Fragebogen für die Sicherheitsüberprüfung und beantragt die Durchführung einer Sicherheitsüberprüfung für den Geheimhaltungsgrad von EU-VS, zu denen die betreffende Person Zugang haben muss.

(4) Werden der Sicherheitsstelle der Kommission sicherheitsrelevante Informationen über eine Person bekannt, die eine Sicherheitsüberprüfung beantragt hat, so teilt sie dies der zuständigen nationalen Sicherheitsbehörde gemäß den einschlägigen Vorschriften und Regelungen mit.

(5) Nach Abschluss der Sicherheitsüberprüfung und so bald wie möglich nach der Benachrichtigung durch die zuständige nationale Sicherheitsbehörde über die Gesamtauswertung der Erkenntnisse der Sicherheitsüberprüfung verfährt die Sicherheitsstelle der Kommission wie folgt:

a) Sofern die Sicherheitsüberprüfung ergeben hat, dass über die betreffende Person keine nachteiligen Erkenntnisse vorliegen, die ihre Loyalität, Vertrauenswürdigkeit und Zuverlässigkeit in Frage stellen, kann sie der betreffenden Person bis zu dem von ihr angegebenen Zeitpunkt, höchstens jedoch für fünf Jahre, eine Ermächtigung für den Zugang zu EU-VS bis zu dem entsprechenden Geheimhaltungsgrad erteilen.

b) Sofern das Ergebnis der Sicherheitsüberprüfung nicht zu einer solchen Feststellung geführt hat, setzt sie die betreffende Person davon in Kenntnis; die betreffende Person kann beantragen, von der Sicherheitsstelle der Kommission gehört zu werden. Letztere wiederum kann ihrerseits die zuständige nationale Sicherheitsbehörde um weitere Auskünfte ersuchen, die diese nach ihren innerstaatlichen Rechtsvorschriften und Regelungen geben darf. Wird das Ergebnis der Sicherheitsüberprüfung bestätigt, darf keine Ermächtigung für den Zugang zu EU-VS erteilt werden.

(6) Für die Sicherheitsüberprüfung und deren Ergebnisse gelten die einschlägigen Rechtsvorschriften und Regelungen des betreffenden Mitgliedstaats einschließlich der Rechtsvorschriften für etwaige Rechtsbehelfe. Gegen Entscheidungen der Sicherheitsstelle der Kommission können Rechtsbehelfe gemäß dem Statut eingelegt werden.

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

(8) Nimmt eine Person innerhalb von 12 Monaten nach Mitteilung des Ergebnisses der Sicherheitsüberprüfung an die Sicherheitsstelle der Kommission ihren Dienst nicht auf oder unterbricht sie diesen für einen Zeitraum von 12 Monaten, in dem sie nicht bei der Kommission oder einem anderen Organ, einer anderen Einrichtung oder Agentur der Union oder bei einer nationalen Verwaltung eines Mitgliedstaats tätig ist, so befasst die Sicherheitsstelle der Kommission die zuständige nationale Sicherheitsbehörde mit der Angelegenheit und ersucht diese um eine Bestätigung, dass die betreffende Person weiterhin als ordnungsgemäß sicherheitsüberprüft gilt.

(9) Werden der Sicherheitsstelle der Kommission Informationen über ein Sicherheitsrisiko bekannt, das von einer Person ausgeht, die eine gültige Sicherheitsermächtigung besitzt, so teilt die Sicherheitsstelle der Kommission dies gemäß den einschlägigen Vorschriften und Regelungen der zuständigen nationalen Sicherheitsbehörde mit.

(10) Teilt eine nationale Sicherheitsbehörde der Sicherheitsstelle der Kommission mit, dass eine gemäß Absatz 5 Buchstabe a erfolgte Feststellung in Bezug auf eine Person, die im Besitz einer gültigen Ermächtigung für den Zugang zu EU-VS ist, zurückgenommen wurde, kann die Kommission die nationale Sicherheitsbehörde um alle weiteren Auskünfte ersuchen, die diese nach ihren innerstaatlichen Rechtsvorschriften und Regelungen geben darf. Bei Bestätigung der nachteiligen Erkenntnisse durch die zuständige nationale Behörde wird die Ermächtigung zurückgenommen und die betreffende Person vom Zugang zu EU-VS und von Dienstposten, auf denen sie auf EU-VS zugreifen oder ein Sicherheitsrisiko darstellen könnte, ausgeschlossen.

(11) Jede Entscheidung über die Rücknahme oder die Aussetzung einer Ermächtigung für den Zugang zu EU-VS für eine Person, auf die dieser Beschluss Anwendung findet, und gegebenenfalls die dafür maßgeblichen Gründe werden der betreffenden Person mitgeteilt; die betreffende Person kann beantragen, von der Sicherheitsstelle der Kommission gehört zu werden. Für die von einer nationalen Sicherheitsbehörde zur Verfügung gestellten Informationen gelten die einschlägigen Rechtsvorschriften und Regelungen des betreffenden Mitgliedstaats. Gegen diesbezügliche Entscheidungen der Sicherheitsstelle der Kommission können im Einklang mit dem Statut Rechtsbehelfe eingelegt werden.

(12) Die Dienststellen der Kommission stellen sicher, dass abgeordnete nationale Sachverständige, die bei ihnen einen Dienstposten bekleiden sollen, der eine Sicherheitsermächtigung für den Zugang zu EU-VS voraussetzt, der Sicherheitsstelle der Kommission im Einklang mit den nationalen Rechts- und Verwaltungsvorschriften vor Dienstantritt eine gültige PSC oder PSCC vorlegen; auf dieser Grundlage gewährt die Sicherheitsstelle der Kommission der betreffenden Person eine Sicherheitsermächtigung für den Zugang zu EU-VS, die bis zu dem Geheimhaltungsgrad, für den die nationale Sicherheitsüberprüfung durchgeführt wurde, und höchstens für die Dauer der Abordnung gültig ist.

Zugang zu EU-VS für Personen, die aufgrund ihrer Tätigkeit ordnungsgemäß ermächtigt sind

(13) Die Mitglieder der Kommission, die nach Maßgabe des Vertrags aufgrund ihrer Aufgaben Zugang zu EU-VS haben, werden über ihre Sicherheitspflichten im Hinblick auf den Schutz von EU-VS belehrt.

Unterlagen über Sicherheitsüberprüfungen und -ermächtigungen

(14) Die Sicherheitsstelle der Kommission führt im Einklang mit diesem Beschluss Unterlagen über Sicherheitsüberprüfungen und -ermächtigungen für den Zugang zu EU-VS. Diese Unterlagen enthalten mindestens Angaben zum Geheimhaltungsgrad der EU-VS, zu denen der betreffenden Person Zugang gewährt werden darf, das Datum der Sicherheitsüberprüfung und deren Gültigkeitsdauer.

(15) Die Sicherheitsstelle der Kommission kann eine PSCC ausstellen, die Angaben zum Geheimhaltungsgrad („CONFIDENTIEL UE/EU CONFIDENTIAL“ oder höher) der EU-VS, zu denen der Person Zugang gewährt werden darf, zur Gültigkeitsdauer der betreffenden Ermächtigung für den Zugang zu EU-VS und zum Ende der Gültigkeitsdauer der Bescheinigung enthält.

Erneuerung von Sicherheitsermächtigungen

(16) Nach der erstmaligen Erteilung einer Sicherheitsermächtigung für den Zugang zu EU-VS ist diese generell alle fünf Jahre (gerechnet ab dem Tag der Mitteilung des Ergebnisses der letzten Sicherheitsüberprüfung, auf deren Grundlage die betreffende Sicherheitsermächtigung erteilt wurde) im Hinblick auf eine Erneuerung zu überprüfen, sofern die betreffende Person ununterbrochen bei der Europäischen Kommission oder bei einem anderen Organ, einer anderen Einrichtung oder einer anderen Agentur der Union tätig gewesen ist und weiterhin Zugang zu EU-VS benötigt.

(17) Die Sicherheitsstelle der Kommission kann die Gültigkeit der bestehenden Sicherheitsermächtigung um bis zu 12 Monate verlängern, sofern sie von der zuständigen nationalen Sicherheitsbehörde oder einer sonstigen zuständigen nationalen Behörde binnen zwei Monaten ab dem Datum der Übermittlung des Erneuerungsantrags und des entsprechenden Sicherheitsfragebogens keine nachteiligen Informationen erhält. Hat die zuständige nationale Sicherheitsbehörde oder die sonstige zuständige nationale Behörde der Sicherheitsstelle der Kommission ihre Stellungnahme nicht übermittelt, so werden der betreffenden Person Aufgaben zugewiesen, für die keine Sicherheitsermächtigung erforderlich ist.

*Artikel 12*

**Sicherheitsunterweisungen**

(1) Nach der Teilnahme an der von der Sicherheitsstelle der Kommission durchgeführten Sicherheitsunterweisung bestätigen alle Personen, denen eine Sicherheitsermächtigung erteilt wurde, schriftlich, dass sie sich ihrer Pflichten in Bezug auf den Schutz von EU-VS und der Folgen einer etwaigen Kompromittierung von EU-VS bewusst sind. Die Sicherheitsstelle der Kommission verwahrt die entsprechenden schriftlichen Bestätigungen.

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

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

*Artikel 13*

**Befristete Sicherheitsermächtigungen**

(1) In Ausnahmefällen und sofern es im dienstlichen Interesse gerechtfertigt ist, kann die Sicherheitsstelle der Kommission in Erwartung des Abschlusses einer umfassenden Sicherheitsüberprüfung nach Konsultation der nationalen Sicherheitsbehörde des Mitgliedstaats, dessen Staatsangehörigkeit die betreffende Person besitzt, und vorbehaltlich der Ergebnisse einer ersten Prüfung, mit der festgestellt werden soll, ob keine relevanten nachteiligen Erkenntnisse vorliegen, unbeschadet der Bestimmungen über die Erneuerung von Sicherheitsüberprüfungen eine vorläufige Ermächtigung zum Zugang zu EU-VS für eine bestimmte Tätigkeit erteilen. Solche vorläufigen Ermächtigungen für den Zugang zu EU-VS gelten einmalig für einen Zeitraum von höchstens sechs Monaten und berechtigen nicht zum Zugang zu Verschlusssachen, die als „TRÈS SECRET UE/EU TOP SECRET“ eingestuft sind.

(2) Nach der Teilnahme an einer Sicherheitsunterweisung gemäß Artikel 12 Absatz 1 bestätigen alle Personen, denen eine vorläufige Ermächtigung erteilt wurde, 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. Die Sicherheitsstelle der Kommission verwahrt die entsprechenden schriftlichen Bestätigungen.

*Artikel 14*

**Teilnahme an von der Kommission organisierten vertraulichen Sitzungen**

(1) Dienststellen der Kommission, die Sitzungen veranstalten, in deren Rahmen als „CONFIDENTIEL UE/EU CONFIDENTIAL" und höher eingestufte Informationen erörtert werden, teilen der Sicherheitsstelle der Kommission über ihren lokalen Sicherheitsbeauftragten oder den Organisator der Sitzung frühzeitig das Datum, die Uhrzeit, den Ort und die Namen der Sitzungsteilnehmer mit.

(2) Vorbehaltlich der Bestimmungen von Artikel 11 Absatz 13 darf Personen, die an von der Kommission organisierten Sitzungen teilnehmen sollen, in deren Rahmen als „CONFIDENTIEL UE/EU CONFIDENTIAL" und höher eingestufte Informationen erörtert werden, die Teilnahme nur gestattet werden, wenn der Status ihrer Sicherheitsüberprüfung oder ihrer Sicherheitsermächtigung bestätigt wurde. Die Teilnahme an solchen vertraulichen Sitzungen wird sowohl Personen verwehrt, für die der Sicherheitsstelle der Kommission keine PSCC oder ein anderer Nachweis für eine Sicherheitsüberprüfung vorliegt, als auch nicht sicherheitsermächtigten Teilnehmern der Kommission.

(3) Vor der Veranstaltung einer vertraulichen Sitzung fordert der lokale Sicherheitsbeauftragte der Kommissionsdienststelle, die die Sitzung organisiert, die externen Teilnehmer auf, der Sicherheitsstelle der Kommission eine PSCC oder einen anderen Nachweis für eine Sicherheitsüberprüfung zu übermitteln. Die Sicherheitsstelle der Kommission informiert den lokalen Sicherheitsbeauftragten oder den Organisator der Sitzung über die von ihr erhaltene PSCC oder über sonstige Nachweise für eine PSC. Gegebenenfalls kann eine konsolidierte Namensliste verwendet werden, die den einschlägigen Nachweis einer Sicherheitsüberprüfung enthält.

(4) Wird die Sicherheitsstelle der Kommission von den zuständigen Behörden darüber informiert, dass einer Person, die im Rahmen ihrer Aufgaben an Sitzungen der Kommission teilnehmen muss, die PSC entzogen wurde, so teilt die Sicherheitsstelle der Kommission dies dem lokalen Sicherheitsbeauftragten der für die Organisation der Sitzung verantwortlichen Kommissionsdienstelle mit.

*Artikel 15*

**Möglicher Zugang zu EU-VS**

Boten, Sicherheitsbedienstete und Begleitpersonen müssen über eine Sicherheitsermächtigung des erforderlichen Geheimhaltungsgrades verfügen 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 werden.

KAPITEL 3

**MATERIELLER GEHEIMSCHUTZ VON VERSCHLUSSSACHEN**

*Artikel 16*

**Grundsätze**

(1) Die Maßnahmen des materiellen Geheimschutzes zielen darauf ab, das heimliche oder gewaltsame Eindringen unbefugter Personen zu verhindern, von unbefugten Handlungen abzuschrecken beziehungsweise 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 im Einklang mit diesem Beschluss und seinen Durchführungsbestimmungen festgelegt.

