II

(Nicht veröffentlichungsbedürftige Rechtsakte)

KOMMISSION

BESCHLUSS DER KOMMISSION
vom 29. November 2001
zur Änderung ihrer Geschäftsordnung

(Bekannt gegeben unter Aktenzeichen K(2001) 3031)

(2001/844/EG, EGKS, Euratom)

DIE KOMMISSION DER EUROPÄISCHEN GEMEINSCHAFTEN —

gestützt auf den Vertrag zur Gründung der Europäischen Gemeinschaft, insbesondere auf Artikel 218 Absatz 2,

gestützt auf den Vertrag über die Gründung der Europäischen Gemeinschaft für Kohle und Stahl, insbesondere auf Artikel 16,

gestützt auf den Vertrag zur Gründung der Europäischen Atomgemeinschaft, insbesondere auf Artikel 131,

gestützt auf den Vertrag über die Europäische Union, insbesondere auf Artikel 28 Absatz 1 und Artikel 41 Absatz 1 —

BESCHLIESST:

Artikel 1

Die Sicherheitsvorschriften der Kommission, deren Wortlaut dem vorliegenden Beschluss im Anhang beigefügt ist, werden dem Anhang der Geschäftsordnung der Kommission angefügt.

Artikel 2

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

Er gilt ab 1. Dezember.

Brüssel, den 29. November 2001

Für die Kommission
Der Präsident
Romano PRODI

ANHANG

SICHERHEITSVORSCHRIFTEN DER KOMMISSION

In Erwägung nachstehender Gründe:

(1) Für die Ausweitung der Tätigkeiten der Kommission in Bereichen, die ein bestimmtes Maß an Geheimhaltung erfordern, sollte ein umfassendes Sicherheitssystem geschaffen werden, das die Kommission, die anderen Organe, Einrichtungen, Ämter und Agenturen, die durch den EG-Vertrag oder den Vertrag über die Europäische Union oder auf deren Grundlage geschaffen wurden, die Mitgliedstaaten sowie jeden anderen Empfänger von EU-Verschlusssachen, hiernach „EU-Verschlusssachen" genannt, einbezieht.

(2) Um die Effizienz des durch diese Vorschriften geschaffenen Sicherheitssystems zu gewährleisten, gibt die Kommission EU-Verschlusssachen nur an die externen Einrichtungen weiter, die garantieren, alle erforderlichen Maßnahmen getroffen zu haben, um Bestimmungen einzuhalten, die diesen Vorschriften absolut gleichwertig sind.

(3) Diese Vorschriften lassen die Verordnung Euratom Nr. 3 des EAG-Rates vom 31. Juli 1958 zur Anwendung des Artikels 24 des EAG-Vertrags [1], die Verordnung des Rates Nr. 1588/90 vom 11. Juni 1990 über die Übermittlung von unter die Geheimhaltungspflicht fallenden Informationen an das Statistische Amt der Europäischen Gemeinschaften [2] und den Beschluss C (95) 1510 endg. der Kommission vom 23. November 1995 über den Schutz der Informationssysteme unberührt.

(4) Um einen reibungslosen Ablauf des Beschlussfassungsprozesses in der Union sicherzustellen, beruht das Sicherheitssystem der Kommission auf den Grundsätzen, die der Rat in seinem Beschluss 2001/264/EG vom 19. März 2001 über die Annahme der Sicherheitsvorschriften des Rates [3] ausgeführt hat.

(5) Die Kommission weist darauf hin, dass es wichtig ist, gegebenenfalls die anderen Organe der Europäischen Union an den Geheimhaltungsregeln und -normen, die zum Schutz der Interessen der Union und ihrer Mitgliedstaaten erforderlich sind, zu beteiligen.

(6) Die Kommission stellt fest, dass sie ein eigenes Sicherheitskonzept einführen muss, das allen Aspekten der Sicherheit und dem spezifischen Charakter der Kommission als Organ Rechnung trägt.

(7) Diese Vorschriften lassen Artikel 255 des Vertrags und die 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 [4] unberührt.

Artikel 1

Die Sicherheitsvorschriften sind im Anhang aufgeführt.

Artikel 2

(1) Das für Sicherheitsfragen zuständige Kommissionsmitglied trifft geeignete Maßnahmen, um dafür zu sorgen, dass die Bestimmungen nach Artikel 1 beim Umgang mit EU-Verschlusssachen in der Kommission von deren Beamten und sonstigen Bediensteten und von an die Kommission abgeordnetem Personal eingehalten werden und ihre Einhaltung an allen Dienstorten der Kommission einschließlich der Vertretungen und Büros in der Europäischen Union und in den Delegationen in Drittländern sowie von Seiten externer Vertragspartner der Kommission gesichert ist.

(2) Die Mitgliedstaaten sowie andere durch die Verträge oder auf deren Grundlage eingerichtete Organe, Einrichtungen, Ämter und Agenturen erhalten EU-Verschlusssachen unter der Voraussetzung, dass sie beim Umgang mit EU-Verschlusssachen in ihren Dienststellen und Gebäuden für die Einhaltung von Bestimmungen sorgen, die den Bestimmungen nach Artikel 1 absolut gleichwertig sind. Das gilt insbesondere für

a) die Mitglieder der Ständigen Vertretungen der Mitgliedstaaten bei der Europäischen Union sowie die Mitglieder der nationalen Delegationen, die an Sitzungen der Kommission oder ihrer Gremien teilnehmen bzw. in sonstige Tätigkeiten der Kommission einbezogen sind;

b) sonstige Mitglieder der nationalen Verwaltungen der Mitgliedstaaten, die mit EU-Verschlusssachen zu tun haben, unabhängig davon, ob sie im Hoheitsgebiet der Mitgliedstaaten oder außerhalb Dienst tun;

c) externe Vertragspartner und abgeordnetes Personal, die mit EU-Verschlusssachen zu tun haben.

[1] ABl. 17 vom 6.10.1958, S. 406.
[2] ABl. L 151 vom 15.6.1990, S. 1.
[3] ABl. L 101 vom 11.4.2001, S. 1.
[4] ABl. L 145 vom 31.5.2001, S. 43.

Artikel 3

Drittländer, internationale Organisationen und andere Einrichtungen erhalten EU-Verschlusssachen unter der Voraussetzung, dass sie beim Umgang damit für die Einhaltung von Bestimmungen sorgen, die den Bestimmungen nach Artikel 1 absolut gleichwertig sind.

Artikel 4

Das für Sicherheitsfragen zuständige Mitglied der Kommission kann unter Beachtung der in Teil I des Anhangs enthaltenen Grundprinzipien und Mindeststandards für die Sicherheit Maßnahmen nach Teil II des Anhangs treffen.

Artikel 5

Die vorliegenden Vorschriften ersetzen ab dem Tag ihrer Anwendung

a) den Beschluss C (94) 3282 vom 30. November 1994 betreffend die Schutzmaßnahmen für die als Verschlusssachen eingestuften Informationen, die im Rahmen der Tätigkeiten der Europäischen Union ausgearbeitet oder ausgetauscht werden;

b) den Beschluss C (99) 423 vom 25. Februar 1999 über das Verfahren zur Ermächtigung der Beamten und sonstigen Bediensteten der Europäischen Kommission zum Zugang zu von der Kommission verwahrten Verschlusssachen;

Artikel 6

Ab dem Tag der Anwendung dieser Vorschriften werden alle von der Kommission bis zu diesem Datum verwahrten Verschlusssachen, ausgenommen die Euratom-Verschlusssachen,

a) die von der Kommission erstellt worden sind, automatisch als „EU — NUR FÜR DEN DIENSTGEBRAUCH“ eingestuft, sofern der Urheber nicht spätestens bis zum 31. Januar 2002 eine andere Einstufung beschließt oder die Geheimhaltung aufhebt; in diesem Fall setzt er alle Empfänger des betreffenden Dokuments in Kenntnis;

b) die von Urhebern außerhalb der Kommission erstellt worden sind, unter der ursprünglichen Einstufung weitergeführt und damit als EU-Verschlusssache der entsprechenden Stufe behandelt, sofern der Urheber nicht der Aufhebung der Geheimhaltung oder der Herabstufung der Verschlusssache zustimmt.

ANHANG

SICHERHEITSVORSCHRIFTEN DER EUROPÄISCHEN KOMMISSION

Inhalt

-

TEIL I: GRUNDPRINZIPIEN UND MINDESTSTANDARDS FÜR DIE SICHERHEIT

1. EINLEITUNG

Die vorliegenden Bestimmungen enthalten die Grundprinzipien und Mindeststandards für die Sicherheit, die von der Kommission an sämtlichen Dienstorten sowie von allen Empfängern von EU-Verschlusssachen in angemessener Weise einzuhalten sind, damit die Sicherheit gewährleistet ist und darauf vertraut werden kann, dass ein gemeinsamer Sicherheitsstandard herrscht.

2. ALLGEMEINE GRUNDSÄTZE

Die Sicherheitspolitik der Kommission ist Bestandteil ihres Gesamtkonzepts für das interne Management und unterliegt damit den Grundsätzen ihrer allgemeinen Politik.

Zu diesen Grundsätzen zählen Legalität, Transparenz, Rechenschaftspflicht und Subsidiarität (Verhältnismäßigkeit).

Legalität bezeichnet das Erfordernis, bei der Ausführung von Sicherheitsfunktionen voll und ganz innerhalb des rechtlichen Rahmens zu bleiben und die Rechtsvorschriften einzuhalten. Es bedeutet auch, dass die Verantwortlichkeiten im Sicherheitsbereich auf angemessenen Rechtsvorschriften beruhen müssen. Das Beamtenstatut ist voll und ganz anwendbar, insbesondere Artikel 17 betreffend die Verpflichtung des Personals, in Bezug auf Informationen der Kommission Stillschweigen zu bewahren sowie Titel VI über Disziplinarmaßnahmen. Des weiteren bedeutet dieser Grundsatz, dass im Verantwortungsbereich der Kommission liegende Sicherheitsverstöße im Einklang mit ihrem Konzept für Disziplinarmaßnahmen und ihrem Konzept für die Zusammenarbeit mit den Mitgliedstaaten im Bereich des Strafrechts behandelt werden müssen.

Transparenz bezeichnet das Erfordernis der Klarheit in Bezug auf alle Sicherheitsvorschriften und -bestimmungen für die einzelnen Dienste und Bereiche (materielle Sicherheit/Schutz von Verschlusssachen usw.) und die Notwendigkeit eines in sich schlüssigen und strukturierten Konzepts für das Sicherheitsbewusstsein. In diesem Zusammenhang sind auch klare schriftliche Leitlinien für die Durchführung von Sicherheitsmaßnahmen erforderlich.

Rechenschaftspflicht bedeutet, dass die Verantwortlichkeiten im Sicherheitsbereich eindeutig festgelegt werden. Des weiteren fällt unter diesen Begriff die Notwendigkeit, in regelmäßigen Abständen festzustellen, ob die Verantwortlichkeiten ordnungsgemäß wahrgenommen worden sind.

Subsidiarität oder Verhältnismäßigkeit bedeutet, dass die Sicherheit auf der niedrigstmöglichen Ebene und möglichst nahe bei den einzelnen Generaldirektionen und Diensten der Kommission organisiert wird. Dieser Grundsatz bedeutet auch, dass Sicherheitsmaßnahmen auf die Bereiche beschränkt werden, in denen sie wirklich erforderlich sind. Schließlich müssen Sicherheitsmaßnahmen auch im richtigen Verhältnis zu den zu schützenden Interessen und zu der tatsächlichen oder potenziellen Bedrohung dieser Interessen stehen und einen Schutz ermöglichen, der zu möglichst geringen Beeinträchtigungen führt.

3. GRUNDLAGEN FÜR DIE SICHERHEIT

Die Grundlagen für die Schaffung einer soliden Sicherheitslage sind

a) in jedem Mitgliedstaat eine nationale Sicherheitsorganisation, die dafür zuständig ist,

   1. Erkenntnisse über Spionage, Sabotage, Terrorismus und andere subversive Tätigkeiten zu sammeln und zu speichern sowie

   2. ihre jeweilige Regierung und — über sie — die Kommission über Art und Umfang von Bedrohungen der Sicherheit und entsprechende Schutzmaßnahmen zu informieren und zu beraten;

b) in jedem Mitgliedstaat und in der Kommission eine technische INFOSEC-Stelle, die dafür zuständig ist, in Zusammenarbeit mit der betreffenden Sicherheitsbehörde Informationen und Beratung über technische Bedrohungen der Sicherheit und entsprechende Schutzmaßnahmen zu liefern;

c) eine regelmäßige Zusammenarbeit von Regierungsstellen und den entsprechenden Dienststellen der europäischen Organe, um erforderlichenfalls

   1. die schutzbedürftigen Personen, Informationen und Ressourcen sowie

   2. gemeinsame Schutzstandards

   zu bestimmen und entsprechende Empfehlungen abzugeben.

d) eine enge Zusammenarbeit zwischen dem Sicherheitsbüro der Kommission und den Sicherheitsdiensten der anderen europäischen Organe sowie dem Sicherheitsbüro der NATO (NOS).

4. GRUNDSÄTZE FÜR DIE SICHERHEIT VON VERSCHLUSSSACHEN

4.1. **Ziele**

Die Hauptziele im Bereich der Sicherheit von Verschlusssachen sind:

a) Schutz von EU-Verschlusssachen vor Spionage, Kenntnisnahme durch Unbefugte oder unerlaubter Weitergabe;

b) Schutz von EU-Informationen, die in Kommunikations- und Informationssystemen und -netzen behandelt werden, vor der Gefährdung ihrer Vertraulichkeit, Integrität und Verfügbarkeit;

c) Schutz von Gebäuden der Kommission, in denen EU-Informationen aufbewahrt werden, vor Sabotage und vorsätzlicher Beschädigung;

d) im Falle eines Versagens der Sicherheitsvorkehrungen Bewertung des entstandenen Schadens, Begrenzung seiner Folgen und Durchführung der erforderlichen Maßnahmen zu seiner Behebung.

4.2. **Begriffsbestimmungen**

In diesen Vorschriften bedeutet

a) „EU-Verschlusssache“: Alle Informationen und Materialien, deren unerlaubte Weitergabe den Interessen der EU oder eines oder mehrerer ihrer Mitgliedstaaten in unterschiedlichem Maße Schaden zufügen könnte, unabhängig davon, ob es sich um ursprüngliche EU-Verschlusssachen handelt oder um Verschlusssachen, die von Mitgliedstaaten, Drittländern oder internationalen Organisationen stammen.

b) „Dokument“: Jede Form von Schreiben, Aufzeichnung, Protokoll, Bericht, Memorandum, Signal/Botschaft, Skizze, Photo, Dia, Film, Karte, Schaubild, Plan, Notizbuch, Matrize, Kohlepapier, Schreibmaschinen- oder Druckerfarbband, Magnetband, Kassette, Computer-Diskette, CD-ROM oder anderer materieller Träger, auf denen Informationen gespeichert sind.

c) „Material“: Dasselbe wie „Dokument“ gemäß der Definition unter Buchstabe b) sowie jeder Ausrüstungsgegenstand, der bereits hergestellt oder noch in Herstellung befindlich ist.

d) „Kenntnis notwendig“: Der Beamte oder Bedienstete muss Zugang zu EU-Verschlusssachen haben, um eine Funktion auszuüben oder eine Aufgabe zu erledigen.

e) „Zugangsermächtigung“: Eine Verfügung des Präsidenten der Kommission, einer Person Zugang zu EU-Verschlusssachen bis zu einem bestimmten Geheimhaltungsgrad zu gewähren auf der Grundlage einer von einer nationalen Sicherheitsbehörde nach einzelstaatlichem Recht durchgeführten Sicherheitsüberprüfung, die zu einem positiven Ergebnis geführt hat.

f) „Geheimhaltungsgrad“: Zuerkennung einer geeigneten Sicherheitsstufe für Informationen, deren unerlaubte Weitergabe die Interessen der Kommission oder der Mitgliedstaaten in gewissem Maße beeinträchtigen könnte.

g) „Herabstufung“: Einstufung in einen niedrigeren Geheimhaltungsgrad.

h) „Aufhebung des Geheimhaltungsgrades“: Löschung jeder Geheimhaltungskennzeichnung.

i) „Urheber“: Ordnungsgemäß ermächtigter Verfasser eines als Verschlusssache eingestuften Dokuments. In der Kommission können die Leiter von Dienststellen ihr Personal ermächtigen, EU-Verschlusssachen zu erstellen.

j) „Kommissionsdienststellen“: Dienststellen und Dienste der Kommission, einschließlich der Kabinette, an allen Dienstorten, eingeschlossen die Gemeinsame Forschungsstelle, die Vertretungen und Büros in der Europäischen Union und die Delegationen in Drittländern.

4.3. **Einstufung in Geheimhaltungsgrade**

a) Im Bereich der Geheimhaltung muss bei der Auswahl der schutzbedürftigen Informationen und Materialien und bei der Bewertung des Ausmaßes des erforderlichen Schutzes mit Sorgfalt vorgegangen und auf Erfahrungen zurückgegriffen werden. Es ist von entscheidender Bedeutung, dass das Ausmaß des Schutzes der Sicherheitsrelevanz der zu schützenden Informationen und Materialien entspricht. Im Interesse eines reibungslosen Informationsflusses muss dafür gesorgt werden, dass eine zu hohe oder zu niedrige Einstufung von Verschlusssachen vermieden wird.

b) Das Einstufungssystem ist das Instrument, mit dem diesen Grundsätzen Wirkung verliehen wird; ein entsprechendes Einstufungssystem sollte bei der Planung und Organisierung von Maßnahmen zur Bekämpfung von Spionage, Sabotage, Terrorismus und anderen Arten der Bedrohung angewandt werden, so dass die wichtigsten Gebäude, in denen Verschlusssachen aufbewahrt werden, und die sensibelsten Punkte innerhalb dieser Gebäude auch den größten Schutz erhalten.

c) Die Verantwortung für die Festlegung des Geheimhaltungsgrades einer Information liegt allein bei deren Urheber.

d) Der Geheimhaltungsgrad hängt allein vom Inhalt dieser Information ab.

e) Sind verschiedene Informationen zu einem Ganzen zusammengestellt, gilt als Geheimhaltungsgrad für das gesamte Dokument der Geheimhaltungsgrad des am höchsten eingestuften Bestandteils. Eine Zusammenstellung von Informationen kann indessen höher eingestuft werden als ihre einzelnen Bestandteile.

f) Eine Einstufung als Verschlusssache erfolgt nur dann, wenn dies erforderlich ist und so lange dieses Erfordernis besteht.

4.4. **Ziele von Sicherheitsmaßnahmen**

Die Sicherheitsmaßnahmen sollen

a) alle Personen, die Zugang zu Verschlusssachen haben, die Träger von Verschlusssachen und alle Gebäude umfassen, in denen sich derartige Verschlusssachen und wichtige Einrichtungen befinden;

b) so ausgelegt sein, dass Personen, die aufgrund ihrer Stellung die Sicherheit von Verschlusssachen und wichtigen Einrichtungen, in denen Verschlusssachen aufbewahrt werden, gefährden könnten, erkannt und vom Zugang ausgeschlossen oder fern gehalten werden;

c) verhindern, dass unbefugte Personen Zugang zu Verschlusssachen oder zu Einrichtungen, in denen Verschlusssachen aufbewahrt werden, erhalten;

d) dafür sorgen, dass Verschlusssachen nur unter Beachtung des für alle Aspekte der Sicherheit grundlegenden Prinzips der Kenntnis nur wenn dies auch nötig ist verbreitet werden;

e) die Integrität (d. h. Verhinderung von Verfälschungen, unbefugten Änderungen oder unbefugten Löschungen) und die Verfügbarkeit (d. h. keine Verweigerung des Zugangs für Personen, die ihn benötigen und dazu befugt sind) aller Informationen, ob sie als Verschlusssachen eingestuft sind oder nicht, und insbesondere der in elektromagnetischer Form gespeicherten, verarbeiteten oder übermittelten Informationen, gewährleisten.

5. ORGANISATION DER SICHERHEIT

5.1. **Gemeinsame Mindeststandards**

Die Kommission sorgt dafür, dass gemeinsame Mindeststandards für die Sicherheit von allen Empfängern von EU-Verschlusssachen innerhalb des Organs und in seinem Zuständigkeitsbereich eingehalten werden, u. a. von allen Dienststellen und Vertragspartnern, so dass bei der Weitergabe von EU-Verschlusssachen darauf vertraut werden kann, dass diese mit derselben Sorgfalt behandelt werden. Zu diesen Mindeststandards gehören Kriterien für die Sicherheitsüberprüfung des Personals und Verfahren zum Schutz von EU-Verschlusssachen.

Die Kommission gewährt externen Stellen nur dann Zugang zu EU-Verschlusssachen, wenn diese gewährleisten, dass für den Umgang damit Bestimmungen eingehalten werden, die wenigstens diesen Mindeststandards entsprechen.

5.2. **Organisation**

In der Kommission ist die Sicherheit auf zwei Ebenen organisiert:

a) Auf der Ebene der Kommission als Ganzes gibt es ein Sicherheitsbüro der Kommission mit einer Akkreditierungsstelle für Sicherheit, die auch als Kryptographische Stelle (CrA) und als TEMPEST-Stelle fungiert sowie mit einer INFOSEC-Stelle (für Informationssicherheit) und einer oder mehreren Zentralen Registraturen für EU-Verschlusssachen, von denen jede über einen Kontrollbeauftragten oder mehrere Kontrollbeauftragte für die Registratur (RCO) verfügt.

b) Auf der Ebene der einzelnen Dienststellen sind für die Sicherheit einer oder mehrere Lokale Sicherheitsbeauftragte (LSO), einer oder mehrere Sicherheitsbeauftragte für die zentrale IT (CISO), Beauftragte für die lokale IT-Sicherheit (LISO) und Lokale Registraturen für EU-Verschlusssachen mit einem oder mehreren Registraturkontrollbeauftragten zuständig.

c) Die zentralen Sicherheitsstellen geben den lokalen Sicherheitsstellen praktische Leitlinien an die Hand.

6. SICHERHEIT DES PERSONALS

6.1. **Sicherheitsüberprüfung**

Alle Personen, die Zugang zu Informationen erhalten wollen, die als „EU — VERTRAULICH“ oder höher eingestuft sind, werden einer Sicherheitsüberprüfung unterzogen, bevor sie eine Zugangsermächtigung erhalten. Eine entsprechende Sicherheitsüberprüfung wird auch im Falle von Personen vorgenommen, zu deren Aufgaben der technische Betrieb oder die Wartung von Kommunikations- und Informationssystemen gehört, die Verschlusssachen enthalten. Bei der Sicherheitsüberprüfung soll festgestellt werden, ob die genannten Personen

a) von unzweifelhafter Loyalität sind;

b) die charakterlichen Merkmale und die Diskretionsfähigkeit besitzen, die ihre Integrität beim Umgang mit Verschlusssachen außer Zweifel stellt;

c) eventuell aus dem Ausland oder von anderer Seite her leicht unter Druck gesetzt werden können.

Besonders gründlich ist die Sicherheitsüberprüfung bei Personen vorzunehmen, die

d) Zugang zu Informationen des Geheimhaltungsgrades „EU — STRENG GEHEIM" erhalten sollen;

e) Stellen bekleiden, bei denen sie regelmäßig mit einer beträchtlichen Menge an Informationen des Geheimhaltungsgrades „EU — GEHEIM" zu tun haben;

f) aufgrund ihres Aufgabenbereichs besonderen Zugang zu gesicherten Kommunikations- oder Informationssystemen und somit Gelegenheit haben, sich unbefugt Zugang zu einer größeren Menge von EU-Verschlusssachen zu verschaffen oder in dem betreffenden Aufgabenbereich durch technische Sabotageakte schweren Schaden zu verursachen.

In den unter den Buchstaben d), e) und f) genannten Fällen soll soweit als nur möglich auf die Methode der Umfeldermittlung zurückgegriffen werden.

Werden Personen, für die die Notwendigkeit einer Kenntnis von Verschlusssachen nicht klar erwiesen ist, unter Umständen beschäftigt, unter denen sie Zugang zu EU-Verschlusssachen erhalten könnten (z. B. Boten, Sicherheitsbedienstete, Wartungs- und Reinigungspersonal usw.), so sind sie zuerst einer Sicherheitsüberprüfung zu unterziehen.

6.2. **Verzeichnis der Zugangsermächtigungen**

Alle Kommissionsdienststellen, die mit EU-Verschlusssachen zu tun haben oder gesicherte Kommunikations- oder Informationssysteme verwalten, führen ein Verzeichnis der Zugangsermächtigungen des bei ihnen arbeitenden Personals. Jede Zugangsermächtigung ist erforderlichenfalls zu überprüfen, um sicherzustellen, dass sie der derzeitigen Tätigkeit der betreffenden Person entspricht; sie ist vorrangig zu überprüfen, wenn neue Informationen eingehen, denen zufolge eine weitere Beschäftigung dieser Person mit Verschlusssachen nicht länger mit den Sicherheitsinteressen vereinbar ist. Der Lokale Sicherheitsbeauftragte der Kommissionsdienststelle führt ein Verzeichnis der Zugangsermächtigungen in seinem Zuständigkeitsbereich.

6.3. **Sicherheitsanweisungen für das Personal**

Alle Angehörigen des Personals, die Stellen bekleiden, an denen sie Zugang zu Verschlusssachen erhalten könnten, sind bei Aufnahme ihrer Tätigkeit und danach in regelmäßigen Abständen eingehend über die Notwendigkeit von Sicherheitsbestimmungen und über die Verfahren zu ihrer Durchführung zu unterrichten. Von diesen Mitarbeiterinnen und Mitarbeitern ist eine schriftliche Bestätigung zu verlangen, dass sie die vorliegenden Sicherheitsbestimmungen gelesen haben und in vollem Umfang verstehen.

6.4. **Verantwortung der Führungskräfte**

Führungskräfte haben die Pflicht, sich Kenntnis darüber zu verschaffen, welche ihrer Mitarbeiter mit Verschlusssachen zu tun haben oder über einen Zugang zu gesicherten Kommunikations- oder Informationssystemen verfügen, sowie alle Vorfälle oder offensichtlichen Schwachpunkte, die sicherheitsrelevant sein könnten, festzuhalten und zu melden.

6.5. **Sicherheitsstatus des Personals**

Es sind Verfahren vorzusehen, um dafür zu sorgen, dass bei Bekanntwerden nachteiliger Informationen über eine Person festgestellt wird, ob diese Person mit Verschlusssachen zu tun hat oder über einen Zugang zu gesicherten Kommunikations- oder Informationssystemen verfügt, und das Sicherheitsbüro der Kommission in Kenntnis zu setzen. Ist klar erwiesen, dass die fragliche Person ein Sicherheitsrisiko darstellt, ist sie von Aufgaben, bei denen sie die Sicherheit gefährden könnte, auszuschließen oder fern zu halten.

7. MATERIELLE SICHERHEIT

7.1. **Schutzbedarf**

Das Ausmaß der anzuwendenden Maßnahmen des materiellen Geheimschutzes zur Gewährleistung des Schutzes von EU-Verschlusssachen muss in angemessenem Verhältnis zum Geheimhaltungsgrad, zum Umfang und zur Bedrohung der entsprechenden Informationen und Materialien stehen. Alle Personen, die EU-Verschlusssachen verwahren, haben einheitliche Praktiken bei der Einstufung der Informationen anzuwenden und gemeinsame Schutzstandards für die Verwahrung, Übermittlung und Vernichtung schutzbedürftiger Informationen und Materialien zu beachten.

7.2. **Kontrolle**

Personen, die Bereiche, in denen sich ihnen anvertraute EU-Verschlusssachen befinden, unbeaufsichtigt lassen, müssen dafür sorgen, dass die Verschlusssachen sicher aufbewahrt und alle Sicherungsvorkehrungen (Schlösser, Alarm usw.) aktiviert worden sind. Weitere hiervon unabhängige Kontrollen sind nach den Dienststunden durchzuführen.

