►B

GESCHÄFTSORDNUNG DER KOMMISSION

(K(2000) 3614)

(ABl. L 308 vom 8.12.2000, S. 26)

Geändert durch:

		Amtsblatt		
		Nr.	Seite	Datum
►M1	Beschluss 2001/844/EG, EGKS, Euratom der Kommission vom 29. November 2001	L 317	1	3.12.2001
►M2	geändert durch den Beschluss 2005/94/EG, Euratom der Kommission vom 3. Februar 2005	L 31	66	4.2.2005
►M3	geändert durch den Beschluss 2006/70/EG, Euratom der Kommission vom 31. Januar 2006	L 34	32	7.2.2006
►M4	geändert durch den Beschluss 2006/548/EG, Euratom der Kommission vom 2. August 2006	L 215	38	5.8.2006
►M5	Beschluss 2001/937/EG, EGKS, Euratom der Kommission vom 5. Dezember 2001	L 345	94	29.12.2001
►M6	Beschluss 2002/47/EG, EGKS, Euratom der Kommission vom 23. Januar 2002	L 21	23	24.1.2002
►M7	Beschluss 2003/246/EG, Euratom der Kommission vom 26. März 2003	L 92	14	9.4.2003
►M8	Beschluss 2004/563/EG, Euratom der Kommission vom 7. Juli 2004	L 251	9	27.7.2004
►M9	Beschluss 2005/960/EG, Euratom der Kommission vom 15. November 2005	L 347	83	30.12.2005
►M10	Beschluss 2006/25/EG, Euratom der Kommission vom 23. Dezember 2005	L 19	20	24.1.2006
►M11	Beschluss 2007/65/EG der Kommission vom 15. Dezember 2006	L 32	144	6.2.2007
►M12	Beschluss 2008/401/EG, Euratom der Kommission vom 30. April 2008	L 140	22	30.5.2008
►M13	Beschluss 2010/138/EU, Euratom der Kommission vom 24. Februar 2010	L 55	60	5.3.2010
►M14	Beschluss 2011/737/EU, Euratom der Kommission vom 9. November 2011	L 296	58	15.11.2011
►M15	Beschluss (EU, Euratom) 2020/555 der Kommission vom 22. April 2020	L 127I	1	22.4.2020

▼B

GESCHÄFTSORDNUNG DER KOMMISSION

(K(2000) 3614)

▼M13

KAPITEL I

DIE KOMMISSION

Artikel 1

Das Kollegialprinzip

Die Kommission handelt als Kollegium nach Maßgabe dieser Geschäftsordnung sowie unter Beachtung der Prioritäten, die sie im Rahmen der vom Präsidenten nach Artikel 17 Absatz 6 des Vertrags über die Europäische Union (EUV) festgelegten politischen Leitlinien formuliert hat.

Artikel 2

Die politischen Leitlinien, die Prioritäten, das Arbeitsprogramm und der Haushalt

Unter Beachtung der vom Präsidenten festgelegten politischen Leitlinien formuliert die Kommission ihre Prioritäten und setzt diese im Arbeitsprogramm sowie im Entwurf des jährlich verabschiedeten Haushaltsplans um.

Artikel 3

Der Präsident

(1) Der Präsident legt die politischen Leitlinien fest, nach denen die Kommission ihre Aufgaben ausübt ([1]). Er lenkt die Arbeiten der Kommission, um ihre Durchführung sicherzustellen.

(2) Der Präsident beschließt über die interne Organisation der Kommission, um die Kohärenz, die Effizienz und das Kollegialitätsprinzip im Rahmen ihrer Tätigkeit sicherzustellen ([2]).

Unbeschadet des Artikels 18 Absatz 4 EUV kann der Präsident den Mitgliedern der Kommission spezielle Aufgabenbereiche zuweisen, in denen sie für die vorbereitenden Arbeiten der Kommission und die Durchführung ihrer Beschlüsse in besonderem Maße verantwortlich sind ([3]).

Der Präsident kann die Kommissionsmitglieder bitten, besondere Maßnahmen durchzuführen, um die Umsetzung der von ihm festgelegten politischen Leitlinien und der von der Kommission formulierten Prioritäten zu gewährleisten.

Er kann die Zuständigkeitsverteilung jederzeit ändern ([4]).

([1]) Vertrag über die Europäische Union, Artikel 17 Absatz 6 Buchstabe a.
([2]) Vertrag über die Europäische Union, Artikel 17 Absatz 6 Buchstabe b.
([3]) Vertrag über die Arbeitsweise der Europäischen Union, Artikel 248.
([4]) Siehe Fußnote 3.

▼M13

Die Mitglieder der Kommission üben die ihnen vom Präsidenten übertragenen Aufgaben unter dessen Leitung aus ([1]).

(3) Der Präsident ernennt, mit Ausnahme des Hohen Vertreters der Union für Außen- und Sicherheitspolitik, die Vizepräsidenten aus dem Kreis der Mitglieder der Kommission ([2]) und legt die Rangfolge innerhalb der Kommission fest.

(4) Der Präsident kann unter den Mitgliedern der Kommission Gruppen bilden, deren Vorsitzende er benennt, deren Auftrag und Arbeitsweise er bestimmt, und deren Zusammensetzung und Bestandsdauer er festlegt.

(5) Der Präsident nimmt die Vertretung der Kommission wahr. Er benennt die Mitglieder der Kommission, die ihn bei dieser Aufgabe unterstützen.

(6) Unbeschadet des Artikels 18 Absatz 1 EUV legt ein Mitglied der Kommission sein Amt nieder, wenn es vom Präsidenten dazu aufgefordert wird ([3]).

Artikel 4

Beschlussverfahren

Die Kommission fasst ihre Beschlüsse

a) in gemeinschaftlicher Sitzung im Wege des mündlichen Verfahrens gemäß Artikel 8 der Geschäftsordnung oder

b) im schriftlichen Verfahren gemäß Artikel 12 der Geschäftsordnung oder

c) im Ermächtigungsverfahren gemäß Artikel 13 der Geschäftsordnung oder

d) im Verfahren der Delegation gemäß Artikel 14 der Geschäftsordnung.

ABSCHNITT 1

Sitzungen der Kommission

Artikel 5

Einberufung

(1) Die Kommission wird vom Präsidenten zu den Sitzungen einberufen.

(2) Die Kommission tritt in der Regel mindestens einmal wöchentlich zusammen. Sie tagt ferner, wenn dies erforderlich ist.

▼M15

Sind einige oder alle Mitglieder der Kommission verhindert, persönlich an einer Sitzung der Kommission teilzunehmen, kann der Präsident sie in Ausnahmefällen zur Teilnahme über Telekommunikationssysteme, die ihre Identifizierung und wirksame Beteiligung ermöglichen, auffordern.

([1]) Siehe Fußnote 3.
([2]) Vertrag über die Europäische Union, Artikel 17 Absatz 6 Buchstabe c.
([3]) Vertrag über die Europäische Union, Artikel 17 Absatz 6 Unterabsatz 2.

▼M13

(3) Die Mitglieder der Kommission sind verpflichtet, an allen Sitzungen teilzunehmen. Bei einer Verhinderung unterrichten sie den Präsidenten rechtzeitig über die Gründe ihrer Abwesenheit. Der Präsident beurteilt, ob eine Situation vorliegt, die sie von dieser Pflicht entbinden könnte.