(2) Die Maßnahmen des materiellen Geheimschutzes zielen insbesondere 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) der Einsatz 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 beziehungsweise diese verhindert und aufgedeckt werden und

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

(3) Die Maßnahmen des materiellen Geheimschutzes werden für alle Gebäude, Büros, Räume und sonstigen Bereiche, in denen EU-VS bearbeitet oder aufbewahrt werden, getroffen, einschließlich Bereiche, in denen Kommunikations- und Informationssysteme gemäß Kapitel 5 untergebracht sind.

(4) Die Bereiche, in denen als „CONFIDENTIEL UE/EU CONFIDENTIAL“ oder höher eingestufte EU-VS aufbewahrt werden, werden als besonders geschützte Bereiche gemäß diesem Kapitel eingerichtet und von der Sicherheitsakkreditierungsstelle der Kommission genehmigt.

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

*Artikel 17*

**Anforderungen und Maßnahmen bezüglich des materiellen Geheimschutzes**

(1) Die Auswahl der Maßnahmen des materiellen Geheimschutzes erfolgt auf der Grundlage einer Einschätzung der Bedrohungslage durch die Sicherheitsstelle der Kommission und gegebenenfalls in Absprache mit anderen Dienststellen der Kommission, anderen Organen, Einrichtungen oder Agenturen der Union und/oder den zuständigen Behörden der Mitgliedstaaten. Die Kommission wendet in ihren Gebäuden einen Risikomanagementprozess für den Schutz von EU-VS an, um zu gewährleisten, dass der Umfang des physischen Schutzes dem festgestellten Risiko entspricht. Der Risikomanagementprozess trägt allen relevanten Faktoren Rechnung, insbesondere

a) dem Geheimhaltungsgrad der EU-VS;

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

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

d) der Einschätzung der Bedrohung der Union, ihrer Organe, Einrichtungen oder Agenturen oder der Mitgliedstaaten durch Nachrichtendienste sowie der Bedrohung durch Sabotage, Terrorismus und andere subversive oder kriminelle Handlungen.

(2) Die Sicherheitsstelle der Kommission legt unter Anwendung des Konzepts der mehrschichtigen Sicherheit eine angemessene Kombination erforderlicher Maßnahmen des materiellen Geheimschutzes fest. Zu diesem Zweck erarbeitet die Sicherheitsstelle der Kommission die in den Durchführungsbestimmungen beschriebenen Mindeststandards, -normen und -kriterien.

(3) Die Sicherheitsstelle der Kommission ist befugt, Durchsuchungen an den Ein- und Ausgängen vorzunehmen, um vom Verbringen unzulässigen Materials in Räumlichkeiten oder Gebäude oder von der unbefugten Mitnahme von EU-VS aus Räumlichkeiten oder Gebäuden abzuschrecken.

(4) Besteht die Gefahr einer — auch versehentlichen — unzulässigen Einsicht in EU-VS, so ergreifen die betroffenen Kommissionsdienststellen gemäß den Vorgaben der Sicherheitsstelle der Kommission geeignete Maßnahmen, um dieser Gefahr entgegenzuwirken.

(5) Bei neuen Einrichtungen werden die Anforderungen hinsichtlich des materiellen Geheimschutzes und deren funktionale Spezifikationen im Einvernehmen mit der Sicherheitsstelle der Kommission bei der Planung und Konzeption der Einrichtungen festgelegt. Bei bestehenden Einrichtungen werden die Anforderungen hinsichtlich des materiellen Geheimschutzes im Einklang mit den in den Durchführungsbestimmungen beschriebenen Mindeststandards, -normen und -kriterien umgesetzt.

*Artikel 18*

**Ausrüstung für den physischen Schutz von EU-VS**

(1) Zum physischen Schutz von EU-VS werden zwei Arten von durch Maßnahmen des materiellen Geheimschutzes geschützten Bereichen eingerichtet:

a) Verwaltungsbereiche und

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

(2) Die Sicherheitsakkreditierungsstelle der Kommission legt fest, ob ein bestimmter Bereich die Anforderungen für eine Ausweisung als Verwaltungsbereich, als besonders geschützter Bereich oder als technisch abgesicherter Bereich erfüllt.

(3) Für Verwaltungsbereiche gilt:

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

b) nur Personen, die von der Sicherheitsstelle der Kommission oder einer anderen 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.

(4) Für besonders geschützte Bereiche gilt:

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

b) nur sicherheitsüberprüfte und speziell ermächtigte Personen, die Zugang zu Verschlusssachen haben müssen, dürfen diesen Bereich unbegleitet betreten;

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

(5) 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 aufbewahrt werden, ist eindeutig anzugeben;

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

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

a) Diese Bereiche werden mit einem Einbruchmeldesystem ausgerüstet, verschlossen gehalten, wenn sie nicht besetzt sind, und bewacht, wenn sie besetzt sind. Die Verwaltung der Schlüssel erfolgt nach Maßgabe von Artikel 20;

b) alle Personen, die diese Bereiche betreten, und alles Material, das dorthin verbracht wird, werden kontrolliert;

c) diese Bereiche werden von der Sicherheitsstelle der Kommission regelmäßig physisch und/oder technisch überprüft. Diese Überprüfungen werden auch dann vorgenommen, 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.

(7) Unbeschadet von Absatz 6 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 Sicherheitsstelle der Kommission untersucht werden, um sicherzustellen, dass mit diesen Geräten keine verständlichen Informationen auf unbeabsichtigte oder unzulässige Weise aus dem betreffenden besonders geschützten Bereich nach außen übermittelt werden können.

(8) Besonders geschützte Bereiche, die nicht rund um die Uhr von diensthabendem Personal besetzt sind, werden gegebenenfalls nach den üblichen Arbeitszeiten und in unregelmäßigen Abständen außerhalb der üblichen Arbeitszeiten kontrolliert, sofern kein Einbruchmeldesystem vorhanden ist.

(9) Innerhalb eines Verwaltungsbereichs können zeitweilig besonders geschützte Bereiche oder technisch abgesicherte Bereiche für eine vertrauliche Sitzung oder einen anderen ähnlichen Zweck eingerichtet werden.

(10) Der lokale Sicherheitsbeauftragte der betreffenden Kommissionsdienststelle erstellt für jeden besonders geschützten Bereich seines Zuständigkeitsbereichs sicherheitsbezogene Betriebsverfahren, die im Einklang mit den Bestimmungen dieses Beschlusses und seinen Durchführungsbestimmungen regeln,

a) welchen Geheimhaltungsgrad die EU-VS, die in diesem Bereich bearbeitet oder aufbewahrt werden dürfen, aufweisen müssen;

b) welche Überwachungs- und Schutzmaßnahmen einzuhalten sind;

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

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

e) welche sonstigen einschlägigen Maßnahmen und Verfahren anzuwenden sind.

(11) Tresorräume werden in besonders geschützte Bereiche eingebaut. Wände, Böden, Decken, Fenster und verschließbare Türen müssen von der Sicherheitsstelle der Kommission zugelassen werden und einen Schutz bieten, der dem eines Sicherheitsbehältnisses entspricht, das für die Aufbewahrung von EU-VS desselben Geheimhaltungsgrads zugelassen ist.

*Artikel 19*

**Physische Schutzmaßnahmen für die Bearbeitung und Aufbewahrung von EU-VS**

(1) 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

c) außerhalb eines besonders geschützten Bereichs oder eines Verwaltungsbereichs, sofern der Besitzer die EU-VS gemäß Artikel 31 befördert und sich verpflichtet hat, die in den Durchführungsbestimmungen festgelegten besonderen Maßnahmen einzuhalten, um sicherzustellen, dass die EU-VS vor dem Zugriff durch unbefugte Personen geschützt sind.

(2) 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 Verwaltungsbereichs oder eines besonders geschützten Bereichs aufbewahrt werden, sofern der Besitzer sich verpflichtet hat, die in den Durchführungsbestimmungen festgelegten besonderen Maßnahmen einzuhalten.

(3) 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 besonders geschützten Bereichs oder eines Verwaltungsbereichs, sofern der Besitzer

i) sich verpflichtet hat, die in den Durchführungsbestimmungen festgelegten besonderen Maßnahmen einzuhalten, um sicherzustellen, dass die EU-VS vor dem Zugang unbefugter Personen geschützt sind;

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

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

(4) EU-VS der Geheimhaltungsgrade „CONFIDENTIEL UE/EU CONFIDENTIAL“ und „SECRET UE/EU SECRET“ werden in einem besonders geschützten Bereich in einem Sicherheitsbehältnis oder in einem Tresorraum aufbewahrt.

(5) EU-VS des Geheimhaltungsgrads „TRÈS SECRET UE/EU TOP SECRET“ werden in einem besonders geschützten Bereich bearbeitet, der von der Sicherheitsstelle der Kommission eingerichtet und verwaltet wird und der bis zu diesem Geheimhaltungsgrad von der Sicherheitsakkreditierungsstelle der Kommission zugelassen ist.

(6) EU-VS des Geheimhaltungsgrads „TRÈS SECRET UE/EU TOP SECRET“ werden in einem besonders geschützten Bereich, der bis zu diesem Geheimhaltungsgrad von der Sicherheitsakkreditierungsstelle der Kommission zugelassen ist, wie folgt aufbewahrt:

a) in einem Sicherheitsbehältnis gemäß Artikel 18 mit einer oder mehreren der folgenden zusätzlichen Kontrollen:

(1) ständige Bewachung oder Kontrolle durch sicherheitsüberprüftes Sicherheitspersonal oder diensthabendes Personal;

(2) zugelassenes Einbruchmeldesystem in Verbindung mit Bereitschaftspersonal im Sicherheitsdienst

oder

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

*Artikel 20*

**Verwaltung der Schlüssel und Kombinationen zum Schutz von EU-VS**

(1) Die Verfahren für die Verwaltung der Schlüssel und Kombinationen für Büros, Räume, Tresorräume und Sicherheitsbehältnisse werden in Durchführungsbestimmungen nach Maßgabe von Artikel 60 festgelegt. Diese Verfahren sollen den Schutz vor unbefugtem Zugang sicherstellen.

(2) Der Kreis der Personen, die die Kombinationen kennen, ist so weit wie möglich zu begrenzen. Die Kombinationen für Sicherheitsbehältnisse und Tresorräume, in denen EU-VS aufbewahrt werden, werden geändert

a) bei Entgegennahme eines neuen Behältnisses;

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

c) bei erfolgter oder vermuteter Kompromittierung;

d) bei Wartung oder Reparatur eines Schlosses und

e) mindestens alle 12 Monate.

KAPITEL 4

**VERWALTUNG VON EU-VERSCHLUSSSACHEN**

*Artikel 21*

**Grundsätze**

(1) Alle EU-VS werden im Einklang mit der Strategie der Kommission über die Dokumentenverwaltung verwaltet; sie sollten daher nach Maßgabe der gemeinsamen Liste für die kommissionsinterne Dokumentenaufbewahrung registriert, als Muster, teilweise oder vollständig abgelegt, aufbewahrt und schließlich vernichtet oder an die historischen Archive übermittelt werden.

(2) Als „CONFIDENTIEL UE/EU CONFIDENTIAL" oder höher eingestufte Verschlusssachen werden zu Sicherheitszwecken bei Erhalt und vor ihrer Weiterleitung registriert. Als „TRÈS SECRET UE/EU TOP SECRET" eingestufte Informationen werden in den benannten Registraturen registriert.

(3) Innerhalb der Kommission wird im Einklang mit Artikel 27 ein Registratursystem für EU-VS eingeführt.

(4) In Dienststellen und Räumlichkeiten der Kommission, in denen EU-VS bearbeitet oder gespeichert beziehungsweise aufbewahrt werden, werden regelmäßig Kontrollen durch die Sicherheitsstelle der Kommission durchgeführt.

(5) 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 Kapitel 5 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, welche gemäß Kapitel 5 zugelassen wurden, oder

   ii) in allen anderen Fällen gemäß den Durchführungsbestimmungen.

*Artikel 22*

**Geheimhaltungsgrade und Kennzeichnungen**

(1) Informationen werden als Verschlusssache eingestuft, wenn sie gemäß Artikel 3 Absatz 1 hinsichtlich ihrer Vertraulichkeit zu schützen sind.

(2) Der Herausgeber einer EU-VS ist dafür zuständig, im Einklang mit den für die Einstufung geltenden Durchführungsbestimmungen, Standards und Leitlinien den Geheimhaltungsgrad und den ursprünglichen Empfängerkreis der Informationen zu bestimmen.

(3) Der Geheimhaltungsgrad von EU-VS wird nach Maßgabe von Artikel 3 Absatz 2 und der einschlägigen Durchführungsbestimmungen festgelegt.

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

(5) Einzelne Teile eines gegebenen Dokuments (d. h. Seiten, Absätze, Abschnitte, Anhänge oder sonstige Anlagen) können eine unterschiedliche Einstufung erfordern und sind entsprechend zu kennzeichnen; dies gilt auch bei einer Speicherung in elektronischer Form.

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

(7) Dokumente, die Teile mit unterschiedlichen Geheimhaltungsgraden umfassen, sollten möglichst so untergliedert werden, dass Teile mit verschiedenen Geheimhaltungsgraden leicht zu erkennen sind und gegebenenfalls voneinander getrennt werden können.