7.3. **Gebäudesicherheit**

Gebäude, in denen sich EU-Verschlusssachen oder gesicherte Kommunikations- und Informationssysteme befinden, sind gegen unerlaubten Zutritt zu schützen. Die Art der Schutzmaßnahmen für EU-Verschlusssachen (z. B. Vergitterung von Fenstern, Schlösser an Türen, Wachen am Eingang, automatische Zugangskontrollsysteme, Sicherheitskontrollen und Rundgänge, Alarmsysteme, Einbruchmeldesysteme und Wachhunde) hängt von folgenden Faktoren ab:

a) Geheimhaltungsgrad und Umfang der zu schützenden Informationen und Materialien sowie Ort ihrer Unterbringung im Gebäude;

b) Qualität der Sicherheitsbehältnisse, in denen sich die Informationsträger und Materialien befinden, und

c) Beschaffenheit und Lage des Gebäudes.

Die Art der Schutzmaßnahmen für Kommunikations- und Informationssysteme hängt in ähnlicher Weise von folgenden Faktoren ab: Einschätzung des Wertes der betreffenden Objekte und der Höhe des im Falle einer Kenntnisnahme durch Unbefugte eventuell entstehenden Schadens; Beschaffenheit und Lage des Gebäudes, in dem das System untergebracht ist sowie Ort der Unterbringung im Gebäude.

7.4. **Notfallpläne**

Es sind detaillierte Pläne auszuarbeiten, um im Falle eines örtlichen oder nationalen Notstands auf den Schutz von Verschlusssachen vorbereitet zu sein.

8. INFORMATIONSSICHERHEIT

Informationssicherheit (INFOSEC) betrifft die Festlegung und Anwendung von Sicherheitsmaßnahmen, mit denen in Kommunikations-, Informations- und sonstigen elektronischen Systemen bearbeitete, gespeicherte oder übermittelte Verschlusssachen davor geschützt werden sollen, versehentlich oder absichtlich in die Hände von Unbefugten zu gelangen bzw. ihre Integrität oder Verfügbarkeit zu verlieren. Es sind geeignete Gegenmaßnahmen zu ergreifen, um zu verhindern, dass unbefugte Nutzer Zugang zu EU-Verschlusssachen erhalten, befugten Nutzern der Zugang zu EU-Verschlusssachen verweigert wird oder es zu einer Verfälschung, unbefugten Änderung oder Löschung von EU-Verschlusssachen kommt.

9. MASSNAHMEN GEGEN SABOTAGE UND ANDERE FORMEN VORSÄTZLICHER BESCHÄDIGUNG

Vorsichtsmaßnahmen im Bereich des Objektschutzes zum Schutz wichtiger Einrichtungen, in denen Verschlusssachen untergebracht sind, sind die besten Sicherheitsgarantien gegen Sabotage und vorsätzliche Beschädigungen; eine Sicherheitsüberprüfung des Personals allein ist kein wirklicher Ersatz. Die zuständige einzelstaatliche Stelle wird gebeten, Erkenntnisse über Spionage, Sabotage, Terrorismus und andere subversive Tätigkeiten zusammenzutragen.

10. WEITERGABE VON VERSCHLUSSSACHEN AN DRITTSTAATEN ODER INTERNATIONALE ORGANISATIONEN

Der Beschluss, von der Kommission stammende EU-Verschlusssachen an einen Drittstaat oder eine internationale Organisation weiterzugeben, wird von der als Kollegium handelnden Kommission gefasst. Stammen die Verschlusssachen, um deren Weitergabe ersucht wird, nicht von der Kommission, so hat diese zunächst die Zustimmung des Urhebers der Verschlusssachen einzuholen. Kann dieser Urheber nicht ermittelt werden, so trifft die Kommission an seiner Stelle die Entscheidung.

Erhält die Kommission Verschlusssachen von Drittstaaten, internationalen Organisationen oder sonstigen Dritten, so werden sie in einer ihrem Geheimhaltungsgrad angemessenen Weise nach Maßgabe der für EU-Verschlusssachen geltenden Standards dieser Vorschriften oder aber höherer Standards, falls diese von der die Verschlusssachen weitergebenden dritten Seite gefordert werden, geschützt. Gegenseitige Kontrollen können vereinbart werden.

Die vorstehend dargelegten Grundprinzipien werden gemäß den detaillierten Vorschriften des Teils II Abschnitt 26 und der Anhänge 3, 4 und 5 verwirklicht.

TEIL II: DIE ORGANISATION DER SICHERHEIT IN DER KOMMISSION

11. DAS FÜR SICHERHEITSFRAGEN ZUSTÄNDIGE MITGLIED DER KOMMISSION

Das für Sicherheitsfragen zuständige Mitglied der Kommission

a) führt das Sicherheitskonzept der Kommission durch;

b) befasst sich mit Sicherheitsproblemen, die die Kommission oder ihre zuständigen Gremien ihm vorlegen;

c) prüft in enger Abstimmung mit den nationalen Sicherheitsbehörden (oder sonstigen geeigneten Behörden) der Mitgliedstaaten Fragen, die eine Änderung des Sicherheitskonzepts der Kommission erforderlich machen.

Das für Sicherheitsfragen zuständige Mitglied der Kommission ist insbesondere für Folgendes zuständig:

a) es koordiniert alle die Tätigkeiten der Kommission betreffenden Sicherheitsfragen;

b) es richtet an die hierfür benannten Behörden der Mitgliedstaaten Anträge auf Sicherheitsüberprüfung in der Kommission beschäftigter Personen durch die jeweilige nationale Sicherheitsbehörde im Einklang mit Abschnitt 20;

c) es ermittelt oder ordnet Ermittlungen an, wenn EU-Verschlusssachen Unbefugten zur Kenntnis gelangt sind und die Ursache hierfür dem ersten Anschein nach in der Kommission zu suchen ist;

d) es ersucht die entsprechenden Sicherheitsbehörden um die Einleitung von Ermittlungen, wenn eine Kenntnisnahme von EU-Verschlusssachen durch Unbefugte außerhalb der Kommission erfolgt zu sein scheint, und koordiniert die Ermittlungen in den Fällen, in denen mehr als eine Sicherheitsbehörde beteiligt ist;

e) es überprüft regelmäßig die Sicherheitsvorkehrungen für den Schutz von EU-Verschlusssachen;

f) es unterhält enge Verbindungen zu allen betroffenen Sicherheitsbehörden, um für eine Gesamtkoordinierung der Sicherheitsmaßnahmen zu sorgen;

g) es behält ständig das Sicherheitskonzept und die Sicherheitsverfahren der Kommission im Auge und arbeitet gegebenenfalls entsprechende Empfehlungen aus. In diesem Zusammenhang legt es der Kommission den von ihrem Sicherheitsdienst erstellten jährlichen Inspektionsplan vor.

12. DIE BERATENDE GRUPPE FÜR DAS SICHERHEITSKONZEPT DER KOMMISSION

Es wird eine Beratende Gruppe für das Sicherheitskonzept der Kommission eingesetzt. Sie besteht aus dem für Sicherheitsfragen zuständigen Mitglied der Kommission und dessen Stellvertreter, das bzw. der den Vorsitz führt, und Vertretern der nationalen Sicherheitsbehörden jedes Mitgliedstaates. Vertreter anderer europäischen Organe können ebenfalls eingeladen werden. Vertreter dezentraler EU-Einrichtungen können eingeladen werden, wenn sie betreffende Fragen erörtert werden.

Die Beratende Gruppe für das Sicherheitskonzept der Kommission tritt auf Antrag des Vorsitzenden oder eines ihrer Mitglieder zusammen. Sie prüft und bewertet alle relevanten Sicherheitsfragen und legt der Kommission gegebenenfalls Empfehlungen vor.

13. DER SICHERHEITSRAT DER KOMMISSION

Es wird ein Sicherheitsrat der Kommission eingesetzt. Er besteht aus dem Generalsekretär, der den Vorsitz führt, und den Generaldirektoren des Juristischen Dienstes, der Generaldirektion Personal und Verwaltung, der Generaldirektion Außenbeziehungen, der Generaldirektion Justiz und Inneres und der Gemeinsamen Forschungsstelle sowie den Leitern des Internen Auditdienstes und des Sicherheitsbüros der Kommission. Andere Kommissionsbeamte können eingeladen werden. Der Sicherheitsrat beurteilt Sicherheitsmaßnahmen innerhalb der Kommission und legt dem für Sicherheitsfragen zuständigen Kommissionsmitglied gegebenenfalls Empfehlungen in diesem Bereich vor.

14. DAS SICHERHEITSBÜRO DER KOMMISSION

Dem für Sicherheitsfragen zuständigen Mitglied der Kommission steht für die Wahrnehmung seiner in Abschnitt 11 genannten Aufgaben das Sicherheitsbüro der Kommission für die Koordinierung, Überwachung und Durchführung von Sicherheitsmaßnahmen zur Verfügung.

Der Leiter des Sicherheitsbüros der Kommission ist der wichtigste Berater des für Sicherheitsfragen zuständigen Mitglieds der Kommission und zugleich Sekretär der Beratenden Gruppe für das Sicherheitskonzept der Kommission. In dieser Hinsicht leitet er die Aktualisierung der Sicherheitsvorschriften und koordiniert die Sicherheitsmaßnahmen mit den zuständigen Behörden der Mitgliedstaaten und gegebenenfalls mit internationalen Organisationen, die Sicherheitsabkommen mit der Kommission geschlossen haben. Er hat hierbei die Rolle einer Verbindungsstelle.

Der Leiter des Sicherheitsbüros der Kommission ist für die Zulassung von IT-Systemen und -netzen in der Kommission zuständig. Er entscheidet im Einvernehmen mit den zuständigen nationalen Sicherheitsbehörden über die Zulassung von IT-Systemen und -netzen, die die Kommission und alle anderen Empfänger von EU-Verschlusssachen umfassen.

15. SICHERHEITSINSPEKTIONEN

Das Sicherheitsbüro der Kommission führt regelmäßige Inspektionen der Sicherheitsvorkehrungen zum Schutz von EU-Verschlusssachen durch.

Das Sicherheitsbüro der Kommission kann sich bei der Ausführung dieser Aufgabe von den Sicherheitsdiensten anderer EU-Organe, die EU-Verschlusssachen verwahren oder von den nationalen Sicherheitsbehörden der Mitgliedstaaten unterstützen lassen ([1]).

Auf Ersuchen eines Mitgliedstaates kann dessen nationale Sicherheitsbehörde in der Kommission gemeinsam mit dem Sicherheitsdienst der Kommission und in gegenseitigem Einvernehmen eine Inspektion von EU-Verschlusssachen durchführen.

([1]) Unbeschadet des Wiener Übereinkommens von 1961 über diplomatische Beziehungen und des Protokolls über die Vorrechte und Befreiungen der Europäischen Gemeinschaften vom 8. April 1965.

16. GEHEIMHALTUNGSGRADE, SICHERHEITSKENNUNGEN UND KENNZEICHNUNGEN

16.1. **Geheimhaltungsgrade ([1])**

Verschlusssachen werden wie folgt eingestuft (siehe auch Anhang 2):

„EU — STRENG GEHEIM“: Dieser Geheimhaltungsgrad findet nur auf Informationen und Material Anwendung, deren unbefugte Weitergabe den wesentlichen Interessen der Europäischen Union oder eines oder mehrerer ihrer Mitgliedstaaten einen äußerst schweren Schaden zufügen könnte.

„EU — GEHEIM“: Dieser Geheimhaltungsgrad findet nur auf Informationen und Material Anwendung, deren unbefugte Weitergabe den wesentlichen Interessen der Europäischen Union oder eines oder mehrerer ihrer Mitgliedstaaten schweren Schaden zufügen könnte.

„EU — VERTRAULICH“: Dieser Geheimhaltungsgrad findet auf Informationen und Material Anwendung, deren unbefugte Weitergabe den wesentlichen Interessen der Europäischen Union oder eines oder mehrerer ihrer Mitgliedstaaten schaden könnte.

„EU — NUR FÜR DEN DIENSTGEBRAUCH“: Dieser Geheimhaltungsgrad findet auf Informationen und Material Anwendung, deren unbefugte Weitergabe für die Interessen der Europäischen Union oder eines oder mehrerer ihrer Mitgliedstaaten nachteilig sein könnte.

Andere Geheimhaltungsgrade sind nicht zulässig.

16.2. **Sicherheitskennungen**

Um die Geltungsdauer eines Geheimhaltungsgrades zu begrenzen (bei Verschlusssachen automatische Herabstufung oder Aufhebung des Geheimhaltungsgrades) kann einvernehmlich eine Sicherheitskennung verwendet werden, die lautet „BIS … (Uhrzeit/Datum)“ oder „BIS … (Ereignis)“.

Zusätzliche Kennzeichnungen wie z. B. „CRYPTO“ oder eine andere von der EU anerkannte Sonderkennung werden verwendet, wenn zusätzlich zu der Behandlung, die sich durch die VS-Einstufung ergibt, eine begrenzte Verteilung und eine besondere Abwicklung erforderlich sind.

Sicherheitskennungen sind nur in Verbindung mit einem Geheimhaltungsgrad zu verwenden.

16.3. **Kennzeichnungen**

Kennzeichnungen können benutzt werden, um den von einem Dokument abgedeckten Bereich, eine besondere Verteilung gemäß dem Grundsatz „Kenntnis notwendig“ oder (bei Dokumenten, die nicht als Verschlusssache eingestuft sind) den Ablauf eines Sperrvermerks anzugeben.

Eine Kennzeichnung ist keine Einstufung und darf nicht anstelle einer solchen verwendet werden.

Die Kennzeichnung „ESVP“ ist auf Dokumenten und Kopien von Dokumenten anzubringen, die die Sicherheit und Verteidigung der Union oder eines oder mehrerer ihrer Mitgliedstaaten, oder die militärische oder nichtmilitärische Krisenbewältigung betreffen.

16.4. **Anbringung des Hinweises auf den Geheimhaltungsgrad**

Der Hinweis auf den Geheimhaltungsgrad wird wie folgt angebracht:

a) bei Dokumenten, die als „EU — NUR FÜR DEN DIENSTGEBRAUCH“ eingestuft werden, mit mechanischen oder elektronischen Mitteln;

b) bei Dokumenten, die als „EU — VERTRAULICH“ eingestuft werden, mit mechanischen Mitteln, von Hand oder durch Druck auf vorgestempeltem, registriertem Papier;

c) auf Dokumenten, die als „EU — GEHEIM“ oder „EU — STRENG GEHEIM“ eingestuft werden, mit mechanischen Mitteln oder von Hand.

16.5. **Anbringen von Sicherheitskennungen**

Sicherheitskennungen werden unmittelbar unter dem Hinweis auf den Geheimhaltungsgrad angebracht; dabei sind die selben Mittel zu verwenden wie bei der Anbringung des Hinweises auf den Geheimhaltungsgrad.

([1]) Anhang 1 enthält eine vergleichende Übersicht über die von der EU, der NATO, der WEU und den Mitgliedstaaten verwendeten Geheimhaltungsgrade.

17. REGELN FÜR DIE EINSTUFUNG ALS VERSCHLUSSSACHE

17.1. **Allgemeines**

Informationen sind nur dann als Verschlusssachen einzustufen, wenn dies nötig ist. Der Geheimhaltungsgrad ist klar und korrekt anzugeben und nur so lange beizubehalten, wie die Informationen geschützt werden müssen.

Die Verantwortung für die Festlegung des Geheimhaltungsgrades einer Information und für jede anschließende Herabstufung oder Aufhebung liegt allein beim Urheber der Information.

Einstufungen, Herabstufungen oder Aufhebungen des Geheimhaltungsgrades von Verschlusssachen werden von den Beamten und sonstigen Bediensteten der Kommission auf Anweisung ihres Dienststellenleiters oder mit dessen Zustimmung vorgenommen.

Die detaillierten Verfahren für die Behandlung von Verschlusssachen sind so ausgelegt, dass gewährleistet ist, dass die betreffenden Dokumente den ihrem Inhalt entsprechenden Schutz erhalten.

Die Zahl der Personen, die dazu ermächtigt sind, Dokumente des Geheimhaltungsgrades „EU — STRENG GEHEIM“ in Umlauf zu bringen, ist möglichst klein zu halten, und ihre Namen sind in einer Liste zu verzeichnen, die vom Sicherheitsbüro der Kommission geführt wird.

17.2. **Anwendung der Geheimhaltungsgrade**

Bei der Festlegung des Geheimhaltungsgrades eines Dokuments wird das Ausmaß der Schutzbedürftigkeit seines Inhalts entsprechend der Definition in Abschnitt 16 zugrunde gelegt. Es ist wichtig, dass die Einstufung korrekt vorgenommen wird und nur bei wirklichem Bedarf erfolgt. Dies gilt insbesondere für eine Einstufung als „EU — STRENG GEHEIM“.

Der Urheber eines Dokuments, das als Verschlusssache eingestuft werden soll, sollte sich der vorstehend genannten Vorschriften bewusst sein und eine zu hohe oder zu niedrige Einstufung vermeiden.

Anhang 2 enthält einen praktischen Leitfaden für die Einstufung.

Einzelne Seiten, Abschnitte, Teile, Anhänge oder sonstige Anlagen eines Dokuments können eine unterschiedliche Einstufung erforderlich machen und sind entsprechend zu kennzeichnen. Als Geheimhaltungsgrad des Gesamtdokuments gilt der Geheimhaltungsgrad seines am höchsten eingestuften Teils.

Ein Begleitschreiben oder ein Übermittlungsvermerk ist so hoch einzustufen wie die am höchsten eingestufte Anlage. Der Urheber sollte klar angeben, welcher Geheimhaltungsgrad für das Begleitschreiben bzw. den Übermittlungsvermerk gilt, wenn ihm seine Anlagen nicht beigefügt sind.

Für den Zugang der Öffentlichkeit ist weiterhin die Verordnung (EG) Nr. 1049/2001 maßgeblich.

17.3. **Herabstufung und Aufhebung des Geheimhaltungsgrades**

EU-Verschlusssachen dürfen nur mit Genehmigung des Urhebers und erforderlichenfalls nach Erörterung mit den übrigen beteiligten Parteien herabgestuft werden; das Gleiche gilt für die Aufhebung des Geheimhaltungsgrades. Die Herabstufung oder die Aufhebung des Geheimhaltungsgrades ist schriftlich zu bestätigen. Dem Urheber obliegt es, die Empfänger des Dokuments über die Änderung der Einstufung zu informieren, wobei letztere wiederum die weiteren Empfänger, denen sie das Original oder eine Kopie des Dokuments zugeleitet haben, davon zu unterrichten haben.

Soweit möglich gibt der Urheber auf dem als Verschlusssache eingestuften Dokument den Zeitpunkt, eine Frist oder ein Ereignis an, ab dem die in dem Dokument enthaltenen Informationen herabgestuft werden können oder deren Geheimhaltungsgrad aufgehoben werden kann. Andernfalls überprüft er die Dokumente spätestens alle fünf Jahre, um sicherzustellen, dass die ursprüngliche Einstufung nach wie vor erforderlich ist.

18. MATERIELLER GEHEIMSCHUTZ

18.1. **Allgemeines**

Mit den Maßnahmen des materiellen Geheimschutzes soll in erster Linie verhindert werden, dass Unbefugte Zugang zu EU-Verschlusssachen und/oder -material erhalten, dass Diebstahl und eine Beschädigung von Material und anderem Eigentum eintritt und dass Beamte oder sonstige Bedienstete sowie Besucher bedrängt oder auf eine andere Weise unter Druck gesetzt werden.

18.2. **Sicherheitsanforderungen**

Alle Gebäude, Bereiche, Büros, Räume, Kommunikations- und Informationssysteme usw., in denen als EU-Verschlusssache eingestufte Informationen und Material aufbewahrt werden und/oder in denen damit gearbeitet wird, sind durch geeignete Maßnahmen des materiellen Geheimschutzes zu sichern.

Bei der Festlegung des erforderlichen materiellen Geheimschutzniveaus ist allen relevanten Faktoren Rechnung zu tragen, wie beispielsweise

a) der Einstufung der Informationen und/oder des Materials;

b) der Menge und der Form (z. B. Papier, EDV-Datenträger) der verwahrten Informationen;

c) der örtlichen Einschätzung der geheimdienstlichen Bedrohung, die gegen die EU, die Mitgliedstaaten und/oder andere Institutionen oder Dritte gerichtet ist, die EU-Verschlusssachen verwahren, sowie der Bedrohung insbesondere durch Sabotage, Terrorismus und andere subversive und/oder kriminelle Handlungen.

Die Maßnahmen des materiellen Geheimschutzes zielen darauf ab,

a) das heimliche oder gewaltsame Eindringen unbefugter Personen von außen zu verhindern;

b) von Tätigkeiten illoyaler Angehöriger des Personals (Spionage von innen) abzuschrecken beziehungsweise diese zu verhindern und aufzudecken;

c) zu verhindern, dass Personen, die die betreffenden Kenntnisse nicht benötigen, Zugang zu EU-Verschlusssachen haben.

18.3. **Maßnahmen des materiellen Geheimschutzes**

18.3.1. *Sicherheitsbereiche*

Die Bereiche, in denen mit als „EU — VERTRAULICH“ oder höher eingestuften Verschlusssachen gearbeitet wird oder in denen diese aufbewahrt werden, sind so zu gestalten und auszustatten, dass sie einer der nachstehenden Kategorien entsprechen:

a) Sicherheitsbereich der Kategorie I: Bereich, in dem mit als „EU — VERTRAULICH“ oder höher eingestuften Verschlusssachen gearbeitet wird oder in dem diese aufbewahrt werden, wobei das Betreten des Bereichs für alle praktischen Zwecke den Zugang zu den Verschlusssachen ermöglicht. Ein derartiger Bereich erfordert

   i) einen klar abgegrenzten und geschützten Raum mit vollständiger Ein- und Ausgangskontrolle;

   ii) ein Zutrittskontrollsystem, mit dem dafür gesorgt wird, dass nur die gehörig überprüften und eigens ermächtigten Personen den Bereich betreten können;

   iii) eine genaue Festlegung der Einstufung der Verschlusssachen, die in der Regel in dem Bereich verwahrt werden, d. h. der Informationen, die durch das Betreten des Bereichs zugänglich werden.

b) Sicherheitsbereich der Kategorie II: Bereich, in dem mit als „EU — VERTRAULICH“ oder höher eingestuften Verschlusssachen gearbeitet wird oder in dem diese aufbewahrt werden, wobei durch interne Kontrollen ein Schutz vor dem Zugang Unbefugter ermöglicht wird, beispielsweise Gebäude mit Büros, in denen regelmäßig mit als „EU-VERTRAULICH“ eingestuften Verschlusssachen gearbeitet wird und in denen diese aufbewahrt werden. Ein derartiger Bereich erfordert

   i) einen klar abgegrenzten und geschützten Raum mit vollständiger Ein- und Ausgangskontrolle;

   ii) ein Zutrittskontrollsystem, mit dem dafür gesorgt wird, dass nur die gehörig überprüften und eigens ermächtigten Personen den Bereich unbegleitet betreten können. Bei allen anderen Personen ist eine Begleitung oder eine gleichwertige Kontrolle sicherzustellen, damit der Zugang Unbefugter zu EU-Verschlusssachen sowie ein unkontrolliertes Betreten von Bereichen, die technischen Sicherheitskontrollen unterliegen, verhindert werden.

   Die Bereiche, die nicht rund um die Uhr von Dienst tuendem Personal besetzt sind, sind unmittelbar nach den üblichen Arbeitszeiten zu inspizieren, um sicherzustellen, dass die EU-Verschlusssachen ordnungsgemäß gesichert sind.

18.3.2. *Verwaltungsbereich*

Um die Sicherheitsbereiche der Kategorien I und II herum oder im Zugangsbereich zu ihnen kann ein Verwaltungsbereich mit geringerem Sicherheitsgrad vorgesehen werden. Ein derartiger Bereich erfordert einen deutlich abgegrenzten Raum, der die Kontrolle von Personal und Fahrzeugen ermöglicht. In den Verwaltungsbereichen darf nur mit Verschlusssachen gearbeitet werden, die als „EU — NUR FÜR DEN DIENSTGEBRAUCH“ eingestuft sind, und es dürfen auch nur diese Verschlusssachen dort aufbewahrt werden.

18.3.3. *Eingangs- und Ausgangskontrollen*

Das Betreten und Verlassen der Sicherheitsbereiche der Kategorien I und II wird mittels eines Berechtigungsausweises oder eines Systems zur persönlichen Identifizierung des ständigen Personals kontrolliert. Ferner wird ein Kontrollsystem für Besucher eingerichtet, damit der Zugang Unbefugter zu EU-Verschlusssachen verhindert werden kann. Eine Regelung mit Berechtigungsausweisen kann durch eine automatisierte Erkennung unterstützt werden, die als Ergänzung zum Einsatz des Personals des Sicherheitsdienstes zu verstehen ist, diesen aber nicht vollständig ersetzen kann. Eine Änderung in der Einschätzung der Bedrohungslage kann eine Verschärfung der Ein- und Ausgangskontrollmaßnahmen zur Folge haben, beispielsweise anlässlich des Besuchs hochrangiger Persönlichkeiten.

18.3.4. *Kontrollgänge*

In Sicherheitsbereichen der Kategorien I und II sind außerhalb der normalen Arbeitszeiten Kontrollgänge durchzuführen, um das Eigentum der EU vor Kenntnisnahme durch Unbefugte, Beschädigung oder Verluste zu schützen. Die Häufigkeit der Kontrollgänge richtet sich nach den örtlichen Gegebenheiten, sie sollten aber in der Regel alle zwei Stunden stattfinden.

18.3.5. *Sicherheitsbehältnisse und Tresorräume*

Zur Aufbewahrung von EU-Verschlusssachen werden drei Arten von Behältnissen verwendet:

— Typ A: Behältnisse, die zur Aufbewahrung von als „EU — STRENG GEHEIM“ eingestuften Verschlusssachen in Sicherheitsbereichen der Kategorie I oder II auf nationaler Ebene zugelassen sind;

— Typ B: Behältnisse, die zur Aufbewahrung von als „EU — GEHEIM“ und „EU — VERTRAULICH“ eingestuften Verschlusssachen in Sicherheitsbereichen der Kategorie I oder II auf nationaler Ebene zugelassen sind;

— Typ C: Büromöbel, die ausschließlich für die Aufbewahrung von als „EU — NUR FÜR DEN DIENSTGEBRAUCH“ eingestuften Verschlusssachen geeignet sind.

In den in einem Sicherheitsbereich der Kategorie I oder II eingebauten Tresorräumen und in allen Sicherheitsbereichen der Kategorie I, wo als „EU — VERTRAULICH“ und höher eingestufte Verschlusssachen in offenen Regalen aufbewahrt werden oder auf Karten, Plänen usw. sichtbar sind, werden Wände, Böden und Decken, Türen einschließlich der Schlösser von der Akkreditierungsstelle für Sicherheit geprüft, um festzustellen, dass sie einen Schutz bieten, der dem Typ des Sicherheitsbehältnisses entspricht, der für die Aufbewahrung von Verschlusssachen desselben Geheimhaltungsgrades zugelassen ist.

18.3.6. *Schlösser*

Die Schlösser der Sicherheitsbehältnisse und Tresorräume, in denen EU-Verschlusssachen aufbewahrt werden, müssen folgende Anforderungen erfüllen:

— Gruppe A: sie müssen auf nationaler Ebene für Behältnisse vom Typ A zugelassen sein;

— Gruppe B: sie müssen auf nationaler Ebene für Behältnisse vom Typ B zugelassen sein;

— Gruppe C: sie müssen ausschließlich für Büromöbel vom Typ C geeignet sein.

18.3.7. *Kontrolle der Schlüssel und Kombinationen*

Die Schlüssel von Sicherheitsbehältnissen dürfen nicht aus den Gebäuden der Kommission entfernt werden. Die Kombinationen für Sicherheitsbehältnisse sind von den Personen, die sie kennen müssen, auswendig zu lernen. Damit sie im Notfall benutzt werden können, ist der Lokale Sicherheitsbeauftragte der betreffenden Kommissionsdienststelle für die Aufbewahrung der Ersatzschlüssel und die schriftliche Registrierung aller Kombinationen verantwortlich; letztere sind einzeln in versiegelten, undurchsichtigen Umschlägen aufzubewahren. Die Arbeitsschlüssel, die Ersatzschlüssel und die Kombinationen sind in gesonderten Sicherheitsbehältnissen aufzubewahren. Für diese Schlüssel und Kombinationen ist kein geringerer Sicherheitsschutz vorzusehen als für das Material, zu dem sie den Zugang ermöglichen.