Artikel 6

Tagesordnung der Kommissionssitzungen

(1) Der Präsident legt für jede Sitzung der Kommission eine Tagesordnung fest.

(2) Unbeschadet der Befugnis des Präsidenten zur Festlegung der Tagesordnung sind mit größeren Ausgaben verbundene Vorschläge im Einvernehmen mit dem für Haushalt zuständigen Kommissionsmitglied vorzulegen.

(3) Punkte, deren Aufnahme in die Tagesordnung von einem Mitglied der Kommission vorgeschlagen wird, müssen dem Präsidenten nach den Bedingungen zugeleitet werden, die die Kommission entsprechend den in Artikel 28 dieser Geschäftsordnung vorgesehenen Durchführungsbestimmungen („die Durchführungsbestimmungen“) festgelegt hat.

(4) Die Tagesordnung und die notwendigen Unterlagen sind den Kommissionsmitgliedern unter den entsprechend den Durchführungsbestimmungen festgelegten Bedingungen zu übermitteln.

(5) Die Kommission kann auf Vorschlag des Präsidenten beschließen, über einen Punkt zu beraten, der in der Tagesordnung nicht enthalten war oder zu dem die erforderlichen Unterlagen verspätet verteilt worden sind.

Artikel 7

Beschlussfähigkeit

Die Kommission ist beschlussfähig, wenn die Mehrheit der im Vertrag vorgesehenen Zahl ihrer Mitglieder anwesend ist.

▼M15

Macht der Präsident von Artikel 5 Absatz 2 Unterabsatz 2 Gebrauch, gelten die Mitglieder der Kommission, die mittels der dort genannten Telekommunikationssysteme an den Beratungen teilnehmen, für die Zwecke der Beschlussfähigkeit als anwesend.

▼M13

Artikel 8

Beschlussfassung

(1) Die Kommission beschließt auf Vorschlag eines oder mehrerer ihrer Mitglieder.

(2) Die Kommission nimmt auf Antrag eines ihrer Mitglieder eine Abstimmung vor. Gegenstand der Abstimmung ist der ursprüngliche oder der von dem (oder den) für die betreffende Initiative verantwortlichen Mitglieder(n) oder dem Präsidenten abgeänderte Entwurf.

(3) Die Beschlüsse der Kommission werden mit der Mehrheit der im Vertrag vorgesehenen Zahl der Mitglieder gefasst.

▼M13

(4) Das Ergebnis der Beratungen wird vom Präsidenten festgestellt und in das Protokoll der Kommissionssitzung gemäß Artikel 11 der Geschäftsordnung aufgenommen.

Artikel 9

Vertraulichkeit

Die Sitzungen der Kommission sind nicht öffentlich. Ihre Beratungen sind vertraulich.

Artikel 10

Anwesenheit von Beamten und anderen Personen

(1) Sofern die Kommission nichts anderes beschließt, nehmen der Generalsekretär und der Kabinettchef des Präsidenten an den Sitzungen teil. In den Durchführungsbestimmungen wird festgelegt, unter welchen Voraussetzungen andere Personen an den Sitzungen teilnehmen dürfen.

(2) Ist ein Mitglied der Kommission abwesend, so kann sein Kabinettschef an der Sitzung teilnehmen und auf Aufforderung des Präsidenten die Meinung des abwesenden Mitglieds vortragen.

(3) Die Kommission kann beschließen, jede andere Person in der Sitzung zu hören.

▼M15

(4) Macht der Präsident von Artikel 5 Absatz 2 Unterabsatz 2 Gebrauch, können die in den Absätzen 1 bis 3 genannten Personen mittels der in dem betreffenden Unterabsatz genannten Telekommunikationssysteme an den Sitzungen teilnehmen.

▼M13

Artikel 11

Sitzungsprotokolle

(1) Über jede Sitzung der Kommission wird ein Protokoll angefertigt.

(2) Der Protokollentwurf wird der Kommission in einer späteren Sitzung zur Genehmigung vorgelegt. Das genehmigte Protokoll wird durch die Unterschrift des Präsidenten und des Generalsekretärs festgestellt.

ABSCHNITT 2

Sonstige Beschlussfassungsverfahren

Artikel 12

Beschlüsse im schriftlichen Verfahren

(1) Die Zustimmung der Kommission zu einer Vorlage, die von einem oder mehreren ihrer Mitglieder unterbreitet wurde, kann im schriftlichen Verfahren festgestellt werden, sofern der Juristische Dienst zuvor eine befürwortende Stellungnahme zu der Vorlage abgegeben hat, und die Dienste, die gemäß Artikel 23 der Geschäftsordnung gehört werden müssen, der Vorlage zugestimmt haben.

▼M13

Diese befürwortende Stellungnahme bzw. diese Zustimmung kann durch die einvernehmliche Zustimmung der Kommissionsmitglieder ersetzt werden, wenn das Kollegium auf Vorschlag des Präsidenten die Einleitung eines in den Durchführungsbestimmungen festgelegten schriftlichen Finalisierungsverfahrens beschließt.

(2) Zu diesem Zweck wird der Wortlaut der Vorlage allen Mitgliedern der Kommission nach den Bedingungen zugeleitet, die die Kommission entsprechend den Durchführungsbestimmungen festgelegt hat, wobei eine Frist gesetzt wird, vor deren Ablauf die Vorbehalte oder Änderungsanträge mitzuteilen sind, zu denen die Vorlage Anlass geben kann.

(3) Jedes Mitglied der Kommission kann während des schriftlichen Verfahrens beantragen, dass die Vorlage in der Sitzung erörtert wird. Dazu stellt es einen mit Gründen versehenen Antrag an den Präsidenten.

(4) Eine Vorlage, zu der kein Mitglied der Kommission bis zum Ablauf der für das schriftliche Verfahren gesetzten Frist einen Antrag auf Aussetzung vorgelegt oder aufrecht erhalten hat, gilt als angenommen.

▼M14

(5) Jedes Mitglied der Kommission, das die Aussetzung eines schriftlichen Verfahrens im Bereich der Koordinierung und der Überwachung der Wirtschafts- und Haushaltspolitik der Mitgliedstaaten – insbesondere im Euro-Währungsgebiet – beantragen möchte, stellt einen mit Gründen versehenen Antrag an den Präsidenten; in dem Antrag sind auf der Grundlage einer unparteiischen und objektiven Bewertung des Zeitpunkts, der Struktur, der Erwägungen oder des Ergebnisses des vorgeschlagenen Beschlusses die betreffenden Aspekte explizit zu nennen.

Hat diese Begründung nach Ansicht des Präsidenten keinen Bestand und wird der Antrag auf Aussetzung aufrechterhalten, kann der Präsident die Aussetzung ablehnen und die Fortsetzung des schriftlichen Verfahrens beschließen; in diesem Fall holt der Generalsekretär die Stellungnahme der anderen Mitglieder der Kommission ein, um sich zu vergewissern, dass die in Artikel 250 des Vertrags über die Arbeitsweise der Europäischen Union festgelegte Mehrheit gewahrt ist. Der Präsident kann die Angelegenheit auch zur Beschlussfassung auf die Tagesordnung der nächsten Kommissionssitzung setzen.