(8) Begleitschreiben oder Übermittlungsvermerke mit Anlagen werden so hoch eingestuft wie die am höchsten eingestufte Anlage. Der Herausgeber muss anhand einer entsprechenden Kennzeichnung klar angeben, welcher Geheimhaltungsgrad für das Begleitschreiben beziehungsweise den Übermittlungsvermerk gilt, wenn diesem die Anlagen nicht beigefügt sind, z. B.:

CONFIDENTIEL UE/EU CONFIDENTIAL

Ohne Anlage(n) RESTREINT UE/EU RESTRICTED

*Artikel 23*

**Kennzeichnungen**

Zusätzlich zu einer der VS-Kennzeichnungen nach Artikel 3 Absatz 2 können EU-VS mit zusätzlichen Kennzeichnungen versehen sein, beispielsweise mit

a) einer Kennzeichnung, die den Herausgeber identifiziert;

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

c) Weitergabekennzeichnungen;

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

*Artikel 24*

**Abgekürzte Einstufungskennzeichnungen**

(1) Um den Geheimhaltungsgrad einzelner Absätze eines Textes auszuweisen, können standardmäßig abgekürzte Einstufungskennzeichnungen verwendet werden. Die Abkürzungen ersetzen nicht die kompletten Einstufungskennzeichnungen.

(2) 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 |

*Artikel 25*

**Erstellung von EU-VS**

(1) Bei der Erstellung einer EU-Verschlusssache

a) wird auf jeder Seite der Geheimhaltungsgrad eindeutig vermerkt;

b) wird jede Seite nummeriert;

c) wird das Dokument mit einer Registrierungsnummer und einem Betreff versehen, der selbst keinen Geheimhaltungsgrad führt, sofern er nicht entsprechend gekennzeichnet ist;

d) wird das Dokument datiert;

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.

(2) Ist die Anwendung von Absatz 1 auf EU-VS nicht möglich, so sind im Einklang mit den Durchführungsbestimmungen andere geeignete Maßnahmen zu treffen.

*Artikel 26*

**Herabstufung und Aufhebung des Geheimhaltungsgrads von EU-VS**

(1) Der Herausgeber teilt, sofern möglich, 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.

(2) Jede Kommissionsdienststelle überprüft die EU-VS, deren Herausgeber sie ist, regelmäßig daraufhin, ob ihr Geheimhaltungsgrad weiterhin zutreffend ist. Mit den Durchführungsbestimmungen wird ein System eingeführt, mit dem der Geheimhaltungsgrad registrierter EU-VS, die von der Kommission herausgegeben wurden, 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.

(3) Von der Kommission erstellte Verschlusssachen des Geheimhaltungsgrads „RESTREINT UE/EU RESTRICTED“ werden im Einklang mit der Verordnung (EWG, Euratom) Nr. 354/83 des Rates, geändert durch die Verordnung (EG, Euratom) Nr. 1700/2003 [1] des Rates, nach dreißig Jahren automatisch herabgestuft.

*Artikel 27*

**EU-VS-Registraturen in der Kommission**

(1) Unbeschadet des nachfolgenden Artikels 53 Absatz 5 wird in jeder Kommissionsdienststelle, in der EU-VS der Geheimhaltungsgrade „CONFIDENTIEL UE/EU CONFIDENTIAL“ oder „SECRET UE/EU SECRET“ bearbeitet, aufbewahrt oder gespeichert werden, eine zuständige lokale Registratur für EU-VS eingerichtet, um sicherzustellen, dass EU-VS im Einklang mit diesem Beschluss behandelt werden.

(2) Die vom Generalsekretariat verwaltete Registratur für EU-VS ist die zentrale Registratur der Kommission für EU-VS. Sie fungiert als

— die lokale EU-VS-Registratur des Generalsekretariats der Kommission;

— die EU-VS-Registratur der Kabinette der Kommissionsmitglieder, sofern letztere nicht über eine eigene lokale EU-VS-Registratur verfügen;

— die EU-VS-Registratur von Generaldirektionen oder Dienststellen, die über keine lokale EU-VS-Registratur verfügen;

— zentrale Ein- und Ausgangsstelle für alle Verschlusssachen der Geheimhaltungsgrade „RESTREINT UE/EU RESTRICTED“ bis einschließlich „SECRET UE/EU SECRET“, die zwischen der Kommission und ihren Dienststellen und Drittstaaten und internationalen Organisationen und - falls in besonderen Regelungen vorgesehen - anderen Organen, Agenturen und Einrichtungen der Union ausgetauscht werden.

(3) Innerhalb der Kommission benennt die Sicherheitsstelle der Kommission eine Registratur, 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.

(4) 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 an externe Stellen übermitteln, ohne dass diese ihre ausdrückliche schriftliche Zustimmung erteilt hat.

(5) Die EU-VS-Registraturen werden als besonders geschützte Bereiche im Sinne des Kapitels 3 eingerichtet und von der Sicherheitsakkreditierungsstelle der Kommission akkreditiert.

*Artikel 28*

**Registraturkontrollbeauftragter**

(1) Jede EU-VS-Registratur wird von einem Registraturkontrollbeauftragten geleitet.

(2) Der Registraturkontrollbeauftragte muss angemessen sicherheitsüberprüft sein.

(3) In Bezug auf die Anwendung der Bestimmungen über die Behandlung von EU-Verschlusssachen und die Einhaltung der einschlägigen Sicherheitsvorschriften, Normen und Leitlinien unterliegt der Registraturkontrollbeauftragte innerhalb der Kommissionsdienststelle der Aufsicht des lokalen Sicherheitsbeauftragten.

(4) Im Rahmen seiner Verantwortung für die Verwaltung der im zugewiesenen EU-VS-Registratur nimmt der Registraturkontrollbeauftragte folgende allgemeine Aufgaben gemäß diesem Beschluss und den einschlägigen Durchführungsbestimmungen, Normen und Leitlinien wahr:

— Leitung sämtlicher Vorgänge im Zusammenhang mit der Registrierung, Aufbewahrung beziehungsweise Speicherung, Vervielfältigung, Übersetzung, Weiterleitung, Versendung und Vernichtung von EU-VS oder deren Überführung in das Historische Archiv;

— regelmäßige Überprüfung, ob die Einstufung der betreffenden Informationen aufrecht erhalten werden muss;

— sonstige in den Durchführungsbestimmungen vorgesehene Aufgaben, die mit dem Schutz von EU-VS zusammenhängen.

*Artikel 29*

**Registrierung von EU-VS zu Sicherheitszwecken**

(1) Im Sinne dieses Beschlusses bezeichnet der Ausdruck „Registrierung zu Sicherheitszwecken“ (im Folgenden „Registrierung“) die Durchführung von Verfahren, bei denen jede Phase des Umlaufs von EU-VS einschließlich ihrer Weitergabe aufgezeichnet wird.

[1] Verordnung (EG, Euratom) Nr. 1700/2003 des Rates vom 22. September 2003 zur Änderung der Verordnung (EWG, Euratom) Nr. 354/83 über die Freigabe der historischen Archive der Europäischen Wirtschaftsgemeinschaft und der Europäischen Atomgemeinschaft (ABl. L 243 vom 27.9.2003, S. 1).

(2) Alle als „CONFIDENTIEL UE/EU CONFIDENTIAL“ oder höher eingestuften Informationen oder Materialien werden in den benannten Registraturen registriert, sobald sie in einer Verwaltungsstelle eingehen oder diese verlassen.

(3) Bei der Bearbeitung und Speicherung von EU-VS mit Hilfe eines Kommunikations- und Informationssystems dürfen die Registrierungsverfahren im Wege systeminterner Abläufe erfolgen.

(4) Detailliertere Vorschriften über die Registrierung von EU-VS zu Sicherheitszwecken werden in den Durchführungsbestimmungen festgelegt.

*Artikel 30*

**Kopieren und Übersetzen von EU-VS**

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

(2) Hat der Herausgeber von als „SECRET UE/EU SECRET“ oder niedriger eingestuften Dokumenten keine Einschränkungen hinsichtlich der Anfertigung von Kopien oder Übersetzungen auferlegt, so dürfen diese Dokumente auf Anweisung des Besitzers kopiert beziehungsweise übersetzt werden.

(3) Die für das Originaldokument geltenden Sicherheitsmaßnahmen finden auf Kopien und Übersetzungen dieses Dokuments Anwendung.

*Artikel 31*

**Beförderung von EU-VS**

(1) EU-VS werden bei ihrer Beförderung vor unbefugter Offenlegung geschützt.

(2) Schutzmaßnahmen für die Beförderung von EU-VS müssen

— dem Geheimhaltungsgrad der beförderten EU-VS angemessen und

— auf die besonderen Bedingungen ihrer Beförderung zugeschnitten sein, insbesondere in Abhängigkeit davon, ob die Beförderung der EU-VS

  — innerhalb eines Kommissionsgebäudes oder einer geschlossenen Gruppe von Kommissionsgebäuden,

  — zwischen Gebäuden der Kommission in ein und demselben Mitgliedstaat,

  — innerhalb der Europäischen Union oder

  — von der Europäischen Union in das Hoheitsgebiet eines Drittstaats erfolgt.

  — Ferner müssen sie auf die Art und die Form der EU-VS zugeschnitten sein.

(3) Diese Schutzmaßnahmen werden im Einzelnen in den Durchführungsbestimmungen oder — im Falle von Projekten und Programmen im Sinne des Artikels 42 — als fester Bestandteil der Sicherheitsanweisungen für das betreffende Programm oder Projekt festgelegt.

(4) Die Durchführungsbestimmungen beziehungsweise Sicherheitsanweisungen umfassen unter anderem dem Geheimhaltungsgrad der EU-VS angemessene Bestimmungen über

— die Art der Beförderung (beispielsweise als Handgepäck, durch diplomatische oder militärische Kurierdienste, durch Postdienste oder durch kommerzielle Kurierdienste),

— die Verpackung von EU-VS,

— technische Gegenmaßnahmen für auf elektronischen Datenträgern beförderte EU-VS,

— sonstige verfahrenstechnische, physische oder elektronische Maßnahmen,

— Registrierungsverfahren,

— den Einsatz von sicherheitsermächtigtem Personal.

(5) Bei der Beförderung von EU-VS auf elektronischen Datenträgern können ungeachtet des Artikels 21 Absatz 5 die in den einschlägigen Durchführungsbestimmungen beschriebenen Schutzmaßnahmen durch geeignete, von der Sicherheitsstelle der Kommission genehmigte technische Gegenmaßnahmen ergänzt werden, um das Verlust- oder Kompromittierungsrisiko so gering wie möglich zu halten.

*Artikel 32*

**Vernichtung von EU-VS**

(1) Nicht länger benötigte EU-Verschlusssachen können unter Berücksichtigung der Vorschriften über Archive und der kommissionsinternen Vorschriften und Bestimmungen über die Dokumentenverwaltung und -archivierung sowie insbesondere der gemeinsamen Liste für die kommissionsinterne Dokumentenaufbewahrung vernichtet werden.

(2) Als „CONFIDENTIEL UE/EU CONFIDENTIAL" oder höher eingestufte EU-VS werden vom Registraturkontrollbeauftragten der zuständigen EU-VS-Registratur auf Anweisung des Besitzers oder einer zuständigen Stelle vernichtet. Der Registraturkontrollbeauftragte aktualisiert die Dienstbücher und sonstigen Registrierungsinformationen entsprechend.

(3) Bei Dokumenten des Geheimhaltungsgrads „SECRET UE/EU SECRET" oder „TRÈS SECRET UE/EU TOP SECRET" erfolgt die Vernichtung durch den Registraturkontrollbeauftragten im Beisein eines Zeugen, der mindestens in Bezug auf Verschlusssachen mit dem Geheimhaltungsgrad des zu vernichtenden Dokuments sicherheitsüberprüft ist.

(4) Der Registerführer und der Zeuge — falls dessen Anwesenheit erforderlich ist — unterschreiben eine Vernichtungsbescheinigung, die in der Registratur abgelegt wird. Der Registraturkontrollbeauftragte der zuständigen EU-VS-Registratur bewahrt die Vernichtungsbescheinigungen von Dokumenten des Geheimhaltungsgrads „TRÈS SECRET UE/EU TOP SECRET" mindestens zehn Jahre und von Dokumenten der Geheimhaltungsgrade „CONFIDENTIEL UE/EU CONFIDENTIAL" und „SECRET UE/EU SECRET" mindestens fünf Jahre auf.

(5) Verschlusssachen, darunter Verschlusssachen des Geheimhaltungsgrads „RESTREINT UE/EU RESTRICTED", werden nach Verfahren vernichtet, die in den Durchführungsbestimmungen festgelegt werden und die die einschlägigen EU-Normen oder gleichwertige Normen erfüllen.

(6) Für EU-VS verwendete elektronische Datenträger werden nach in den Durchführungsbestimmungen festgelegten Verfahren vernichtet.

*Artikel 33*

**Vernichtung von EU-VS in Notfällen**

(1) Kommissionsdienststellen, die im Besitz von EU-VS sind, arbeiten unter Berücksichtigung der örtlichen Gegebenheiten Pläne zum Schutz von EU-Verschlusssachen im Krisenfall aus, die, falls erforderlich, auch Pläne für eine Vernichtung oder Auslagerung der EU-Verschlusssachen im Notfall umfassen. Sie erteilen die Anweisungen, die sie für notwendig erachten, um zu verhindern, dass EU-VS in unbefugte Hände gelangen.

(2) Regelungen zum Schutz und/oder zur Vernichtung von „CONFIDENTIEL UE/EU CONFIDENTIAL"- und „SECRET UE/EU SECRET"-Materialien im Krisenfall dürfen auf keinen Fall den Schutz oder die Vernichtung von „TRÈS SECRET UE/EU TOP SECRET"-Materialien einschließlich der Verschlüsselungseinrichtungen beeinträchtigen, die Vorrang vor allen anderen Aufgaben haben.

(3) Wenn in Notfällen das unmittelbare Risiko einer unbefugten Weitergabe besteht, werden die EU-VS vom Besitzer so vernichtet, dass eine vollständige oder teilweise Wiederherstellung ausgeschlossen ist. Der Herausgeber und die herausgebende Registratur werden von der als Notfallmaßnahme durchgeführten Vernichtung der registrierten EU-VS in Kenntnis gesetzt.

(4) Detailliertere Vorschriften über die Vernichtung von EU-VS werden in den Durchführungsbestimmungen festgelegt.