Der Kreis der Personen, die die Kombinationen der Sicherheitsbehältnisse kennen, ist so weitgehend wie möglich zu begrenzen. Die Kombinationen sind zu ändern

a) bei Entgegennahme eines neuen Behälters;

b) bei jedem Benutzerwechsel;

c) bei tatsächlicher oder vermuteter Kenntnisnahme durch Unbefugte;

d) vorzugsweise alle sechs Monate und mindestens alle zwölf Monate.

18.3.8. *Intrusionsmeldeanlagen*

Kommen zum Schutz von EU-Verschlusssachen Alarmanlagen, hauseigene Fernsehsysteme und andere elektrische Vorrichtungen zum Einsatz, so ist eine Notstromversorgung vorzusehen, um bei Ausfall der Hauptstromversorgung den ununterbrochenen Betrieb der Anlagen sicherzustellen. Ein weiteres grundlegendes Erfordernis ist das Auslösen eines für das Überwachungspersonal bestimmten Alarmsignals oder anderen verlässlichen Signals bei Funktionsstörungen dieser Anlagen oder Manipulationen an ihnen.

18.3.9. *Zugelassene Ausrüstung*

Das Sicherheitsbüro der Kommission unterhält aktualisierte, nach Typ und Modell gegliederte Verzeichnisse der Sicherheitsausrüstung, die es für den unmittelbaren oder mittelbaren Schutz von Verschlusssachen unter verschiedenen genau bezeichneten Voraussetzungen und Bedingungen zugelassen hat. Das Sicherheitsbüro der Kommission unterhält diese Verzeichnisse unter anderem auf der Grundlage der von den nationalen Sicherheitsbehörden mitgeteilten Informationen.

18.3.10. *Materieller Geheimschutz für Kopier- und Faxgeräte*

Für Kopier- und Faxgeräte ist im erforderlichen Maß durch Maßnahmen des materiellen Geheimschutzes dafür zu sorgen, dass sie lediglich von befugten Personen verwendet werden können und dass alle Verschlusssachen einer ordnungsgemäßen Überwachung unterliegen.

18.4. **SICHT- UND ABHÖRSCHUTZ**

18.4.1. *Sichtschutz*

Es sind alle geeigneten Maßnahmen zu treffen, damit bei Tag und bei Nacht gewährleistet ist, dass EU-Verschlusssachen nicht — auch nicht versehentlich — von Unbefugten eingesehen werden können.

18.4.2. *Abhörschutz*

Die Büroräume oder Bereiche, in denen regelmäßig über als „EU — GEHEIM“ und höher eingestufte Verschlusssachen gesprochen wird, sind bei entsprechendem Risiko gegen Ab- und Mithören zu schützen. Für die Einschätzung des Risikos ist das Sicherheitsbüro der Kommission zuständig, das erforderlichenfalls zuvor die betreffenden nationalen Sicherheitsbehörden zurate zieht.

18.4.3. *Einbringen elektronischer Geräte und von Aufzeichnungsgeräten*

Es ist nicht gestattet, Mobiltelefone, PCs, Tonaufnahmegeräte, Kameras und andere elektronische Geräte oder Aufzeichnungsgeräte ohne vorherige Genehmigung durch den zuständigen Lokalen Sicherheitsbeauftragten in Sicherheitsbereiche oder Hochsicherheitszonen zu bringen.

Zur Festlegung der Schutzmaßnahmen für mithörgefährdete Bereiche (beispielsweise Schalldämmung von Wänden, Türen, Böden und Decken, Lautstärkemessung) in Bezug auf Mit- bzw. Abhörgefahr bzw. abhörgefährdete Bereiche (beispielsweise Suche nach Mikrofonen), kann das Sicherheitsbüro der Kommission die nationalen Sicherheitsbehörden um Unterstützung durch Sachverständige ersuchen.

Ebenso können für die technische Sicherheit zuständige Sachverständige der nationalen Sicherheitsbehörden erforderlichenfalls die Telekommunikationseinrichtungen und die elektrischen oder elektronischen Büromaschinen aller Art, die in den Sitzungen des Geheimhaltungsgrades „EU — GEHEIM“ und höher verwendet werden, auf Ersuchen des Leiters des Sicherheitsbüros der Kommission überprüfen.

18.5. **HOCHSICHERHEITSZONEN**

Bestimmte Bereiche können als Hochsicherheitszonen ausgewiesen werden. Hier findet eine besondere Zutrittskontrolle statt. Diese Zonen bleiben nach einem zugelassenen Verfahren verschlossen, wenn sie nicht besetzt sind, und alle Schlüssel sind als Sicherheitsschlüssel zu behandeln. Diese Zonen unterliegen regelmäßigen Objektschutzkontrollen, die auch durchgeführt werden, wenn festgestellt oder vermutet wird, dass die Zonen ohne Genehmigung betreten wurden.

Es wird eine detaillierte Bestandsaufnahme der Geräte und Möbel vorgenommen, um deren Platzveränderungen zu überwachen. Kein Möbelstück oder Gerät wird in eine dieser Zonen verbracht, bevor es nicht durch Sicherheitspersonal, das für das Aufspüren von Abhörvorrichtungen besonders geschult ist, sorgfältig kontrolliert worden ist. In der Regel dürfen in Hochsicherheitszonen keine Telekommunikationsverbindungen ohne vorherige Genehmigung durch die zuständige Stelle installiert werden.

19. ALLGEMEINE BESTIMMUNGEN ZU DEM GRUNDSATZ „KENNTNIS NOTWENDIG“ UND DER EU-SICHERHEITS-ÜBERPRÜFUNG VON PERSONEN

19.1. **Allgemeines**

Der Zugang zu EU-Verschlusssachen wird nur Personen gestattet, die Kenntnis von ihnen haben müssen, um die ihnen übertragenen Aufgaben oder Aufträge erfüllen zu können. Der Zugang zu als „EU — STRENG GEHEIM“, „EU — GEHEIM“ und „EU — VERTRAULICH“ eingestuften Verschlusssachen wird nur Personen gestattet, die der entsprechenden Sicherheitsüberprüfung unterzogen worden sind.

Für die Entscheidung darüber, wer Kenntnis haben muss, ist die Dienststelle zuständig, in der die betreffende Person eingesetzt werden soll.

Die Sicherheitsüberprüfung ist von der betreffenden Dienststelle zu beantragen.

Am Ende des Verfahrens wird eine „EU-Sicherheitsunbedenklichkeitsbescheinigung für Personen“ ausgestellt, in dem der Geheimhaltungsgrad der Verschlusssachen, zu denen die überprüfte Person Zugang erhalten kann, und das Ende der Gültigkeitsdauer der Bescheinigung angegeben werden.

Eine Sicherheitsunbedenklichkeitsbescheinigung für einen bestimmten Geheimhaltungsgrad kann den Inhaber zum Zugang zu Informationen eines niedrigeren Geheimhaltungsgrades berechtigen.

Andere Personen als Beamte oder sonstige Bedienstete, z. B. externe Vertragspartner, Sachverständige oder Berater, mit denen möglicherweise EU-Verschlusssachen erörtert werden müssen oder die möglicherweise Einblick in solche Verschlusssachen erhalten müssen, sind einer EU-Sicherheitsüberprüfung für EU-Verschlusssachen zu unterziehen und über ihre Sicherheitsverantwortung zu belehren.

Für den Zugang der Öffentlichkeit ist weiterhin die Verordnung (EG) Nr. 1049/2001 maßgeblich.

19.2. **Besondere Vorschriften für den Zugang zu als „EU — STRENG GEHEIM“ eingestuften Verschlusssachen**

Alle Personen, die Zugang zu als „EU — STRENG GEHEIM“ eingestuften Verschlusssachen benötigen, müssen zunächst einer Sicherheitsüberprüfung in Bezug auf den Zugang zu den betreffenden Verschlusssachen unterzogen werden.

Alle Personen, die Zugang zu als „EU — STRENG GEHEIM“ eingestuften Verschlusssachen benötigen, sind von dem für Sicherheitsfragen zuständigen Mitglied der Kommission zu benennen, und ihre Namen sind in das einschlägige „EU — STRENG GEHEIM“-Register einzutragen. Dieses Register wird vom Sicherheitsbüro der Kommission angelegt und geführt.

Bevor diesen Personen der Zugang zu als „EU — STRENG GEHEIM“ eingestuften Verschlusssachen gewährt wird, müssen sie eine Bestätigung unterzeichnen, dass sie über die Sicherheitsverfahren der Kommission belehrt worden und sich ihrer besonderen Verantwortung für den Schutz von als „EU — STRENG GEHEIM“ eingestuften Verschlusssachen und der Folgen vollständig bewusst sind, die die EU-Vorschriften und die einzelstaatlichen Rechts- und Verwaltungsvorschriften für den Fall vorsehen, dass Verschlusssachen durch Vorsatz oder durch Fahrlässigkeit in die Hände Unbefugter gelangen.

Wenn Personen in Sitzungen usw. Zugang zu als „EU — STRENG GEHEIM“ eingestuften Verschlusssachen erhalten, so teilt der Kontrollbeauftragte der Dienststelle oder des Gremiums, bei der bzw. dem die Betreffenden beschäftigt sind, der die Sitzung veranstaltenden Stelle mit, dass die betreffenden Personen die entsprechende Ermächtigung besitzen.

Die Namen aller Personen, die nicht mehr für Aufgaben eingesetzt werden, bei denen sie über den Zugang zu als „EU — STRENG GEHEIM“ eingestuften Verschlusssachen verfügen müssen, werden aus dem „EU — STRENG GEHEIM“-Verzeichnis gestrichen. Ferner werden alle betreffenden Personen erneut auf ihre besondere Verantwortung für den Schutz von als „EU — STRENG GEHEIM“ eingestuften Verschlusssachen belehrt. Sie haben ferner eine Erklärung zu unterzeichnen, wonach sie ihre Kenntnisse über als „EU — STRENG GEHEIM“ eingestufte Verschlusssachen weder verwenden noch weitergeben werden.

19.3. **Besondere Vorschriften für den Zugang zu als „EU — GEHEIM“ und „EU — VERTRAULICH“ eingestuften Verschlusssachen**

Alle Personen, die Zugang zu als „EU — GEHEIM“ oder „EU — VERTRAULICH“ eingestuften Verschlusssachen benötigen, müssen zunächst einer Sicherheitsüberprüfung in Bezug auf den geeigneten Geheimhaltungsgrad unterzogen werden.

Alle Personen, die Zugang zu als „EU — GEHEIM“ oder „EU — VERTRAULICH“ eingestuften Verschlusssachen benötigen, müssen über die entsprechenden Sicherheitsvorschriftenregelungen unterrichtet werden und sich der Folgen fahrlässigen Handelns bewusst sein.

Wenn Personen in Sitzungen Zugang zu als „EU — GEHEIM“ oder „EU — VERTRAULICH“ eingestuften Verschlusssachen erhalten, so teilt der Kontrollbeauftragte der Dienststelle oder des Gremiums, bei der bzw. dem die Betreffenden beschäftigt sind, der die Sitzung veranstaltenden Stelle mit, dass die betreffenden Personen die entsprechende Ermächtigung besitzen.

19.4. **Besondere Vorschriften für den Zugang zu als „EU — NUR FÜR DEN DIENSTGEBRAUCH“ eingestuften Verschlusssachen**

Alle Personen, die Zugang zu als „EU — NUR FÜR DEN DIENSTGEBRAUCH“ eingestuften Verschlusssachen haben, werden auf diese Sicherheitsvorschriften und die Folgen fahrlässigen Handelns aufmerksam gemacht.

19.5. **WEITERGABE**

Wird ein Angehöriger des Personals von einem Dienstposten, der mit der Arbeit mit EU-Verschlusssachen verbunden ist, wegversetzt, so achtet die Registratur darauf, dass die betreffenden Verschlusssachen ordnungsgemäß von dem ausscheidenden an den eintretenden Beamten weitergegeben werden.

Wird ein Angehöriger des Personals auf einen anderen Dienstposten versetzt, der mit der Arbeit mit EU-Verschlusssachen verbunden ist, wird er von dem Lokalen Sicherheitsbeauftragten entsprechend belehrt.

19.6. **BESONDERE ANWEISUNGEN**

Personen, die mit EU-Verschlusssachen arbeiten müssen, sollten bei Aufnahme ihrer Tätigkeit und danach in regelmäßigen Abständen auf Folgendes hingewiesen werden:

a) die mögliche Gefährdung der Sicherheit durch indiskrete Gespräche;

b) die in den Beziehungen zur Presse und zu Vertretern besonderer Interessengruppen zu treffenden Vorsichtsmaßnahmen;

c) die Bedrohung für EU-Verschlusssachen und -tätigkeiten durch die gegen die EU und ihre Mitgliedstaaten gerichteten nachrichtendienstlichen Tätigkeiten;

d) die Verpflichtung, die zuständigen Sicherheitsbehörden unverzüglich über jeden Annäherungsversuch oder jede Handlungsweise, bei denen ein Verdacht auf Spionage entsteht, sowie über alle ungewöhnlichen Umstände in Bezug auf die Sicherheit zu unterrichten.

Alle Personen, die gewöhnlich häufige Kontakte mit Vertretern von Ländern haben, deren Nachrichtendienste in Bezug auf EU-Verschlusssachen und Tätigkeiten gegen die EU und ihre Mitgliedstaaten arbeiten, sind über die Techniken zu belehren, von denen bekannt ist, dass sich die einzelnen Nachrichtendienste ihrer bedienen.

Es bestehen keine Sicherheitsvorschriften der Kommission für private Reisen der zum Zugang zu EU-Verschlusssachen ermächtigten Personen nach irgendeinem Zielland. Das Sicherheitsbüro der Kommission wird jedoch die Beamten und sonstigen Bediensteten, für die es zuständig ist, über Reiseregelungen unterrichten, denen sie möglicherweise unterliegen.

20. VERFAHREN FÜR DIE SICHERHEITSÜBERPRÜFUNG VON BEAMTEN UND SONSTIGEN BEDIENSTETEN DER KOMMISSION

a) Nur Beamte und sonstige Bedienstete der Kommission oder andere bei der Kommission tätige Personen, die aufgrund ihrer Aufgabenbereiche und dienstlicher Erfordernisse von den von der Kommission verwahrten Verschlusssachen Kenntnis nehmen müssen, oder sie zu bearbeiten haben, erhalten Zugang zu diesen Verschlusssachen.

b) Um Zugang zu den als „EU — STRENG GEHEIM“, „EU — GEHEIM“ und „EU — VERTRAULICH“ eingestuften Verschlusssachen zu erhalten, müssen die in Buchstabe a) genannten Personen hierzu nach dem Verfahren der Buchstaben c) und d) ermächtigt worden sein.

c) Die Ermächtigung wird nur den Personen erteilt, die durch die zuständigen nationalen Behörden der Mitgliedstaaten (nationale Sicherheitsbehörden) einer Sicherheitsüberprüfung nach dem in den Buchstaben i) bis n) beschriebenen Verfahren unterzogen worden sind.

d) Die Erteilung der Ermächtigungen gemäß den Buchstaben a), b) und c) obliegt dem Leiter des Sicherheitsbüros der Kommission.

e) Der Leiter des Sicherheitsbüros erteilt die Ermächtigung nach Einholung der Stellungnahme der zuständigen nationalen Behörden der Mitgliedstaaten auf der Grundlage der gemäß den Buchstaben i) bis n) durchgeführten Sicherheitsüberprüfung.

f) Das Sicherheitsbüro der Kommission führt ein ständig aktualisiertes Verzeichnis aller sensitiven Posten, die ihm von den betreffenden Kommissionsdienststellen gemeldet werden und von allen Personen, die eine (befristete) Ermächtigung erhalten haben.

g) Die Ermächtigung, die eine Geltungsdauer von fünf Jahren hat, erlischt, wenn die betreffende Person die Aufgaben, die die Erteilung der Ermächtigung gerechtfertigt haben, nicht mehr wahrnimmt. Sie kann nach dem Verfahren des Buchstabens e) erneuert werden.

h) Die Ermächtigung wird vom Leiter des Sicherheitsbüros der Kommission entzogen, wenn seiner Ansicht nach hierzu Grund besteht. Die Entzugsverfügung wird der betreffenden Person, die beantragen kann, vom Leiter des Sicherheitsbüros der Kommission gehört zu werden, sowie der zuständigen nationalen Behörde mitgeteilt.

i) Die Sicherheitsüberprüfung wird unter Mitwirkung der betreffenden Person auf Ersuchen des Leiters des Sicherheitsbüros der Kommission von der zuständigen nationalen Behörde desjenigen Mitgliedstaats vorgenommen, dessen Staatsangehörigkeit die zu ermächtigende Person besitzt. Besitzt die betreffende Person nicht die Staatsangehörigkeit eines der Mitgliedstaaten der EU, so ersucht der Leiter des Sicherheitsbüros der Kommission den EU-Mitgliedstaat, in dem die Person ihren Wohnsitz oder gewöhnlichen Aufenthalt hat, um eine Sicherheitsüberprüfung.

j) Die betreffende Person hat im Hinblick auf die Sicherheitsüberprüfung einen Fragebogen auszufüllen.

k) Der Leiter des Sicherheitsbüros der Kommission benennt in seinem Ersuchen die Art und den Geheimhaltungsgrad der Informationen, zu denen die betreffende Person Zugang erhalten soll, damit die zuständigen nationalen Behörden das Sicherheitsüberprüfungsverfahren durchführen und zu der der betreffenden Person zu erteilenden Ermächtigungsstufe Stellung nehmen können.

l) Für den gesamten Ablauf und die Ergebnisse des Sicherheitsüberprüfungsverfahrens gelten die einschlägigen Vorschriften und Regelungen des betreffenden Mitgliedstaats, einschließlich der Vorschriften und Regelungen für etwaige Rechtsbehelfe.

m) Bei befürwortender Stellungnahme der zuständigen nationalen Behörden der Mitgliedstaaten kann der Leiter des Sicherheitsbüros der betreffenden Person die Ermächtigung erteilen.

n) Bei ablehnender Stellungnahme der zuständigen nationalen Behörden wird diese Ablehnung der betreffenden Person mitgeteilt, die beantragen kann, von dem Leiter des Sicherheitsbüros der Kommission gehört zu werden. Der Leiter des Sicherheitsbüros der Kommission kann, wenn er dies für erforderlich hält, bei den zuständigen nationalen Behörden um weitere Auskünfte, die diese zu geben vermögen, nachsuchen. Bei Bestätigung der ablehnenden Stellungnahme kann die Ermächtigung nicht erteilt werden.

o) Jede ermächtigte Person im Sinne der Buchstaben d) und e) erhält zum Zeitpunkt der Ermächtigung und danach in regelmäßigen Abständen die gebotenen Anweisungen zum Schutz der Verschlusssachen und zu den Verfahren zur Sicherstellung dieses Schutzes. Sie unterzeichnet eine Erklärung, mit der sie den Erhalt dieser Anweisungen bestätigt und sich zu ihrer Einhaltung verpflichtet.

p) Der Leiter des Sicherheitsbüros der Kommission ergreift alle erforderlichen Maßnahmen für die Durchführung dieses Abschnitts, insbesondere hinsichtlich der Vorschriften für den Zugang zum Verzeichnis der ermächtigten Personen.

q) Ausnahmsweise kann der Leiter des Sicherheitsbüros der Kommission aufgrund dienstlicher Erfordernisse, nachdem er die zuständigen nationalen Behörden hiervon im Voraus unterrichtet hat und diese binnen einem Monat nicht dazu Stellung genommen haben, auch eine einstweilige Ermächtigung für höchstens sechs Monate erteilen, bis ihm die Ergebnisse der Sicherheitsüberprüfung nach Buchstabe i) vorliegen.

r) Die so erteilten vorläufigen und einstweiligen Ermächtigungen berechtigen nicht zum Zugang zu als „EU — STRENG GEHEIM“ eingestuften Verschlusssachen; der Zugang wird auf die Beamten beschränkt, bei denen tatsächlich eine Sicherheitsüberprüfung gemäß Buchstabe i) mit befürwortender Stellungnahme abgeschlossen worden ist. Bis die Ergebnisse der Sicherheitsüberprüfung vorliegen, können die Beamten, die die Ermächtigungsstufe „EU — STRENG GEHEIM“ erhalten sollen, vorläufig und befristet zum Zugang zu als „EU — GEHEIM“ oder niedriger eingestuften Verschlusssachen ermächtigt werden.

21. HERSTELLUNG, VERTEILUNG UND ÜBERMITTLUNG VON EU-VERSCHLUSSSACHEN, SICHERHEIT DER KURIERE, ZUSÄTZLICHE KOPIEN ODER ÜBERSETZUNGEN SOWIE AUSZÜGE

21.1. **Herstellung**

1. Die EU-Geheimhaltungsgrade sind in der in Abschnitt 16 angegebenen Weise im Falle von als „EU — VERTRAULICH“ oder höher eingestuften Verschlusssachen oben und unten in der Mitte jeder Seite anzubringen, wobei jede Seite zu nummerieren ist. Auf jeder EU-Verschlusssache sind ein Aktenzeichen und ein Datum anzugeben. Im Falle von Dokumenten der Geheimhaltungsgrade „EU — STRENG GEHEIM“ und „EU — GEHEIM“ muss das Aktenzeichen auf jeder Seite erscheinen. Werden die Dokumente in mehreren Ausfertigungen verteilt, so erhält jede Ausfertigung eine eigene Nummer, die auf der ersten Seite zusammen mit der Gesamtzahl der Seiten anzugeben ist. Alle Anhänge und Anlagen sind auf der ersten Seite von Dokumenten aufzulisten, die als „EU — VERTRAULICH“ oder höher eingestuft werden.

2. Dokumente, die als „EU — VERTRAULICH“ oder höher eingestuft werden, dürfen nur von Personen maschinegeschrieben, übersetzt, archiviert, fotokopiert und auf Magnetband oder Mikrofiche gespeichert werden, die eine zumindest dem Geheimhaltungsgrad des betreffenden Dokuments entsprechende Zugangsermächtigung zu EU-Verschlusssachen haben.

3. Abschnitt 25 enthält die Vorschriften für die Erstellung von Verschlusssachen mit Hilfe eines Computers.

21.2. **Verteilung**

1. EU-Verschlusssachen dürfen nur an Personen verteilt werden, für die deren Kenntnis nötig ist und die in entsprechender Weise sicherheitsüberprüft worden sind. Der Urheber bestimmt die Empfänger der erstmaligen Verteilung.

2. Dokumente des Geheimhaltungsgrades „EU — STRENG GEHEIM" werden über Registraturen verteilt, die den Vermerk „EU — STRENG GEHEIM" tragen (siehe Abschnitt 22.2). Im Falle von Mitteilungen, die als „EU — STRENG GEHEIM" eingestuft sind, kann die zuständige Registratur dem Leiter des Kommunikationszentrums gestatten, die in der Liste der Empfänger angegebene Anzahl von Ausfertigungen zu erstellen.

3. Als „EU — GEHEIM" oder niedriger eingestufte Dokumente können vom Erstempfänger an weitere Empfänger, für die deren Kenntnis nötig ist, weitergegeben werden. Die Stellen, von denen die Verschlusssachen stammen, können allerdings von ihnen gewünschte Einschränkungen bei der Verteilung mitteilen. In diesem Fall dürfen die Empfänger die Dokumente nur mit der Genehmigung der Stellen, von denen sie stammen, weitergeben.

4. Ein- und Ausgang jedes als „EU — VERTRAULICH" oder höher eingestuften Dokuments sind in der jeweiligen Generaldirektion bzw. dem jeweiligen Dienst von der lokalen Registratur für EU-Verschlusssachen zu erfassen. Die Angaben, die hierbei zu erfassen sind (Aktenzeichen, Datum und gegebenenfalls Nummer der Ausfertigung) müssen eine Identifizierung des Dokuments ermöglichen und sind in einem Dienstbuch oder in einem besonders geschützten Computermedium festzuhalten (siehe Abschnitt 22.1).

21.3. **Übermittlung von EU-Verschlusssachen**

21.3.1. *Vorkehrungen für den Versand, Empfangsbestätigung*

1. Als „EU — VERTRAULICH" oder höher eingestufte Dokumente sind in einem doppelten, widerstandsfähigen und undurchsichtigen Umschlag zu übermitteln. Auf dem inneren Umschlag sind der entsprechende EU-Geheimhaltungsgrad sowie möglichst die vollständige Amtsbezeichnung und Anschrift des Empfängers anzugeben.

2. Nur der Registraturkontrollbeamte (siehe Abschnitt 22.1) oder sein Stellvertreter darf den inneren Umschlag öffnen und den Empfang der übermittelten Verschlusssachen bestätigen, es sei denn, der Umschlag ist ausdrücklich an einen bestimmten Empfänger gerichtet. In diesem Fall vermerkt die zuständige Registratur (siehe Abschnitt 22.1) den Eingang des Umschlags und nur der genannte Empfänger darf den inneren Umschlag öffnen und den Empfang der darin enthaltenen Verschlusssachen bestätigen.

3. In dem inneren Umschlag ist eine Empfangsbestätigung beizulegen. In dieser Bestätigung, die nicht als Verschlusssache eingestuft wird, sind Aktenzeichen, Datum und die Nummer der Ausfertigung der Verschlusssache, niemals jedoch deren Betreff, anzugeben.

4. Der innere Umschlag wird in einen Außenumschlag gelegt, der für Empfangszwecke eine Versandnummer erhält. Der Geheimhaltungsgrad darf unter keinen Umständen auf dem Außenumschlag erscheinen.

5. Bei als „EU — VERTRAULICH" oder höher eingestuften Dokumenten ist Kurieren und Boten eine Empfangsbestätigung auszustellen, auf der die Versandnummern der übermittelten Versandstücke angegeben sind.

21.3.2. *Übermittlung innerhalb eines Gebäudes oder Gebäudekomplexes*

Innerhalb eines bestimmten Gebäudes oder Gebäudekomplexes dürfen als Verschlusssachen eingestufte Dokumente in einem versiegelten Umschlag, der nur den Namen des Empfängers trägt, befördert werden, sofern die Beförderung durch eine für den betreffenden Geheimhaltungsgrad ermächtigte Person erfolgt.

21.3.3. *Übermittlung innerhalb ein und desselben Landes*

1. Innerhalb ein und desselben Landes sollten Dokumente mit der Einstufung „EU — STRENG GEHEIM" nur unter Zuhilfenahme offizieller Kurierdienste oder durch Personen übermittelt werden, die eine Zugangsermächtigung zu als „EU — STRENG GEHEIM" eingestuften Verschlusssachen haben.

2. Wird zur Übermittlung eines als „EU — STRENG GEHEIM" eingestuften Dokuments an einen Empfänger außerhalb desselben Gebäudes oder Gebäudekomplexes ein Kurierdienst verwendet, so sind die Bestimmungen über den Versand und die Empfangsbestätigung in diesem Kapitel einzuhalten. Die Zustelldienste sind personell so auszustatten, dass gewährleistet ist, dass sich Versandstücke mit als EU — STRENG GEHEIM eingestuften Dokumenten jederzeit unter der direkten Aufsicht eines verantwortlichen Beamten befinden.

3. In Ausnahmefällen können Beamte, die nicht Boten sind, als „EU — STRENG GEHEIM“ eingestufte Dokumente außerhalb des Gebäudes oder Gebäudekomplexes zur Benutzung vor Ort anlässlich von Sitzungen oder Erörterungen mitnehmen, vorausgesetzt, dass

   a) der betreffende Beamte zum Zugang zu diesen als „EU — STRENG GEHEIM“ eingestuften Dokumenten ermächtigt ist;

   b) die Form der Beförderung den Vorschriften für die Übermittlung von Dokumenten des Geheimhaltungsgrades „EU — STRENG GEHEIM“ entspricht;

   c) der Beamte die Dokumente des Geheimhaltungsgrades „EU — STRENG GEHEIM“ unter keinen Umständen unbeaufsichtigt lässt;

   d) Vorkehrungen getroffen werden, damit die Liste der Dokumente, die mitgenommen werden, in der „EU — STRENG GEHEIM“-Registratur verwahrt, in einem Dienstbuch vermerkt und bei Rückkehr anhand dieses Eintrags kontrolliert wird.