▼M13

Artikel 13

Beschlüsse im Ermächtigungsverfahren

(1) Die Kommission kann — unter der Voraussetzung, dass der Grundsatz der kollegialen Verantwortlichkeit voll gewahrt bleibt — eines oder mehrere ihrer Mitglieder ermächtigen, in ihrem Namen innerhalb der Grenzen und gemäß den Bedingungen, die sie festlegt, Maßnahmen der Geschäftsführung und der Verwaltung zu treffen.

(2) Sie kann auch eines oder mehrere ihrer Mitglieder beauftragen, den Wortlaut eines Beschlusses oder eines den übrigen Organen vorzulegenden Vorschlags, dessen wesentlichen Inhalt sie bereits in ihren Beratungen festgelegt hat, im Einvernehmen mit dem Präsidenten endgültig anzunehmen.

(3) Die so zugewiesenen Befugnisse können durch Subdelegation auf die Generaldirektoren und Dienststellenleiter weiterübertragen werden, soweit die Ermächtigungsentscheidung dies nicht ausdrücklich untersagt.

▼M13

(4) Die Bestimmungen der Absätze 1, 2 und 3 gelten unbeschadet der Regeln über die Delegation in Finanzangelegenheiten und der Befugnisse der Anstellungsbehörde sowie der zum Abschluss von Einstellungsverträgen ermächtigten Behörde.

Artikel 14

Beschlüsse im Verfahren der Befugnisübertragung (Delegation)

Die Kommission kann — unter der Voraussetzung, dass der Grundsatz der kollegialen Verantwortung voll gewahrt bleibt — den Generaldirektoren und Dienststellenleitern die Befugnis übertragen, in ihrem Namen innerhalb der Grenzen und gemäß den Bedingungen, die sie festlegt, Maßnahmen der Geschäftsführung und der Verwaltung zu treffen.

Artikel 15

Weiterübertragung der Befugnisse für Einzelentscheidungen über die Gewährung von Finanzhilfen und die Vergabe von Aufträgen

Der Generaldirektor oder Dienststellenleiter, dem im Wege der Delegation oder der Subdelegation gemäß den Artikeln 13 und 14 Befugnisse zur Annahme von Finanzierungsbeschlüssen übertragen oder weiterübertragen wurden, kann beschließen, innerhalb der Grenzen und unter Einhaltung der Bedingungen, die in den Durchführungsbestimmungen festgelegt sind, die Befugnis zur Annahme bestimmter Entscheidungen betreffend die Auswahl von Projekten sowie bestimmter Einzelentscheidungen über die Gewährung von Finanzhilfen und die Vergabe öffentlicher Aufträge im Wege der Subdelegation auf den zuständigen Direktor, bzw., im Einvernehmen mit dem verantwortlichen Mitglied der Kommission, auf den zuständigen Referatsleiter zu übertragen.

Artikel 16

Unterrichtung über gefasste Beschlüsse

Die im schriftlichen Verfahren, im Verfahren der Ermächtigung und im Verfahren der Delegation gefassten Beschlüsse werden in einem Tages- oder Wochenvermerk aufgeführt, auf den im Protokoll der nächsten Kommissionssitzung Bezug genommen wird.

ABSCHNITT 3

Gemeinsame Bestimmungen für Beschlussverfahren

Artikel 17

Feststellung der von der Kommission angenommenen Akte

(1) Die von der Kommission in einer Sitzung gefassten Beschlüsse sind in der Sprache oder in den Sprachen, in denen sie verbindlich sind, untrennbar mit der Zusammenfassung verbunden, die bei der Kommissionssitzung, in der sie angenommen wurden, erstellt wird. Diese Akte werden durch die Unterschrift des Präsidenten und des Generalsekretärs auf der letzten Seite der Zusammenfassung festgestellt.

▼M15

Macht der Präsident von Artikel 5 Absatz 2 Unterabsatz 2 Gebrauch und verhindern die Umstände die Unterzeichnung der Zusammenfassung, kann die ausdrückliche schriftliche Zustimmung des Präsidenten und des Generalsekretärs der Kommission deren jeweilige Unterschrift ausnahmsweise ersetzen und wird mit der Zusammenfassung verbunden.

▼**M13**

(2) Die in Artikel 297 Absatz 2 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV) genannten und im schriftlichen Verfahren von der Kommission erlassenen Rechtsakte ohne Gesetzescharakter werden durch die Unterschrift des Präsidenten und des Generalsekretärs auf der letzten Seite der im vorstehenden Absatz genannten Zusammenfassung festgestellt, es sei denn, diese Akte erfordern eine Veröffentlichung und ein Datum des Inkrafttretens, die nicht bis zur nächsten Sitzung der Kommission aufgeschoben werden können. Zum Zwecke dieser Feststellung ist eine Kopie der in Artikel 16 der Geschäftsordnung erwähnten Tagesvermerke untrennbar mit der im vorstehenden Absatz genannten Zusammenfassung verbunden.

Die übrigen im schriftlichen Verfahren und die gemäß Artikel 12 sowie Artikel 13 Absätze 1 und 2 der Geschäftsordnung im Ermächtigungsverfahren gefassten Beschlüsse sind in der Sprache oder in den Sprachen, in denen sie verbindlich sind, untrennbar mit dem in Artikel 16 der Geschäftsordnung genannten Tagesvermerk verbunden. Diese Akte werden durch die Unterschrift des Generalsekretärs auf der letzten Seite des Tagesvermerks festgestellt.

(3) Die im Verfahren der Delegation oder durch Subdelegation gefassten Beschlüsse sind mittels der hierfür vorgesehenen EDV-Anwendung in der Sprache oder in den Sprachen, in denen sie verbindlich sind, untrennbar mit dem in Artikel 16 der Geschäftsordnung genannten Tagesvermerk verbunden. Diese Beschlüsse werden durch eine Selbstbescheinigungserklärung festgestellt, die gemäß Artikel 13 Absatz 3 sowie gemäß den Artikeln 14 und 15 der Geschäftsordnung der nachgeordnet befugte bzw. befugte Beamte unterzeichnet.

(4) Im Sinne dieser Geschäftsordnung bezeichnet der Begriff „Beschluss“ die in Artikel 288 AEUV genannten Rechtsakte.

(5) Im Sinne dieser Geschäftsordnung bezeichnet der Begriff „verbindliche Sprachen“ unbeschadet der Anwendung der Verordnung (EG) Nr. 920/2005 des Rates [1] alle Amtssprachen der Europäischen Union, sofern es sich um Rechtsakte mit allgemeiner Geltung handelt; andernfalls bezeichnet er die Sprache(n) der Adressaten.

ABSCHNITT 4

Vorbereitung und Durchführung der Kommissionsbeschlüsse

Artikel 18

Gruppen der Kommissionsmitglieder

Die Gruppen der Kommissionsmitglieder tragen nach Maßgabe der vom Präsidenten festgelegten politischen Leitlinien und Aufgaben zur Koordinierung und Vorbereitung der Kommissionsarbeiten bei.

Artikel 19

Kabinette und Beziehungen zu den Diensten

(1) Die Kommissionsmitglieder verfügen über einen eigenen Mitarbeiterstab („Kabinett“), der sie bei der Wahrnehmung ihrer Aufgaben und der Vorbereitung der Kommissionsbeschlüsse unterstützt. Die Regeln für die Zusammensetzung und die Arbeitsweise der Kabinette werden vom Präsidenten erlassen.