KAPITEL 5

**SCHUTZ VON EU-VS IN KOMMUNIKATIONS- UND INFORMATIONSSYSTEMEN**

*Artikel 34*

**Grundsätze der Informationssicherung**

(1) Die Informationssicherung im Bereich von Kommunikations- und Informationssystemen beruht auf dem Vertrauen darauf, dass die in diesen Systemen bearbeiteten Informationen geschützt sind und dass diese Systeme unter der Kontrolle rechtmäßiger Nutzer jederzeit ordnungsgemäß funktionieren.

(2) Um wirksam zu sein, muss die Informationssicherung Folgendes in angemessenem Umfang sicherstellen:

Authentizität: Es ist sichergestellt, dass die Informationen echt sind und von in gutem Glauben handelnden Quellen stammen.

Verfügbarkeit: Die Informationen sind auf Anfrage einer befugten Stelle verfügbar und nutzbar.

Vertraulichkeit: Die Informationen werden nicht gegenüber unbefugten Personen, Stellen oder im Rahmen von Verarbeitungsprozessen offengelegt.

Integrität: Die Genauigkeit und die Vollständigkeit der Informationen und Vermögenswerte sind gewährleistet.

Beweisbarkeit: Es kann nachgewiesen werden, dass ein Vorgang oder ein Ereignis stattgefunden hat, sodass dieser Vorgang oder dieses Ereignis nicht nachträglich abgestritten werden kann.

(3) Die Informationssicherung stützt sich auf einen Risikomanagementprozess.

*Artikel 35*

**Begriffsbestimmungen**

Für die Zwecke dieses Kapitels gelten folgende Begriffsbestimmungen:

a) „Akkreditierung“: förmliche Abnahme und Zulassung eines Kommunikations- und Informationssystems durch die Sicherheitsakkreditierungsstelle zur Verarbeitung von EU-VS in dessen Betriebsumgebung im Anschluss an die förmliche Validierung des Sicherheitsplans und dessen ordnungsgemäße Umsetzung;

b) „Akkreditierungsverfahren“: notwendige, der Akkreditierung durch die Sicherheitsakkreditierungsstelle vorausgehende Schritte und Aufgaben, die in einer Norm für den Akkreditierungsprozess festgelegt werden;

c) „Kommunikations- und Informationssystem“: 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;

d) „Restrisiko“: nach dem Ergreifen von Sicherheitsmaßnahmen verbleibendes Risiko, falls nicht alle Bedrohungen erfasst werden und nicht alle Schwachstellen beseitigt werden können;

e) „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 Vermögenswerte geschädigt werden. Gemessen wird das Risiko als die Kombination der Wahrscheinlichkeit des Eintretens von Bedrohungen und ihrer Auswirkungen;

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

g) „Risikobewertung“: Ermittlung von Bedrohungen und Schwachstellen sowie Durchführung diesbezüglicher Risikoanalysen (Analyse der Eintrittswahrscheinlichkeit und der Auswirkungen);

h) „Risikokommunikation“: Sensibilisierung der Nutzer eines Kommunikations- und Informationssystems für Risiken sowie Unterrichtung von Zulassungsstellen über diese Risiken und entsprechende Unterrichtung der für den Betrieb zuständigen Stellen;

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

*Artikel 36*

**Bearbeitung von EU-VS in Kommunikations- und Informationssystemen**

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

(2) Die Bearbeitung von EU-VS in Kommunikations- und Informationssystemen erfolgt nach Maßgabe des von der Kommission festgelegten Sicherheitskonzepts für Informationssysteme gemäß der Entscheidung C (2006) 3602 der Kommission [1]:

a) Die Umsetzung des Sicherheitskonzepts erfolgt während der gesamten Lebensdauer der Informationssysteme gemäß dem Regelkreis „Plan-Do-Check-Act“ (Planen-Umsetzen-Kontrollieren-Handeln);

b) der Sicherheitsbedarf wird mittels einer Folgenabschätzung ermittelt;

c) das Informationssystem und die darin enthaltenen Daten werden einer förmlichen Einstufung unterzogen;

[1] Beschluss C(2006) 3602 vom 16. August 2006 betreffend die Sicherheit der von den Dienststellen der Kommission genutzten Informationssysteme.

d) sämtliche nach Maßgabe des Sicherheitskonzepts für Informationssysteme vorgeschriebenen Sicherheitsmaßnahmen werden umgesetzt;

e) es wird ein Risikomanagementverfahren angewandt, das aus folgenden Schritten besteht: Bedrohungs- und Anfälligkeitsermittlung, Risikobewertung, Risikobehandlung, Risikoakzeptanz und Risikokommunikation;

f) es wird ein Sicherheitsplan einschließlich Sicherheitskonzept und sicherheitsbezogener Betriebsverfahren erstellt, umgesetzt, kontrolliert und überprüft.

(3) Alle an Konzeption, Entwicklung, Erprobung, Betrieb, Verwaltung und Nutzung von Kommunikations- und Informationssystemen, in denen EU-VS bearbeitet werden, beteiligten Mitarbeiter melden der Sicherheitsakkreditierungsstelle alle potenziellen Sicherheitsmängel, Vorfälle und Sicherheitsverstöße oder -verletzungen, die sich auf den Schutz des Kommunikations- und Informationssystems und/oder der darin gespeicherten EU-VS auswirken könnten.

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

a) Vorzugsweise werden vom Rat oder vom Generalsekretär des Rates in dessen Funktion als Krypto-Zulassungsstelle des Rates zugelassene Produkte auf Empfehlung der Sicherheitsexpertengruppe der Kommission verwendet;

b) wenn es aus bestimmten operativen Gründen gerechtfertigt ist, kann die Krypto-Zulassungsstelle der Kommission auf Empfehlung der Sicherheitsexpertengruppe der Kommission eine Befreiung von den unter (a) genannten Anforderungen aussprechen und eine vorläufige Zulassung für einen spezifischen Zeitraum erteilen.

(5) Bei der elektronischen Übermittlung, Verarbeitung und Speicherung von EU-VS werden zugelassene kryptografische Produkte verwendet. Ungeachtet dieser Anforderung können in Notsituationen oder im Rahmen bestimmter technischer Konfigurationen nach Genehmigung durch die Krypto-Zulassungsstelle spezielle Verfahren angewandt werden.

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

(7) Die Sicherheitsstelle der Kommission fungiert als:

— Informationssicherungsstelle;

— Sicherheitsakkreditierungsstelle;

— TEMPEST-Stelle;

— Krypto-Zulassungsstelle;

— Krypto-Verteilungsstelle.

(8) Die Sicherheitsstelle der Kommission ernennt für jedes System eine für den Betrieb zuständige Informationssicherungsstelle.

(9) Die Zuständigkeiten der in den Absätzen 7 und 8 beschriebenen Funktionen werden in den Durchführungsbestimmungen festgelegt.

*Artikel 37*

**Akkreditierung von Kommunikations- und Informationssystemen, in denen EU-VS bearbeitet werden**

(1) Sämtliche Kommunikations- und Informationssysteme, in denen EU-VS bearbeitet werden, werden einem auf den Grundsätzen der Informationssicherung basierenden Akkreditierungsverfahren unterzogen, dessen Detailliertheit der geforderten Sicherheitsstufe entspricht.

(2) Das Akkreditierungsverfahren umfasst die förmliche Validierung des Sicherheitsplans für das betreffende Kommunikations- und Informationssystem durch die Sicherheitsakkreditierungsstelle der Kommission mit dem Ziel, Gewähr dafür zu erlangen, dass

a) der in Artikel 36 Absatz 2 genannte Risikomanagementprozess ordnungsgemäß durchgeführt worden ist,

b) der Systemeigentümer das Restrisiko wissentlich akzeptiert hat und

c) ein hinreichender Schutz des Kommunikations- und Informationssystems und der in diesem bearbeiteten EU-VS in Übereinstimmung mit diesem Beschluss sichergestellt ist.

(3) Die Sicherheitsakkreditierungsstelle der Kommission gibt eine schriftliche Akkreditierungserklärung ab, in der festgelegt ist, bis zu welchem Geheimhaltungsgrad und unter welchen Voraussetzungen EU-VS in dem Kommunikations- und Informationssystem bearbeitet werden dürfen. Die Aufgaben des Gremiums für die Sicherheitsakkreditierung nach Artikel 11 der Verordnung (EU) Nr. 512/2014 des Europäischen Parlaments und des Rates ([1]) bleiben davon unberührt.

(4) Für die Akkreditierung von Kommunikations- und Informationssystemen der Kommission, an denen mehrere Parteien mitwirken, ist ein gemeinsames Gremium für die Sicherheitsakkreditierung zuständig, das sich aus je einem Vertreter der Sicherheitsakkreditierungsstelle der einzelnen Parteien zusammensetzt und in dem ein Vertreter der Sicherheitsakkreditierungsstelle der Kommission den Vorsitz führt.

(5) Das Akkreditierungsverfahren besteht aus einer Reihe von Aufgaben, die von den beteiligten Parteien wahrgenommen werden. Die alleinige Verantwortung für die Vorbereitung der Akkreditierungsdateien und -unterlagen trägt der Systemeigentümer des betreffenden Kommunikations- und Informationssystems.

(6) Die Akkreditierung ist Aufgabe der Sicherheitsakkreditierungsstelle der Kommission; diese hat zu jedem beliebigen Zeitpunkt im Lebenszyklus des Kommunikations- und Informationssystems das Recht,

a) die Durchführung eines Akkreditierungsverfahrens zu verlangen,

b) eine Prüfung oder Kontrolle des Kommunikations- und Informationssystems vorzunehmen,

c) in Fällen, in denen die Voraussetzungen für den Betrieb des Systems nicht mehr erfüllt sind, die Ausarbeitung und wirksame Umsetzung eines Plans zur Verbesserung der Sicherheit binnen eines genau festgelegten zeitlichen Rahmens anzuordnen und gegebenenfalls die Betriebserlaubnis für das Kommunikations- und Informationssystem so lange zu entziehen, bis die Voraussetzungen für den Betrieb wieder erfüllt sind.

(7) Das Akkreditierungsverfahren wird in einer Norm für das Akkreditierungsverfahren für Kommunikations- und Informationssysteme, in denen EU-VS bearbeitet werden, festgelegt, die im Einklang mit Artikel 10 Absatz 3 des Beschlusses C (2006) 3602 der Kommission angenommen wird.

*Artikel 38*

**Notsituationen**

(1) Unbeschadet der Bestimmungen dieses Kapitels können in Notsituationen wie beispielsweise bei drohenden oder bereits eingetretenen Krisen, Konflikten, Kriegssituationen oder im Fall besonderer operativer Umstände die nachstehend beschriebenen besonderen Verfahren angewandt werden.

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

a) Absender und Empfänger nicht über die erforderliche Verschlüsselungseinrichtung verfügen und

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

(3) Verschlusssachen, die unter den in Absatz 1 erläuterten Umständen übermittelt werden, dürfen nicht mit Kennzeichnungen oder Angaben versehen werden, 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.

(4) Anschließend wird der zuständigen Stelle und der Sicherheitsexpertengruppe der Kommission Bericht erstattet.

KAPITEL 6

**GEHEIMSCHUTZ IN DER WIRTSCHAFT**

*Artikel 39*

**Grundsätze**

(1) Unter dem Geheimschutz in der Wirtschaft versteht man die Anwendung von Maßnahmen zum Schutz von EU-VS

a) im Rahmen von als Verschlusssachen eingestuften Aufträgen durch

i) Bewerber oder Bieter während des gesamten Verfahrens zur Vergabe eines Auftrags;

ii) Auftragnehmer oder Unterauftragnehmer während der Laufzeit von als Verschlusssachen eingestuften Aufträgen;

([1]) Verordnung (EU) Nr. 512/2014 des Europäischen Parlaments und des Rates vom 16. April 2014 zur Änderung der Verordnung (EU) Nr. 912/2010 über die Errichtung der Agentur für das Europäische GNSS (ABl. L 150 vom 20.5.2014, S. 72).

b) im Rahmen von als Verschlusssachen eingestuften Finanzhilfevereinbarungen durch

i) Antragsteller während Verfahren zur Vergabe von Finanzhilfen;

ii) Empfänger während der Laufzeit von als Verschlusssache eingestuften Finanzhilfevereinbarungen.

(2) Derartige Aufträge oder Finanzhilfevereinbarungen beinhalten nicht den Zugang zu als „TRÈS SECRET UE/EU TOP SECRET" eingestuften Informationen.

(3) Sofern nichts anderes angegeben ist, finden die sich auf als Verschlusssachen eingestufte Aufträge beziehungsweise auf die betreffenden Auftragnehmer beziehenden Bestimmungen dieses Kapitels auch Anwendung auf als Verschlusssachen eingestufte Unteraufträge beziehungsweise auf die betreffenden Unterauftragnehmer.