4. Innerhalb ein und desselben Landes dürfen als „EU — GEHEIM“ oder „EU — VERTRAULICH“ eingestufte Dokumente entweder mit der Post, wenn eine derartige Übermittlung nach den einzelstaatlichen Regelungen gestattet ist und mit den einschlägigen Vorschriften in Einklang steht, oder über einen Kurierdienst oder durch Personen übermittelt werden, die zum Zugang zu EU-Verschlusssachen ermächtigt sind.

5. Das Sicherheitsbüro der Kommission arbeitet für das Personal, das EU-Verschlusssachen befördert, auf diesen Vorschriften beruhende Weisungen aus. Es ist vorzusehen, dass Personen, die Verschlusssachen befördern, diese Weisungen lesen und unterzeichnen. In den Weisungen sollte insbesondere deutlich gemacht werden, dass Dokumente unter keinen Umständen

   a) von der sie befördernden Person aus den Händen gegeben werden dürfen, es sei denn, sie seien entsprechend den Bestimmungen in Abschnitt 18 in sicherem Gewahrsam;

   b) in öffentlichen Transportmitteln oder Privatfahrzeugen oder an Orten wie Restaurants oder Hotels unbeaufsichtigt bleiben dürfen. Sie dürfen nicht in Hotelsafes verwahrt werden oder unbeaufsichtigt in Hotelzimmern zurückbleiben;

   c) in der Öffentlichkeit (beispielsweise in Flugzeugen oder Zügen) gelesen werden dürfen.

21.3.4. *Beförderung von einem Staat in einen anderen*

1. Als „EU — VERTRAULICH“ oder höher eingestuftes Material ist durch diplomatische oder militärische Kurierdienste zu befördern.

2. Eine persönliche Beförderung von als „EU — GEHEIM“ oder „EU — VERTRAULICH“ eingestuftem Material kann jedoch gestattet werden, wenn durch die für die Beförderung geltenden Vorschriften gewährleistet wird, dass das Material nicht in die Hände Unbefugter fallen kann.

3. Das für Sicherheitsfragen zuständige Mitglied der Kommission kann eine persönliche Beförderung gestatten, wenn keine diplomatischen oder militärischen Kuriere zur Verfügung stehen oder der Rückgriff auf derartige Kuriere zu einer Verzögerung führen würde, die sich nachteilig auf Maßnahmen der EU auswirken könnte, und wenn das Material vom Empfänger dringend benötigt wird. Das Sicherheitsbüro der Kommission arbeitet Anweisungen über die zwischenstaatliche persönliche Beförderung von Material des Geheimhaltungsgrades „EU — GEHEIM“ oder geringer durch Personen, die keine diplomatischen oder militärischen Kuriere sind, aus. In diesen Anweisungen ist vorzusehen, dass

   a) die Person, die das Material mit sich führt, über die entsprechende Zugangsermächtigung verfügt;

   b) sämtliches auf diese Weise beförderte Material in der zuständigen Dienststelle oder Registratur verzeichnet sein muss;

   c) Versandstücke oder Taschen, die EU-Material enthalten, mit einem Dienstsiegel zu versehen sind, um Zollkontrollen zu vermeiden oder diesen vorzubeugen, sowie mit Etiketten zu ihrer Erkennung und mit Weisungen für den Finder;

   d) die Person, die das Material mit sich führt, einen Kurierausweis und/oder einen Dienstreiseauftrag mitführen muss, die von allen EU-Mitgliedstaaten anerkannt sind und ihn ermächtigen, das betreffende Versandstück in der beschriebenen Weise zu befördern;

   e) bei Überlandreisen die Grenze keines Staates, der nicht EU-Mitglied ist, überschritten oder dieser Staat durchfahren werden darf, es sei denn, dass der Staat, von dem die Beförderung ausgeht, über eine besondere Garantie seitens des erstgenannten Staates verfügt;

   f) die Reiseplanung der Person, die das Material mit sich führt, im Hinblick auf Bestimmungsorte, Fahrtrouten und Beförderungsmittel mit den EU-Vorschriften oder mit einzelstaatlichen Vorschriften, falls diese in dieser Hinsicht strenger sind, in Einklang stehen muss;

g) das Material von der Person, die es mit sich führt, nicht aus der Hand gegeben werden darf, außer wenn es nach den Bestimmungen des Abschnitts 18 über sicheren Gewahrsam verwahrt ist;

h) das Material nicht in öffentlichen Transportmitteln oder Privatfahrzeugen oder an Orten wie Restaurants oder Hotels unbeaufsichtigt bleiben darf. Es darf nicht in Hotelsafes verwahrt werden oder unbeaufsichtigt in Hotelzimmern zurückbleiben;

i) Dokumente, falls solche Bestandteil des beförderten Materials sind, nicht in der Öffentlichkeit (beispielsweise in Flugzeugen, Zügen usw.) gelesen werden dürfen.

4. Die mit der Beförderung der Verschlusssachen beauftragte Person muss eine Geheimschutzunterweisung lesen und unterzeichnen, die mindestens die vorstehenden Weisungen sowie Verfahren enthält, die im Notfall oder für den Fall zu beachten sind, dass das Versandstück mit den Verschlusssachen von Zollbeamten oder Sicherheitsbeamten auf einem Flughafen kontrolliert werden soll.

21.3.5. *Übermittlung von Verschlusssachen mit der Einstufung „EU — NUR FÜR DEN DIENSTGEBRAUCH"*

Für die Beförderung von als „EU — NUR FÜR DEN DIENSTGEBRAUCH" eingestuften Dokumenten werden keine besonderen Vorschriften eingeführt; bei ihrer Beförderung ist allerdings sicherzustellen, dass sie nicht in die Hände Unbefugter geraten können.

21.4. **SICHERHEIT DER KURIERE**

Alle Kuriere und Boten, die mit der Beförderung von Dokumenten beauftragt werden, die als „EU — GEHEIM" und „EU — VERTRAULICH" eingestuft sind, müssen entsprechend sicherheitsermächtigt sein.

21.5. **Elektronische und andere technische Übermittlungswege**

1. Mit den Maßnahmen für die Kommunikationssicherheit soll die sichere Übermittlung von EU-Verschlusssachen gewährleistet werden. Die für die Übermittlung dieser EU-Verschlusssachen geltenden Vorschriften sind in Abschnitt 25 dargelegt.

2. Als „EU — VERTRAULICH" oder „EU — GEHEIM" eingestufte Informationen dürfen nur von zugelassenen Kommunikationszentren und -netzen und/oder Terminals bzw. über entsprechende Systeme übermittelt werden.

21.6. **Zusätzliche Kopien und Übersetzungen von beziehungsweise Auszüge aus EU-Verschlusssachen**

1. Das Kopieren oder die Übersetzung von „EU — STRENG GEHEIM"-Dokumenten kann ausschließlich der Urheber gestatten.

2. Fordern Personen, die nicht über eine „EU — STRENG GEHEIM"-Sicherheitsermächtigung verfügen, Informationen an, die zwar in einem „EU — STRENG GEHEIM"-Dokument enthalten, aber nicht als solche eingestuft sind, so kann der Leiter der „EU — STRENG GEHEIM"-Registratur (siehe Abschnitt 22.2) ermächtigt werden, die notwendige Anzahl von Auszügen aus diesem Dokument auszuhändigen. Gleichzeitig ergreift er die erforderlichen Maßnahmen, um sicherzustellen, dass diese Auszüge einen angemessenen Geheimhaltungsgrad erhalten.

3. Als „EU — GEHEIM" und niedriger eingestufte Dokumente können vom Empfänger unter Einhaltung der Sicherheitsvorschriften und strikter Befolgung des Grundsatzes „Kenntnis notwendig" vervielfältigt und übersetzt werden. Die für das Originaldokument geltenden Sicherheitsvorschriften finden auch auf Vervielfältigungen und/oder Übersetzungen dieses Dokuments Anwendung.

22. REGISTER FÜR EU-VERSCHLUSSSACHEN, BESTANDSAUFNAHME, PRÜFUNG, ARCHIVIERUNG UND VERNICHTUNG VON EU-VERSCHLUSSSACHEN

22.1. **Lokale Registraturen für EU-Verschlusssachen**

1. In jeder Dienststelle der Kommission sind erforderlichenfalls eine oder mehrere Lokale Registraturen für EU-Verschlusssachen für die Registrierung, die Vervielfältigung, den Versand und die Vernichtung von Dokumenten zuständig, die als „EU — GEHEIM" und „EU — VERTRAULICH" eingestuft sind.

2. Dienststellen, die über keine Lokale Registratur für EU-Verschlusssachen verfügen, nehmen die Registratur des Generalsekretariats in Anspruch.

3. Die Lokalen Registraturen für EU-Verschlusssachen erstatten dem Leiter der Dienststelle Bericht, von dem sie ihre Anweisungen erhalten. Geleitet werden die Registraturen von dem Registraturkontrollbeauftragten (RCO).

4. Im Hinblick auf die Anwendung der Bestimmungen für die Handhabung von EU-Verschlusssachen und die Einhaltung der entsprechenden Sicherheitsvorschriften stehen sie unter der Aufsicht des Lokalen Sicherheitsbeauftragten.

5. Den Lokalen Registraturen für EU-Verschlusssachen zugewiesene Beamte haben gemäß Abschnitt 20 Zugang zu EU-Verschlusssachen.

6. Die Lokalen Registraturen für EU-Verschlusssachen nehmen unter der Verantwortung des betreffenden Dienststellenleiters folgende Aufgaben wahr:

   a) Verwaltung der Registrierung, Vervielfältigung, Übersetzung, Weiterleitung, Versendung und Vernichtung der Informationen;

   b) Führung des Verschlusssachenregisters;

   c) regelmäßige Anfragen bei den Urhebern, ob die Einstufung der betreffenden Informationen aufrechtzuerhalten ist;

7. Die Lokalen Registraturen für EU-Verschlusssachen führen ein Register mit folgenden Angaben:

   a) Datum der Erstellung der Verschlusssache,

   b) Geheimhaltungsgrad,

   c) Sperrfrist,

   d) Name und Dienststelle des Urhebers,

   e) der oder die Empfänger mit laufender Nummer,

   f) Gegenstand,

   g) Nummer,

   h) Zahl der verbreiteten Exemplare,

   i) Erstellung von Bestandsverzeichnissen der der Dienststelle unterbreiteten Verschlusssachen,

   j) Register betreffend die Aufhebung des Geheimhaltungsgrades und die Herabstufung von Verschlusssachen.

8. Für die Lokalen Registraturen für EU-Verschlusssachen gelten die allgemeinen Vorschriften des Abschnitts 21, soweit sie nicht durch die spezifischen Vorschriften dieses Abschnitts geändert werden.

22.2. **Die „EU — STRENG GEHEIM"-Registratur**

22.2.1. *Allgemeines*

1. Durch eine „EU — STRENG GEHEIM"-Zentralregistratur wird die Registrierung, Handhabung und Verteilung von „EU — STRENG GEHEIM"-Dokumenten gemäß den Sicherheitsvorschriften gewährleistet. Die „EU — STRENG GEHEIM"-Registratur wird von dem Kontrollbeauftragten für die „EU — STRENG GEHEIM"-Registratur geleitet.

2. Die „EU — STRENG GEHEIM"-Zentralregistratur ist die hauptsächliche Empfangs- und Versandbehörde in der Kommission gegenüber anderen EU-Organen, den Mitgliedstaaten, internationalen Organisationen und Drittstaaten, mit denen die Kommission Abkommen über Sicherheitsverfahren für den Austausch von Verschlusssachen geschlossen hat.

3. Erforderlichenfalls werden Unterregistraturen eingerichtet, die für die interne Verwaltung von „EU — STRENG GEHEIM"-Dokumenten zuständig sind; sie führen ein Register der von ihnen aufbewahrten Dokumente, das stets auf dem neuesten Stand gehalten wird.

4. „EU — STRENG GEHEIM"-Unterregistraturen werden nach Maßgabe des Abschnitts 22.2.3 eingerichtet, damit längerfristigen Notwendigkeiten entsprochen werden kann; sie werden einer zentralen „EU — STRENG GEHEIM"-Registratur zugeordnet. Müssen „EU — STRENG GEHEIM"-Dokumente nur zeitweilig und gelegentlich konsultiert werden, so können sie ohne Einrichtung einer „EU — STRENG GEHEIM"-Unterregistratur weitergeleitet werden, sofern Vorschriften festgelegt wurden, die gewährleisten, dass diese Dokumente unter der Kontrolle der entsprechenden „EU — STRENG GEHEIM"-Registratur verbleiben und alle materiellen und personenbezogenen Sicherheitsmaßnahmen eingehalten werden.

5. Unterregistraturen ist es nicht gestattet, ohne ausdrückliche Zustimmung ihrer „EU — STRENG GEHEIM"-Zentralregistratur „EU — STRENG GEHEIM"-Dokumente unmittelbar an andere Unterregistraturen derselben Zentralregistratur zu übermitteln.

6. Der Austausch von „EU — STRENG GEHEIM"-Dokumenten zwischen Unterregistraturen, die nicht derselben Zentralregistratur zugeordnet sind, muss über die „EU — STRENG GEHEIM"-Zentralregistraturen abgewickelt werden.

22.2.2. *Die „EU — STRENG GEHEIM"-Zentralregistratur*

In seiner Eigenschaft als Kontrollbeauftragter ist der Leiter der „EU — STRENG GEHEIM"-Zentralregistratur zuständig für

a) die Übermittlung von „EU — STRENG GEHEIM"-Dokumenten gemäß den in Abschnitt 21.3 festgelegten Vorschriften;

b) die Führung einer Liste aller ihm unterstehenden „EU — STRENG GEHEIM"-Unterregistraturen mit Name und Unterschrift der ernannten Kontrollbeauftragten und ihrer bevollmächtigten Stellvertreter;

c) die Aufbewahrung der Empfangsbescheinigungen der Registraturen für alle von der Zentralregistratur verteilten „EU — STRENG GEHEIM"-Dokumente;

d) die Führung eines Registers aller aufbewahrten und verteilten „EU — STRENG GEHEIM"-Dokumente;

e) die Führung einer aktuellen Liste aller „EU — STRENG GEHEIM"-Zentralregistraturen, mit denen er üblicherweise korrespondiert, mit Name und Unterschrift der ernannten Kontrollbeauftragten und ihrer bevollmächtigten Stellvertreter;

f) den materiellen Schutz aller in der Registratur aufbewahrten „EU — STRENG GEHEIM"-Dokumente gemäß den Vorschriften des Abschnitts 18.

22.2.3. *„EU — STRENG GEHEIM"-Unterregistraturen*

In seiner Eigenschaft als Kontrollbeauftragter ist der Leiter einer „EU — STRENG GEHEIM"-Unterregistratur zuständig für

a) die Übermittlung von „EU— STRENG GEHEIM"-Dokumenten gemäß den in Abschnitt 21.3 festgelegten Vorschriften;

b) die Führung einer aktuellen Liste aller Personen, die befugt sind, Zugang zu den „EU — STRENG GEHEIM"-Informationen zu erhalten, welche seiner Aufsicht unterliegen;

c) die Verteilung von „EU — STRENG GEHEIM"-Dokumenten gemäß den Vorschriften des Urhebers oder nach dem Grundsatz „Kenntnis notwendig", nach vorheriger Prüfung, ob der Empfänger die erforderliche Sicherheitsermächtigung besitzt;

d) die Führung eines auf neuestem Stand zu haltenden Registers aller aufbewahrten oder in Umlauf befindlichen „EU — STRENG GEHEIM"-Dokumente, die seiner Aufsicht unterliegen oder die an andere „EU — STRENG GEHEIM"-Registraturen weitergeleitet wurden, und Aufbewahrung aller entsprechenden Empfangsbescheinigungen;

e) die Führung einer aktuellen Liste der „EU — STRENG GEHEIM"-Registraturen, mit denen er „EU — STRENG GEHEIM"-Dokumente austauschen darf, mit Name und Unterschrift ihrer Kontrollbeauftragten und bevollmächtigten Stellvertreter;

f) den materiellen Schutz aller in der Unterregistratur aufbewahrten „EU — STRENG GEHEIM"-Dokumente gemäß den Vorschriften des Abschnitts 18.

22.3. **Bestandsaufnahme und Prüfung von EU-Verschlusssachen**

1. Alljährlich führt jede „EU — STRENG GEHEIM"- Registratur im Sinne dieses Abschnitts eine detaillierte Bestandsaufnahme der „EU — STRENG GEHEIM"-Dokumente durch. Als nachgewiesen gilt jedes Dokument, das in der Registratur materiell vorhanden ist oder für das die Empfangsbescheinigung einer „EU — STRENG GEHEIM"-Registratur, der das Dokument übermittelt wurde, bzw. eine Vernichtungsbescheinigung oder aber eine Anweisung zur Herabstufung dieses Dokuments oder der Aufhebung seines Geheimhaltungsgrades vorliegt. Die Ergebnisse der jährlichen Bestandsaufnahmen werden bis spätestens 1. April jeden Jahres dem für Sicherheitsfragen zuständigen Mitglied der Kommission übermittelt.

2. Die „EU — STRENG GEHEIM"-Unterregistraturen übermitteln die Ergebnisse ihrer jährlichen Bestandsaufnahme der Zentralregistratur, der sie unterstehen, zu einem von dieser festgelegten Datum.

3. EU-Verschlusssachen mit einer niedrigeren Einstufung als „EU — STRENG GEHEIM" werden den Anweisungen des für Sicherheitsfragen zuständigen Mitglieds der Kommission entsprechend einer internen Überprüfung unterzogen.

4. Hierbei soll ermittelt werden, ob nach Auffassung der Verwahrer

   a) bestimmte Dokumente heruntergestuft oder der Geheimhaltungsgrad aufgehoben werden kann,

   b) Dokumente vernichtet werden sollten.

22.4. **Archivierung von EU-Verschlusssachen**

1. EU-Verschlusssachen werden unter Bedingungen archiviert, die allen in Abschnitt genannten Anforderungen entsprechen.

2. Um Archivierungsprobleme möglichst gering zu halten, ist es den Kontrollbeauftragten aller Registraturen gestattet, „EU — STRENG GEHEIM", „EU — GEHEIM" und „EU — VERTRAULICH"-Dokumente auf Mikrofilm aufzunehmen oder auf andere Weise auf magnetischen oder optischen Datenträgern zu Archivzwecken zu speichern, vorausgesetzt

   a) das Verfahren zur Aufnahme auf Mikrofilm oder zur sonstigen Speicherung wird von Personen durchgeführt, die über eine Sicherheitsermächtigung für den dem Dokument entsprechenden Geheimhaltungsgrad verfügen;

   b) für den Mikrofilm/Datenträger wird die gleiche Sicherheit gewährleistet wie für die Originaldokumente;

   c) das Mikrofilmen/die Speicherung eines „EU — STRENG GEHEIM"-Dokuments wird dem Urheber mitgeteilt;

   d) die Filmrollen oder sonstigen Träger enthalten nur Dokumente der gleichen „EU — STRENG GEHEIM", „EU — GEHEIM" oder „EU — VERTRAULICH"-Einstufung;

   e) das Mikrofilmen/die Speicherung eines „EU — STRENG GEHEIM" oder „EU — GEHEIM"-Dokuments wird in dem für die jährliche Bestandsaufnahme verwendeten Register deutlich kenntlich gemacht;

   f) die Originaldokumente, die auf Mikrofilm aufgenommen oder in anderer Weise gespeichert sind, werden gemäß den Vorschriften des Abschnitts 22.5 vernichtet.

3. Diese Vorschriften gelten auch für alle anderen zugelassenen Speichermedien wie elektromagnetische Träger und optische Speicherplatten.

22.5. **Vernichtung von EU-Verschlusssachen**

1. Um eine unnötige Anhäufung von EU-Verschlusssachen zu vermeiden, werden die nach Auffassung des Leiters der aufbewahrenden Stelle inhaltlich überholten oder überzähligen Dokumente so bald wie praktisch möglich auf folgende Weise vernichtet:

   a) „EU — STRENG GEHEIM"-Dokumente werden nur von der für diese Dokumente zuständigen Zentralregistratur vernichtet. Jedes der Vernichtung zugeführte Dokument wird auf einer Vernichtungsbescheinigung eingetragen, die vom „EU — STRENG GEHEIM"-Kontrollbeauftragten und von dem der Vernichtung als Zeuge beiwohnenden Beamten, der über die betreffende Sicherheitsermächtigung verfügt, zu unterzeichnen ist. Der Vorgang wird im Dienstbuch festgehalten.

   b) Die Registratur bewahrt die Vernichtungsbescheinigungen zusammen mit den Verteilungsunterlagen zehn Jahre lang auf. Dem Urheber oder der zuständigen Zentralregistratur werden Kopien nur zugesandt, wenn dies ausdrücklich verlangt wird.

   c) „EU — STRENG GEHEIM"-Dokumente einschließlich des bei ihrer Herstellung angefallenen und als Verschlusssache zu behandelnden Abfalls oder Zwischenmaterials wie fehlerhafte Kopien, Arbeitsvorlagen, maschinegeschriebene Aufzeichnungen und Disketten werden unter der Aufsicht eines „EU — STRENG GEHEIM"-Kontrollbeauftragten durch Verbrennen, Einstampfen, Zerkleinern oder andere geeignete Verfahren so vernichtet, dass der Inhalt weder erkennbar ist noch erkennbar gemacht werden kann.

2. „EU — GEHEIM"-Dokumente werden mittels eines der in Nummer 1 Buchstabe c) genannten Verfahren unter der Aufsicht einer Person, die über die betreffende Sicherheitsermächtigung verfügt, von der für diese Dokumente zuständigen Registratur vernichtet. Vernichtete „EU — GEHEIM"-Dokumente werden auf einer unterzeichneten Vernichtungsbescheinigung eingetragen, die von der Registratur zusammen mit den Verteilungsunterlagen mindestens drei Jahre lang aufbewahrt wird.

3. „EU — VERTRAULICH"-Dokumente werden mittels eines der in Nummer 1 Buchstabe c) genannten Verfahren unter der Aufsicht einer Person, die über die betreffende Sicherheitsermächtigung verfügt, von der für diese Dokumente zuständigen Registratur vernichtet. Ihre Vernichtung wird gemäß den Anweisungen des für Sicherheitsfragen zuständigen Mitglieds der Kommission registriert.

4. „EU — NUR FÜR DEN DIENSTGEBRAUCH"-Dokumente werden gemäß den Anweisungen des für Sicherheitsfragen zuständigen Mitglieds der Kommission von der für diese Dokumente zuständigen Registratur oder vom Nutzer vernichtet.

22.6. **VERNICHTUNG IM NOTFALL**

1. Die Kommissionsdienststellen 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, damit EU-Verschlusssachen nicht in unbefugte Hände gelangen.

2. Vorschriften zum Schutz und/oder zur Vernichtung von „EU — GEHEIM"- und „EU — VERTRAULICH"-Unterlagen im Krisenfall dürfen auf keinen Fall den Schutz oder die Vernichtung von „EU — STRENG GEHEIM"-Materialien, einschließlich der Verschlüsselungseinrichtungen, beeinträchtigen, die Vorrang vor allen anderen Aufgaben haben.

3. Die für den Schutz und die Vernichtung der Verschlüsselungseinrichtungen vorzusehenden Maßnahmen sind durch Ad-hoc-Anweisungen zu regeln.

4. Die Anweisungen sind an Ort und Stelle in einem versiegelten Umschlag zu hinterlegen. Es müssen Vorrichtungen/Werkzeuge für die Vernichtung vorhanden sein.

23. SICHERHEITSMASSNAHMEN BEI BESONDEREN SITZUNGEN AUSSERHALB DER KOMMISSIONSGEBÄUDE, BEI DENEN VERSCHLUSSSACHEN BENÖTIGT WERDEN

23.1. **Allgemeines**

Finden außerhalb der Kommissionsgebäude Sitzungen der Kommission oder andere wichtige Sitzungen statt und ist es durch die besonderen Sicherheitsanforderungen aufgrund der hohen Empfindlichkeit der behandelten Fragen oder Informationen gerechtfertigt, so werden die nachstehend beschriebenen Sicherheitsmaßnahmen ergriffen. Diese Maßnahmen betreffen lediglich den Schutz von EU-Verschlusssachen; möglicherweise sind weitere Sicherheitsmaßnahmen vorzusehen.

23.2. **Zuständigkeiten**

23.2.1. *Sicherheitsbüro der Kommission*

Das Sicherheitsbüro der Kommission arbeitet mit den zuständigen Behörden des Mitgliedstaates zusammen, auf dessen Hoheitsgebiet die Sitzung stattfindet (gastgebender Mitgliedstaat), um die Sicherheit der Kommissionssitzung oder anderer wichtiger Sitzungen und die Sicherheit der Delegierten und ihrer Mitarbeiter zu gewährleisten. In Bezug auf den Sicherheitsschutz sollte es insbesondere gewährleisten, dass

a) Pläne für den Umgang mit Sicherheitsrisiken und sicherheitsrelevanten Zwischenfällen aufgestellt werden, wobei die betreffenden Maßnahmen insbesondere auf die sichere Verwahrung von EU-Verschlusssachen in Büroräumen abzielen;

b) Maßnahmen getroffen werden, um den etwaigen Zugang zum Kommunikationssystem der Kommission für den Empfang und die Versendung von als Verschlusssache eingestuften EU-Mitteilungen bereitzustellen. Der gastgebende Mitgliedstaat wird gebeten, erforderlichenfalls den Zugang zu sicheren Telefonsystemen zu ermöglichen.

Das Sicherheitsbüro der Kommission fungiert als Sicherheitsberatungsstelle für die Vorbereitung der Sitzung; es sollte auf der Sitzung vertreten sein, um erforderlichenfalls den Sicherheitsbeauftragten für die Sitzung und die Delegationen zu unterstützen und zu beraten.

Jede an der Sitzung teilnehmende Delegation wird gebeten, einen Sicherheitsbeauftragten zu benennen, der für die Behandlung von Sicherheitsfragen in seiner Delegation zuständig ist und die Verbindung zu dem Sicherheitsbeauftragten für die Sitzung sowie mit dem Vertreter des Sicherheitsbüros der Kommission aufrechterhält.

23.2.2. *Sicherheitsbeauftragter für die Sitzung*

Es wird ein Sicherheitsbeauftragter ernannt, der für die allgemeine Vorbereitung und Überwachung der allgemeinen internen Sicherheitsmaßnahmen und für die Koordinierung mit den anderen betroffenen Sicherheitsbehörden verantwortlich ist. Die von ihm getroffenen Maßnahmen erstrecken sich im Allgemeinen auf Folgendes:

a) Schutzmaßnahmen am Sitzungsort, mit denen sichergestellt wird, dass es auf der Sitzung zu keinem Zwischenfall kommt, der die Sicherheit einer dort verwendeten EU-Verschlusssache gefährden könnte;

b) Überprüfung des Personals, das den Sitzungsort, die Bereiche der Delegationen und die Konferenzräume betreten darf, sowie sämtlicher Ausrüstungsgegenstände;

c) ständige Abstimmung mit den zuständigen Behörden des gastgebenden Mitgliedstaats und dem Sicherheitsbüro der Kommission;

d) Einfügung von Sicherheitsanweisungen in das Sitzungsdossier unter gebührender Berücksichtigung der Erfordernisse, die in diesen Sicherheitsvorschriften und anderen für erforderlich erachteten Sicherheitsanweisungen enthalten sind.