[1] ABl. L 156 vom 18.6.2005, S. 3.

▼M13

(2) Unter Wahrung der vom Präsidenten festgelegten Grundsätze bestätigt das Kommissionsmitglied die Modalitäten für die Arbeit mit den seiner Verantwortung unterstehenden Dienststellen. Diese Modalitäten regeln insbesondere die Art und Weise, wie das Kommissionsmitglied den beteiligten Dienststellen, die ihm regelmäßig alle seinen Tätigkeitsbereich betreffenden und für die Wahrnehmung seiner Verantwortung erforderlichen Informationen übermitteln, Anweisung erteilt.

Artikel 20

Der Generalsekretär

(1) Der Generalsekretär unterstützt den Präsidenten, damit die Kommission die Prioritäten, die sich gesetzt hat, im Rahmen der vom Präsidenten vorgegebenen politischen Leitlinien verwirklichen kann.

(2) Der Generalsekretär trägt zur Gewährleistung der politischen Kohärenz bei, indem er gemäß Artikel 23 der Geschäftsordnung für die bei den vorbereitenden Arbeiten notwendige Koordinierung zwischen den Dienststellen sorgt.

Er trägt dafür Sorge, dass bei den Dokumenten, die der Kommission vorgelegt werden, die inhaltliche Qualität gesichert ist und die Formerfordernisse beachtet werden, und gewährleistet hierdurch, dass sie den Grundsätzen der Subsidiarität und der Verhältnismäßigkeit, externen Anforderungen, interinstitutionellen Erwägungen und der Kommunikationsstrategie der Kommission entsprechen.

(3) Der Generalsekretär unterstützt den Präsidenten bei der Vorbereitung der Arbeiten und bei der Abhaltung der Sitzungen der Kommission.

Er unterstützt auch die Vorsitzenden der gemäß Artikel 3 Absatz 4 der Geschäftsordnung gebildeten Gruppen bei der Vorbereitung und Abhaltung der Gruppensitzungen. Er nimmt die Sekretariatsaufgaben dieser Gruppen wahr.

(4) Der Generalsekretär gewährleistet die Anwendung der Beschlussfassungsverfahren und sorgt für den Vollzug der Beschlüsse gemäß Artikel 4 der Geschäftsordnung.

Außer in Sonderfällen trifft er insbesondere die erforderlichen Maßnahmen für die amtliche Bekanntgabe und die Veröffentlichung der Kommissionsbeschlüsse im *Amtsblatt der Europäischen Union* sowie für die Übermittlung der Dokumente der Kommission und ihrer Dienste an die anderen Organe der Europäischen Union und an die Parlamente der Mitgliedstaaten.

Er sorgt für die Verteilung der Unterlagen, die die Mitglieder der Kommission ihren Kollegen zukommen lassen möchten.

(5) Der Generalsekretär unterhält die offiziellen Beziehungen zu den anderen Organen der Europäischen Union vorbehaltlich der Zuständigkeiten, die die Kommission selbst auszuüben beschließt oder die sie einem ihrer Mitglieder oder ihrer Verwaltung überträgt.

In diesem Zusammenhang sorgt er durch eine Koordinierung zwischen den Dienststellen dafür, dass die allgemeine Kohärenz während der Arbeiten der anderen Organe gewährleistet ist.

(6) Der Generalsekretär sorgt für eine angemessene Unterrichtung der Kommission über den Stand der internen und interinstitutionellen Verfahren.

▼M13

KAPITEL II

DIENSTSTELLEN DER KOMMISSION

Artikel 21

Struktur der Dienststellen

Die Kommission richtet zur Vorbereitung und zur Durchführung ihrer Amtstätigkeit und zur Verwirklichung der vom Präsidenten festgelegten Prioritäten und politischen Leitlinien eine Reihe von Dienststellen ein, die in Generaldirektionen und gleichgestellte Dienste gegliedert sind.

In der Regel sind die Generaldirektionen und die gleichgestellten Dienste in Direktionen, die Direktionen in Referate gegliedert.

Artikel 22

Einrichtung besonderer Funktionen und Strukturen

Um speziellen Anforderungen gerecht zu werden, kann der Präsident besondere Funktionen und Verwaltungsstrukturen einrichten, denen er genau umschriebene Aufgaben überträgt und deren Befugnisse und Arbeitsbedingungen er festlegt.

Artikel 23

Zusammenarbeit und Koordinierung der Dienststellen

(1) Um die Effizienz der Amtstätigkeit der Kommission sicherzustellen, arbeiten die Dienstellen, die an der Ausarbeitung oder Durchführung von Beschlüssen mitwirken, bereits mit Beginn der jeweiligen Arbeiten so eng wie möglich zusammen.

(2) Die für die Vorbereitung einer Initiative federführende Dienststelle trägt bereits mit Beginn der Vorarbeiten dafür Sorge, dass eine wirkungsvolle Koordinierung zwischen allen Dienststellen gewährleistet ist, die nach den Zuständigkeitsbereichen und Befugnissen oder nach der Natur der Sache ein berechtigtes Interesse an dieser Initiative haben.

(3) Bevor der Kommission eine Vorlage unterbreitet wird, hat die federführende Dienststelle die Dienststellen, die ein berechtigtes Interesse an der betreffenden Vorlage haben, nach Maßgabe der Durchführungsbestimmungen rechtzeitig zu hören.

(4) Der Juristische Dienst ist zu allen Entwürfen von Beschlüssen und Vorschlägen von Rechtsakten sowie zu allen Vorlagen, die rechtliche Wirkungen haben können, zu hören.

Der Juristische Dienst muss ebenfalls gehört werden bei der Einleitung der Beschlussfassungsverfahren gemäß den Artikeln 12, 13 und 14 der Geschäftsordnung, ausgenommen Beschlüsse über Standardrechtsakte, die zuvor die Zustimmung des Juristischen Dienstes erhalten haben (Rechtsakte mit Wiederholungscharakter). Für die in Artikel 15 der Geschäftsordnung genannten Entscheidungen ist die Anhörung des Juristischen Dienstes nicht erforderlich.

(5) Das Generalsekretariat muss bei allen Initiativen gehört werden, die

▼M13

— im mündlichen Verfahren genehmigt werden müssen (hiervon unberührt bleiben individuelle Personalfragen) oder

— von politischer Bedeutung sind oder

— im Jahresarbeitsprogramm der Kommission sowie im geltenden Programmierungsinstrument der Kommission aufgeführt sind oder

— institutionelle Aspekte betreffen oder

— einer Folgenabschätzung oder öffentlichen Konsultation unterzogen werden

sowie bei allen Stellungnahmen oder gemeinsame Initiativen, die die Kommission gegenüber anderen Organen oder Einrichtungen verpflichten können.

▼M14

(5a) Die für Wirtschaft und Finanzen zuständige Generaldirektion muss zu allen Initiativen konsultiert werden, die das Wachstum, die Wettbewerbsfähigkeit oder die wirtschaftliche Stabilität in der Europäischen Union oder im Euro-Währungsgebiet betreffen oder sich darauf auswirken können.