*Artikel 40*

**Begriffsbestimmungen**

Im Sinne dieses Kapitels gelten folgende Begriffsbestimmungen:

a) „als Verschlusssache eingestufter Vertrag": Vertrag oder Rahmenvertrag im Sinne der Verordnung (EG, Euratom) Nr. 1605/2002 ([1]) zwischen der Kommission oder einer Kommissionsdienststelle und einem Auftragnehmer über die Lieferung beweglicher oder unbeweglicher Vermögenswerte, die Durchführung von Arbeiten oder die Erbringung von Dienstleistungen, deren Ausführung die Erstellung, Bearbeitung und Aufbewahrung beziehungsweise Speicherung von EU-VS mit sich bringt;

b) „als Verschlusssache eingestufter Unterauftrag": Vertrag zwischen einem Auftragnehmer der Kommission oder einer Kommissionsdienststelle und einem anderen Auftragnehmer („Unterauftragnehmer") über die Lieferung beweglicher oder unbeweglicher Vermögenswerte, die Durchführung von Arbeiten oder die Erbringung von Dienstleistungen, deren Ausführung die Erstellung, Bearbeitung und Aufbewahrung beziehungsweise Speicherung von EU-VS umfasst;

c) „als Verschlusssache eingestufte Finanzhilfevereinbarung": Vereinbarung, mit der die Kommission eine Finanzhilfe im Sinne von Teil I Titel VI der Verordnung (EG, Euratom) Nr. 1605/2002 gewährt und deren Erfüllung die Erstellung, Bearbeitung und Aufbewahrung beziehungsweise Speicherung von EU-VS erforderlich macht oder umfasst;

d) „beauftragte Sicherheitsbehörde": von der nationalen Sicherheitsbehörde eines Mitgliedstaats beauftragte Behörde, die die Aufgabe hat, Wirtschafts- oder andere Unternehmen über die nationale Politik in allen Fragen des Geheimschutzes in der Wirtschaft zu informieren und ihnen Anleitung und Hilfe bei ihrer Umsetzung zu bieten. Die Funktion der beauftragten Sicherheitsbehörde kann von der nationalen Sicherheitsbehörde oder einer anderen dazu qualifizierten Behörde wahrgenommen werden.

*Artikel 41*

**Verfahren für als Verschlusssache eingestufte Verträge oder Finanzhilfevereinbarungen**

(1) Jede Kommissionsdienststelle stellt in ihrer Funktion als Vergabebehörde sicher, dass bei der Vergabe von als Verschlusssache eingestuften Aufträgen oder Finanzhilfevereinbarungen die in diesem Kapitel festgelegten Mindeststandards für den Geheimschutz in der Wirtschaft in dem betreffenden Vertrag erwähnt beziehungsweise aufgeführt sowie eingehalten werden.

(2) Für die Zwecke von Absatz 1 ziehen die zuständigen Kommissionsdienststellen die Generaldirektion „Humanressourcen und Sicherheit" und insbesondere deren Direktion „Sicherheit" zu Rate und stellen sicher, dass die Musterverträge, -unteraufträge und -finanzhilfevereinbarungen Bestimmungen enthalten, in denen die von den Auftragnehmern und Unterauftragnehmern beziehungsweise Empfängern von Finanzhilfevereinbarungen zu befolgenden Grundprinzipien und Mindeststandards für den Schutz von EU-VS widergegeben werden.

(3) Die Kommission arbeitet eng mit der nationalen Sicherheitsbehörde, der beauftragten Sicherheitsbehörde oder einer sonstigen zuständigen Behörde des betreffenden Mitgliedstaats zusammen.

(4) Wenn ein öffentlicher Auftraggeber beabsichtigt, ein Verfahren im Hinblick auf den Abschluss eines als Verschlusssache eingestuften Auftrags oder einer als Verschlusssache eingestuften Finanzhilfevereinbarung einzuleiten, so zieht er in allen Phasen des Verfahrens die Sicherheitsstelle der Kommission zu etwaigen die Vertraulichkeit oder die Merkmale des Verfahrens betreffenden Fragen zu Rate.

(5) Vorlagen und Muster für als Verschlusssache eingestufte Aufträge, Unteraufträge und Finanzhilfevereinbarungen, Bekanntmachungen, Leitlinien für Fälle, in denen Sicherheitsbescheide für Einrichtungen erforderlich sind, Programm- oder Projektsicherheitsanweisungen, Geheimschutzklauseln, Besuche sowie die Übermittlung und Beförderung von EU-VS im Rahmen von als Verschlusssache eingestuften Aufträgen oder Finanzhilfevereinbarungen werden nach Zurateziehung der Sicherheitsexpertengruppe der Kommission in Durchführungsbestimmungen über den Geheimschutz in der Wirtschaft festgelegt.

([1]) Verordnung (EG, Euratom) Nr. 1605/2002 des Rates vom 25. Juni 2002 über die Haushaltsordnung für den Gesamthaushaltsplan der Europäischen Gemeinschaften (ABl. L 248 vom 16.9.2002, S. 1).

(6) Die Kommission kann als Verschlusssache eingestufte Verträge und Finanzhilfevereinbarungen abschließen, durch die Wirtschaftsteilnehmer, die in einem Mitgliedstaat oder in einem Drittstaat, mit dem ein Abkommen oder eine Verwaltungsvereinbarung im Sinne von Kapitel 7 dieses Beschlusses besteht, registriert sind, mit Aufgaben betraut werden, die den Zugang zu oder die Bearbeitung oder Aufbewahrung beziehungsweise Speicherung von EU-VS beinhalten oder nach sich ziehen.

*Artikel 42*

**Sicherheitsmerkmale von als Verschlusssache eingestuften Aufträgen oder Finanzhilfevereinbarungen**

(1) Als Verschlusssache eingestufte Aufträge oder Finanzhilfevereinbarungen weisen folgende Sicherheitsmerkmale auf:

Programm- oder Projektsicherheitsanweisungen

a) „Programm- oder Projektsicherheitsanweisungen“: Liste von Sicherheitsverfahren, die für ein spezifisches Programm oder Projekt verwendet werden, um die Sicherheitsverfahren zu vereinheitlichen. Die Anweisungen können im Verlauf des Programms oder Projekts überarbeitet werden.

b) Die Generaldirektion „Humanressourcen und Sicherheit“ arbeitet allgemeine Programm- oder Projektsicherheitsanweisungen aus, auf deren Grundlage die für Programme oder Projekte, in deren Rahmen EU-VS bearbeitet, aufbewahrt oder gespeichert werden, zuständigen Kommissionsdienststellen gegebenenfalls spezifische Programm- oder Projektsicherheitsanweisungen ausarbeiten können.

c) Spezifische Programm- oder Projektsicherheitsanweisungen werden insbesondere für Programme oder Projekte ausgearbeitet, die sich durch ihren Umfang, ihre Reichweite, ihre Komplexität oder eine Vielzahl von (beispielsweise aufgrund ihrer rechtlichen Stellung sehr unterschiedlichen) Auftragnehmern, Empfängern und sonstigen Partnern und Beteiligten auszeichnen. Die spezifischen Programm- oder Projektsicherheitsanweisungen werden von der Kommissionsdienststelle beziehungsweise den Kommissionsdienststellen, die das betreffende Programm oder Projekt leitet beziehungsweise leiten, in enger Zusammenarbeit mit der Generaldirektion „Humanressourcen und Sicherheit“ ausgearbeitet.

d) Die Generaldirektion „Humanressourcen und Sicherheit“ legt sowohl die allgemeinen als auch die spezifischen Programm- oder Projektsicherheitsanweisungen der Sicherheitsexpertengruppe der Kommission zur Stellungnahme vor.

Geheimschutzklausel

a) „Geheimschutzklausel“: besondere vom öffentlichen Auftraggeber festgelegte Auftragsbedingungen, die einen festen Bestandteil jedes als Verschlusssache eingestuften und mit dem Zugang zu oder der Erstellung von EU-VS verbundenen Auftrags bilden und in denen die Sicherheitsanforderungen und die sicherheitsschutzbedürftigen Teile des Auftrags festgelegt sind.

b) Die auftragsspezifischen Sicherheitsanforderungen werden in einer Geheimschutzklausel beschrieben. Die Geheimschutzklausel enthält gegebenenfalls den Einstufungsleitfaden für Verschlusssachen und ist fester Bestandteil aller als Verschlusssache eingestuften Aufträge, Unteraufträge und Finanzhilfevereinbarungen.

c) Die Geheimschutzklausel enthält die Bestimmungen, mit denen der Auftragnehmer beziehungsweise Finanzhilfeempfänger verpflichtet wird, die Mindeststandards dieses Beschlusses einzuhalten. Der öffentliche Auftraggeber stellt sicher, dass in der Geheimschutzklausel darauf hingewiesen wird, dass die Nichteinhaltung dieser Mindeststandards einen hinreichenden Grund für die Kündigung des Vertrags beziehungsweise der Finanzhilfevereinbarung darstellt.

(2) Sowohl die Programm- oder Projektsicherheitsanweisungen als auch die Geheimschutzklausel enthalten als obligatorisches Sicherheitsmerkmal einen Einstufungsleitfaden für Verschlusssachen:

a) „Einstufungsleitfaden für Verschlusssachen“: Dokument, in dem die Komponenten eines als Verschlusssache eingestuften Programms, Projekts oder Auftrags beziehungsweise einer als Verschlusssache eingestuften Finanzhilfevereinbarung beschrieben und die anzuwendenden Geheimhaltungsgrade angegeben sind. Der Einstufungsleitfaden für Verschlusssachen kann während der Laufzeit des Programms, Projekts oder Auftrags beziehungsweise der Finanzhilfevereinbarung erweitert werden, und Teile der Informationen können neu eingestuft oder herabgestuft werden. Sofern ein Einstufungsleitfaden für Verschlusssachen besteht, ist dieser Teil der Geheimschutzklausel.

b) Vor der Ausschreibung oder der Vergabe eines als Verschlusssache eingestuften Auftrags legt die betreffende Kommissionsdienststelle in ihrer Eigenschaft als öffentlicher Auftraggeber den Geheimhaltungsgrad der den Bewerbern, Bietern oder Auftragnehmern zur Verfügung zu stellenden Informationen sowie den Geheimhaltungsgrad etwaiger vom Auftragnehmer herauszugebender Informationen fest. Zu diesem Zweck erstellt sie nach Rücksprache mit der Sicherheitsstelle der Kommission einen Einstufungsleitfaden für Verschlusssachen, der für die Erfüllung des Vertrags im Einklang mit den Bestimmungen dieses Beschlusses und seiner Durchführungsbestimmungen maßgeblich ist.

c) Für die Bestimmung des Geheimhaltungsgrads der verschiedenen Bestandteile eines als Verschlusssache eingestuften Auftrags gelten folgende Grundsätze:

i) Bei der Erstellung eines Einstufungsleitfadens für Verschlusssachen trägt die betreffende Kommissionsdienststelle in ihrer Eigenschaft als öffentlicher Auftraggeber allen relevanten Sicherheitsaspekten Rechnung, so unter anderem auch dem Geheimhaltungsgrad, den der Herausgeber der von diesem zur Nutzung für den Auftrag freigegebenen Informationen letzteren zugewiesen hat;

ii) der globale Geheimhaltungsgrad des Auftrags darf nicht niedriger sein als der höchste Grad jeder einzelnen Auftragskomponente; und

iii) gegebenenfalls setzt sich der öffentliche Auftraggeber über die Sicherheitsstelle der Kommission mit den nationalen beziehungsweise beauftragten Sicherheitsbehörden der Mitgliedstaaten oder mit der betreffenden sonstigen zuständigen Sicherheitsbehörde in Verbindung, wenn er den Geheimhaltungsgrad von Verschlusssachen, die bei der Ausführung eines Auftrags von den Auftragnehmern erstellt oder diesen zur Verfügung gestellt werden, ändert und wenn er etwaige nachfolgende Änderungen am Einstufungsleitfaden für Verschlusssachen vornimmt.

*Artikel 43*

**Zugang von Mitarbeitern der Auftragnehmer und Empfänger zu EU-VS**

Der öffentliche Auftraggeber beziehungsweise die Vergabebehörde stellt sicher, dass der als Verschlusssache eingestufte Auftrag beziehungsweise die als Verschlusssache eingestufte Finanzhilfevereinbarung Bestimmungen enthält, welche vorsehen, dass Mitarbeiter von Auftragnehmern, Unterauftragnehmern oder Finanzhilfeempfängern, die für die Ausführung des als Verschlusssache eingestuften Auftrags oder Unterauftrags beziehungsweise der als Verschlusssache eingestuften Finanzhilfevereinbarung Zugang zu EU-VS benötigen, ein solcher Zugang gewährt wird, sofern folgende Anforderungen erfüllt sind:

a) die Mitarbeiter sind für den betreffenden Geheimhaltungsgrad sicherheitsermächtigt oder auf andere Weise ordnungsgemäß ermächtigt, da sie nachweislich Kenntnis von Verschlusssachen haben müssen;

b) die Mitarbeiter wurden über die geltenden Sicherheitsvorschriften für den Schutz von EU-VS belehrt und haben ihre Verantwortlichkeiten hinsichtlich des Schutzes solcher Verschlusssachen anerkannt;

c) die Mitarbeiter wurden von der zuständigen nationalen oder beauftragten Sicherheitsbehörde oder einer sonstigen zuständigen Behörde einer Sicherheitsüberprüfung für den entsprechenden Geheimhaltungsgrad für Verschlusssachen des Geheimhaltungsgrads „CONFIDENTIEL UE/EU CONFIDENTIAL“ oder „SECRET UE/EU SECRET“ unterzogen und zum Zugang zu diesen Verschlusssachen ermächtigt.

*Artikel 44*

**Sicherheitsbescheid für Einrichtungen**

(1) „Sicherheitsbescheid für Einrichtungen“: verwaltungsrechtliche Entscheidung einer nationalen, beauftragten oder sonstigen zuständigen Sicherheitsbehörde, welche besagt, dass die betreffende Einrichtung einen angemessenen Schutz von EU-VS bis zu einem bestimmten Geheimhaltungsgrad gewährleisten kann.

(2) Bevor einem Bewerber, Bieter, Auftragnehmer, Antragsteller oder Empfänger Zugang zu EU-VS gewährt werden kann, ist der Sicherheitsstelle der Kommission ein von einer nationalen, beauftragten oder sonstigen zuständigen Sicherheitsbehörde eines Mitgliedstaats ausgestellter Sicherheitsbescheid für Einrichtungen vorzulegen, aus dem hervorgeht, dass der betreffende Wirtschaftsteilnehmer in der Lage ist, EU-VS des geeigneten Geheimhaltungsgrades („CONFIDENTIEL UE/EU CONFIDENTIAL“ oder „SECRET UE/EU SECRET“) in Übereinstimmung mit den nationalen Rechts- und Verwaltungsvorschriften in seinen Einrichtungen zu schützen. Die Sicherheitsstelle der Kommission leitet den Antrag an die als öffentlicher Auftraggeber beziehungsweise als Vergabebehörde fungierende Kommissionsdienststelle weiter.