23.3. **Sicherheitsmaßnahmen**

23.3.1. *Sicherheitsbereiche*

Es werden folgende Sicherheitsbereiche angelegt:

a) ein Sicherheitsbereich der Kategorie II, der nach Maßgabe der Erfordernisse einen Redaktionsraum, die Büroräume der Kommission und die Vervielfältigungsausrüstung sowie Büroräume der Delegationen umfasst;

b) ein Sicherheitsbereich der Kategorie I, der den Konferenzraum sowie die Dolmetschkabinen und die Kabinen für die Tontechnik umfasst;

c) einen Verwaltungsbereich, der aus dem Pressebereich und den für Verwaltung, Verpflegung und Unterkunft genutzten Bereichen des Sitzungsortes sowie aus dem sich unmittelbar an das Pressezentrum und den Sitzungsort anschließenden Bereich besteht.

23.3.2. *Berechtigungsausweise*

Der Sicherheitsbeauftragte für die Sitzung gibt entsprechend dem von den Delegationen gemeldeten Bedarf geeignete Berechtigungsausweise aus. Erforderlichenfalls kann eine Abstufung der Zugangsberechtigung für die verschiedenen Sicherheitsbereiche vorgesehen werden.

Mit den Sicherheitsanweisungen für die Sitzung werden alle Betroffenen verpflichtet, am Sitzungsort ihre Berechtigungsausweise stets gut sichtbar mit sich zu führen, so dass sie erforderlichenfalls vom Sicherheitspersonal überprüft werden können.

Abgesehen von den mit einem Berechtigungsausweis versehenen Sitzungsteilnehmern sollten so wenige Personen wie möglich Zugang zum Sitzungsort erhalten. Der Sicherheitsbeauftragte für die Sitzung erteilt einzelstaatlichen Delegationen nur auf Antrag die Genehmigung, während der Sitzung Besucher zu empfangen. Die Besucher sollten einen Besucherausweis erhalten. Der Name des Besuchers und der besuchten Person wird auf einem Besucherschein eingetragen. Besucher sind stets von einem Angehörigen des Sicherheitspersonals oder von der besuchten Person zu begleiten. Der Besucherschein wird von der Begleitperson mitgeführt und von dieser zusammen mit dem Besucherausweis dem Sicherheitspersonal zurückgegeben, sobald der Besucher den Sitzungsort verlässt.

23.3.3. *Kontrolle von fotografischen Ausrüstungen und Tonaufzeichnungsgeräten*

Bild- oder Tonaufzeichnungsgeräte dürfen nicht in einen Sicherheitsbereich der Kategorie I gebracht werden, sofern es sich nicht um die Ausrüstung von Fotografen und Tontechnikern handelt, die vom Sicherheitsbeauftragten für die Sitzung vorschriftsgemäß zugelassen worden sind.

23.3.4. *Überprüfung von Aktentaschen, tragbaren Computern und Paketen*

Inhaber von Berechtigungsausweisen, denen der Zugang zu einem Sicherheitsbereich gestattet ist, dürfen in der Regel ihre Aktentaschen und tragbaren Computer (nur mit eigener Stromversorgung) mitbringen, ohne dass diese überprüft werden. Bei für die Delegationen bestimmten Paketen dürfen die Delegationen die Lieferung in Empfang nehmen; diese wird entweder vom Sicherheitsbeauftragten der Delegation überprüft, mit Spezialgeräten kontrolliert oder aber vom Sicherheitspersonal zur Überprüfung geöffnet. Wenn der Sicherheitsbeauftragte für die Sitzung es für erforderlich hält, können strengere Maßnahmen für die Überprüfung von Aktentaschen und Paketen festgelegt werden.

23.3.5. *Technische Sicherheit*

Der Sitzungsraum kann von einem für die technische Sicherheit zuständigen Team technisch gesichert werden; dieses Team kann ferner während der Sitzung eine elektronische Überwachung vornehmen.

23.3.6. *Dokumente der Delegationen*

Die Delegationen sind für die Beförderung von EU-Verschlusssachen zu und von Sitzungen verantwortlich. Sie sind auch für die Überprüfung und Sicherheit der betreffenden Unterlagen bei der Verwendung in den ihnen zugewiesenen Räumlichkeiten verantwortlich. Der gastgebende Mitgliedstaat kann für die Beförderung der Verschlusssachen zum und vom Sitzungsort um Hilfe ersucht werden.

23.3.7. *Sichere Aufbewahrung der Dokumente*

Sind die Kommission oder die Delegationen nicht in der Lage, ihre Verschlusssachen gemäß den anerkannten Standards aufzubewahren, so können sie diese Unterlagen in einem versiegelten Umschlag beim Sicherheitsbeauftragten für die Sitzung gegen Empfangsbescheinigung hinterlegen, so dass dieser für eine den genannten Standards entsprechenden Aufbewahrung Sorge tragen kann.

23.3.8. *Überprüfung der Büroräume*

Der Sicherheitsbeauftragte für die Sitzung sorgt dafür, dass die Büroräume der Kommission und der Delegationen am Ende jedes Arbeitstages überprüft werden, damit sichergestellt ist, dass alle EU-Verschlusssachen an einem sicheren Ort aufbewahrt werden; andernfalls trifft er die erforderlichen Abhilfemaßnahmen.

23.3.9. *Abfallbeseitigung bei EU-Verschlusssachen*

Sämtliche Abfälle sind als EU-Verschlusssachen zu behandeln, und die Kommission und die Delegationen sollten zur Entsorgung Papierkörbe oder Abfallsäcke erhalten. Vor Verlassen der ihnen zugewiesenen Räumlichkeiten bringen die Kommission und die Delegationen die Abfälle zum Sicherheitsbeauftragten für die Sitzung, der ihre vorschriftsmäßige Vernichtung veranlasst.

Am Ende der Sitzung werden alle Dokumente, die die Kommission oder die Delegationen in ihrem Besitz hatten, aber nicht behalten wollen, als Abfall behandelt. Es wird eine umfassende Inspektion der Räumlichkeiten der Kommission und der Delegationen durchgeführt, bevor die für die Sitzung getroffenen Sicherheitsmaßnahmen aufgehoben werden. Dokumente, für die eine Empfangsbescheinigung unterzeichnet wurde, werden soweit möglich gemäß den Vorschriften des Abschnitts 22.5 vernichtet.

24. VERLETZUNG DER SICHERHEIT UND KENNTNISNAHME VON EU-VERSCHLUSSSACHEN DURCH UNBEFUGTE

24.1. **Begriffsbestimmungen**

Eine Verletzung der Sicherheit liegt vor, wenn durch eine Handlung oder durch eine Unterlassung, die den Sicherheitsvorschriften der Kommission zuwiderläuft, EU-Verschlusssachen in Gefahr geraten oder Unbefugten zur Kenntnis gelangen könnten.

Eine Kenntnisnahme von EU-Verschlusssachen durch Unbefugte liegt vor, wenn die Verschlusssache ganz oder teilweise in die Hände unbefugter Personen (d. h. von Personen, die nicht die erforderliche Zugangsermächtigung haben oder deren Kenntnis der Verschlusssachen nicht nötig ist) gelangt ist oder es wahrscheinlich ist, dass eine derartige Kenntnisnahme stattgefunden hat.

Die Kenntnisnahme von EU-Verschlusssachen durch Unbefugte kann die Folge von Nachlässigkeit, Fahrlässigkeit oder Indiskretion, aber auch der Tätigkeit von Diensten, die in der EU oder ihren Mitgliedstaaten Kenntnis von EU-Verschlusssachen und geheimen Tätigkeiten erlangen wollen, oder von subversiven Organisationen sein.

24.2. **Meldung von Verstößen gegen die Sicherheit**

Alle Personen, die mit EU-Verschlusssachen umgehen müssen, werden eingehend über ihre Verantwortung in diesem Bereich unterrichtet. Sie melden unverzüglich jede Verletzung der Sicherheit, von der sie Kenntnis erhalten.

Wenn ein Lokaler Sicherheitsbeauftragter oder ein Sicherheitsbeauftragter für eine Sitzung eine Verletzung der Sicherheit betreffend EU-Verschlusssachen oder den Verlust bzw. das Verschwinden von als EU-Verschlusssache eingestuftem Material entdeckt oder hiervon unterrichtet wird, trifft er rasch Maßnahmen, um

a) Beweise zu sichern;

b) den Sachverhalt zu klären;

c) den entstandenen Schaden zu bewerten und möglichst klein zu halten;

d) zu verhindern, dass sich ein derartiger Vorfall wiederholt;

e) die zuständigen Behörden von den Folgen der Verletzung der Sicherheit zu unterrichten.

In diesem Zusammenhang sind folgende Angaben zu machen:

i) eine Beschreibung der entsprechenden Verschlusssache unter Angabe ihres Geheimhaltungsgrades, ihres Aktenzeichens und der Ausfertigungsnummer, des Datums, des Urhebers, des Themas und des Umfangs;

ii) eine kurze Beschreibung der Umstände, unter denen die Verletzung der Sicherheit erfolgt ist, unter Angabe des Datums und des Zeitraums, während dessen die Verschlusssache Unbefugten zur Kenntnis gelangen konnte;

iii) eine Erklärung darüber, ob der Urheber informiert worden ist.

Jede Sicherheitsbehörde hat die Pflicht, unmittelbar nach ihrer Unterrichtung von einer möglichen Verletzung der Sicherheit das Sicherheitsbüro der Kommission zu benachrichtigen.

Fälle, in denen es um als „EU — NUR FÜR DEN DIENSTGEBRAUCH“ eingestufte Verschlusssachen geht, müssen nur dann gemeldet werden, wenn sie ungewöhnlicher Art sind.

Wird das für Sicherheitsfragen zuständige Mitglied der Kommission von einer Verletzung der Sicherheit unterrichtet, so

a) unterrichtet es die Stelle, von der die entsprechende Verschlusssache stammt;

b) bittet es die zuständigen Sicherheitsbehörden um die Einleitung von Ermittlungen;

c) koordiniert es die Ermittlungen, falls mehr als eine Sicherheitsbehörde betroffen ist;

d) lässt es einen Bericht erstellen über die Umstände der Verletzung der Sicherheit, das Datum oder den Zeitraum, an dem bzw. während dessen die Verletzung erfolgt ist und der Verstoß entdeckt wurde; der Bericht umfasst eine detaillierte Beschreibung des Inhalts und des Geheimhaltungsgrades des betreffenden Materials. Es ist auch zu berichten, welcher Schaden den Interessen der EU oder eines oder mehrerer ihrer Mitgliedstaaten entstanden ist und welche Maßnahmen ergriffen worden sind, um eine Wiederholung des Vorfalls zu verhindern.

Die Stelle, von der die Verschlusssache stammt, unterrichtet die Empfänger des Dokuments und gibt ihnen entsprechende Anweisungen.

24.3. **Rechtliche Schritte**

Gegen jede für die Kenntnisnahme von EU-Verschlusssachen durch Unbefugte verantwortliche Person können nach den geltenden Vorschriften und Regelungen, insbesondere nach Titel VI des Statuts Disziplinarmaßnahmen ergriffen werden. Diese Maßnahmen lassen ein etwaiges gerichtliches Vorgehen unberührt.

In geeigneten Fällen leitet das für Sicherheitsfragen zuständige Mitglied der Kommission auf der Grundlage des Berichts nach Abschnitt 24.2 alle erforderlichen Schritte ein, um den zuständigen einzelstaatlichen Behörden die Einleitung von Strafverfahren zu ermöglichen.

25. SCHUTZ VON EU-VERSCHLUSSSACHEN IN INFORMATIONSTECHNISCHEN SYSTEMEN UND KOMMUNIKATIONSSYSTEMEN

25.1. **Einleitung**

25.1.1. *Allgemeines*

Das Sicherheitskonzept und die Sicherheitsanforderungen gelten für alle Kommunikations- und Informationssysteme und -netze (nachstehend als „Systeme“ bezeichnet), in denen Informationen des Geheimhaltungsgrades „EU — VERTRAULICH“ oder höher verarbeitet werden. Sie gelten ergänzend zum Beschluss der Kommission C(95) 1510 endg. der Kommission vom 23. November 1995 über den Schutz der Informatiksysteme.

Auch bei Systemen, in denen als „EU — NUR FÜR DEN DIENSTGEBRAUCH“ eingestufte Informationen verarbeitet werden, sind Sicherheitsmaßnahmen zum Schutz der Vertraulichkeit dieser Informationen erforderlich. Bei allen Systemen sind Sicherheitsmaßnahmen zum Schutz der Integrität und der Verfügbarkeit dieser Systeme und der darin enthaltenen Informationen erforderlich.

Das von der Kommission angewandte IT-Sicherheitskonzept stützt sich auf folgende Grundsätze:

— Es ist Bestandteil der Sicherheit im Allgemeinen und ergänzt alle Teilaspekte der Datensicherheit der personalbezogenen Sicherheit und der materiellen Sicherheit;

— Aufteilung der Zuständigkeiten auf Eigentümer der technischen Systeme, Eigentümer von EU-Verschlusssachen, die in technischen Systemen gespeichert oder verarbeitet werden, IT-Sicherheitsexperten und Nutzer;

— Beschreibung der Sicherheitsgrundsätze und Anforderungen jedes IT-Systems;

— Genehmigung dieser Grundsätze und Anforderungen durch eine dafür bestimmte Stelle;

— Berücksichtigung der spezifischen Bedrohungen und Schwachstellen in der IT-Umgebung.

25.1.2. *Bedrohungen und Schwachstellen von Systemen*

Eine Bedrohung kann als Möglichkeit einer unabsichtlichen oder absichtlichen Beeinträchtigung der Sicherheit definiert werden. Bei Systemen ist dies mit dem Verlust einer oder mehrerer der Eigenschaften Vertraulichkeit, Integrität und Verfügbarkeit verbunden. Eine Schwachstelle kann als unzureichende oder fehlende Kontrolle definiert werden, die die Bedrohung eines bestimmten Objekts oder Ziels erleichtern oder ermöglichen könnte.

EU-Verschlusssachen und sonstige Informationen, die in Systemen in einer zur raschen Abfrage, Übermittlung und Nutzung konzipierten konzentrierten Form vorliegen, sind in vielerlei Hinsicht gefährdet. So könnten z. B. Unbefugte auf die Informationen zugreifen oder Befugten könnte der Zugriff verweigert werden. Ferner besteht das Risiko einer unerlaubten Verbreitung, einer Verfälschung, Änderung oder Löschung der Informationen. Außerdem sind die komplexen und manchmal empfindlichen Geräte teuer in der Anschaffung, und es ist häufig schwierig, sie rasch zu reparieren oder zu ersetzen.

25.1.3. *Hauptzweck von Sicherheitsmaßnahmen*

Die in diesem Abschnitt festgelegten Sicherheitsmaßnahmen dienen in erster Linie dem Schutz von EU-Verschlusssachen vor unerlaubter Preisgabe (Verlust der Vertraulichkeit) sowie dem Schutz vor dem Verlust der Integrität und der Verfügbarkeit von Informationen. Um ein System, in dem EU-Verschlusssachen verarbeitet werden, angemessen zu schützen, sind die einschlägigen konventionellen Sicherheitsstandards vom Sicherheitsbüro der Kommission festzulegen, zu denen geeignete, auf das jeweilige System zugeschnittene spezielle Sicherheitsverfahren und -techniken hinzukommen.

25.1.4. *Aufstellung der systemspezifischen Sicherheitsanforderungen (SSRS)*

Für alle Systeme, in denen als „EU — VERTRAULICH“ oder höher eingestufte Informationen verarbeitet werden, ist eine Aufstellung der systemspezifischen Sicherheitsanforderungen SSRS) erforderlich, die vom Eigentümer des technischen Systems (TSO) (siehe Abschnitt 25.3.4) und dem Eigentümer der Information (siehe Abschnitt 25.3.5) gegebenenfalls mit Beiträgen und Unterstützung des Projektpersonals und des Sicherheitsbüros der Kommission (als INFOSEC-Stelle (IA) siehe Abschnitt 25.3.3) erstellt und von der Akkreditierungsstelle für IT-Sicherheit (SAA, siehe Abschnitt 25.3.2) genehmigt werden.

Eine SSRS ist auch dann erforderlich, wenn die Verfügbarkeit und Integrität von als „EU - NUR FÜR DEN DIENSTGEBRAUCH“ eingestuften Informationen oder von Informationen ohne VS-Einstufung von der Akkreditierungsstelle für IT-Sicherheit (SAA) als sicherheitskritisch angesehen wird.

Die SSRS wird im frühesten Stadium der Konzeption eines Projekts formuliert und parallel zum Projektverlauf weiterentwickelt und verbessert; sie erfüllt unterschiedliche Aufgaben in verschiedenen Stadien des Projekts und des Lebenszyklus des Systems.

25.1.5. *Sicherheitsmodus*

Alle Systeme, in denen als „EU — VERTRAULICH“ oder höher eingestufte Informationen verarbeitet werden, werden für den Betrieb in einem einzigen Sicherheitsmodus oder — aufgrund zeitlich unterschiedlicher Anforderungen — in mehreren der folgenden sicherheitsbezogenen Betriebsarten (oder deren einzelstaatlichen Entsprechungen) freigegeben:

a) Dedicated,

b) System high,

c) Multi-level.

25.2. **Begriffsbestimmungen**

„Akkreditierung“ bezeichnet die Abnahme und Zulassung eines SYSTEMS zur Verarbeitung von EU-Verschlusssachen in seinem betrieblichen Umfeld.

Anmerkung:

Die Akkreditierung sollte erfolgen, nachdem alle einschlägigen sicherheitsrelevanten Verfahren durchgeführt worden sind und der Schutz der Systemressourcen in ausreichendem Maße sichergestellt worden ist. Die Akkreditierung sollte in der Regel auf der Grundlage der SSRS erfolgen und Folgendes umfassen:

a) Festlegung der Zielvorgaben der Akkreditierung dieses System, insbesondere welche Geheimhaltungsgrade verarbeitet werden sollen und welcher Sicherheitsmodus für das System oder Netz vorgeschlagen wird;

b) Bestandsaufnahme des Risikomanagements, in der Bedrohungen und Schwachstellen benannt und entsprechende Gegenmaßnahmen dargelegt werden;

c) sicherheitsbezogene Betriebsverfahren (SecOP) mit einer detaillierten Beschreibung der vorgesehenen Abläufe (z. B. Betriebsarten und Funktionen) und mit einer Beschreibung der Sicherheitseigenschaften des Systems, die die Grundlage für die Akkreditierung bildet;

d) Plan für die Implementierung und Aufrechterhaltung der Sicherheitseigenschaften;

e) Plan für die erstmalige und nachfolgende Prüfung, Evaluation und Zertifizierung der System- oder Netzsicherheit;

f) gegebenenfalls Zertifizierung zusammen mit anderen Teilaspekten der Akkreditierung.

Der „Beauftragte für die zentrale IT-Sicherheit“ (CISO) ist der Beamte in einer zentralen IT-Dienststelle, der Sicherheitsmaßnahmen für zentral organisierte Systeme koordiniert und überwacht.

„Zertifizierung“ bezeichnet eine - durch eine unabhängige Überprüfung der Durchführung und der Ergebnisse einer Evaluation gestützte - förmliche Bescheinigung darüber, inwieweit ein System die Sicherheitsanforderungen erfüllt oder inwieweit ein Computersicherheitsprodukt vorgegebene Sicherheitsleistungen erbringt.

„Kommunikationssicherheit“ (COMSEC) bezeichnet die Anwendung von Sicherheitsmaßnahmen auf den Telekommunikationsverkehr, um zu verhindern, dass Unbefugte in den Besitz wertvoller Informationen gelangen, die aus dem Zugriff auf den Telekommunikationsverkehr und dessen Auswertung gewonnen werden könnten, oder um die Authentizität des Telekommunikationsverkehrs sicherzustellen.

Anmerkung:

Diese Maßnahmen umfassen die kryptografische Sicherheit, die Sicherheit der Übermittlung und die Sicherheit vor Abstrahlung und ferner die verfahrens-, objekt- und personenbezogene Sicherheit sowie die Dokumenten- und Computersicherheit.

„Computersicherheit“ (COMPUSEC) bezeichnet den Einsatz der Sicherheitseigenschaften von Hardware, Firmware und Software eines Computersystems zum Schutz vor unerlaubter Preisgabe, Manipulation, Änderung bzw. Löschung von Informationen sowie vor einem Systemausfall (Denial of Service).

„Computersicherheitsprodukt“ ist ein allgemeines, der Computersicherheit dienendes Produkt, das zur Integration in ein IT-System und zur Verbesserung bzw. Gewährleistung der Vertraulichkeit, Integrität oder Verfügbarkeit der verarbeiteten Informationen bestimmt ist.

Der „Sicherheitsmodus ‚DEDICATED‘“ bezeichnet eine Betriebsart, bei der ALLE Personen, die Zugang zum SYSTEM haben, zum Zugriff auf den höchsten im System verarbeiteten Geheimhaltungsgrad berechtigt sind und generell einen berechtigten Informationsbedarf in Bezug auf ALLE im System verarbeiteten Informationen haben.

Anmerkungen:

(1) Da alle Nutzer einen berechtigten Informationsbedarf haben, muss sicherheitstechnisch nicht unbedingt zwischen unterschiedlichen Informationen innerhalb des Systems unterschieden werden.

(2) Andere Sicherheitseigenschaften (z. B. objekt-, personen- und verfahrensbezogene Funktionen) müssen den Anforderungen für den höchsten Geheimhaltungsgrad und für alle Kategorien von Informationen, die im System verarbeitet werden, entsprechen.

„EVALUATION“ bezeichnet die eingehende technische Prüfung der Sicherheitsaspekte eines SYSTEMS oder eines Produkts für kryptografische Sicherheit oder Computersicherheit durch eine zuständige Stelle.

Anmerkungen:

(1) Bei der Evaluation wird geprüft, ob die verlangten Sicherheitsfunktionen tatsächlich vorhanden sind und ob sie negative Nebeneffekte haben, und es wird bewertet, inwieweit diese Funktionen verfälscht werden könnten.

(2) Bei der Evaluation wird ferner bestimmt, inwieweit die für ein System geltenden Sicherheitsanforderungen erfüllt bzw. die geltend gemachten Sicherheitsleistungen eines Computersicherheitsprodukts erbracht werden, und es wird die Vertrauenswürdigkeitsstufe des Systems oder des Produkts für kryptografische Sicherheit oder Computersicherheit bestimmt.

Eigentümer der Information (IO) ist die Stelle (Dienststellenleiter), die für die Schaffung, Verarbeitung und Nutzung von Informationen verantwortlich ist, einschließlich der Entscheidung, wem der Zugriff auf diese Informationen gewährt werden soll.

„Informationssicherheit“ (INFOSEC) bezeichnet die Anwendung von Sicherheitsmaßnahmen zum Schutz von Informationen, die in Kommunikations- und Informationssystemen und anderen elektronischen Systemen verarbeitet, gespeichert oder übermittelt werden, vor dem unabsichtlichen oder absichtlichen Verlust der Vertraulichkeit, Integrität oder Verfügbarkeit, sowie zur Vermeidung des Verlustes der Integrität und Verfügbarkeit der Systeme selbst.

„INFOSEC-Maßnahmen“ erstrecken sich auf die Sicherheit von Computern, die Sicherheit der Übertragung, die Sicherheit vor Abstrahlung und die kryptografische Sicherheit sowie die Aufdeckung, Dokumentation und Bekämpfung von Bedrohungen für Informationen und Systeme.

„IT-Umgebung“ bezeichnet einen Bereich, in dem sich ein oder mehrere Computer, deren lokale Peripheriegeräte und Speichereinheiten, Steuereinheiten sowie ihnen fest zugeordnete Netz- und Kommunikationseinrichtungen befinden.

Anmerkung:

Nicht eingeschlossen sind davon abgetrennte Bereiche, in denen sich dezentrale Peripheriegeräte oder Terminals bzw. Datenstationen befinden, auch wenn diese an Geräte innerhalb der IT-Umgebung angeschlossen sind.

„IT-Netz“ bezeichnet eine Gesamtheit von geografisch verteilten IT-Systemen, die für den Datenaustausch miteinander verbunden sind; darin eingeschlossen sind die Bestandteile der vernetzten IT-Systeme sowie deren Schnittstelle mit den zugrunde liegenden Daten- oder Kommunikationsnetzen.

Anmerkungen:

(1) Ein IT-Netz kann die Funktionen eines oder mehrerer Kommunikationsnetze zum Datenaustausch nutzen; mehrere IT-Netze können die Funktionen eines gemeinsamen Kommunikationsnetzes nutzen.

(2) Ein IT-Netz wird als „lokal“ bezeichnet, wenn es mehrere am selben Standort befindliche Computer miteinander verbindet.

Die „Sicherheitseigenschaften eines IT-Netzes“ umfassen die Sicherheitseigenschaften der einzelnen IT-Systeme, aus denen das Netz besteht, sowie jene zusätzlichen Bestandteile und Eigenschaften, die mit dem Netz als solchem verbunden sind (z. B. Kommunikation im Netz, Mechanismen und Verfahren zur Sicherheitsidentifikation und zur Kennzeichnung, Zugriffskontrollen, Programme und automatische Ereignisprotokolle), und die erforderlich sind, um einen angemessenen Schutz der Verschlusssachen sicherzustellen.

„IT-System“ bezeichnet eine Gesamtheit von Betriebsmitteln, Methoden und Verfahren sowie gegebenenfalls Personal, die zusammenwirken, um Aufgaben der Informationsverarbeitung zu erfüllen.

Anmerkungen:

(1) Darunter wird eine Gesamtheit von Einrichtungen verstanden, die zur Verarbeitung von Informationen innerhalb des Systems konfiguriert sind.

(2) Diese Systeme können der Abfrage, der Steuerung, der Kontrolle, der Kommunikation und wissenschaftlichen oder administrativen Anwendungen einschließlich der Textverarbeitung dienen.

(3) Die Grenzen eines Systems werden im Allgemeinen in Bezug auf die Bestandteile definiert, die der Kontrolle eines einzigen TSO) unterliegen.

(4) Ein IT-System kann Teilsysteme enthalten, von denen einige selbst wiederum IT-Systeme sind.

Die „Sicherheitseigenschaften eines IT-Systems" umfassen alle Funktionen, Merkmale und Eigenschaften der Hardware, Firmware und Software; dazu gehören die Betriebsverfahren, die Nachvollziehbarkeit, die Zugangs- und Zugriffskontrollen, die IT-Umgebung, die Umgebung dezentraler Terminals bzw. Datenstationen, der vorgegebene Managementrahmen, die physischen Strukturen und Geräte sowie Personal- und Kommunikationskontrollen, die erforderlich sind, um einen annehmbaren Schutz der Verschlusssachen sicherzustellen, die in einem IT-System verarbeitet werden sollen.

Der „Beauftragte für die lokale IT-Sicherheit" (LISO) ist der Beamte in einer Dienststelle der Kommission, der für die Koordinierung und Überwachung von Sicherheitsmaßnahmen in seinem Bereich zuständig ist.

Der „Sicherheitsmodus ‚Multi-level'" bezeichnet eine Betriebsart, bei der NICHT ALLE Personen, die Zugang zum System haben, zum Zugriff auf den höchsten Geheimhaltungsgrad im System berechtigt sind und bei der NICHT ALLE Personen, die Zugang zum System haben, generell einen berechtigten Informationsbedarf in Bezug auf die im System verarbeiteten Informationen haben.

Anmerkungen:

(1) In dieser Betriebsart ist derzeit die Verarbeitung von Informationen unterschiedlicher Geheimhaltungsgrade und verschiedener Kategorien von Informationen möglich.

(2) Da nicht alle Personen zum Zugriff auf die höchsten Geheimhaltungsgrade berechtigt sind und da nicht alle Personen generell einen berechtigten Informationsbedarf in Bezug auf die im System verarbeiteten Informationen haben, muss die sicherheitstechnische Ausgestaltung einen selektiven Zugriff auf Informationen und eine Trennung von Informationen innerhalb des Systems gewährleisten.

„Umgebung von dezentralen Terminals bzw. Datenstationen" bezeichnet einen Bereich außerhalb einer IT-Umgebung, in dem sich Computer, deren lokale Peripheriegeräte oder Terminals bzw. Datenstationen und alle zugehörigen Kommunikationseinrichtungen befinden.