▼M13

(6) Die mit dem Haushalt sowie mit den Humanressourcen und der Sicherheit befassten Generaldirektionen sind zu allen Vorlagen, mit Ausnahme der Rechtsakte gemäß Artikel 15 der Geschäftsordnung, zu hören, die Auswirkungen auf den Haushaltsplan, die Finanzen, das Personal und die Verwaltung haben können. Gleiches gilt, soweit erforderlich, auch für den mit der Betrugsbekämpfung befassten Dienst.

(7) Die federführende Dienststelle ist bemüht, einen Vorschlag zu erarbeiten, der die Zustimmung der gehörten Dienststellen findet. Unbeschadet des Artikels 12 der Geschäftsordnung hat sie — falls es zu keiner Einigung kommt — abweichende Stellungnahmen dieser Dienststellen in ihrem Vorschlag zu erwähnen.

KAPITEL III

VERTRETUNG

Artikel 24

Die Kontinuität des Dienstes

Die Mitglieder der Kommission und die Dienststellen treffen alle zweckdienlichen Maßnahmen, um die Kontinuität des Dienstes unter Beachtung der hierfür von der Kommission oder vom Präsidenten erlassenen Bestimmungen sicherzustellen.

Artikel 25

Vertretung des Präsidenten

Die Aufgaben des Präsidenten werden im Fall seiner Verhinderung von einem Vizepräsidenten oder einem Mitglied in der vom Präsidenten festgelegten Reihenfolge wahrgenommen.

▼M13

Artikel 26

Vertretung des Generalsekretärs

Die Aufgaben des Generalsekretärs werden, falls dieser verhindert ist oder die Stelle des Generalsekretärs nicht besetzt ist, von dem in der höchsten Besoldungsgruppe anwesenden stellvertretenden Generalsekretär und, bei gleicher Besoldungsgruppe, von dem in seiner Besoldungsgruppe dienstältesten anwesenden stellvertretenden Generalsekretär und, bei gleichem Dienstalter, vom ältesten anwesenden stellvertretenden Generalsekretär oder von einem von der Kommission bestimmten Beamten wahrgenommen.

Ist kein stellvertretender Generalsekretär anwesend oder hat die Kommission keinen Beamten zur Vertretung bestimmt, wird diese von dem anwesenden Untergebenen in der höchsten Funktionsgruppe und innerhalb dieser der höchsten Besoldungsgruppe und, bei gleicher Besoldungsgruppe, von dem in seiner Besoldungsgruppe dienstältesten anwesenden Untergebenen und, bei gleichem Dienstalter, vom ältesten anwesenden Untergebenen wahrgenommen.

Artikel 27

Vertretung der Dienstvorgesetzten

(1) Der Generaldirektor wird, falls er verhindert ist oder die Stelle des Generaldirektors nicht besetzt ist, von dem in der höchsten Besoldungsgruppe anwesenden stellvertretenden Generaldirektor und, bei gleicher Besoldungsgruppe, von dem in seiner Besoldungsgruppe dienstältesten anwesenden stellvertretenden Generaldirektor und, bei gleichem Dienstalter, vom ältesten anwesenden stellvertretenden Generaldirektor oder von einem von der Kommission bestimmten Beamten wahrgenommen.

Ist kein stellvertretender Generaldirektor anwesend oder hat die Kommission keinen Beamten zur Vertretung bestimmt, wird diese von dem anwesenden Untergebenen in der höchsten Funktionsgruppe und innerhalb dieser der höchsten Besoldungsgruppe und, bei gleicher Besoldungsgruppe, von dem in seiner Besoldungsgruppe dienstältesten anwesenden Untergebenen und, bei gleichem Dienstalter, vom ältesten anwesenden Untergebenen wahrgenommen.

(2) Der Referatsleiter wird, falls er verhindert ist oder die Stelle des Referatsleiters nicht besetzt ist, vom stellvertretenden Referatsleiter oder von einem vom Generaldirektor bestimmten Beamten vertreten.

Ist kein stellvertretender Referatsleiter anwesend oder hat der Generaldirektor keinen Beamten zur Vertretung bestimmt, wird diese von dem anwesenden Untergebenen in der höchsten Funktionsgruppe und innerhalb dieser der höchsten Besoldungsgruppe und, bei gleicher Besoldungsgruppe, von dem in seiner Besoldungsgruppe dienstältesten anwesenden Untergebenen und, bei gleichem Dienstalter, vom ältesten anwesenden Untergebenen wahrgenommen.

(3) Jeder andere Dienstvorgesetzte wird im Fall seiner Verhinderung oder wenn die Stelle nicht besetzt ist, von einem vom Generaldirektor im Einvernehmen mit dem zuständigen Kommissionsmitglied bestimmten Beamten vertreten. Hat der Generaldirektor keinen Beamten zur Vertretung bestimmt, wird diese von dem anwesenden Untergebenen in der höchsten Funktionsgruppe und innerhalb dieser der höchsten Besoldungsgruppe und, bei gleicher Besoldungsgruppe, von dem in seiner Besoldungsgruppe dienstältesten anwesenden Untergebenen und, bei gleichem Dienstalter, vom ältesten anwesenden Untergebenen wahrgenommen.

▼**M13**

KAPITEL IV

SCHLUSSBESTIMMUNGEN

Artikel 28

Die Kommission erlässt, soweit erforderlich, Durchführungsbestimmungen zu dieser Geschäftsordnung.

Die Kommission kann in Bezug auf ihre Arbeitsweise und auf die ihrer Dienstellen weitere Maßnahmen ergreifen.

Artikel 29

Diese Geschäftsordnung tritt am Tag nach ihrer Veröffentlichung im *Amtsblatt der Europäischen Union* in Kraft.

▼B

ANHANG

KODEX FÜR GUTE VERWALTUNGSPRAXIS IN DEN BEZIEHUNGEN DER BEDIENSTETEN DER EUROPÄISCHEN KOMMISSION ZUR ÖFFENTLICHKEIT

Dienst von hoher Qualität

Die Kommission und ihre Bediensteten haben die Pflicht, dem Interesse der Gemeinschaft und hierdurch auch dem öffentlichen Interesse zu dienen.

Die Öffentlichkeit erwartet zu Recht eine offene, zugängliche Verwaltung, die effizient geführt wird und Dienste von hoher Qualität erbringt.

Hohe Qualität setzt voraus, dass sich die Kommission und ihre Bediensteten höflich, sachlich und unparteiisch verhalten.

Zweck

Um die Kommission in die Lage zu versetzen, ihrer Verpflichtung zu einer guten Verwaltungspraxis nachzukommen — insbesondere in Hinblick auf die Beziehungen der Kommission mit der Öffentlichkeit —, verpflichtet sich die Kommission, die in diesem Kodex niedergelegten Leitlinien einer guten Verwaltungspraxis zu beachten und sich durch sie in ihrer täglichen Arbeit leiten zu lassen.

Geltungsbereich

Der Kodex ist für das gesamte Personal verbindlich, auf welches das Statut der Beamten der Europäischen Gemeinschaften und die Beschäftigungsbedingungen für die sonstigen Bediensteten dieser Gemeinschaften (das Statut) oder andere Vorschriften zur Beziehung zwischen der Kommission und ihrem Personal, die sich auf Beamte bzw. sonstige Bedienstete der Europäischen Gemeinschaften beziehen, Anwendung finden. Personen mit privatrechtlichem Arbeitsvertrag, abgeordnete nationale Sachverständige oder Praktikanten, die für die Kommission arbeiten, sollten sich jedoch ebenfalls in ihrer täglichen Arbeit durch den Kodex leiten lassen.