(3) Der öffentliche Auftraggeber teilt der zuständigen nationalen, beauftragten oder sonstigen zuständigen Sicherheitsbehörde über die Sicherheitsstelle der Kommission gegebenenfalls mit, dass für die Ausführung des Auftrags ein Sicherheitsbescheid für Einrichtungen erforderlich ist. Wenn während eines Verfahrens für die Auftragsvergabe oder die Gewährung von Finanzhilfen EU-VS mit dem Geheimhaltungsgrad „CONFIDENTIEL UE/EU CONFIDENTIAL“ oder „SECRET UE/EU SECRET“ zur Verfügung gestellt werden müssen, ist ein Sicherheitsbescheid für Einrichtungen oder eine PSC erforderlich.

(4) Der öffentliche Auftraggeber beziehungsweise die Vergabebehörde vergibt keinen als Verschlusssache eingestuften Auftrag an einen bevorzugten Bieter beziehungsweise schließt keine als Verschlusssache eingestufte Finanzhilfevereinbarung mit einem Teilnehmer, bevor sie nicht von der nationalen, beauftragten oder einer sonstigen zuständigen Sicherheitsbehörde des Mitgliedstaats, in dem der betreffende Auftragnehmer oder Unterauftragnehmer eingetragen ist, die Bestätigung erhalten hat, dass erforderlichenfalls ein entsprechender Sicherheitsbescheid für Einrichtungen erteilt wurde.

(5) Falls die Sicherheitsstelle der Kommission von der nationalen, beauftragten oder sonstigen zuständigen Sicherheitsbehörde, die einen Sicherheitsbescheid für Einrichtungen erteilt hat, über etwaige sich auf den Sicherheitsbescheid auswirkende Änderungen in Kenntnis gesetzt wird, informiert sie in ihrer Funktion als öffentlicher Auftraggeber beziehungsweise Vergabebehörde die zuständige Kommissionsdienststelle. Bei Unteraufträgen wird die nationale, die beauftragte oder eine sonstige zuständige Sicherheitsbehörde entsprechend informiert.

(6) Die Aufhebung eines Sicherheitsbescheids für Einrichtungen durch die zuständige nationale, beauftragte oder sonstige zuständige Sicherheitsbehörde stellt für den öffentlichen Auftraggeber beziehungsweise die Vergabebehörde einen hinreichenden Grund dar, den als Verschlusssache eingestuften Auftrag zu kündigen oder einen Bewerber, Bieter oder Antragsteller von dem Vergabeverfahren auszuschließen. Eine diesbezügliche Bestimmung wird in die auszuarbeitenden Musteraufträge und -finanzhilfevereinbarungen aufgenommen.

*Artikel 45*

**Bestimmungen für als Verschlusssache eingestufte Verträge oder Finanzhilfevereinbarungen**

(1) Werden einem Bewerber, Bieter oder Antragsteller während des Vergabeverfahrens EU-VS zur Verfügung gestellt, so enthält die Aufforderung zur Angebotsabgabe beziehungsweise zur Einreichung von Vorschlägen eine Klausel, welche vorsieht, dass jeder Bewerber, Bieter oder Antragsteller, der kein Angebot abgibt beziehungsweise keinen Vorschlag einreicht oder der nicht ausgewählt wird, sämtliche als Verschlusssache eingestuften Unterlagen binnen einer vorgegebenen Frist zurückzugeben hat.

(2) Der öffentliche Auftraggeber beziehungsweise die Vergabebehörde teilt der zuständigen nationalen, beauftragten oder sonstigen zuständigen Sicherheitsbehörde mit, dass ein als Verschlusssache eingestufter Auftrag oder eine als Verschlusssache eingestufte Finanzhilfevereinbarung vergeben beziehungsweise gewährt wurde und übermitteln ihr die einschlägigen Daten wie den Namen der Auftragnehmer oder Empfänger, die Laufzeit des Vertrags und die höchste mögliche Einstufung.

(3) Im Falle der Kündigung derartiger Verträge oder Finanzhilfevereinbarungen setzt der öffentliche Auftraggeber beziehungsweise die Vergabebehörde unverzüglich über die Sicherheitsstelle der Kommission die nationale, beauftragte oder sonstige zuständige Sicherheitsbehörde des Mitgliedstaats, in dem der Auftragnehmer oder der Finanzhilfeempfänger eingetragen ist, in Kenntnis.

(4) Im Falle der Kündigung eines als Verschlusssache eingestuften Auftrags, einer als Verschlusssache eingestuften Finanzhilfevereinbarung oder der Teilnahme eines Finanzhilfeempfängers ist der Auftragnehmer oder Finanzhilfeempfänger grundsätzlich verpflichtet, der Vergabebehörde etwaige in seinem Besitz befindliche EU-VS zurückzugeben.

(5) Die besonderen Bestimmungen für die Vernichtung von EU-VS während der Ausführung eines als Verschlusssache eingestuften Auftrags beziehungsweise einer als Verschlusssache eingestuften Finanzhilfevereinbarung oder im Falle seiner beziehungsweise ihrer Kündigung werden in der Geheimschutzklausel festgelegt.

(6) Wird dem Auftragnehmer oder Finanzhilfeempfänger nach der Kündigung eines als Verschlusssache eingestuften Auftrags beziehungsweise einer als Verschlusssache eingestuften Finanzhilfevereinbarung gestattet, EU-VS in seinem Besitz zu behalten, so muss der Auftragnehmer oder Finanzhilfeempfänger die in diesem Beschluss niedergelegten Mindeststandards weiterhin einhalten und die Vertraulichkeit der EU-VS weiterhin schützen.

*Artikel 46*

**Besondere Bestimmungen für als Verschlusssache eingestufte Aufträge**

(1) Die für den Schutz von EU-VS maßgeblichen Bedingungen, unter denen der Auftragnehmer Unteraufträge vergeben darf, werden sowohl in der Ausschreibung als auch in dem als Verschlusssache eingestuften Auftrag festgelegt.

(2) Vor einer etwaigen Untervergabe von Teilen eines als Verschlusssache eingestuften Auftrags holt der Auftragnehmer die Erlaubnis des öffentlichen Auftraggebers ein. Unteraufträge, die den Zugriff auf EU-VS mit sich bringen, dürfen an in einem Drittstaat eingetragene Unterauftragnehmer nur vergeben werden, wenn ein rechtlicher Rahmen für die Sicherheit der Verschlusssachen gemäß Kapitel 7 besteht.

(3) Der Auftragnehmer stellt sicher, dass alle im Rahmen von Unteraufträgen vergebenen Tätigkeiten im Einklang mit den Mindeststandards dieses Beschlusses ausgeführt werden; Unterauftragnehmern darf er EU-VS nur mit vorheriger schriftliche Einwilligung der Vergabebehörde zur Verfügung stellen.

(4) Bei EU-VS, die von einem Auftragnehmer herausgegeben oder bearbeitet werden, gilt die Kommission als Herausgeber, und die dem Herausgeber obliegenden Rechte werden vom öffentlichen Auftraggeber ausgeübt.

*Artikel 47*

**Besuche im Zusammenhang mit als Verschlusssache eingestuften Aufträgen**

(1) Falls Bedienstete der Kommission, eines Auftragnehmers oder eines Finanzhilfeempfängers zur Ausführung eines als Verschlusssache eingestuften Auftrags beziehungsweise einer als Verschlusssache eingestuften Finanzhilfevereinbarung Zugang zu Verschlusssachen des Geheimhaltungsgrads „CONFIDENTIEL UE/EU CONFIDENTIAL“ oder „SECRET UE/EU SECRET“ in den Räumlichkeiten des jeweils anderen benötigen, werden im Benehmen mit der zuständigen nationalen, beauftragten oder sonstigen zuständigen Sicherheitsbehörde Besuche vereinbart. Die Sicherheitsstelle der Kommission wird von derartigen Besuchen in Kenntnis gesetzt. Im Zusammenhang mit speziellen Programmen oder Projekten können die zuständigen nationalen, beauftragten oder sonstigen zuständigen Sicherheitsbehörden zudem ein Verfahren vereinbaren, nach dem Besuche unmittelbar verabredet werden können.

(2) Alle Besucher müssen entsprechend sicherheitsüberprüft sein und im Zusammenhang mit dem als Verschlusssache eingestuften Auftrag nachweislich von den betreffenden EU-VS Kenntnis haben müssen.

(3) Besucher erhalten ausschließlich Zugang zu EU-VS, die mit dem Zweck des Besuchs in Beziehung stehen.

(4) Detaillierte Bestimmungen werden in den Durchführungsbestimmungen festgelegt.

(5) Die in diesem Beschluss und in den Durchführungsbestimmungen gemäß Absatz 4 festgelegten Bestimmungen über Besuche im Zusammenhang mit als Verschlusssachen eingestuften Aufträgen sind zwingend einzuhalten.

*Artikel 48*

**Übermittlung und Beförderung von EU-VS im Zusammenhang mit als Verschlusssachen eingestuften Aufträgen oder Finanzhilfevereinbarungen**

(1) Für die Übermittlung von EU-VS auf elektronischem Wege gelten die einschlägigen Bestimmungen von Kapitel 5 dieses Beschlusses.

(2) Für die Beförderung von EU-VS gelten die einschlägigen Bestimmungen von Kapitel 4 dieses Beschlusses und der Durchführungsbestimmungen im Einklang mit den innerstaatlichen Rechtsvorschriften.

(3) Für die Festlegung von Sicherheitsvorkehrungen für die Beförderung von Verschlusssachen als Fracht gelten folgende Grundsätze:

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) vor jeder grenzüberschreitenden Verbringung von als „CONFIDENTIEL UE/EU CONFIDENTIAL“ oder „SECRET UE/EU SECRET“ eingestuftem Material stellt der Absender einen Beförderungsplan auf, der von den zuständigen nationalen, beauftragten oder sonstigen zuständigen Sicherheitsbehörden genehmigt werden muss;

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

e) nach Möglichkeit werden nur Transportrouten gewählt, die durch Mitgliedstaaten führen. Transportrouten, die durch andere Länder führen, werden nur gewählt, wenn dies von der zuständigen nationalen, beauftragten oder sonstigen zuständigen Sicherheitsbehörde sowohl des Staates des Absenders als auch des Staates des Empfängers genehmigt worden ist.

*Artikel 49*

**Weitergabe von EU-VS an Auftragnehmer oder Finanzhilfeempfänger in Drittstaaten**

Die Weitergabe von EU-VS an Auftragnehmer oder Finanzhilfeempfänger in Drittstaaten erfolgt nach Maßgabe der Sicherheitsmaßnahmen, die die Sicherheitsstelle der Kommission, die als öffentlicher Auftraggeber beziehungsweise Vergabebehörde fungierende Kommissionsdienststelle sowie die nationale, beauftragte oder sonstige zuständige Sicherheitsbehörde des Drittlandes, in dem der Auftragnehmer beziehungsweise Finanzhilfeempfänger eingetragen ist, miteinander vereinbaren.

*Artikel 50*

**Behandlung von Verschlusssachen des Geheimhaltungsgrads „RESTREINT UE/EU RESTRICTED“ im Zusammenhang mit als Verschlusssache eingestuften Aufträgen oder Finanzhilfevereinbarungen**

(1) Der Schutz von Verschlusssachen des Geheimhaltungsgrads „RESTREINT UE/EU RESTRICTED“, die im Zusammenhang mit als Verschlusssache eingestuften Aufträgen oder Finanzhilfevereinbarungen bearbeitet oder aufbewahrt beziehungsweise gespeichert werden, erfolgt nach den Grundsätzen der Verhältnismäßigkeit und der Kostenwirksamkeit.

(2) Bei als Verschlusssache eingestuften Aufträgen oder als Verschlusssache eingestuften Finanzhilfevereinbarungen, die die Bearbeitung von Verschlusssachen des Geheimhaltungsgrads „RESTREINT UE/EU RESTRICTED“ mit sich bringen, ist weder ein Sicherheitsbescheid für Einrichtungen noch eine PSC erforderlich.

(3) Ist mit einem Auftrag oder einer Finanzhilfevereinbarung die Bearbeitung von Verschlusssachen des Geheimhaltungsgrads „RESTREINT UE/EU RESTRICTED“ in einem Kommunikations- und Informationssystem verbunden, das von einem Auftragnehmer oder einem Finanzhilfeempfänger betrieben wird, so stellt der öffentliche Auftraggeber oder die Vergabebehörde nach Rücksprache mit der Sicherheitsstelle der Kommission sicher, dass in dem betreffenden Auftrag beziehungsweise in der betreffenden Finanzhilfevereinbarung die notwendigen technischen und administrativen Anforderungen in Bezug auf die Akkreditierung oder Zulassung des Kommunikations- und Informationssystems entsprechend dem festgestellten Risiko unter Berücksichtigung aller relevanter Faktoren festgelegt werden. Der Umfang der Akkreditierung oder Zulassung eines solchen Kommunikations- und Informationssystems wird von der Sicherheitsstelle der Kommission mit der zuständigen nationalen oder beauftragten Sicherheitsbehörde vereinbart.