Die „sicherheitsbezogenen Betriebsverfahren" sind die vom Eigentümer des technischen Systems aufgestellten Verfahren zur Festlegung der in Sicherheitsfragen geltenden Grundsätze, der einzuhaltenden Betriebsverfahren sowie der Zuständigkeiten des Personals.

Der „Sicherheitsmodus ‚SYSTEM-HIGH'" bezeichnet eine Betriebsart, bei der ALLE Personen, die Zugang zum System haben, zum Zugriff auf den höchsten im System verarbeiteten Geheimhaltungsgrad berechtigt sind, bei der aber NICHT ALLE Personen, die Zugang zum System haben, generell einen berechtigten Informationsbedarf in Bezug auf die im System verarbeiteten Informationen haben.

Anmerkungen:

(1) Da nicht alle Nutzer generell einen berechtigten Informationsbedarf haben, muss die sicherheitstechnische Ausgestaltung einen selektiven Zugriff auf Informationen und eine Trennung von Informationen innerhalb des Systems gewährleisten.

(2) Andere Sicherheitseigenschaften (z. B. objekt-, personen- und verfahrensbezogene Funktionen) müssen den Anforderungen für den höchsten Geheimhaltungsgrad und für alle Kategorien von Informationen, die im System verarbeitet werden, entsprechen.

(3) Bei dieser Betriebsart werden alle im System verarbeiteten oder für das System verfügbaren Informationen sowie die entsprechenden Ausgaben — solange nichts anderes festgelegt wurde — so geschützt, als würden sie unter die jeweilige Kategorie von Informationen und den höchsten verarbeiteten Geheimhaltungsgrad fallen, es sei denn, eine vorhandene Kennzeichnungsfunktion ist in ausreichendem Maße vertrauenswürdig.

Die „Aufstellung der systemspezifischen Sicherheitsanforderungen" (SSRS) ist eine vollständige und ausführliche Festlegung der einzuhaltenden Sicherheitsgrundsätze und der zu erfüllenden detaillierten Sicherheitsanforderungen. Sie beruht auf dem Sicherheitskonzept und der Risikobewertung der Kommission bzw. wird von Faktoren des betrieblichen Umfelds bestimmt, vom niedrigsten Berechtigungsstatus des Personals, dem höchsten Geheimhaltungsgrad der verarbeiteten Informationen, vom jeweiligen Sicherheitsmodus oder den Benutzeranforderungen. Die SSRS ist Bestandteil der Projektdokumentation, die den zuständigen Stellen zur Billigung der technischen, haushaltsbezogenen und sicherheitsrelevanten Aspekte unterbreitet wird. In ihrer endgültigen Fassung ist die SSRS eine vollständige Beschreibung der Voraussetzungen, die gegeben sein müssen, damit ein bestimmtes System sicher ist.

Der „Eigentümer des technischen Systems“ (TSO) ist die für Einrichtung, Wartung, Betrieb und Abschaltung eines Systems zuständige Stelle.

„Tempest“-Schutzmaßnahmen (Transient Electromagnetic Pulse Emanation Standard) bezeichnen Sicherheitsmaßnahmen zum Schutz von Geräten und Kommunikationsinfrastruktur gegen die Preisgabe von Verschlusssachen durch unabsichtliche elektromagnetische Abstrahlung oder durch Leitfähigkeit.

25.3. **Zuständigkeiten im Sicherheitsbereich**

25.3.1. *Allgemeines*

Die beratenden Aufgaben der gemäß Abschnitt 12 eingesetzten Beratenden Gruppe für das Sicherheitskonzept der Kommission umfassen auch INFOSEC-Fragen. Die Gruppe organisiert ihre Tätigkeit so, dass sie zu den vorstehenden Punkten sachverständigen Rat geben kann.

Das Sicherheitsbüro der Kommission ist dafür zuständig, auf der Grundlage der Bestimmungen dieses Kapitels ausführliche INFOSEC-Bestimmungen aufzustellen.

Im Falle von Sicherheitsproblemen (Zwischenfälle, Verstoß gegen Vorschriften usw.) wird das Sicherheitsbüro der Kommission sofort tätig.

Das Sicherheitsbüro der Kommission hat ein INFOSEC-Referat.

25.3.2. *Akkreditierungsstelle für IT-Sicherheit (SAA)*

Der Leiter des Sicherheitsbüros der Kommission ist die Akkreditierungsstelle für IT-Sicherheit (SAA) für die Kommission. Die SAA ist zuständig im allgemeinen Sicherheitsbereich und in den Sonderbereichen INFOSEC, Kommunikationssicherheit, kryptografische Sicherheit und Tempest-Sicherheit.

Die SAA hat sicherzustellen, dass die Systeme dem Sicherheitskonzept der Kommission entsprechen. Sie hat unter anderem die Aufgabe, die Verarbeitung von EU-Verschlusssachen bis zu einem bestimmten Geheimhaltungsgrad mit dem betreffenden SYSTEM in seinem betrieblichen Umfeld zu genehmigen.

Die Zuständigkeit der SAA der Kommission erstreckt sich auf alle Systeme, die innerhalb der Räumlichkeiten der Kommission betrieben werden. Wenn unterschiedliche Bestandteile eines Systems in die Zuständigkeit der SAA der Kommission und anderer SAA fallen, können alle Parteien ein gemeinsames Akkreditierungsgremium einsetzen, dessen Koordinierung die SAA der Kommission übernimmt.

25.3.3. *INFOSEC-Stelle (IA)*

Der Leiter des INFOSEC-Referats des Sicherheitsbüros der Kommission ist die INFOSEC-Stelle für die Kommission. Die INFOSEC-Stelle ist für Folgendes verantwortlich:

— technische Beratung und Unterstützung der SAA,

— Unterstützung bei der Entwicklung der SSRS,

— Überprüfung der SSRS im Hinblick auf deren Konsistenz mit diesen Sicherheitsvorschriften und den Dokumenten betreffend die INFOSEC-Politik und -Architektur,

— gegebenenfalls Teilnahme an den Sitzungen der Akkreditierungsgremien bzw. -ausschüsse und Erstellung von INFOSEC-Empfehlungen für die SAA betreffend Akkreditierung,

— Unterstützung bei Schulungs- und Ausbildungsmaßnahmen im INFOSEC-Bereich,

— technische Beratung bei der Untersuchung von Zwischenfällen im INFOSEC-Bereich,

— Erstellung technischer strategischer Leitlinien, um sicherzustellen, dass nur zugelassene Software verwendet wird.

25.3.4. *Eigentümer des technischen Systems (TSO)*

Für die Implementierung und Kontrolle spezieller Sicherheitseigenschaften eines Systems ist der Eigentümer des betreffenden Systems, d.h. der Eigentümer des technischen Systems (TSO) zuständig. Bei zentral organisierten Systemen ist ein Beauftragter für die zentrale IT-Sicherheit (CISO) zu benennen. Jede Dienststelle benennt gegebenenfalls einen Beauftragten für die lokale IT-Sicherheit (LISO). Die Zuständigkeit eines TSO umfasst auch die Festlegung von sicherheitsbezogenen Betriebsverfahren (SecOPs) und erstreckt sich über die gesamte Lebensdauer eines Systems von der Konzeption des Projekts bis zur endgültigen Entsorgung.

Der TSO legt die Sicherheitsstandards und -verfahren fest, die vom Lieferanten des Systems eingehalten werden müssen.

Der TSO kann gegebenenfalls einen Teil seiner Zuständigkeiten an einen Beauftragten für die lokale IT-Sicherheit delegieren. Die verschiedenen INFOSEC-Aufgaben können von einer einzigen Person wahrgenommen werden.

25.3.5. *Eigentümer der Informationen (IO)*

Der Eigentümer der Informationen (IO) ist für EU-Verschlusssachen (und andere Daten), die in technische Systeme eingebracht bzw. in technischen Systemen verarbeitet und erstellt werden sollen, verantwortlich. Er legt die Anforderungen für den Zugang zu diesen Daten in Systemen fest. Er kann diese Zuständigkeit an einen Informationsmanager oder an einen Datenbankverwalter in seinem Bereich delegieren.

25.3.6. *Nutzer*

Alle Nutzer müssen sicherstellen, dass ihr Handeln die Sicherheit des von ihnen verwendeten Systems nicht beeinträchtigt.

25.3.7. *INFOSEC-Schulung*

INFOSEC-Ausbildung und -schulung wird allen Mitarbeitern geboten, die sie benötigen.

25.4. **Nichttechnische Sicherheitsmaßnahmen**

25.4.1. *Personalbezogene Sicherheit*

Nutzer des Systems müssen sich erfolgreich einer Sicherheitsüberprüfung unterzogen haben, die dem Geheimhaltungsgrad der in ihrem bestimmten System verarbeiteten Informationen entspricht, und sie müssen einen entsprechenden berechtigten Informationsbedarf haben. Der Zugang zu bestimmten Einrichtungen oder Informationen, die für die Systeme sicherheitsrelevant sind, erfordert eine besondere Ermächtigung, die gemäß den Verfahren der Kommission erteilt wird.

Die SAA benennt alle sicherheitskritischen Arbeitsplätze und legt fest, welcher Sicherheitsüberprüfung und Überwachung sich alle Personen an diesen Arbeitsplätzen unterziehen müssen.

Systeme werden so spezifiziert und konzipiert, dass die Zuweisung von Aufgaben und Zuständigkeiten erleichtert wird und dass vermieden wird, dass eine einzige Person umfassende Kenntnis oder Kontrolle über die für die Systemsicherheit entscheidenden Punkte erhält.

IT-Umgebungen und Umgebungen von dezentralen Terminals bzw. Datenstationen, in denen die Sicherheit des Systems beeinflusst werden kann, dürfen nicht mit nur einem befugten Beamten oder sonstigen Bediensteten besetzt werden.

Die Sicherheitseinstellungen eines Systems dürfen nur in Zusammenarbeit von mindestens zwei befugte Personen geändert werden.

25.4.2. *Materielle Sicherheit*

IT-Umgebungen und Umgebungen von dezentralen Terminals bzw. Datenstationen (gemäß Abschnitt 25.2), in denen als „EU — VERTRAULICH“ und höher eingestufte Informationen mit informationstechnischen Mitteln verarbeitet werden oder in denen der Zugriff auf solche Informationen potenziell möglich ist, werden je nach Sachlage als EU-Sicherheitsbereiche der Kategorie I oder II eingestuft.

25.4.3. *Kontrolle des Zugangs zu einem System*

Alle Informationen und jegliches Material, das die Kontrolle des Zugangs zu einem System ermöglicht, werden durch Vorkehrungen geschützt, die dem höchsten Geheimhaltungsgrad und der Kategorie von Informationen, zu denen sie Zugang gewähren könnten, entsprechen.

Informationen und Material zur Zugangskontrolle werden gemäß Abschnitt 25.5.4 vernichtet, wenn sie nicht mehr zu diesem Zweck verwendet werden.

25.5. **Technische Sicherheitsmaßnahmen**

25.5.1. *Informationssicherheit*

Der Urheber einer Information hat die Aufgabe, alle informationstragenden Dokumente zu identifizieren und ihnen einen Geheimhaltungsgrad zuzuordnen, unabhängig davon, ob sie als Papierausdruck oder auf einem elektronischen Datenträger vorliegen. Auf jeder Seite eines Papierausdrucks wird oben und unten der Geheimhaltungsgrad vermerkt. Jeder Ausgabe, ob als Papierausdruck oder auf einem elektronischen Datenträger, wird der höchste Geheimhaltungsgrad der zu ihrer Erstellung verarbeiteten Informationen zugeordnet. Die Betriebsart eines Systems kann den Geheimhaltungsgrad für Ausgaben dieses Systems ebenfalls beeinflussen.

Die Kommissionsdienststellen und ihre Informationsträger müssen sich mit der Problematik der Zusammenstellung einzelner Informationsbestandteile und den Schlussfolgerungen, die aus den miteinander verknüpften Bestandteilen gewonnen werden können, auseinander setzen und entscheiden, ob die Gesamtheit der Informationen höher eingestuft werden muss oder nicht.

Die Tatsache, dass die Information in einer Kurzform, als Übertragungscode oder in einer beliebigen binären Darstellung vorliegt, bietet keinen Schutz und sollte deshalb die Einstufung der Information nicht beeinflussen.

Wenn Informationen von einem System zu einem anderen übertragen werden, werden diese Informationen bei der Übertragung und im Empfängersystem entsprechend dem ursprünglichen Geheimhaltungsgrad und der ursprünglichen Kategorie geschützt.

Die Behandlung aller elektronischen Datenträger muss dem höchsten Geheimhaltungsgrad der gespeicherten Informationen bzw. der Datenträger-Kennzeichnung entsprechen; elektronische Datenträger müssen jederzeit angemessen geschützt werden.

Wieder verwendbare elektronische Datenträger, die zur Speicherung von EU-Verschlusssachen verwendet werden, behalten den höchsten Geheimhaltungsgrad bei, für den sie jemals verwendet wurden, bis diese Informationen ordnungsgemäß herabgestuft worden sind oder der Geheimhaltungsgrad aufgehoben wurde und der Datenträger entsprechend neu eingestuft beziehungsweise der Geheimhaltungsgrad aufgehoben oder durch ein von der SAA zugelassenes Verfahren vernichtet wurde (siehe 25.5.4).

25.5.2. *Kontrolle und Nachvollziehbarkeit in Bezug auf Informationen*

Der Zugriff auf Informationen, die als „EU — GEHEIM“ und höher eingestuft sind, wird automatisch („audit trails“) oder manuell protokolliert und dokumentiert. Die Protokolle werden im Einklang mit diesen Sicherheitsvorschriften aufbewahrt.

EU-Verschlusssachen, die als Ausgaben innerhalb der IT-Umgebung vorliegen, können als eine einzige Verschlusssache behandelt werden und brauchen nicht registriert zu werden, sofern sie in geeigneter Weise identifiziert, mit dem Geheimhaltungsgrad gekennzeichnet und angemessen kontrolliert werden.

Für die Fälle, in denen ein System, in dem EU-Verschlusssachen verarbeitet werden, Ausgaben erstellt und diese Ausgaben aus einer IT-Umgebung in die Umgebung von dezentralen Terminals bzw. Datenstationen übermittelt werden, werden — von der SAA genehmigte — Verfahren festgelegt, um die Ausgabe zu kontrollieren und aufzuzeichnen. Für Informationen, die als „EU — GEHEIM“ oder höher eingestuft sind, beinhalten diese Verfahren besondere Anweisungen für die Nachvollziehbarkeit in Bezug auf diese Informationen.

25.5.3. *Behandlung und Kontrolle von austauschbaren elektronischen Datenträgern*

Alle austauschbaren elektronischen Datenträger, die als „EU — VERTRAULICH“ und höher eingestuft sind, werden als Material angesehen und unterliegen den allgemeinen Regeln. Die Identifizierung und Kennzeichnung des Geheimhaltungsgrades muss an das besondere physische Erscheinungsbild der Datenträger angepasst werden, so dass diese eindeutig erkannt werden können.

Die Nutzer sind dafür verantwortlich, dass EU-Verschlusssachen auf Datenträgern gespeichert werden, die korrekt mit dem Geheimhaltungsgrad gekennzeichnet sind und angemessen geschützt werden. Um sicherzustellen, dass die Speicherung von Informationen auf elektronischen Datenträgern für alle EU-Geheimhaltungsgrade im Einklang mit diesen Sicherheitsvorschriften erfolgt, werden entsprechende Verfahren festgelegt.

25.5.4. *Freigabe und Vernichtung von elektronischen Datenträgern*

Elektronische Datenträger, die zur Speicherung von EU-Verschlusssachen verwendet werden, können herabgestuft werden oder ihr Geheimhaltungsgrad kann aufgehoben werden, sofern Verfahren angewandt werden, die von der SAA zugelassen sind.

Elektronische Datenträger, die Informationen des Geheimhaltungsgrades „EU — STRENG GEHEIM“ oder Informationen spezieller Kategorien enthalten haben, werden nicht freigegeben oder wiederverwendet.

Wenn elektronische Datenträger nicht freigegeben werden können oder nicht wiederverwendbar sind, werden sie nach dem obengenannten Verfahren vernichtet.

25.5.5. *Kommunikationssicherheit*

Der Leiter des Sicherheitsbüros der Kommission ist die Kryptografische Stelle.

Wenn EU-Verschlusssachen elektromagnetisch übermittelt werden, werden besondere Maßnahmen zum Schutz von Vertraulichkeit, Integrität und Verfügbarkeit solcher Übermittlungsvorgänge ergriffen. Die SAA legt die Anforderungen an den Schutz von Übermittlungsvorgängen vor Aufdeckungs- und Abhörmaßnahmen fest. Der Schutz von Informationen, die in einem Kommunikationssystem übermittelt werden, richtet sich nach den Anforderungen an die Vertraulichkeit, Integrität und Verfügbarkeit.

Wenn zum Schutz von Vertraulichkeit, Integrität und Verfügbarkeit kryptografische Methoden erforderlich sind, werden diese Methoden und die damit verbundenen Produkte speziell zu diesem Zweck von der SAA in ihrer Funktion als Kryptografische Stelle zugelassen.

Während der Übermittlung wird die Vertraulichkeit von als „EU — GEHEIM" und höher eingestuften Informationen durch kryptografische Methoden oder Produkte geschützt, die das für Sicherheitsfragen zuständige Mitglied der Kommission nach Konsultation der Beratenden Gruppe für das Sicherheitskonzept der Kommission zugelassen hat. Während der Übermittlung wird die Vertraulichkeit von als „EU — VERTRAULICH" oder „EU — NUR FÜR DEN DIENSTGEBRAUCH" eingestuften Informationen durch kryptografische Methoden oder Produkte geschützt, die die Kryptografische Stelle der Kommission nach Konsultation der Beratenden Gruppe für das Sicherheitskonzept der Kommission zugelassen hat.

Detaillierte Regeln für die Übermittlung von EU-Verschlusssachen werden in besonderen Sicherheitsanweisungen festgelegt, die das Sicherheitsbüro der Kommission nach Konsultation der Beratenden Gruppe für das Sicherheitskonzept der Kommission erlässt.

Unter außergewöhnlichen Betriebsbedingungen können Informationen der Geheimhaltungsgrade „EU — NUR FÜR DEN DIENSTGEBRAUCH", „EU — VERTRAULICH" und „EU — GEHEIM" als Klartext übermittelt werden, sofern dies in jedem einzelnen Fall vom Eigentümer der Informationen ausdrücklich genehmigt und ordnungsgemäß registriert wird. Solche außergewöhnlichen Bedingungen sind gegeben

a) während einer drohenden oder aktuellen Krisen-, Konflikt- oder Kriegssituation und

b) wenn die Schnelligkeit der Zustellung von vordringlicher Bedeutung ist und keine Verschlüsselungsmittel verfügbar sind und wenn davon ausgegangen wird, dass die übermittelte Information nicht rechtzeitig dazu missbraucht werden kann, Vorgänge negativ zu beeinflussen.

Ein System muss in der Lage sein, bei Bedarf den Zugriff auf EU-Verschlusssachen an einzelnen oder allen seiner dezentralen Datenstationen bzw. Terminals zu verweigern, und zwar entweder durch eine physische Abschaltung oder durch spezielle, von der SAA genehmigte Softwarefunktionen.

25.5.6. *Sicherheit der Installation und Sicherheit vor Abstrahlung*

Die Erstinstallation von Systemen und nachfolgende größere Änderungen werden so geregelt, dass die Arbeiten von sicherheitsüberprüften Personen durchgeführt und ständig durch technisch qualifiziertes Personal überwacht werden, das zum Zugang zu EU-Verschlusssachen des höchsten im System voraussichtlich gespeicherten und verarbeiteten Geheimhaltungsgrades ermächtigt ist.

Systeme, in denen als „EU — VERTRAULICH" und höher eingestufte Informationen verarbeitet werden, werden so geschützt, dass ihre Sicherheit nicht durch kompromittierende Abstrahlung oder Leitfähigkeit bedroht werden kann, wobei entsprechende Analyse- und Kontrollmaßnahmen als „TEMPEST" bezeichnet werden.

Tempest-Schutzmaßnahmen werden von der Tempest-Stelle (siehe Abschnitt 25.3.2) überprüft und genehmigt.

25.6. **Sicherheit bei der Verarbeitung**

25.6.1. *Sicherheitsbezogene Betriebsverfahren (SecOPs)*

In den sicherheitsbezogenen Betriebsverfahren (SecOPs) werden die in Sicherheitsfragen geltenden Grundsätze, die einzuhaltenden Betriebsverfahren sowie die Zuständigkeiten des Personals festgelegt. Für die Erstellung der sicherheitsbezogenen Betriebsverfahren ist der Eigentümer des technischen Systems (TSO) verantwortlich.

25.6.2. *Softwareschutz und Konfigurationsmanagement*

Der Schutz von Anwendungsprogrammen wird auf der Grundlage einer Bewertung der Sicherheitseinstufung des Programms selbst festgelegt, und nicht aufgrund der Einstufung der zu verarbeitenden Informationen. Die benutzten Software-Versionen sollten in regelmäßigen Abständen überprüft werden, um ihre Integrität und korrekte Funktion sicherzustellen.

Neue oder geänderte Versionen einer Software sollten erst für die Verarbeitung von EU-Verschlusssachen benutzt werden, wenn sie vom TSO geprüft worden sind.

25.6.3. *Prüfung auf das Vorhandensein von Programmen mit Schadensfunktionen und von Computerviren*

Die Prüfung auf das Vorhandensein von Programmen mit Schadensfunktionen und von Computerviren wird regelmäßig und im Einklang mit den Anforderungen der SAA durchgeführt.

Alle elektronischen Datenträger, die bei der Kommission eingehen, sind auf das Vorhandensein von Programmen mit Schadensfunktionen und von Computerviren zu überprüfen, bevor sie in ein System eingebracht werden.

25.6.4. *Wartung*

In Verträgen und Verfahrensanweisungen für die planmäßige und außerplanmäßige Wartung von Systemen, für die eine SSRS erstellt worden ist, werden Anforderungen und Vorkehrungen für den Zutritt von Wartungspersonal zu einer IT-Umgebung und für die zugehörige Wartungsausrüstung festgelegt.

Die Anforderungen werden in der SSRS und die Verfahren in den SecOPs präzise festgelegt. Wartungsarbeiten durch einen Auftragnehmer, die Diagnoseverfahren mit Fernzugriff erfordern, sind nur unter außergewöhnlichen Umständen und unter strenger Sicherheitskontrolle und nur nach Genehmigung durch die SAA zulässig.

25.7. **Beschaffungswesen**

25.7.1. *Allgemeines*

Jedes zu beschaffende Sicherheitsprodukt, das zusammen mit dem System verwendet werden soll, sollte auf der Grundlage international anerkannter Kriterien (wie z. B. Common Criteria for Information Technology Security Evaluation, ISO 15408) entweder bereits evaluiert und zertifiziert sein oder sich in der Phase der Evaluation und Zertifizierung durch eine geeignete Evaluations- und Zertifizierungsstelle eines der Mitgliedstaaten befinden. Für besondere Verfahren ist die Genehmigung des Vergabebeirats einzuholen.

Bei der Überlegung, ob Ausrüstung, insbesondere elektronische Speichermedien, eher geleast als gekauft werden soll, ist zu berücksichtigen, dass diese Ausrüstung, sobald sie zur Verarbeitung von EU-Verschlusssachen verwendet wurde, nicht mehr aus einem angemessen sicheren Umfeld herausgegeben werden kann, ohne dass sie zuvor mit Zustimmung der SAA freigegeben worden ist, und dass diese Zustimmung eventuell nicht immer gegeben werden kann.

25.7.2. *Akkreditierung*

Alle Systeme, für die eine SSRS erstellt werden muss, müssen von der SAA akkreditiert werden, bevor EU-Verschlusssachen damit verarbeitet werden, und zwar auf der Grundlage der Angaben in der SSRS, in den SecOPs und in anderer relevanter Dokumentation. Teilsysteme und dezentrale Terminals bzw. Datenstationen werden als Teil aller Systeme akkreditiert, mit denen sie verbunden sind. Wenn ein System sowohl von der Kommission als auch von anderen Organisationen genutzt wird, nehmen die Kommission und die relevanten Sicherheitsstellen die Akkreditierung einvernehmlich vor.

Die Akkreditierung kann gemäß einer für das jeweilige System geeigneten und von der SAA definierten Akkreditierungsstrategie durchgeführt werden.

25.7.3. *Evaluation und Zertifizierung*

Vor der Akkreditierung werden in bestimmten Fällen die Sicherheitseigenschaften der Hardware, Firmware und Software eines Systems evaluiert und daraufhin zertifiziert, dass sie in der Lage sind, Informationen des beabsichtigten Geheimhaltungsgrades zu schützen.

Die Anforderungen für Evaluation und Zertifizierung werden in die Systemplanung einbezogen und in der SSRS präzise festgelegt.

Die Evaluation und Zertifizierung wird gemäß genehmigter Leitlinien und von technisch qualifiziertem und ausreichend sicherheitsüberprüftem Personal durchgeführt, das im Auftrag des TSO tätig wird.

Das betreffende Personal kann von einer benannten Evaluations- und Zertifizierungsstelle eines Mitgliedstaates oder dessen benannten Vertretern, z. B. einem fachkundigen und ermächtigten Vertragspartner, bereitgestellt werden.

Wenn die Systeme auf bestehenden, einzelstaatlich evaluierten und zertifizierten Computersicherheitsprodukten beruhen, kann die Evaluation und die Zertifizierung vereinfacht werden (z. B. durch Beschränkung auf Integrationsaspekte).

25.7.4. *Regelmäßige Überprüfung von Sicherheitseigenschaften zur Aufrechterhaltung der Akkreditierung*

Der TSO legt Verfahren für eine regelmäßige Kontrolle fest, durch die garantiert wird, dass alle Sicherheitseigenschaften des Systems noch ordnungsgemäß vorhanden sind.

Welche Änderungen eine neue Akkreditierung bzw. die vorherige Genehmigung durch die SAA erfordern, wird in der SSRS präzise festgelegt. Nach jeder Änderung, Instandsetzung oder Störung, die sich auf die Sicherheitseigenschaften des Systems ausgewirkt haben könnte, sorgt der TSO dafür, dass eine Überprüfung durchgeführt wird, um die korrekte Funktion der Sicherheitseigenschaften sicherzustellen. Eine Aufrechterhaltung der Akkreditierung des Systems hängt normalerweise vom zufrieden stellenden Ergebnis dieser Überprüfung ab.

Alle Systeme, die Sicherheitseigenschaften aufweisen, werden regelmäßig von der SAA kontrolliert oder überprüft. Bei Systemen, die Informationen des Geheimhaltungsgrades „EU — STRENG GEHEIM“ verarbeiten, werden die Kontrollen mindestens einmal jährlich durchgeführt.

25.8. **Zeitlich befristete oder gelegentliche Nutzung**

25.8.1. *Sicherheit von Mikrocomputern bzw. PCs*

Mikrocomputer bzw. PCs mit eingebauten Speicherplatten (oder anderen nichtflüchtigen Datenträgern), die als Einzelrechner oder in einem Netz betrieben werden, sowie tragbare Computer (z. B. tragbare PCs und Notebook-Computer) mit eingebauten Festplatten werden im selben Sinne wie Disketten oder andere austauschbare elektronische Datenträger als Speichermedium für Informationen eingestuft.

Der Schutz dieser Geräte muss in Bezug auf Zugang, Verarbeitung, Speicherung und Transport dem höchsten Geheimhaltungsgrad der jemals gespeicherten oder verarbeiteten Informationen entsprechen (bis zur Herabstufung oder Aufhebung des Geheimhaltungsgrades gemäß genehmigter Verfahren).

25.8.2. *Nutzung von privater IT-Ausrüstung für dienstliche Zwecke der Kommission*

Die Nutzung von privaten austauschbaren elektronischen Datenträgern, privater Software und IT-Hardware mit Speichermöglichkeit (z. B. PCs und tragbare Computer) zur Verarbeitung von EU-Verschlusssachen ist untersagt.