Die Beziehungen der Kommission zu ihren Bediensteten werden ausschließlich durch das Statut geregelt.

1. ALLGEMEINE GRUNDSÄTZE GUTER VERWALTUNGSPRAXIS

Die Kommission beachtet in ihren Beziehungen zur Öffentlichkeit die folgenden Grundsätze:

Rechtmäßigkeit

Die Kommission richtet sich in ihrem Handeln nach dem Recht und wendet die gemeinschaftsrechtlichen Vorschriften und Verfahren an.

Diskriminierungsverbot und Gleichbehandlung

Die Kommission befolgt den Grundsatz der Nichtdiskriminierung und garantiert insbesondere die Gleichbehandlung der Bürger unabhängig von ihrer Nationalität, Geschlechtszugehörigkeit, Rasse oder ethnischen Zugehörigkeit, Religion oder Weltanschauung, Behinderung, Alter oder sexuellen Ausrichtung. Somit muss jedwede Ungleichbehandlung ähnlicher Fälle durch die Umstände des Einzelfalls sachlich begründet sein.

Verhältnismäßigkeit

Die Kommission achtet darauf, dass die Maßnahmen in einem angemessenen Verhältnis zu den angestrebten Zielen stehen.

Insbesondere wird sie stets dafür Sorge tragen, dass bei der Anwendung dieses Kodexes der angestrebte Nutzen im konkreten Einzelfall nicht mit einem unvertretbaren Verwaltungsaufwand verbunden ist.

Kohärenz

Die Kommission achtet auf eine kohärente Verwaltungspraxis und wendet die gängigen Verwaltungsverfahren an. Abweichungen hiervon sind entsprechend sachlich zu begründen.

▼B

2. LEITLINIEN FÜR GUTE VERWALTUNGSPRAXIS

Objektivität und Unparteilichkeit

Bedienstete handeln stets objektiv und unparteiisch sowie im Interesse der Gemeinschaft und zum Wohl der Allgemeinheit. Innerhalb des von der Kommission festgelegten politischen Rahmens entscheiden sie in voller Unabhängigkeit, ohne sich von persönlichen oder nationalen Interessen leiten zu lassen oder politischem Druck nachzugeben.

Informationen über Verwaltungsverfahren

Ersuchen Bürger um Auskünfte über Verwaltungsverfahren der Kommission, so stellen die Bediensteten sicher, dass diese Auskünfte innerhalb der im jeweiligen Verfahren festgelegten Fristen erteilt werden.

3. ERTEILUNG VON INFORMATIONEN ÜBER DIE RECHTE DER BETEILIGTEN

Anhörung aller unmittelbar Beteiligten

Sieht das Gemeinschaftsrecht die Anhörung Beteiligter vor, so sorgen die Bediensteten dafür, dass ihnen die Möglichkeit zur Äußerung gegeben wird.

Begründungspflicht

Entscheidungen der Kommission sind zu begründen und den Betroffenen mitzuteilen.

Im Allgemeinen sollte eine vollständige Begründung erteilt werden. Soweit es nicht möglich ist, eine detaillierte Angabe der Entscheidungsgründe im Einzelfall vorzunehmen, zum Beispiel weil der Kreis derer, die von gleichartigen Entscheidungen betroffen sind, zu groß ist, dürfen Standardantworten erteilt werden. Diese Standardantworten sollten die wesentlichen Gründe enthalten, auf denen die Entscheidung basiert. Darüber hinaus ist Beteiligten auf ausdrückliches Ersuchen eine detaillierte Begründung zu übermitteln.

Informationspflicht über Rechtsbehelfe

Soweit das Gemeinschaftsrecht dies vorsieht, enthalten bekannt gegebene Entscheidungen Angaben zu deren Anfechtbarkeit; ebenso ist anzugeben, wie die Anfechtung vorgenommen werden kann (Name und Büroanschrift der Person, bzw. der Dienststelle, bei der dieser Rechtsbehelf eingelegt werden kann) und welche Frist zu beachten ist.

Gegebenenfalls weisen Entscheidungen auf die Möglichkeit der Einleitung eines Gerichtsverfahrens und/oder zur Anrufung des Europäischen Bürgerbeauftragten gemäß Artikel 230 bzw. 195 EG-Vertrag hin.

4. BEHANDLUNG VON ANFRAGEN

Die Kommission verpflichtet sich, Anfragen von Bürgern in angemessener Weise und so schnell wie möglich zu beantworten.

Anforderung von Dokumenten

Ist das angeforderte Dokument bereits veröffentlicht, so ist auf die Verkaufsstellen des Amtes für amtliche Veröffentlichungen der Europäischen Gemeinschaften sowie die Dokumentations- und Informationsstellen („Info-points“, Europäische Dokumentationszentren, usw.) zu verweisen. Viele Dokumente sind auch elektronisch verfügbar.

Der Zugang zu Dokumenten der Kommission wird durch einschlägige Bestimmungen geregelt.

▼B

Schriftverkehr

Gemäß Artikel 21 EG-Vertrag sind Schreiben an die Kommission in der Sprache zu beantworten, in der sie verfasst wurden, sofern es sich um eine Amtssprache der Gemeinschaft handelt.

Die Antwort auf ein an die Kommission gerichtetes Schreiben ist innerhalb einer Frist von fünfzehn Arbeitstagen ab dem Tag des Eingangs bei der zuständigen Dienststelle abzusenden. Im Antwortschreiben ist der Name des zuständigen Bediensteten anzugeben. Ebenfalls ist anzugeben, wie dieser Bedienstete erreicht werden kann.

Kann ein Schreiben nicht innerhalb von fünfzehn Arbeitstagen beantwortet werden, so gibt der Bedienstete in einem vorläufigen Schreiben einen Zeitpunkt an, an dem mit einer Antwort zu rechnen ist; dies gilt auch für alle Fälle, in denen eine Kontaktaufnahme mit anderen Dienststellen erforderlich ist oder Übersetzungen vorzunehmen sind. Der Zeitpunkt für die endgültige Beantwortung bestimmt sich nach der relativen Dringlichkeit der Anfrage und der Komplexität der Materie.

Erfolgt die Beantwortung durch eine andere als die ursprünglich als Adressat bezeichnete Dienststelle, sind der Name und die Büroadresse des Bediensteten, an den die Anfrage weitergeleitet wurde, anzugeben.

Diese Bestimmungen gelten nicht bei Missbrauch, d. h. wenn immer wieder gleichlautende Schreiben mit beleidigendem Inhalt bzw. Äußerungen ohne erkennbaren Sinn und Zweck eingehen. In diesen Fällen behält sich die Kommission somit das Recht vor, den Schriftwechsel einzustellen.

Telefon

Bei der Annahme eines Telefongesprächs hat sich der Bedienstete mit seinem Namen oder der Angabe seiner Dienststelle zu melden. Rückrufe sind so rasch wie möglich vorzunehmen.