KAPITEL 7

## AUSTAUSCH VON VERSCHLUSSSACHEN MIT ANDEREN EU-ORGANEN, -EINRICHTUNGEN, -ÄMTERN UND -AGENTUREN SOWIE MIT DEN MITGLIEDSTAATEN, MIT DRITTSTAATEN UND MIT INTERNATIONALEN ORGANISATIONEN

*Artikel 51*

### Grundsätze

(1) Wenn die Kommission oder eine Kommissionsdienststelle zu dem Schluss gelangt, dass ein Austausch von EU-VS mit einer beziehungsweise einem anderen EU-Organ, -Einrichtung, -Amt oder -Agentur, mit einem Drittstaat oder mit einer internationalen Organisation notwendig ist, werden die notwendigen Maßnahmen ergriffen, um einen geeigneten (verwaltungs)rechtlichen Rahmen zu schaffen, der auch Vereinbarungen über die Informationssicherheit oder Verwaltungsvereinbarungen nach Maßgabe der einschlägigen Vorschriften einschließen kann.

(2) Unbeschadet des Artikels 57 ist ein Austausch von EU-VS mit einer beziehungsweise einem anderen EU-Organ, -Einrichtung, -Amt oder -Agentur, mit einem Drittstaat oder mit einer internationalen Organisation nur zulässig, wenn ein solcher geeigneter (verwaltungs)rechtlicher Rahmen vorhanden ist und hinreichende Garantien dafür bestehen, dass die beziehungsweise das betreffende Organ, Einrichtung, Amt oder Agentur, der betreffende Drittstaat oder die betreffende internationale Organisation gleichwertige Grundprinzipien und Mindeststandards für den Schutz von Verschlusssachen anwendet.

*Artikel 52*

### Austausch von EU-VS mit anderen EU-Organen, -Einrichtungen, -Ämtern und -Agenturen

(1) Vor dem Abschluss einer Verwaltungsvereinbarung über den Austausch von EU-VS mit einer beziehungsweise einem anderen EU-Organ, -Einrichtung, -Amt oder -Agentur vergewissert sich die Kommission, dass die beziehungsweise das betreffende Organ, Einrichtung, Amt oder Agentur

a) über einen Rechtsrahmen für den Schutz von EU-VS verfügt, in dem Grundprinzipien und Mindeststandards festgelegt sind, die den in diesem Beschluss und den Durchführungsbestimmungen festgelegten gleichwertig sind;

b) Sicherheitsstandards und Leitlinien für die Sicherheit des Personals, die physische Sicherheit, die Verwaltung von EU-VS und die Sicherheit von Kommunikations- und Informationssystemen anwendet, durch die ein gleichwertiges Schutzniveau für EU-VS wie in der Kommission gewährleistet wird;

c) von ihm beziehungsweise ihr erstellte Verschlusssachen als EU-VS kennzeichnet.

(2) Innerhalb der Kommission fungiert die Generaldirektion „Humanressourcen und Sicherheit“ in enger Zusammenarbeit mit anderen zuständigen Kommissionsdienststellen als federführende Dienststelle für den Abschluss von Verwaltungsvereinbarungen über den Austausch von EU-VS mit anderen EU-Organen, -Einrichtungen, -Ämtern und -Agenturen.

(3) Verwaltungsvereinbarungen werden in der Regel in Form eines vom Generaldirektor für Humanressourcen und Sicherheit im Namen der Kommission unterzeichneten Briefwechsels abgeschlossen.

(4) Vor dem Abschluss einer Verwaltungsvereinbarung über den Austausch von EU-VS führt die Sicherheitsstelle der Kommission einen Bewertungsbesuch durch, um den rechtlichen Rahmen für den Schutz von EU-VS zu bewerten und sich der Wirksamkeit der zum Schutz von EU-VS ergriffenen Maßnahmen zu vergewissern. Wenn die Ergebnisse dieser Bewertung zufriedenstellend und die im Anschluss an den Besuch abgegebenen Empfehlungen für Folgemaßnahmen umgesetzt worden sind, tritt die Verwaltungsvereinbarung in Kraft und es dürfen EU-VS ausgetauscht werden. Es werden regelmäßig Folgebesuche durchgeführt, um zu überprüfen, ob die Verwaltungsvereinbarung eingehalten wird und ob die bestehenden Sicherheitsmaßnahmen noch den vereinbarten Grundprinzipien und Mindeststandards entsprechen.

(5) Innerhalb der Kommission fungiert die vom Generalsekretariat verwaltete EU-VS-Registratur in der Regel als zentrale Ein- und Ausgangsstelle für den Austausch von Verschlusssachen mit anderen EU-Organen, Einrichtungen, Ämtern und Agenturen. In Fällen, in denen es aus sicherheitstechnischen, organisatorischen oder operativen Gründen im Hinblick auf den Schutz von EU-VS eher angebracht ist, fungieren lokale EU-VS-Registraturen, die nach Maßgabe dieses Beschlusses und seiner Durchführungsbestimmungen in Kommissionsdienststellen eingerichtet wurden, als Ein- und Ausgangsstelle für Verschlusssachen in Bezug auf in die Zuständigkeit der betreffenden Kommissionsdienststellen fallende Angelegenheiten.

(6) Die Sicherheitsexpertengruppe der Kommission wird über den Prozess des Abschlusses von Verwaltungsvereinbarungen gemäß Absatz 2 unterrichtet.

*Artikel 53*

**Austausch von EU-VS mit Mitgliedstaaten**

(1) EU-VS dürfen mit Mitgliedstaaten ausgetauscht beziehungsweise für Mitgliedstaaten freigegeben werden, wenn sie in diesen Mitgliedstaaten in Übereinstimmung mit den Anforderungen, die für mit einem nationalen Geheimhaltungsgrad gekennzeichnete EU-VS der entsprechenden Geheimhaltungsstufe gemäß der Entsprechungstabelle der Geheimhaltungsgrade in Anhang I gelten, geschützt werden.

(2) Bringt ein Mitgliedstaat mit einem nationalen Geheimhaltungsgrad gekennzeichnete Verschlusssachen in die Strukturen oder Netze der Europäischen Union ein, so schützt die Kommission diese Verschlusssachen nach Maßgabe der Anforderungen, die für EU-VS der entsprechenden Geheimhaltungsstufe gemäß der Entsprechungstabelle der Geheimhaltungsgrade in Anhang I gelten.

*Artikel 54*

**Austausch von EU-VS mit Drittstaaten und internationalen Organisationen**

(1) Stellt die Kommission fest, dass es langfristig notwendig ist, mit Drittstaaten oder internationalen Organisationen Verschlusssachen auszutauschen, so werden die notwendigen Maßnahmen ergriffen, um einen geeigneten straf- oder verwaltungsrechtlichen Rahmen zu schaffen, welcher auch Geheimschutzabkommen oder entsprechende Verwaltungsvereinbarungen nach Maßgabe der einschlägigen Vorschriften einschließen kann.

(2) Geheimschutzabkommen oder Verwaltungsvereinbarungen nach Absatz 1 enthalten Bestimmungen, mit denen sichergestellt wird, dass EU-VS nach ihrer Entgegennahme durch Drittstaaten oder internationale Organisationen in einer ihrem Geheimhaltungsgrad angemessenen Weise nach Maßgabe von Mindeststandards geschützt werden, die den in diesem Beschluss festgelegten Mindeststandards entsprechen.

(3) Die Kommission kann Verwaltungsvereinbarungen gemäß Artikel 56 abschließen, sofern die betreffenden EU-VS in der Regel nicht höher als „RESTREINT UE/EU RESTRICTED“ eingestuft sind.

(4) Verwaltungsvereinbarungen über den Austausch von Verschlusssachen nach Absatz 3 enthalten Bestimmungen, mit denen sichergestellt wird, dass EU-VS nach ihrer Entgegennahme durch Drittstaaten oder internationale Organisationen in einer ihrem Geheimhaltungsgrad angemessenen Weise nach Maßgabe von Mindeststandards geschützt werden, die den in diesem Beschluss festgelegten Mindeststandards entsprechen. Bezüglich des Abschlusses von Geheimschutzabkommen oder Verwaltungsvereinbarungen wird die Sicherheitsexpertengruppe der Kommission zu Rate gezogen.

(5) Der Beschluss, eine EU-VS der Kommission an einen Drittstaat oder eine internationale Organisation weiterzugeben, wird von der Kommissionsdienststelle, die die EU-VS erstellt hat, von Fall zu Fall nach Maßgabe von Art und Inhalt der Verschlusssache, des Grundsatzes „Kenntnis nur, wenn nötig“ und der Vorteile für die Union gefasst. Ist die Verschlusssache oder etwaiges in ihr enthaltenes Quellenmaterial, um deren beziehungsweise dessen Weitergabe ersucht wird, nicht von der Kommission herausgegeben worden, so holt die Kommissionsdienststelle, in deren Besitz sich die Verschlusssache befindet, zunächst die schriftliche Zustimmung des Herausgebers zur Weitergabe der Verschlusssache ein. Kann der Herausgeber nicht ermittelt werden, so übernimmt die Kommissionsdienststelle, in deren Besitz sich die Verschlusssache befindet, nach Rücksprache mit der Sicherheitsexpertengruppe der Kommission dessen Verantwortung.

*Artikel 55*

**Geheimschutzabkommen**

(1) Für den Abschluss von Geheimschutzabkommen mit Drittstaaten oder internationalen Organisationen sind die Bestimmungen von Artikel 218 AEUV maßgeblich.

(2) In Geheimschutzabkommen

a) werden die Grundprinzipien und Mindeststandards für den Austausch von Verschlusssachen zwischen der Union und einem Drittstaat oder einer internationalen Organisation niedergelegt;

b) werden die technischen Durchführungsbestimmungen geregelt, die zwischen den zuständigen Sicherheitsbehörden der betreffenden Organe und Einrichtungen der Union und der zuständigen Sicherheitsbehörde des betreffenden Drittstaats beziehungsweise der betreffenden internationalen Organisation zu vereinbaren sind. In den Durchführungsbestimmungen wird das Schutzniveau, das die in dem betreffenden Drittstaat oder bei der betreffenden internationalen Organisation bestehenden Sicherheitsvorschriften, -strukturen und -verfahren gewährleisten, berücksichtigt;

c) wird vorgesehen, dass vor einem Austausch von Verschlusssachen nach dem Abkommen sichergestellt wird, dass der Empfänger in der Lage ist, die ihm zur Verfügung gestellten Verschlusssachen angemessen zu schützen und zu verwahren.

(3) Wenn die Kommission im Sinne von Artikel 51 Absatz 1 zu dem Schluss gelangt, dass der Austausch von Verschlusssachen erforderlich ist, zieht sie, soweit zweckmäßig, den Europäischen Auswärtigen Dienst, das Generalsekretariat des Rates und andere Organe und Einrichtungen der Union zu Rate, um zu ermitteln, ob eine Empfehlung nach Artikel 218 Absatz 3 AEUV abgegeben werden sollte.

(4) EU-VS werden nicht auf elektronischem Wege ausgetauscht, es sei denn, dies ist in dem Geheimschutzabkommen oder den technischen Durchführungsvereinbarungen ausdrücklich vorgesehen.

(5) Innerhalb der Kommission fungiert die vom Generalsekretariat verwaltete EU-VS-Registratur in der Regel als zentrale Ein- und Ausgangsstelle für den Austausch von Verschlusssachen mit Drittstaaten und internationalen Organisationen. In Fällen, in denen es aus sicherheitstechnischen, organisatorischen oder operativen Gründen im Hinblick auf den Schutz von EU-VS eher angebracht ist, fungieren lokale EU-VS-Registraturen, die nach Maßgabe dieses Beschlusses und seiner Durchführungsbestimmungen in Kommissionsdienststellen eingerichtet wurden, als Ein- und Ausgangsstelle für Verschlusssachen in Bezug auf in die Zuständigkeit der betreffenden Kommissionsdienststellen fallende Angelegenheiten.

(6) Zur Bewertung der Wirksamkeit der Sicherheitsvorschriften, -strukturen und verfahren des betreffenden Drittstaats beziehungsweise der betreffenden internationalen Organisation nimmt die Kommission in Zusammenarbeit mit anderen EU-Organen, -Einrichtungen, -Ämtern und Agenturen sowie im gegenseitigen Einvernehmen mit dem betreffenden Drittstaat beziehungsweise der betreffenden internationalen Organisation an Bewertungsbesuchen teil. Bei diesen Besuchen wird Folgendes bewertet:

a) der für den Schutz von Verschlusssachen geltende Rechtsrahmen:

b) die spezifischen Merkmale des Sicherheitskonzepts sowie 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 ausgetauschten 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.

*Artikel 56*

**Verwaltungsvereinbarungen**

(1) 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 die Sicherheitsstelle der Kommission nach Rücksprache mit der Sicherheitsexpertengruppe der Kommission insbesondere festgestellt hat, dass die betreffende Vertragspartei nicht über ein ausreichend entwickeltes Sicherheitssystem verfügt, um ein Geheimschutzabkommen abschließen zu können, kann die Kommission eine Verwaltungsvereinbarung mit den zuständigen Stellen des betreffenden Drittstaats oder mit der betreffenden internationalen Organisation schließen.

(2) Derartige Verwaltungsvereinbarungen werden in der Regel in Form eines Briefwechsels geschlossen.

(3) Vor dem Abschluss einer solchen Verwaltungsvereinbarung wird ein Bewertungsbesuch durchgeführt. Die Ergebnisse des Bewertungsbesuchs werden der Sicherheitsexpertengruppe der Kommission mitgeteilt. Liegen außergewöhnliche Gründe für einen dringenden Austausch von Verschlusssachen vor, so dürfen die EU-VS weitergegeben werden, sofern alle Anstrengungen unternommen werden, den Bewertungsbesuch so bald wie möglich durchzuführen.

(4) EU-VS werden nicht auf elektronischem Wege ausgetauscht, es sei denn, dies ist in der Verwaltungsvereinbarung ausdrücklich vorgesehen.