Private Hardware, Software und Speichermedien dürfen in Bereiche der Kategorien I oder II, in denen EU-Verschlusssachen verarbeitet werden, nur mit schriftlicher Genehmigung des Leiters des Sicherheitsbüros der Kommission verbracht werden. Diese Genehmigung kann nur ausnahmsweise aus technischen Gründen erteilt werden.

25.8.3. *Nutzung von IT-Ausrüstung eines Auftragnehmers oder eines Mitgliedstaats für dienstliche Zwecke der Kommission*

Die Nutzung von IT-Ausrüstung und Software eines Auftragnehmers für dienstliche Zwecke der Kommission kann vom Leiter des Sicherheitsbüros der Kommission erlaubt werden. Die Verwendung der IT-Ausrüstung und Software eines Mitgliedstaats kann ebenfalls erlaubt werden; in diesem Fall unterliegt die IT-Ausrüstung der jeweiligen Bestandskontrolle der Kommission. Wenn die IT-Ausrüstung zur Verarbeitung von EU-Verschlusssachen verwendet werden soll, wird in jedem Fall die SAA konsultiert, damit die INFOSEC-Aspekte, die auf die Nutzung dieser Ausrüstung anwendbar sind, angemessen berücksichtigt und umgesetzt werden.

26. WEITERGABE VON EU-VERSCHLUSSSACHEN AN DRITTSTAATEN ODER INTERNATIONALE ORGANISATIONEN

26.1.1. *Grundsätze für die Weitergabe von EU-Verschlusssachen*

Über die Weitergabe von EU-Verschlusssachen an Drittstaaten oder internationale Organisationen beschließt die Kommission als Kollegium nach Maßgabe

— von Art und Inhalt dieser Verschlusssachen;

— des Grundsatzes „Kenntnis notwendig“;

— der Vorteile für die EU.

Der Urheber der EU-Verschlusssache, die weitergegeben werden soll, wird um Zustimmung ersucht.

Einschlägige Beschlüsse werden von Fall zu Fall gefasst und richten sich nach

— dem gewünschten Maß an Zusammenarbeit mit den betreffenden Drittstaaten oder internationalen Organisationen;

— deren Vertrauenswürdigkeit, die nach dem Geheimhaltungsgrad, der für die diesen Staaten oder Organisationen anvertrauten Verschlusssachen vorgesehen würde, und nach der Vereinbarkeit der dort geltenden Sicherheitsvorschriften mit den Sicherheitsvorschriften der EU zu bemessen ist; die Beratende Gruppe für das Sicherheitskonzept der Kommission gibt dazu für die Kommission ein technisches Gutachten ab.

Durch die Annahme von EU-Verschlusssachen verpflichten sich die betreffenden Drittstaaten oder internationalen Organisationen, die übermittelten Informationen nur zu den Zwecken zu verwenden, für die die Weitergabe oder der Austausch von Informationen beantragt worden ist, und den von der Kommission verlangten Schutz zu bieten.

26.1.2. *Kooperationsstufen*

Hat die Kommission beschlossen, die Weitergabe oder den Austausch von Verschlusssachen im Falle eines bestimmten Staates oder einer internationalen Organisation zu gestatten, so legt sie außerdem fest, wie weit diese Zusammenarbeit gehen kann. Dies hängt insbesondere von dem Sicherheitskonzept und den Sicherheitsvorschriften dieses Staates oder dieser Organisation ab.

Es gibt drei Kooperationsstufen:

Stufe 1

Zusammenarbeit mit Drittstaaten oder internationalen Organisationen, deren Sicherheitskonzept und -vorschriften sehr weitgehend mit denen der EU übereinstimmen;

Stufe 2

Zusammenarbeit mit Drittstaaten oder internationalen Organisationen, deren Sicherheitskonzept und -vorschriften deutlich von denen der EU abweichen;

Stufe 3

Gelegentliche Zusammenarbeit mit Drittstaaten oder internationalen Organisationen, deren Sicherheitskonzept und -vorschriften nicht eingeschätzt werden können.

Die in den Anhängen 3, 4 und 5 erläuterten Verfahren und Sicherheitsbestimmungen richten sich nach der jeweiligen Kooperationsstufe.

26.1.3. *Abkommen*

Beschließt die Kommission, dass ein ständiger oder langfristiger Austausch von Verschlusssachen zwischen der EU und Drittstaaten oder anderen internationalen Organisationen erforderlich ist, so arbeitet sie mit diesen „Abkommen über die Sicherheitsverfahren für den Austausch von Verschlusssachen" aus, die das Ziel der Zusammenarbeit und die gegenseitigen Vorschriften für den Schutz der ausgetauschten Informationen festlegen.

Für den Fall einer gelegentlichen Zusammenarbeit im Rahmen der Stufe 3, die per Definition zeitlich und sachlich begrenzt ist, kann eine einfache Vereinbarung, die die Art der auszutauschenden Verschlusssache und die gegenseitigen Verpflichtungen festlegt, an die Stelle des „Abkommens über die Sicherheitsverfahren für den Austausch von Verschlusssachen" treten, sofern die Verschlusssache nicht höher als „EU — NUR FÜR DEN DIENSTGEBRAUCH" eingestuft ist.

Die Entwürfe für Abkommen über die Sicherheitsverfahren oder für Vereinbarungen werden von der Beratenden Gruppe für das Sicherheitskonzept der Kommission erörtert, bevor sie der Kommission zur Entscheidung vorgelegt werden.

Das für Sicherheitsfragen zuständige Mitglied der Kommission ersucht die nationalen Sicherheitsbehörden der Mitgliedstaaten um die erforderliche Unterstützung, damit sichergestellt ist, dass die Informationen, die weitergegeben werden sollen, gemäß den Bestimmungen der Abkommen über die Sicherheitsverfahren oder der betreffenden Vereinbarungen genutzt und geschützt werden.

Anlage 1

VERGLEICHSTABELLE DER NATIONALEN SICHERHEITSEINSTUFUNGEN

EU-Einstufung	EU-STRENG GEHEIM	EU-GEHEIM	EU-VERTRAULICH	EU-NUR FÜR DEN DIENSTGEBRAUCH
NATO-Einstufung (1)				
WEU-Einstufung	Focal Top Secret	WEU SECRET	WEU CONFIDENTIAL	WEU RESTRICTED
Euratom-Einstufung (2)	EURATOM Top Secret	EURATOM Secret	EURATOM Confidential	EURATOM Restricted
Belgien	Très Secret Zeer Geheim	Secret Geheim	Confidentiel Vertrouwelijk	Diffusion restreinte Beperkte Verspreiding
Dänemark	Yderst hemmeligt	Hemmeligt	Fortroligt	Til tjenestebrug
Deutschland	STRENG GEHEIM	GEHEIM	VS (3) — VERTRAULICH	VS — NUR FÜR DEN DIENSTGEBRAUCH
Griechenland	Άκρως Απόρρητο	Απόρρητο	Εμπιστευτικό	Περιορισμένης χρήσης
Spanien	Secreto	Reservado	Confidencial	Difusión limitada
Frankreich	Très Secret Défense (4)	Secret Défense	Confidentiel Défense	Diffusion restreinte
Irland	Top Secret	Secret	Confidential	Restricted
Italien	Segretissimo	Segreto	Riservatissimo	Riservato
Luxemburg	Très Secret	Secret	Confidentiel	Diffusion restreinte
Niederlande	Stg. Zeer Geheim	Stg. Geheim	Stg. Confidentieel	
Österreich	Streng Geheim	Geheim	Vertraulich	Eingeschränkt
Portugal	Muito Secreto	Secreto	Confidencial	Reservado
Finnland	Erittäin salainen	Erittäin salainen	Salainen	Luottamuksellinen
Schweden	Kvalificerat hemlig	Hemlig	Hemlig	Hemlig
Vereinigtes Königreich	Top Secret	Secret	Confidential	Restricted

(1) NATO: Die Übereinstimmung mit den Einstufungskriterien der NATO wird bei der Aushandlung des Sicherheitsabkommens zwischen der Europäischen Union und der NATO hergestellt.
(2) Euratom: Verordnung Nr. 3 vom 31 Juli 1958 über den Schutz von Euratom-Verschlusssachen.
(3) Deutschland: VS = Verschlusssache.
(4) Frankreich: Die Einstufung „Très Secret Défense“, die für Regierungsprioritäten gilt, bedeutet, dass ein Austausch nur mit Zustimmung des Premierministers erfolgen darf.

Anlage 2

LEITFADEN FÜR DIE EINSTUFUNGSPRAXIS

Dieser Leitfaden hat lediglich Hinweischarakter und darf nicht im Sinne einer Änderung der Kernvorschriften der Abschnitte 16, 17, 20 und 21 ausgelegt werden.

Einstufung	Wann	Wer	Anbringung	Herabstufung/Aufhebung des Geheimhaltungsgrades/Vernichtung	
				Wer	Wann
EU — STRENG GEHEIM: Diese Einstufung ist nur bei Informationen und Materialien vorzunehmen, deren unbefugte Weitergabe den wesentlichen Interessen der Europäischen Union oder eines oder mehrerer ihrer Mitgliedstaaten außerordentlich schweren Schaden zufügen könnte [16.1].	Eine Kenntnisnahme durch Unbefugte würde bei Gegenständen mit der Einstufung „EU — STRENG GEHEIM“ wahrscheinlich Folgendes bewirken: — unmittelbare Gefährdung der inneren Stabilität der EU oder eines ihrer Mitgliedstaaten oder befreundeter Länder, — außerordentlich schwerwiegende Schädigung der Beziehungen zu befreundeten Regierungen, — unmittelbarer Verlust zahlreicher Menschenleben, — außerordentlich schwerwiegende Schädigung der Einsatzfähigkeit oder der Sicherheit von Streitkräften der Mitgliedstaaten oder anderer Partner bzw. der andauernden Wirksamkeit äußerst wertvoller Sicherheits- oder Intelligence-Operationen, — schwere und langfristige Schädigung der Wirtschaft der EU oder ihrer Mitgliedstaaten.	Förmlich dazu befugte Personen (Urheber), Generaldirektoren, Leiter von Diensten [17.1] Die Urheber bestimmen ein Datum, einen Zeitraum oder ein Ereignis, nach dessen Ablauf Inhalte herabgestuft oder deren Geheimhaltungsgrade aufgehoben werden können [16.2]. Andernfalls überprüfen sie spätestens alle fünf Jahre die betreffenden Dokumente, um sicherzustellen, dass die ursprüngliche Einstufung nach wie vor erforderlich ist [17.3].	Die Einstufung „EU — STRENG GEHEIM“ ist auf Dokumenten dieser Kategorie, gegebenenfalls mit einer Sicherheitskennung und/oder mit dem Zusatz „-ESVP“ bei Verteidigungssachen, mit mechanischen Mitteln oder von Hand anzubringen [16.4, 16.5, 16.3]. Die EU-Einstufungen und sonstigen Sicherheitskennungen müssen am oberen und am unteren Rand in der Mitte jeder Seite erscheinen, und jede Seite ist zu nummerieren. Jedes Dokument trägt ein Aktenzeichen und ein Datum; das Aktenzeichen wird auf jeder Seite angegeben. Soll eine Verteilung in mehreren Kopien erfolgen, so ist jede Kopie mit einer laufenden Nummer zu versehen, die auf der ersten Seite zusammen mit der Gesamtseitenzahl angegeben wird. Alle Anhänge und Beilagen sind auf der ersten Seite aufzuführen [21.1].	Eine Aufhebung des Geheimhaltungsgrades oder Herabstufung erfolgt ausschließlich durch den Urheber, der alle nachgeordneten Empfänger, denen das Original oder eine Kopie des Dokuments zugeleitet wurde, über die Änderung unterrichtet [17.3]. „EU — STRENG GEHEIM“-Dokumente werden durch die Zentralregistratur oder die für diese Dokumente zuständige Unterregistratur vernichtet. Jedes der Vernichtung zugeführte Dokument ist in einer Vernichtungsbescheinigung aufzuführen, die von dem für die Überwachung der „EU — STRENG GEHEIM“-Dokumente zuständigen Beamten und dem der Vernichtung als Zeuge beiwohnenden Beamten, der einer Sicherheitsüberprüfung für „EU — STRENG GEHEIM“-Dokumente unterzogen wurde, zu unterzeichnen ist. Der Vorgang ist im Dienstbuch festzuhalten. Die Vernichtungsbescheinigungen sind zusammen mit dem Verteilungsnachweis durch die Registratur zehn Jahre lang aufzubewahren [22.5].	Überzählige Exemplare und nicht länger benötigte Dokumente sind zu vernichten [22.5]. „EU — STRENG GEHEIM“-Dokumente einschließlich des bei ihrer Herstellung angefallenen und als Verschlusssache einzustufenden Zwischenmaterials, wie fehlerhafte Kopien, Arbeitsentwürfe, maschinenschriftliche Aufzeichnungen und Kohlepapier, sind unter der Aufsicht eines „EU — STRENG GEHEIM“-ermächtigten Beamten durch Verbrennen, Einstampfen, Zerkleinern oder andere geeignete Verfahren so zu vernichten, dass der Inhalt weder erkennbar ist noch erkennbar gemacht werden kann [22.5].

Einstufung	Wann	Wer	Anbringung	Herabstufung/Aufhebung des Geheimhaltungsgrades/Vernichtung	
				Wer	Wann
EU-GEHEIM: Diese Einstufung ist nur bei Informationen und Materialien vorzunehmen, deren unbefugte Weitergabe den wesentlichen Interessen der Europäischen Union oder eines oder mehrerer ihrer Mitgliedstaaten schweren Schaden zufügen könnte [16.1].	Eine Kenntnisnahme durch Unbefugte würde bei Gegenständen mit der Kennzeichnung „EU — GEHEIM“ wahrscheinlich Folgendes bewirken: — Hervorrufen internationaler Spannungen, — schwerwiegende Schädigung der Beziehungen zu befreundeten Regierungen, — unmittelbare Bedrohung von Leben oder schwerwiegende Beeinträchtigung der öffentlichen Ordnung oder der individuellen Sicherheit oder Freiheit, — schwerwiegende Schädigung der Einsatzfähigkeit oder der Sicherheit von Streitkräften der Mitgliedstaaten oder anderer Partner bzw. der andauernden Wirksamkeit sehr wertvoller Sicherheits- oder Intelligence-Operationen, — erhebliche materielle Schädigung der finanziellen, monetären, wirtschaftlichen und handelspolitischen Interessen der EU oder eines ihrer Mitgliedstaaten.	Befugte Personen (Urheber), Generaldirektoren, Leiter von Diensten [17.1]. Die Urheber bestimmen ein Datum oder einen Zeitraum, nach dessen Ablauf, Inhalte herabgestuft oder deren Geheimhaltungsgrade aufgehoben werden können [16.2]. Andernfalls überprüfen sie spätestens alle fünf Jahre die betreffenden Dokumente, um sicherzustellen, dass die ursprüngliche Einstufung weiterhin erforderlich ist [17.3].	Die Einstufung „EU — GEHEIM“ ist auf Dokumenten dieser Kategorie, gegebenenfalls mit einer Sicherheitskennung und/oder mit dem Zusatz „-ESVP“ bei Verteidigungssachen, mit mechanischen Mitteln oder von Hand anzubringen [16.4, 16.5, 16.3]. Die EU-Einstufungen und sonstigen Sicherheitskennungen müssen am oberen und am unteren Rand in der Mitte jeder Seite erscheinen, und jede Seite ist zu nummerieren. Jedes Dokument trägt ein Aktenzeichen und ein Datum; das Aktenzeichen wird auf jeder Seite angegeben. Soll eine Verteilung in mehreren Kopien erfolgen, so ist jede Kopie mit einer laufenden Nummer zu versehen, die auf der ersten Seite zusammen mit der Gesamtseitenzahl angegeben wird. Alle Anhänge und Beilagen sind auf der ersten Seite aufzuführen [21.1].	Eine Aufhebung des Geheimhaltungsgrades oder Herabstufung erfolgt ausschließlich durch den Urheber, der alle nachgeordneten Empfänger, denen das Original oder eine Kopie des Dokuments zugeleitet wurde, über die Änderung unterrichtet [17.3]. „EU — GEHEIM“-Dokumente werden von der für diese Dokumente zuständigen Registratur unter der Aufsicht einer sicherheitsüberprüften Person vernichtet. „EU — GEHEIM“-Dokumente, die vernichtet werden, sind auf Vernichtungsbescheinigungen aufzuführen, die zu unterzeichnen und zusammen mit dem Verteilungsnachweis durch die Registratur mindestens drei Jahre lang aufzubewahren sind [22.5].	Überzählige Exemplare und nicht länger benötigte Dokumente sind zu vernichten [22.5]. „EU — GEHEIM“-Dokumente einschließlich des bei ihrer Herstellung angefallenen und als Verschlusssache einzustufenden Zwischenmaterials, wie fehlerhafte Kopien, Arbeitsentwürfe, maschinenschriftliche Aufzeichnungen und Kohlepapier, sind durch Verbrennen, Einstampfen, Zerkleinern oder andere geeignete Verfahren so zu vernichten, dass der Inhalt weder erkennbar ist noch erkennbar gemacht werden kann [22.5].

Einstufung	Wann	Wer	Anbringung	Herabstufung/Aufhebung des Geheimhaltungsgrades/Vernichtung	
				Wer	Wann
EU-VERTRAULICH: Diese Einstufung ist bei Informationen und Materialien vorzunehmen, deren unbefugte Weitergabe den wesentlichen Interessen der Europäischen Union oder eines oder mehrerer ihrer Mitgliedstaaten abträglich wäre [16.1].	Eine Kenntnisnahme durch Unbefugte würde bei Gegenständen mit der Kennzeichnung „EU — VERTRAULICH“ wahrscheinlich Folgendes bewirken: — konkrete Schädigung diplomatischer Beziehungen in dem Sinne, dass förmliche Proteste oder andere Sanktionen hervorgerufen werden, — Beeinträchtigung individueller Sicherheit oder Freiheit, — Schädigung der Einsatzfähigkeit oder der Sicherheit von Streitkräften der Mitgliedstaaten oder anderer Partner bzw. der Wirksamkeit wertvoller Sicherheits- oder Intelligence-Operationen, — wesentliche Beeinträchtigung der finanziellen Tragfähigkeit wichtiger Organisationen, — Behinderung der Ermittlungstätigkeit oder Erleichterung des Begehens schwerer Straftaten, — wesentliche Beeinträchtigung der finanziellen, monetären, wirtschaftlichen und handelspolitischen Interessen der EU oder ihrer Mitgliedstaaten, — ernstliche Behinderung der Ausarbeitung oder Durchführung wichtiger EU-Politiken, — Abbruch oder erhebliche Unterbrechung wichtiger EU-Aktivitäten.	Befugte Personen (Urheber), Generaldirektoren, Leiter von Diensten [17.1]. Die Urheber bestimmen ein Datum oder einen Zeitraum, nach dessen Ablauf Inhalte herabgestuft oder deren Geheimhaltungsgrade aufgehoben werden können. Andernfalls überprüfen sie spätestens alle fünf Jahre die betreffenden Dokumente, um sicherzustellen, dass die ursprüngliche Einstufung weiterhin erforderlich ist [17.3].	Die Einstufung „EU — VERTRAULICH“ ist auf Dokumenten dieser Kategorie, gegebenenfalls mit einer Sicherheitskennung und/oder mit dem Zusatz „- ESVP“ bei Verteidigungssachen, mit mechanischen Mitteln oder von Hand anzubringen [16.4, 16.5, 16.3]. Die EU-Einstufungen müssen am oberen und am unteren Rand in der Mitte jeder Seite erscheinen, und jede Seite ist zu nummerieren. Jedes Dokument trägt ein Aktenzeichen und ein Datum. Alle Anhänge und Beilagen sind auf der ersten Seite aufzuführen [21.1].	Eine Aufhebung des Geheimhaltungsgrades oder Herabstufung erfolgt ausschließlich durch den Urheber, der alle nachgeordneten Empfänger, denen das Original oder eine Kopie des Dokuments zugeleitet wurde, über die Änderung unterrichtet [17.3]. „EU — VERTRAULICH“-Dokumente werden von der für diese Dokumente zuständigen Registratur unter der Aufsicht einer sicherheitsüberprüften Person vernichtet. Die Vernichtung der Dokumente ist gemäß den einzelstaatlichen Vorschriften bzw., im Falle der Kommission oder dezentraler EU-Einrichtungen, gemäß den Anweisungen des Präsidenten zu dokumentieren [22.5].	Überzählige Exemplare und nicht länger benötigte Dokumente sind zu vernichten [22.5]. „EU — VERTRAULICH“-Dokumente einschließlich des bei ihrer Herstellung angefallenen und als Verschlusssache einzustufenden Zwischenmaterials, wie fehlerhafte Kopien, Arbeitsentwürfe, maschinenschriftliche Aufzeichnungen und Kohlepapier, sind durch Verbrennen, Einstampfen, Zerkleinern oder andere geeignete Verfahren so zu vernichten, dass der Inhalt weder erkennbar ist noch erkennbar gemacht werden kann [22.5].

Einstufung	Wann	Wer	Anbringung	Herabstufung/Aufhebung des Geheimhaltungsgrades/Vernichtung	
				Wer	Wann
EU — NUR FÜR DEN DIENSTGEBRAUCH: Diese Einstufung ist bei Informationen und Materialien vorzunehmen, deren unbefugte Weitergabe sich auf die wesentlichen Interessen der Europäischen Union oder eines oder mehrerer ihrer Mitgliedstaaten nachteilig auswirken könnte [16.1].	Eine Kenntnisnahme durch Unbefugte würde bei Gegenständen mit der Kennzeichnung „EU — NUR FÜR DEN DIENSTGEBRAUCH“ wahrscheinlich Folgendes bewirken: — Belastung diplomatischer Beziehungen, — erhebliche Unannehmlichkeiten für Einzelpersonen, — Erschwerung der Wahrung der Einsatzfähigkeit oder der Sicherheit von Streitkräften der Mitgliedstaaten oder anderer Partner, — finanzielle Verluste oder die Ermöglichung ungerechtfertigter Gewinne oder Vorteile für Einzelpersonen oder Unternehmen, — Bruch eigener Verpflichtungen zur Wahrung der Vertraulichkeit von Informationen, die von dritter Seite erteilt wurden, — Verstoß gegen gesetzlich begründete Einschränkungen der Weitergabe von Informationen, — Beeinträchtigung der Ermittlungstätigkeit oder Erleichterung des Begehens schwerer Straftaten, — Benachteiligung der EU oder ihrer Mitgliedstaaten bei Verhandlungen mit Dritten über handelspolitische oder allgemein politische Fragen, — Behinderung der wirksamen Ausarbeitung oder Durchführung von EU-Politiken, — Gefährdung einer sachgerechten Verwaltung der EU und ihrer Tätigkeiten.	Befugte Personen (Urheber), Generaldirektoren, Leiter von Diensten [17.1]. Die Urheber bestimmen ein Datum, einen Zeitraum oder ein Ereignis, nach dessen Ablauf Inhalte herabgestuft oder deren Geheimhaltungsgrade aufgehoben werden können [16.2] Andernfalls überprüfen sie spätestens alle fünf Jahre die betreffenden Dokumente, um sicherzustellen, dass die ursprüngliche Einstufung nach wie vor erforderlich ist [17.3].	Die Einstufung „EU — NUR FÜR DEN DIENSTGEBRAUCH“ ist auf Dokumenten dieser Kategorie, gegebenenfalls mit einer Sicherheitskennung und/oder mit dem Zusatz „-ESVP“ bei Verteidigungssachen, mit mechanischen oder elektronischen Mitteln anzubringen [16.4, 16.5, 16.3]. Die EU-Einstufungen müssen am oberen und am unteren Rand in der Mitte jeder Seite erscheinen, und jede Seite ist zu nummerieren. Jedes Dokument trägt ein Aktenzeichen und ein Datum [21.1].	Eine Aufhebung des Geheimhaltungsgrades erfolgt ausschließlich durch den Urheber, der alle nachgeordneten Empfänger, denen das Original oder eine Kopie des Dokuments zugeleitet wurde, über die Änderung unterrichtet [17.3]. „EU — NUR FÜR DEN DIENSTGEBRAUCH“-Dokumente werden von der für diese Dokumente zuständigen Registratur gemäß den Weisungen des Präsidenten vernichtet [22.5].	Überzählige Exemplare und nicht länger benötigte Dokumente sind zu vernichten [22.5].

Anlage 3

LEITLINIEN FÜR DIE WEITERGABE VON EU-VERSCHLUSSSACHEN AN DRITTSTAATEN ODER INTERNATIONALE ORGANISATIONEN: KOOPERATIONSSTUFE 1

VERFAHREN

1. Für die Weitergabe von EU-Verschlusssachen an Länder, die nicht Mitglied der Europäischen Union sind, oder an andere internationale Organisationen, deren Sicherheitskonzept und -vorschriften mit denen der EU vergleichbar sind, ist die Kommission als Kollegium zuständig.

2. Bis zum Abschluss eines Geheimschutzabkommens sind Anträge auf Weitergabe von EU-Verschlusssachen durch das für Sicherheitsfragen zuständige Mitglied der Kommission zu prüfen.

3. Das Mitglied der Kommission
   — holt die Stellungnahme der Urheber der EU-Verschlusssache ein, welche weitergegeben werden soll;
   — knüpft die nötigen Kontakte zu den Sicherheitsbehörden der als Empfänger vorgesehenen Länder oder internationalen Organisationen, um zu prüfen, ob deren Sicherheitskonzept und -vorschriften gewährleisten können, dass die weitergegebenen Verschlusssachen gemäß diesen Sicherheitsvorschriften geschützt werden;
   — fordert ein Gutachten der Beratenden Gruppe für das Sicherheitskonzept der Kommission hinsichtlich der Vertrauenswürdigkeit der als Empfänger vorgesehenen Länder oder internationalen Stellen an.

4. Das für Sicherheitsfragen zuständige Mitglied der Kommission legt der Beratenden Gruppe für das Sicherheitskonzept der Kommission den Antrag zur Entscheidung vor.

VON DEN EMPFÄNGERN EINZUHALTENDE SICHERHEITSVORSCHRIFTEN

5. Das für Sicherheitsfragen zuständige Mitglied der Kommission stellt den als Empfänger vorgesehenen Ländern oder internationalen Organisationen den Beschluss der Kommission zur Genehmigung der Weitergabe von EU-Verschlusssachen zu.

6. Der Weitergabebeschluss tritt nur dann in Kraft, wenn die Empfänger sich schriftlich verpflichten,
   — die Informationen nur zu den vereinbarten Zwecken zu nutzen;
   — die Informationen gemäß diesen Sicherheitsvorschriften und insbesondere unter Einhaltung der nachfolgenden speziellen Bestimmungen zu schützen.

7. Personal

   a) Die Zahl der Bediensteten, die Zugang zu EU-Verschlusssachen erhalten, beschränkt sich nach dem Grundsatz „Kenntnis notwendig“ strikt auf die Personen, deren Aufgabenstellung diesen Zugang erfordert.

   b) Alle Bediensteten oder Staatsangehörigen, denen der Zugang zu Informationen des Geheimhaltungsgrades „EU — VERTRAULICH“ oder darüber gestattet wird, müssen Inhaber einer für die betreffende Stufe gültigen Sicherheitsunbedenklichkeitsbescheinigung oder einer entsprechenden Sicherheitsermächtigung sein, wobei diese Sicherheitsunbedenklichkeitsbescheinigung oder die Ermächtigung von der Regierung ihres eigenen Staates ausgestellt beziehungsweise erteilt wird.

8. Übermittlung von Dokumenten

   a) Die praktischen Verfahren für die Übermittlung von Dokumenten werden durch ein Abkommen festgelegt. Bis zum Abschluss dieses Abkommens gelten die Bestimmungen des Abschnitts 21. Darin wird insbesondere die Registratur angeführt, an die EU-Verschlusssachen weitergegeben werden sollen.

   b) Umfassen die Verschlusssachen, deren Weitergabe von der Kommission genehmigt wird, Informationen der Stufe „EU — STRENG GEHEIM“, so richtet der Empfänger ein EU-Zentralregister und gegebenenfalls EU-Unterregister ein. Für diese Register gelten die Bestimmungen des Abschnitts 22 dieser Sicherheitsvorschriften.