Auskunftsersuchen zu Fragen, die seinen unmittelbaren Zuständigkeitsbereich betreffen, beantwortet der Bedienstete selbst; ansonsten sollte er den Gesprächspartner an die zuständige Stelle verweisen. Falls erforderlich, verweist der Bedienstete seinen Gesprächspartner an seinen Vorgesetzten oder nimmt mit diesem Rücksprache, bevor er das Auskunftsersuchen beantwortet.

Fällt eine Anfrage in den unmittelbaren Zuständigkeitsbereich des Bediensteten, so holt er Auskünfte über die Person des Informationssuchenden ein und prüft vor der Weitergabe der Information, ob sie der Öffentlichkeit bereits zugänglich gemacht wurde. Wenn nicht, so kann der Bedienstete davon ausgehen, dass die Information im Interesse der Gemeinschaft nicht verbreitet werden darf. In diesen Fällen sollte er die Gründe hierfür erläutern und gegebenenfalls auf die ihm nach Artikel 17 des Beamtenstatuts auferlegte Schweigepflicht verweisen.

Der Bedienstete ersucht den Informationssuchenden gegebenenfalls, die telefonische Anfrage schriftlich zu bestätigen.

Elektronische Post

Der Bedienstete beantwortet elektronische Post unverzüglich unter Berücksichtigung der Leitlinien für Telefongespräche.

Sollte eine Anfrage durch elektronische Post aufgrund ihrer Komplexität einer schriftlichen Anfrage gleichzusetzen sein, so gelten jedoch die Leitlinien für den Schriftverkehr einschließlich der entsprechenden Fristen.

Anfragen der Medien

Der Presse- und Informationsdienst ist für die Beziehungen zu den Medien zuständig. Die Beantwortung fachspezifischer Fragen der Medien zu seinem eigenen Zuständigkeitsbereich kann jedoch der Bedienstete übernehmen.

▼B

5. SCHUTZ PERSÖNLICHER DATEN UND GEHEIMER INFORMATIONEN

Die Kommission und ihre Bediensteten beachten insbesondere:

— die Vorschriften über den Schutz der Privatsphäre und personenbezogener Daten;

— die Verpflichtungen gemäß Artikel 287 EG-Vertrag, insbesondere diejenige betreffend das Berufsgeheimnis;

— die Geheimhaltungsvorschriften im Zusammenhang mit strafrechtlichen Untersuchungen;

— die Geheimhaltungspflicht in Angelegenheiten, die im Rahmen der in Artikel 9 und der Anhänge II und III zum Statut vorgesehenen verschiedenen Ausschüsse behandelt werden.

6. BESCHWERDEN

Europäische Kommission

Verstößt ein Bediensteter gegen die in diesem Kodex festgeschriebenen Verhaltensregeln, kann beim Generalsekretariat [1] der Europäischen Kommission Beschwerde dagegen eingelegt werden.

Der Generaldirektor bzw. der Leiter der Dienststelle unterrichtet den Beschwerdeführer binnen zwei Monaten schriftlich darüber, welche Maßnahmen zur weiteren Behandlung der Beschwerde getroffen wurden. Der Beschwerdeführer kann sich daraufllin binnen eines Monats an den Generalsekretär der Europäischen Kommission wenden und ihn bitten, das Ergebnis des Beschwerdeverfahrens zu überprüfen. Der Generalsekretär beantwortet dieses Überprüfungsersuchen innerhalb eines Monats.

Europäischer Bürgerbeauftragter

Beschwerden können nach Artikel 195 EG-Vertrag und dem Statut des Europäischen Bürgerbeauftragten auch an letzteren gerichtet werden.

▼M1

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 [2], 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 [3] und den Beschluss C (95) 1510 endg. der Kommission vom 23. November 1995 über den Schutz der Informationssysteme unberührt.

[1] *Postanschrift*:Generalsekretariat der Europäischen Kommission, Referat SG/B/2 „Transparenz, Zugang zu Dokumenten und Beziehungen zur Zivilgesellschaft“, Rue de la Loi/Wetstraat 200, B-1049 Brüssel (Fax: (32-2)-296 72 42).
Elektronische Adresse: SG-Code-de-bonne-conduite@cec.eu.int.

[2] ABl. 17 vom 6.10.1958, S. 406.

[3] ABl. L 151 vom 15.6.1990, S. 1.

▼M1

(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 [1] 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 [2] unberührt.

▼M3

(8) Diese Vorschriften lassen Artikel 286 des Vertrags und die Verordnung (EG) Nr. 45/2001 des Europäischen Parlaments und des Rates vom 18. Dezember 2000 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft und zum freien Datenverkehr unberührt.

▼M1

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.

▼M4

Beinhaltet ein Vertrag oder eine Finanzhilfevereinbarung zwischen der Kommission und einem externen Auftragnehmer oder Begünstigten die Verarbeitung von EU-Verschlusssachen in den Räumlichkeiten des Auftragnehmers oder Begünstigten, so sind die vom externen Auftragnehmer oder Begünstigten zu ergreifenden angemessenen Maßnahmen, mit denen gewährleistet wird, dass die in Artikel 1 genannten Vorschriften bei der Verarbeitung von EU-Verschlusssachen eingehalten werden, fester Bestandteil des Vertrags oder der Finanzhilfevereinbarung.

▼M1

(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;

[1] ABl. L 101 vom 11.4.2001, S. 1.
[2] ABl. L 145 vom 31.5.2001, S. 43.

▼**M1**

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.

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 „►**M2** RESTREINT UE ◄“ 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.

▼**M1**

ANHANG

SICHERHEITSVORSCHRIFTEN DER EUROPÄISCHEN KOMMISSION

Inhalt

▼M1

16. GEHEIMHALTUNGSGRADE, SICHERHEITSKENNUNGEN UND KENNZEICHNUNGEN

16.1. **Geheimhaltungsgrade**

16.2. **Sicherheitskennungen**

16.3. **Kennzeichnungen**

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

16.5. **Anbringen von Sicherheitskennungen**

17. REGELN FÜR DIE EINSTUFUNG ALS VERSCHLUSSSACHE

17.1. **Allgemeines**

17.2. **Anwendung der Geheimhaltungsgrade**

17.3. **Herabstufung und Aufhebung des Geheimhaltungsgrades**

18. MATERIELLER GEHEIMSCHUTZ

18.1. **Allgemeines**

18.2. **Sicherheitsanforderungen**

18.3. **Maßnahmen des materiellen Geheimschutzes**

18.3.1. *Sicherheitsbereiche*

18.3.2. *Verwaltungsbereich*

18.3.3. *Eingangs- und Ausgangskontrollen*

18.3.4. *Kontrollgänge*

18.3.5. *Sicherheitsbehältnisse und Tresorräume*

18.3.6. *Schlösser*

18.3.7. *Kontrolle der Schlüssel und Kombinationen*

18.3.8. *Intrusionsmeldeanlagen*

18.3.9. *Zugelassene Ausrüstung*

18.3.10. *Materieller Geheimschutz für Kopier- und Faxgeräte*

18.4. **Sicht- und Abhörschutz**

18.4.1. *Sichtschutz*

18.4.2. *Abhörschutz*

18.4.3. *Einbringen elektronischer Geräte und von Aufzeichnungsgeräten*

18.5. **Hochsicherheitzonen**

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

19.1. **Allgemeines**

19.2. **Besondere Vorschriften für den Zugang zu als „►M2 TRES SECRET UE/EU TOP SECRET ◄“ eingestuften Verschlussachen**