*Artikel 57*

**Ad-hoc-Weitergabe von EU-VS in Ausnahmefällen**

(1) Falls weder ein Geheimschutzabkommen noch eine Verwaltungsvereinbarung besteht und die Kommission oder eine ihrer Dienststellen zu dem Schluss gelangt, dass im Zusammenhang mit einem politischen oder rechtlichen Rahmen der Union eine außergewöhnliche Notwendigkeit besteht, EU-VS an einen Drittstaat oder eine internationale Organisation weiterzugeben, so überprüft die Sicherheitsstelle der Kommission soweit möglich zusammen mit den Sicherheitsbehörden des betreffenden Drittstaats oder der betreffenden internationalen Organisation, ob dessen beziehungsweise deren Sicherheitsvorschriften, -strukturen und -verfahren sicherstellen, dass weitergegebene EU-VS nach Maßgabe von Standards geschützt werden, die nicht weniger streng als die in diesem Beschluss festgelegten Standards sind.

(2) Die Entscheidung über eine etwaige Weitergabe der EU-VS an den betreffenden Drittstaat oder die betreffende internationale Organisation trifft die Kommission nach Rücksprache mit der Sicherheitsexpertengruppe der Kommission auf der Grundlage eines Vorschlags des für Sicherheitsfragen zuständigen Kommissionsmitglieds.

(3) Wenn die Kommission entschieden hat, dass die EU-VS weitergegeben werden dürfen, holt die zuständige Kommissionsdienststelle zunächst die schriftliche Zustimmung des Herausgebers einschließlich der Zustimmung der Urheber etwaigen darin enthaltenen Quellenmaterials ein und leitet dann die EU-VS, auf denen durch eine Weitergabekennzeichnung angegeben wird, an welchen Drittstaat oder welche internationale Organisation die Weitergabe erfolgt, weiter. 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.

KAPITEL 8

**SCHLUSSBESTIMMUNGEN**

*Artikel 58*

**Ersetzung des bisherigen Beschlusses**

Der Beschluss 2001/844/EG, EGKS, Euratom der Kommission ([1]) wird durch den vorliegenden Beschluss aufgehoben und ersetzt.

*Artikel 59*

**Vor Inkrafttreten dieses Beschlusses erstellte Verschlusssachen**

(1) Alle gemäß dem Beschluss 2001/844/EG, EGKS, Euratom eingestuften EU-VS werden weiter gemäß den einschlägigen Bestimmungen des vorliegenden Beschlusses geschützt.

(2) Mit Ausnahme von Euratom-Verschlusssachen gilt für alle Verschlusssachen, die sich zum Zeitpunkt des Inkrafttretens des Beschlusses 2001/844/EG, EGKS, Euratom im Besitz der Kommission befanden, Folgendes:

a) Verschlusssachen, die von der Kommission erstellt wurden, gelten standardmäßig weiterhin als in den Geheimhaltungsgrad „RESTREINT UE“ eingestuft, sofern der Urheber nicht bis spätestens 31. Januar 2002 eine andere Einstufung beschlossen und dies allen Empfängern des betreffenden Dokuments mitgeteilt hatte;

b) Verschlusssachen, die von Urhebern außerhalb der Kommission erstellt wurden, werden unter der ursprünglichen Einstufung weitergeführt und als EU-VS der entsprechenden Stufe behandelt, sofern der Urheber nicht der Aufhebung der Geheimhaltung oder der Herabstufung des Geheimhaltungsgrades der Verschlusssache zustimmt.

*Artikel 60*

**Durchführungsbestimmungen und Sicherheitshinweise**

(1) Die Durchführungsbestimmungen für diesen Beschluss werden gegebenenfalls im Wege eines gesonderten Beschlusses der Kommission zur Ermächtigung des für Sicherheitsfragen zuständigen Kommissionsmitglieds im Einklang mit der Geschäftsordnung erlassen.

(2) Das für Sicherheitsfragen zuständige Kommissionsmitglied kann nach seiner Ermächtigung durch den oben genannten Kommissionsbeschluss Sicherheitshinweise ausarbeiten, in denen Sicherheitsleitlinien und bewährte Verfahren im Rahmen dieses Beschlusses und seiner Durchführungsbestimmungen festgelegt werden.

(3) Die Kommission kann die in den Absätzen 1 und 2 dieses Artikels genannten Aufgaben im Wege eines gesonderten Befugnisübertragungsbeschlusses im Einklang mit der Geschäftsordnung dem Generaldirektor für Humanressourcen und Sicherheit übertragen.

*Artikel 61*

**Inkrafttreten**

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

Brüssel, den 13. März 2015

*Für die Kommission*

*Der Präsident*

Jean-Claude JUNCKER

([1]) Beschluss 2001/844/EG, EGKS, Euratom der Kommission vom 29. November 2001 zur Änderung ihrer Geschäftsordnung (ABl. L 317 vom 3.12.2001, S. 1).

*ANHANG I*

**ENTSPRECHUNGSTABELLE DER GEHEIMHALTUNGSGRADE**

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

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

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

([2]) Deutschland: VS = Verschlusssache.

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

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

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

*ANHANG II*

**ABKÜRZUNGSVERZEICHNIS**

| Abkürzung | Bedeutung |
|---|---|
| AEUV | Vertrag über die Arbeitsweise der Europäischen Union |
| CA | Crypto Authority (Kryptostelle) |
| CAA | Crypto Approval Authority (Krypto-Zulassungsstelle) |
| CCTV | Closed Circuit Television (Videoüberwachung) |
| CDA | Crypto Distribution Authority (Krypto-Verteilungsstelle) |
| CIS | Communication and Information Systems handling EUCI (Kommunikations- und Informationssysteme, in denen EU-VS bearbeitet werden) |
| DSA | Designated Security Authority (Beauftragte Sicherheitsbehörde) |
| EUCI | EU Classified Information (EU-Verschlusssachen, EU-VS) |
| FSC | Facility Security Clearance (Sicherheitsbescheid für Unternehmen) |
| IA | Information Assurance (Informationssicherung) |
| IAA | Information Assurance Authority (Stelle für Informationssicherung) |
| IDS | Intrusion Detection System (Einbruchmeldesystem) |
| IT | Information Technology (Informationstechnologie) |
| LSO | Local Security Officer (lokaler Sicherheitsbeauftragter) |
| NSA | National Security Authority (nationale Sicherheitsbehörde) |
| PSC | Personnel Security Clearance (Erklärung über die Sicherheitsüberprüfung von Personal) |
| PSCC | Personnel Security Clearance Certificate (Sicherheitsüberprüfungsbescheinigung) |
| PSI | Programme/Project Security Instructions (Sicherheitsanweisung für ein Programm/Projekt) |
| RKO | Registry Control Officer (Registraturkontrollbeauftragter) |
| SAA | Security Accreditation Authority (Sicherheitsakkreditierungsstelle) |
| SAL | Security Aspects Letter (Geheimschutzklausel) |
| SCG | Security Classification Guide (VS-Einstufungsliste) |
| SecOP | Security Operating Procedures (sicherheitsbezogene Betriebsverfahren) |
| TA | TEMPEST Authority (TEMPEST-Stelle) |

*ANHANG III*

**VERZEICHNIS 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. Sekretariat: +32 25014542
Fax +32 25014596
E-Mail: nvo-ans@diplobel.fed.be

BULGARIEN

State Commission on Information Security
90 Cherkovna Str.
1505 Sofia
Tel.: +359 29333600
Fax +359 29873750
E-Mail: dksi@government.bg
Website: www.dksi.bg

TSCHECHISCHE REPUBLIK

Národní bezpečnostní úřad
(National Security Authority)
Na Popelce 2/16
150 06 Praha 56
Tel.: +420 257283335
Fax +420 257283110
E-Mail: czech.nsa@nbu.cz
Website: www.nbu.cz

DÄNEMARK

Politiets Efterretningstjeneste
(Danish Security Intelligence Service)
Klausdalsbrovej 1
2860 Søborg
Tel.: +45 33148888
Fax +45 33430190

Forsvarets Efterretningstjeneste
(Danish Defence Intelligence Service)
Kastellet 30
2100 Copenhagen Ø
Tel.: +45 33325566
Fax +45 33931320

DEUTSCHLAND

Bundesministerium des Innern
Referat ATS III 3
Alt-Moabit 101 D
11014 Berlin
Tel.: +49 30186810
Fax +49 30186811441
E-Mail: oesIII3@bmi.bund.de

ESTLAND

National Security Authority Department
Estonian Ministry of Defence
Sakala 1
15094 Tallinn
Tel.: +372 717 0019, +372 7170117
Fax +372 7170213
E-Mail: nsa@mod.gov.ee

GRIECHENLAND

Γενικό Επιτελείο Εθνικής Άμυνας (ΓΕΕΘΑ)
Διακλαδική Διεύθυνση Στρατιωτικών Πληροφοριών (ΔΔΣΠ)
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)
Military Intelligence Sectoral Directorate
Security Counterintelligence Directorate
GR-STG 1020 Holargos — Athens
Tel.: +30 2106572045
+ 30 2106572009
Fax +30 2106536279, +30 2106577612

SPANIEN

Autoridad Nacional de Seguridad
Oficina Nacional de Seguridad
Avenida Padre Huidobro s/n
28023 Madrid
Tel.: +34 913725000
Fax +34 913725808
E-Mail: nsa-sp@areatec.com

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

KROATIEN

Office of the National Security Council
Croatian NSA
Jurjevska 34
10000 Zagreb
Kroatien
Tel.: +385 14681222
Fax + 385 14686049
Website: www.uvns.hr

IRLAND

National Security Authority
Department of Foreign Affairs
76-78 Harcourt Street
Dublin 2
Tel.: +353 14780822
Fax +353 14082959

ITALIEN

Presidenza del Consiglio dei Ministri
D.I.S. — U.C.Se.
Via di Santa Susanna, 15
00187 Roma
Tel.: +39 0661174266
Fax +39 064885273

ZYPERN

ΥΠΟΥΡΓΕΙΟ ΑΜΥΝΑΣ
ΣΤΡΑΤΙΩΤΙΚΟ ΕΠΙΤΕΛΕΙΟ ΤΟΥ ΥΠΟΥΡΓΟΥ
Εθνική Αρχή Ασφάλειας (ΕΑΑ)
Υπουργείο Άμυνας
Λεωφόρος Εμμανουήλ Ροΐδη 4
1432 Λευκωσία, Κύπρος
Τηλέφωνα: +357 22807569, +357 22807643,
+357 22807764
Τηλεομοιότυπο: +357 22302351

Ministry of Defence
Minister's Military Staff
National Security Authority (NSA)
4 Emanuel Roidi street
1432 Nicosia
Tel.: +357 22807569, +357 22807643,
+357 22807764
Fax +357 22302351
E-Mail: cynsa@mod.gov.cy

LETTLAND

National Security Authority
Constitution Protection Bureau of the Republic of Latvia
P.O. Box 286
LV-1001 Riga
Tel.: +371 67025418
Fax +371 67025454
E-Mail: ndi@sab.gov.lv

LITAUEN

Lietuvos Respublikos paslapčių apsaugos koordinavimo komisija
(The Commission for Secrets Protection Coordination of the Republic of Lithuania National Security Authority)
Gedimino 40/1
LT-01110 Vilnius
Tel.: +370 706 66701 + 370 706 66702
Fax +370 706 66700
E-Mail: nsa@vsd.lt

LUXEMBURG

Autorité nationale de Sécurité
Boîte postale 2379
1023 Luxemburg
Tel.: +352 24782210 (Zentrale)
+ 352 24782253 (Durchwahl)
Fax +352 24782243

UNGARN

Nemzeti Biztonsági Felügyelet
(National Security Authority of Hungary)
H-1024 Budapest, Szilágyi Erzsébet fasor 11/B
Tel.: +36 (1) 7952303
Fax +36 (1) 7950344

Postanschrift:
1357 Budapest, P.O. Box 2
E-Mail: nbf@nbf.hu
Website: www.nbf.hu

MALTA

Ministry for Home Affairs and National Security
P.O. Box 146
MT-Valletta
Tel.: +356 21249844
Fax +356 25695321

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

ÖSTERREICH

Informationssicherheitskommission
Bundeskanzleramt
Ballhausplatz 2
1014 Wien
Tel.: +43 1531152594
Fax +43 1531152615
E-Mail: ISK@bka.gv.at

POLEN

Agencja Bezpieczeństwa Wewnętrznego — ABW
(Internal Security Agency)
2A Rakowiecka St.
00-993 Warszawa
Tel.: +48 22 58 57 944
Fax +48 22 58 57 443
E-Mail: nsa@abw.gov.pl
Website: www.abw.gov.pl

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 Național al Informațiilor Secrete de Stat
(Romanian NSA — ORNISS National Registry Office for Classified Information)
4 Mures Street
012275 Bucharest
Tel.: +40 212245830
Fax +40 212240714
E-Mail: nsa.romania@nsa.ro
Website: www.orniss.ro

SLOWENIEN

Urad Vlade RS za varovanje tajnih podatkov
Gregorčičeva 27
1000 Ljubljana
Tel.: +386 14781390
Fax +386 14781399
E-Mail: gp.uvtp@gov.si

SLOWAKEI

Národný bezpečnostný úrad
National Security Authority
Budatínska 30
P.O. Box 16
850 07 Bratislava
Tel.: +421 268692314
Fax +421 263824005
Website: www.nbusr.sk

FINNLAND

National Security Authority
Ministry for Foreign Affairs
P.O. Box 453
FI-00023 Government
Tel. 16055890
Fax +358 916055140
E-Mail: NSA@formin.fi

SCHWEDEN

Utrikesdepartementet
(Ministry for Foreign Affairs)
SSSB
S-103 39 Stockholm
Tel.: +46 84051000
Fax +46 87231176
E-Mail: ud-nsa@foreign.ministry.se

VEREINIGTES KÖNIGREICH

UK National Security Authority
Room 335, 3rd Floor
70 Whitehall
London
SW1A 2AS
Tel. 1: +44 2072765649
Tel. 2: +44 2072765497
Fax +44 2072765651
E-Mail: UK-NSA@cabinet-office.x.gsi.gov.uk