9. Registrierung

   Sobald eine Registratur ein als „EU — VERTRAULICH“ oder höher eingestuftes EU-Dokument erhält, trägt sie dieses Dokument in einem eigens dafür angelegten Register ihrer Organisation ein; dieses Register umfasst Spalten, in denen das Eingangsdatum, die Bestimmungsmerkmale des Dokuments (Datum, Aktenzeichen und Nummer des Exemplars), sein Geheimhaltungsgrad, sein Titel, der Name oder Titel des Empfängers, das Rücksendedatum der Empfangsbestätigung und das Datum, zu dem das Dokument an den EU-Urheber zurückgesandt oder vernichtet wird, zu verzeichnen sind.

10. Vernichtung

a) EU-Verschlusssachen sind gemäß den Anweisungen des Abschnitts 22 dieser Sicherheitsvorschriften zu vernichten. Bei Dokumenten der Stufen „EU — GEHEIM“ und „EU — STRENG GEHEIM“ sind Kopien der Vernichtungsbescheinigungen an die EU-Registratur zu senden, von der die Dokumente übermittelt wurden.

b) EU-Verschlusssachen sind in die Notfall-Vernichtungspläne einzubeziehen, die die zuständigen Stellen des Empfängers für ihre eigenen Verschlusssachen aufgestellt haben.

11. Schutz der Dokumente

Es sind alle erforderlichen Maßnahmen zu ergreifen, damit Unbefugte keinen Zugang zu EU-Verschlusssachen erhalten.

12. Kopien, Übersetzungen und Auszüge

Fotokopien, Übersetzungen oder Auszüge eines als „EU — VERTRAULICH“ oder „EU — GEHEIM“ eingestuften Dokuments dürfen nur mit Genehmigung des Leiters des betreffenden Sicherheitsorgans angefertigt werden, der diese Kopien, Übersetzungen oder Auszüge registriert und prüft und nötigenfalls mit einem Stempel versieht.

Die Vervielfältigung oder Übersetzung eines Dokuments der Stufe „EU — STRENG GEHEIM“ kann nur von der Behörde genehmigt werden, von der das Dokument stammt; sie legt die Anzahl der zulässigen Exemplare fest; kann die Behörde, von der das Dokument stammt, nicht ermittelt werden, so ist der Antrag an den Sicherheitsdienst der Kommission zu richten.

13. Verstöße gegen die Sicherheitsvorschriften

Bei Verstößen gegen die Sicherheitsvorschriften im Zusammenhang mit einer EU-Verschlusssache oder bei einem entsprechenden Verdacht sollten vorbehaltlich des Abschlusses eines Geheimschutzabkommens unverzüglich folgende Schritte unternommen werden:

a) Einleitung einer Untersuchung zur Klärung der Umstände des Verstoßes gegen die Sicherheitsvorschriften;

b) Benachrichtigung des Sicherheitsdienstes der Kommission und der zuständigen nationalen Sicherheitsbehörde sowie der Behörde, von der die Informationen stammen, oder aber gegebenenfalls eindeutige Mitteilung, dass die letztgenannte Behörde nicht benachrichtigt wurde;

c) Ergreifen von Maßnahmen, damit die Folgen eines Verstoßes gegen die Sicherheitsvorschriften so weit wie möglich eingeschränkt werden;

d) erneute Prüfung und Durchführung von Maßnahmen, damit sich der Vorfall nicht wiederholt;

e) Durchführung der vom Sicherheitsbüro der Kommission empfohlenen Maßnahmen, damit sich der Vorfall nicht wiederholt.

14. Inspektionen

Der Sicherheitsdienst der Kommission kann im Benehmen mit den betreffenden Staaten oder internationalen Organisationen eine Bewertung der Effizienz der Maßnahmen zum Schutz der weitergegebenen EU-Verschlusssachen vornehmen.

15. Berichterstattung

Solange Staaten oder internationale Organisationen EU-Verschlusssachen aufbewahren, erstellen sie vorbehaltlich des Abschlusses eines Geheimschutzabkommens jährlich zu dem Datum, das in der Genehmigung zur Informationsweitergabe angegeben ist, einen Bericht, mit dem bestätigt wird, dass diese Sicherheitsvorschriften eingehalten wurden.

Anlage 4

LEITLINIEN FÜR DIE WEITERGABE VON EU-VERSCHLUSSSACHEN AN DRITTSTAATEN ODER INTERNATIONALE ORGANISATIONEN: KOOPERATIONSSTUFE 2

VERFAHREN

1. Für die Weitergabe von EU-Verschlusssachen an Drittstaaten oder internationale Organisationen, deren Sicherheitskonzept und -vorschriften deutlich von denen der EU abweichen, ist der Urheber zuständig. Für die Weitergabe von EU-Verschlusssachen, die von der Kommission stammen, ist die Kommission als Kollegium zuständig.

2. Prinzipiell ist die Weitergabe auf Informationen bis einschließlich des Geheimhaltungsgrades „EU — GEHEIM" beschränkt; ausgenommen sind Verschlusssachen, die durch besondere Sicherheitskennungen oder -zusätze geschützt sind.

3. Bis zum Abschluss eines Geheimschutzabkommens sind Anträge auf Weitergabe von EU-Verschlusssachen durch das für Sicherheitsfragen zuständige Mitglied der Kommission zu prüfen.

4. Das Mitglied der Kommission:
   — holt die Stellungnahme der Urheber der EU-Verschlusssache ein, welche weitergegeben werden soll;
   — knüpft die erforderlichen Kontakte zu den Sicherheitsbehörden der als Empfänger vorgesehenen Länder oder internationalen Organisation, um Informationen über deren Sicherheitskonzept und -vorschriften einzuholen, und insbesondere eine Vergleichstabelle der in der EU und in den betreffenden Staaten oder Organisationen geltenden Geheimhaltungsgrade zu erstellen;
   — beruft eine Sitzung der Beratenden Gruppe für das Sicherheitskonzept der Kommission ein oder ersucht, falls erforderlich im Wege des vereinfachten schriftlichen Verfahrens, die nationalen Sicherheitsbehörden der Mitgliedstaaten um Prüfung im Hinblick auf ein Gutachten der Beratenden Gruppe für das Sicherheitskonzept der Kommission.

5. In dem Gutachten äußert sich die Beratende Gruppe für das Sicherheitskonzept der Kommission zu folgenden Aspekten:
   — Vertrauenswürdigkeit der als Empfänger vorgesehenen Staaten oder internationalen Organisationen im Hinblick auf eine Bewertung der für die EU oder deren Mitgliedstaaten bestehenden Sicherheitsrisiken;
   — Bewertung der Fähigkeit des Empfängers, von der EU weitergegebene Verschlusssachen zu schützen;
   — Vorschläge für die praktische Behandlung der EU-Verschlusssachen (beispielsweise Übermittlung bearbeiteter Textfassungen) und der übermittelten Dokumente (Beibehaltung oder Streichung von EU-Einstufungsvermerken, besonderen Kennzeichnungen usw.);
   — Herabstufung oder Aufhebung des Geheimhaltungsgrades, bevor die Informationen an die als Empfänger vorgesehenen Länder oder internationalen Organisationen weitergegeben werden.

6. Das für Sicherheitsfragen zuständige Mitglied der Kommission legt der Kommission den Antrag sowie das Gutachten der Beratenden Gruppe für das Sicherheitskonzept der Kommission zur Entscheidung vor.

VON DEN EMPFÄNGERN EINZUHALTENDE SICHERHEITSVORSCHRIFTEN

7. Das für Sicherheitsfragen zuständige Mitglied der Kommission unterrichtet die als Empfänger vorgesehenen Länder oder internationalen Organisationen über den Beschluss der Kommission zur Genehmigung der Weitergabe von EU-Verschlusssachen und die entsprechenden Einschränkungen.

8. Der Weitergabebeschluss tritt nur dann in Kraft, wenn die Empfänger sich schriftlich verpflichten,
   — die Informationen nur zu den vereinbarten Zwecken zu nutzen;
   — die Informationen gemäß den Sicherheitsvorschriften der Kommission zu schützen.

9. Es werden folgende Schutzvorschriften festgelegt, sofern nicht die Kommission nach Einholung des technischen Gutachtens der Beratenden Gruppe für das Sicherheitskonzept der Kommission ein besonderes Verfahren (Streichung des Einstufungsvermerks, der besonderen Kennzeichnung usw.) für die Behandlung von EU-Verschlusssachen vorsieht.

10. Personal

    a) Die Zahl der Bediensteten, die Zugang zu EU-Verschlusssachen erhalten, beschränkt sich nach dem Grundsatz „Kenntnis notwendig" strikt auf die Personen, deren Aufgabenstellung diesen Zugang erfordert.

    b) Alle Bediensteten oder Staatsangehörigen, denen der Zugang zu von der Kommission weitergegebenen Verschlusssachen gestattet wird, müssen Inhaber einer nationalen Sicherheitsunbedenklichkeitsbescheinigung oder einer Zugangsermächtigung für den Fall nationaler Verschlusssachen, auf einer entsprechenden und der EU-Einstufung gemäß der Vergleichstabelle gleichwertigen Stufe sein.

    c) Diese nationalen Sicherheitsunbedenklichkeitsbescheinigungen oder Zugangsermächtigungen werden vom Präsidenten zur Information mitgeteilt.

11. Übermittlung von Dokumenten

Die praktischen Verfahren für die Übermittlung von Dokumenten werden durch ein Abkommen festgelegt. Bis zum Abschluss dieses Abkommens gelten die Bestimmungen des Abschnitts 21. Darin wird insbesondere die Registratur angeführt, an die EU-Verschlusssachen weitergegeben werden sollen, sowie die genaue Anschrift, an die die Dokumente zuzustellen sind, und der Kurier- oder Postdienst, der für die Übermittlung von EU-Verschlusssachen eingesetzt wird.

12. Registrierung am Bestimmungsort

Die nationale Sicherheitsbehörde des Empfängerstaats, die ihr gleichzusetzende Stelle, die in diesem Staat im Auftrag ihrer Regierung die von der Kommission weitergegebene Verschlusssache in Empfang nimmt, oder das Sicherheitsbüro der als Empfänger vorgesehenen internationalen Organisation legt ein spezielles Register für EU-Verschlusssachen an und registriert diese, sobald sie dort eingehen. Dieses Register umfasst Spalten, in denen das Eingangsdatum, die Bestimmungsmerkmale des Dokuments (Datum, Aktenzeichen und Nummer des Exemplars), sein Geheimhaltungsgrad, sein Titel, der Name oder Titel des Empfängers, das Rücksendedatum der Empfangsbescheinigung und das Datum, zu dem das Dokument an die EU zurückgesandt oder vernichtet wird, zu verzeichnen sind.

13. Rücksendung von Dokumenten

Bei Rücksendung einer Verschlusssache durch den Empfänger an die Kommission ist das unter der Rubrik „Übermittlung von Dokumenten“ beschriebene Verfahren zu befolgen.

14. Schutz der Dokumente

a) Nicht benutzte Dokumente sind in einem Sicherheitsbehältnis aufzubewahren, das für die Aufbewahrung nationaler Verschlusssachen desselben Geheimhaltungsgrades zugelassen ist. Das Behältnis darf keine Angaben tragen, die Aufschluss über seinen Inhalt geben könnten; dieser Inhalt ist nur den Personen zugänglich, die zur Behandlung von EU-Verschlusssachen ermächtigt sind. Wenn Kombinationsschlösser verwendet werden, so darf die Kombination nur den Bediensteten des Staates oder der Organisation bekannt sein, denen der Zugang zu der in dem Behältnis aufbewahrten EU-Verschlusssache gestattet ist; die Kombination ist alle sechs Monate oder - bei Versetzung eines Bediensteten, bei Entzug der Sicherheitsermächtigung für einen der Bediensteten, denen die Kombination bekannt ist, oder bei Gefahr der Verletzung des Kombinationsgeheimnisses - früher zu ändern.

b) EU-Verschlusssachen dürfen aus dem Sicherheitsbehältnis nur von Bediensteten entnommen werden, die aufgrund einer Sicherheitsüberprüfung zum Zugang zu EU-Verschlusssachen ermächtigt sind und eine Kenntnisnahme benötigen. Solange die Dokumente in ihrem Besitz sind, tragen die Bediensteten die Verantwortung für deren sichere Aufbewahrung und insbesondere dafür, dass Unbefugte keinen Zugang zu den Dokumenten erhalten. Sie sorgen außerdem dafür, dass die Dokumente nach erfolgter Einsichtnahme sowie außerhalb der Arbeitszeiten in einem Sicherheitsbehältnis aufbewahrt werden.

c) Fotokopien von bzw. Auszüge aus als „EU — VERTRAULICH“ oder darüber eingestuften Dokumenten dürfen nur mit Genehmigung des Sicherheitsbüros der Kommission angefertigt werden.

d) Das Verfahren zur raschen und vollständigen Vernichtung der Dokumente im Notfall sollte im Benehmen mit dem Sicherheitsbüro der Kommission festgelegt und bestätigt werden.

15. MATERIELLE SICHERHEIT

a) Nicht benutzte Sicherheitsbehältnisse, die zur Aufbewahrung von EU-Verschlusssachen dienen, sind stets verschlossen zu halten.

b) Wartungs- oder Reinigungspersonal, das einen Raum betritt, in dem solche Sicherheitsbehältnisse untergebracht sind, oder dort arbeitet, muss stets von einem Angehörigen des Sicherheitsdienstes des Staates oder der Organisation oder von dem Bediensteten begleitet werden, der speziell für die Sicherheitsaufsicht über diesen Raum verantwortlich ist.

c) Außerhalb der normalen Arbeitszeiten (nachts, an Wochenenden oder Feiertagen) sind die Sicherheitsbehältnisse, die EU-Verschlusssachen enthalten, entweder durch einen Wachbeamten oder durch ein automatisches Alarmsystem zu sichern.

16. Verstöße gegen die Sicherheitsvorschriften

Bei Verstößen gegen die Sicherheitsvorschriften im Zusammenhang mit einer EU-Verschlusssache oder bei einem entsprechenden Verdacht, sollten unverzüglich folgende Schritte unternommen werden:

a) sofortige Übermittlung eines Berichts an das Sicherheitsbüro der Kommission oder an die nationale Sicherheitsbehörde des Mitgliedstaats, der die Initiative zur Übermittlung von Dokumenten ergriffen hat (mit einer Abschrift an das Sicherheitsbüro der Kommission);

b) Einleitung einer Untersuchung und nach deren Abschluss Übermittlung eines umfassenden Berichts an die Sicherheitsstelle (siehe Buchstabe a)). Anschließend sollten die nötigen Maßnahmen ergriffen werden, um Abhilfe zu schaffen.

17. Inspektionen

Das Sicherheitsbüro der Kommission kann im Benehmen mit den betreffenden Staaten oder internationalen Organisationen eine Bewertung der Effizienz der Maßnahmen zum Schutz der weitergegebenen EU-Verschlusssachen vornehmen.

18. Berichterstattung

Solange Staaten oder internationale Organisationen EU-Verschlusssachen aufbewahren, erstellen sie vorbehaltlich des Abschlusses eines Geheimschutzabkommens jährlich zu dem Datum, das in der Genehmigung zur Informationsweitergabe angegeben ist, einen Bericht, mit dem bestätigt wird, dass diese Sicherheitsvorschriften eingehalten wurden.

Anlage 5

LEITLINIEN FÜR DIE WEITERGABE VON EU-VERSCHLUSSSACHEN AN DRITTSTAATEN ODER INTERNATIONALE ORGANISATIONEN: KOOPERATIONSSTUFE 3

VERFAHREN

1. Es kann gelegentlich vorkommen, dass die Kommission unter bestimmten Umständen mit Staaten oder Organisationen zusammenarbeiten möchte, die die von diesen Sicherheitsvorschriften verlangten Garantien nicht bieten können; eine solche Zusammenarbeit kann jedoch die Weitergabe von EU-Verschlusssachen erforderlich machen.

2. Für die Weitergabe von EU-Verschlusssachen an Drittstaaten oder internationale Organisationen, deren Sicherheitskonzept und -vorschriften deutlich von denen der EU abweichen, ist der Urheber zuständig. Für die Weitergabe von EU-Verschlusssachen, die von der Kommission stammen, ist die Kommission als Kollegium zuständig.

   Prinzipiell ist die Weitergabe auf Informationen bis einschließlich des Geheimhaltungsgrades „EU — GEHEIM" beschränkt; ausgenommen sind Verschlusssachen, die durch besondere Sicherheitskennungen oder -zusätze geschützt sind.

3. Die Kommission prüft die Ratsamkeit einer Weitergabe von Verschlusssachen, bewertet, inwieweit der Empfänger Kenntnis von diesen Informationen haben muss, und beschließt, welche Kategorien von Verschlusssachen übermittelt werden können.

4. Spricht sich die Kommission für eine Weitergabe von Informationen aus, so unternimmt das für Sicherheitsfragen zuständige Mitglied der Kommission Folgendes. Es
   — holt die Stellungnahme der Urheber der EU-Verschlusssache ein, welche weitergegeben werden soll;
   — beruft eine Sitzung der Beratenden Gruppe für das Sicherheitskonzept der Kommission ein oder ersucht, falls erforderlich im Wege des vereinfachten schriftlichen Verfahrens, die nationalen Sicherheitsbehörden der Mitgliedstaaten um Prüfung im Hinblick auf ein Gutachten der Beratenden Gruppe für das Sicherheitskonzept der Kommission.

5. In ihrem Gutachten äußert sich die Beratende Gruppe für das Sicherheitskonzept der Kommission zu folgenden Aspekten:

   a) Einschätzung der für die EU oder ihre Mitgliedstaaten bestehenden Sicherheitsrisiken;

   b) Geheimhaltungsgrad der Informationen, die weitergegeben werden können;

   c) Herabstufung oder Aufhebung des Geheimhaltungsgrads, bevor die Informationen weitergegeben werden;

   d) Behandlung der Dokumente, die weitergegeben werden sollen (s. unten);

   e) mögliche Übermittlungswege (mit dem öffentlichen Postdienst, über öffentliche oder sichere Telekommunikationssysteme, mit Diplomatenpost, sicherheitsüberprüften Kurieren, usw.).

6. Dokumente, die an Staaten oder Organisationen weitergegeben werden, die unter diesen Anhang fallen, werden prinzipiell ohne Bezugnahme auf die Quelle oder eine EU-Einstufung erstellt. Die Beratende Gruppe für das Sicherheitskonzept der Kommission kann empfehlen,
   — eine besondere Kennzeichnung oder einen Codenamen zu verwenden;
   — ein spezielles Einstufungssystem zu verwenden, bei dem die Sensibilität der Informationen im Zusammenhang mit den Kontrollmaßnahmen gesehen wird, die aufgrund der vom Empfänger befolgten Methoden für die Übermittlung von Dokumenten erforderlich werden.

7. Der Präsident legt der Kommission das Gutachten der Beratenden Gruppe für das Sicherheitskonzept der Kommission zur Entscheidung vor.

8. Hat die Kommission die Weitergabe von EU-Verschlusssachen beschlossen und die praktischen Durchführungsverfahren festgelegt, knüpft das Sicherheitsbüro der Kommission die nötigen Kontakte mit der Sicherheitsbehörde der betreffenden Staaten oder Organisationen, um die Anwendung der geplanten Sicherheitsmaßnahmen zu erleichtern.

9. Das für Sicherheitsfragen zuständige Mitglied der Kommission unterrichtet die Mitgliedstaaten über Art und Einstufung der Informationen sowie über die Organisationen und Länder, an welche die Informationen gemäß dem Beschluss der Kommission weitergegeben werden können.

10. Das Sicherheitsbüro der Kommission trifft alle erforderlichen Maßnahmen, um eine Bewertung späteren Schadens und eine Überarbeitung der Verfahren zu erleichtern.

    Wenn sich die Bedingungen für eine Zusammenarbeitet ändern, wird sich die Kommission erneut mit diesem Thema befassen.

VON DEN EMPFÄNGERN EINZUHALTENDE SICHERHEITSVORSCHRIFTEN

11. Das für Sicherheitsfragen zuständige Mitglied der Kommission stellt den als Empfänger vorgesehenen Ländern oder internationalen Organisationen den Beschluss der Kommission zur Genehmigung der Weitergabe von EU-Verschlusssachen zusammen mit den von der Beratenden Gruppe für das Sicherheitskonzept der Kommission vorgeschlagenen und von der Kommission angenommenen Schutzvorschriften zu.

12. Der Weitergabebeschluss tritt nur dann in Kraft, wenn die Empfänger sich schriftlich verpflichten,

— die Informationen nur zum Zweck der von der Kommission beschlossenen Zusammenarbeit zu nutzen;

— den Informationen den von der Kommission verlangten Schutz zu gewähren.

13. Übermittlung von Dokumenten

a) Die praktischen Verfahren für die Übermittlung von Dokumenten werden vom Sicherheitsbüro der Kommission und den Sicherheitsbehörden der als Empfänger vorgesehenen Staaten oder internationalen Organisationen vereinbart. Sie regeln insbesondere die genaue Anschrift, an die die Dokumente zuzustellen sind.

b) Verschlusssachen des Geheimhaltungsgrades „EU — VERTRAULICH“ und darüber werden in doppeltem Umschlag zugestellt. Der innere Umschlag trägt einen eigenen Stempel oder den festgelegten Codenamen und einen Vermerk der für dieses Dokument genehmigten speziellen Einstufung. Für jede Verschlusssache wird eine Empfangsbescheinigung beigelegt. In der Empfangsbescheinigung, die als solche nicht eingestuft ist, werden nur die Bestimmungsmerkmale des Dokuments (sein Aktenzeichen, das Datum, die Nummer des Exemplars) und dessen Sprachfassung, nicht aber der Titel, aufgeführt.

c) Der innere Umschlag wird in den äußeren Umschlag geschoben, der zu Empfangszwecken eine Paketnummer trägt. Auf dem äußeren Umschlag wird kein Geheimhaltungsgrad angegeben.

d) Den Kurieren wird stets eine Empfangsbescheinigung mit der Paketnummer ausgehändigt.

14. Registrierung am Bestimmungsort

Die nationale Sicherheitsbehörde des Empfängerstaates, die ihr gleichzusetzende Stelle, die in diesem Staat im Auftrag ihrer Regierung die von der Kommission weitergegebene Verschlusssache in Empfang nimmt, oder das Sicherheitsbüro der als Empfänger vorgesehenen internationalen Organisation legt ein spezielles Register für EU-Verschlusssachen an und registriert diese, sobald sie dort eingehen. Dieses Register umfasst Spalten, in denen das Eingangsdatum, die Bestimmungsmerkmale des Dokuments (Datum, Aktenzeichen und Nummer des Exemplars), sein Geheimhaltungsgrad, sein Titel, der Name oder Titel des Empfängers, das Rücksendedatum der Empfangsbescheinigung und das Datum, zu dem das Dokument an die EU zurückgesandt oder vernichtet wird, zu verzeichnen sind.

15. Verwendung und Schutz von ausgetauschten Verschlusssachen

a) Der Umgang mit Verschlusssachen des Geheimhaltungsgrades „EU — GEHEIM“ ist auf eigens dafür bestimmte Bedienstete zu beschränken, die über eine Zugangsermächtigung für Informationen dieser Stufe verfügen. Die Informationen werden in Panzerschränken von guter Qualität aufbewahrt, die nur von den Personen geöffnet werden können, die zum Zugang zu den darin befindlichen Informationen berechtigt sind. Die Bereiche, in denen diese Panzerschränke untergebracht sind, werden ständig bewacht, und es wird ein Überprüfungssystem eingerichtet, damit sichergestellt ist, dass nur ordnungsmäßig ermächtigten Personen der Zugang gestattet wird. Informationen des Geheimhaltungsgrades „EU — GEHEIM“ werden mit Diplomatenpost, sicheren Postdiensten und sicheren Telekommunikationsmitteln übermittelt. Ein „EU — GEHEIM“-Dokument darf nur mit schriftlicher Genehmigung der herausgebenden Stelle kopiert werden. Alle Kopien werden registriert, und ihre Verteilung wird überwacht. Für alle Verrichtungen mit EU — GEHEIM-Dokumenten werden Empfangsbescheinigungen ausgestellt.

b) Der Umgang mit Verschlusssachen des Geheimhaltungsgrades „EU — VERTRAULICH“ ist auf Bedienstete zu beschränken, die ordnungsgemäß ermächtigt sind, über das Thema informiert zu werden. Die Dokumente werden in verschlossenen Panzerschränken in überwachten Bereichen aufbewahrt.

Verschlusssachen des Geheimhaltungsgrades „EU — VERTRAULICH“ werden mit Diplomatenpost, dem militärischen Postdienst und sicheren Telekommunikationsmitteln übermittelt. Die empfangende Stelle kann Kopien anfertigen, deren Anzahl und Verteilung in speziellen Registern zu verzeichnen sind.

c) Der Umgang mit Verschlusssachen des Geheimhaltungsgrades „EU — NUR FÜR DEN DIENSTGEBRAUCH“ ist auf Räume zu beschränken, die Unbefugten nicht zugänglich sind; die Dokumente sind in verschlossenen Behältnissen aufzubewahren. Die Dokumente können mit dem öffentlichen Postdienst als Einschreiben in doppeltem Umschlag und im Zuge von Operationen in Notfällen auch über nicht gesicherte öffentliche Telekommunikationssysteme übermittelt werden. Die Empfänger können Kopien anfertigen.

d) Nicht eingestufte Informationen erfordern keine speziellen Schutzmaßnahmen und können auf dem Postweg und über öffentliche Telekommunikationssysteme übermittelt werden. Die Empfänger können Kopien anfertigen.

16. Vernichtung

Dokumente, für die keine Verwendung mehr besteht, werden vernichtet. Für Verschlusssachen des Geheimhaltungsgrades „EU — NUR FÜR DEN DIENSTGEBRAUCH“ und „EU — VERTRAULICH“ wird ein entsprechender Vermerk in die speziellen Register aufgenommen. Für „EU - GEHEIM“-Verschlusssachen sind Vernichtungsbescheinigungen auszustellen, die von zwei Personen unterzeichnet werden, die der Vernichtung als Zeuge bewohnen.

17. Verstöße gegen die Sicherheitsvorschriften

Wurde bei einer Verschlusssache der Geheimhaltungsgrade „EU — VERTRAULICH“ oder „EU — GEHEIM“ die Geheimschutzvorschrift verletzt oder besteht ein entsprechender Verdacht, so leitet die nationale Sicherheitsbehörde des Staates oder der Sicherheitsverantwortliche der Organisation eine Untersuchung der Umstände ein. Das Sicherheitsbüro der Kommission wird über die Ergebnisse unterrichtet. Es werden die nötigen Maßnahmen getroffen, um bei ungeeigneten Verfahren oder Aufbewahrungsmethoden, die zu der Verletzung geführt haben, für Abhilfe zu sorgen.

Anlage 6

ABKÜRZUNGSVERZEICHNIS

CrA	Kryptographische Stelle
CCAM	Vergabebeirat
CISO	Sicherheitsbeauftragter für die zentrale IT
COMPUSEC	Computersicherheit
COMSEC	Kommunikationssicherheit
CSO	Sicherheitsbüro der Kommission
ESVP	Europäische Sicherheits- und Verteidigungspolitik
INFOSEC	Informationssicherheit
IO	Eigentümer der Information
ISO	Internationale Organisation für Normung
IT	Informationstechnologie
LISO	Beauftragter für die lokale IT-Sicherheit
LSO	Lokaler Sicherheitsbeauftragter
MSO	Sicherheitsbeauftragter für die Sitzung
NSA	Nationale Sicherheitsbehörde
PC	Personalcomputer
RCO	Kontrollbeauftragter für die Registratur
SAA	Akkreditierungsstelle für Sicherheit
SecOP	Sicherheitsbezogene Betriebsverfahren
SSRS	Systemspezifische Sicherheitsanforderungen
TA	TEMPEST-Stelle
TSO	Eigentümer des technischen Systems