19.3. **Besondere Vorschriften für den Zugang zu als „►M2 SECRET UE ◄“ und „►M2 CONFIDENTIEL UE ◄“ eingestuften Verschlusssachen**

19.4. **Besondere Vorschriften für den Zugang zu als „►M2 RESTREINT UE ◄“ eingestuften Verschlusssachen**

▼**M1**

19.5. **Weitergabe**

19.6. **Besondere Anweisungen**

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

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

21.1. **Herstellung**

21.2. **Verteilung**

21.3. **Übermittlung von EU-Verschlusssachen**

21.3.1. *Vorkehrungen für den Versand, Empfangsbestätigung*

21.3.2. *Übermittlung innerhalb eines Gebäudes oder Gebäudekomplexes*

21.3.3. *Übermittlung innerhalb ein und desselben Landes*

21.3.4. *Beförderung von einem Staat in einen anderen*

21.3.5. *Übermittlung von Verschlusssachen mit der Einstufung „►**M2** RESTREINT UE ◄“*

21.4. **Sicherheit der Kuriere**

21.5. **Elektronische und andere technische Übermittlungswege**

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

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

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

22.2. **Die „►**M2** TRES SECRET UE/EU TOP SECRET ◄“-Registratur**

22.2.1. *Allgemeines*

22.2.2. *Die „►**M2** TRES SECRET UE/EU TOP SECRET ◄“-Zentralregistratur*

22.2.3. *„►**M2** TRES SECRET UE/EU TOP SECRET ◄“-Unterregistraturen*

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

22.4. **Archivierung von EU-Verschlusssachen**

22.5. **Vernichtung von EU-Verschlusssachen**

22.6. **Vernichtung im Notfall**

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

23.1. **Allgemeines**

23.2. **Zuständigkeiten**

23.2.1. ►**M3** *DIREKTION SICHERHEIT DER KOMMISSION* ◄

23.2.2. *Sicherheitsbeauftragter für die Sitzung*

▼**M1**

23.3 **Sicherheitsmaßnahmen**

23.3.1. *Sicherheitsbereiche*

23.3.2. *Berechtigungsausweise*

23.3.3. *Kontrolle von fotografischen Ausrüstungen und Tonaufzeichnungsgeräten*

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

23.3.5. *Technische Sicherheit*

23.3.6. *Dokumente der Delegationen*

23.3.7. *Sichere Aufbewahrung der Dokumente*

23.3.8. *Überprüfung der Büroräume*

23.3.9. *Abfallbeseitigung bei EU-Verschlusssachen*

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

24.1. **Begriffsbestimmungen**

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

24.3. **Rechtliche Schritte**

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

25.1. **Einleitung**

25.1.1. *Allgemeines*

25.1.2. *Bedrohungen und Schwachstellen von Systemen*

25.1.3. *Hauptzweck von Sicherheitsmaßnahmen*

25.1.4. *Aufstellung der systemspezifischen Sicherheitsanforderungen (SSRS)*

25.1.5. *Sicherheitsmodus*

25.2. **Begriffsbestimmungen**

25.3. **Zuständigkeiten im Sicherheitsbereich**

25.3.1. *Allgemeines*

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

25.3.3. *INFOSEC-Stelle (IA)*

25.3.4. *Eigentümer des technischen Systems (TSO)*

25.3.5. *Eigentümer der Informationen (IO)*

25.3.6. *Nutzer*

25.3.7. *INFOSEC-Schulung*

25.4. **Nichttechnische Sicherheitsmaßnahmen**

25.4.1. *Personalbezogene Sicherheit*

25.4.2. *Materielle Sicherheit*

25.4.3. *Kontrolle des Zugangs zu einem System*

25.5. **Technische Sicherheitsmaßnahmen**

25.5.1. *Informationssicherheit*

25.5.2. *Kontrolle und Nachvollziehbarkeit in Bezug auf Informationen*

25.5.3. *Behandlung und Kontrolle von austauschbaren elektronischen Datenträgern*

▼M1

▼M1

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;

▼**M1**

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 ►**M3** Direktion Sicherheit 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 ►**M3** des Direktors der Direktion Sicherheit 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.

▼**M1**

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;

▼M1

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.

▼M4

Solche Mindestnormen gelten auch, wenn die Kommission industrielle oder andere Stellen vertraglich oder durch eine Finanzhilfevereinbarung mit Aufgaben betraut, bei denen EU-Verschlusssachen herangezogen werden, gebraucht werden und/oder mit eingeschlossen sind. Diese gemeinsamen Mindestnormen sind in Teil II Abschnitt 27 enthalten.

▼M1

5.2. **Organisation**

In der Kommission ist die Sicherheit auf zwei Ebenen organisiert:

a) Auf der Ebene der Kommission als Ganzes gibt es ein ►M3 Direktion Sicherheit 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 „►M2 CONFIDENTIEL UE ◄“ 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;

▼M1

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 „►M2 TRES SECRET UE/EU TOP SECRET ◄“ erhalten sollen;

e) Stellen bekleiden, bei denen sie regelmäßig mit einer beträchtlichen Menge an Informationen des Geheimhaltungsgrades „►M2 SECRET UE ◄“ 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 ►M3 Direktion Sicherheit 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.

▼**M1**

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.

▼M1

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;

▼M1

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.

▼M3

13. DER SICHERHEITSRAT DER KOMMISSION

Es wird ein Sicherheitsrat der Kommission eingesetzt. Er besteht aus dem Generaldirektor für Personal und Verwaltung, der den Vorsitz führt, einem Mitglied des Kabinetts des für Sicherheitsfragen zuständigen Kommissionsmitglieds, einem Mitglied des Kabinetts des Präsidenten, dem Stellvertretenden Generalsekretär, der der Gruppe für Krisenmanagement der Kommission vorsitzt, den Generaldirektoren des Juristischen Dienstes, der Generaldirektion Außenbeziehungen, der Generaldirektion Justiz, Freiheit und Sicherheit, der Gemeinsamen Forschungsstelle, der Generaldirektion Informatik und des Internen Auditdienstes sowie dem Direktor der Direktion Sicherheit der Kommission oder deren Vertreter. Andere Kommissionsbeamte können eingeladen werden. Der Sicherheitsrat beurteilt die Sicherheitsmaßnahmen innerhalb der Kommission und legt dem für Sicherheitsfragen zuständigen Kommissionsmitglied gegebenenfalls Empfehlungen in diesem Bereich vor.

▼M1

14. DAS ►M3 DIREKTION SICHERHEIT DER KOMMISSION ◄

Dem für Sicherheitsfragen zuständigen Mitglied der Kommission steht für die Wahrnehmung seiner in Abschnitt 11 genannten Aufgaben das ►M3 Direktion Sicherheit der Kommission ◄ für die Koordinierung, Überwachung und Durchführung von Sicherheitsmaßnahmen zur Verfügung.

Der ►M3 Direktor der Direktion Sicherheit 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 ►M3 Direktor der Direktion Sicherheit 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 ►M3 Direktion Sicherheit der Kommission ◄ führt regelmäßige Inspektionen der Sicherheitsvorkehrungen zum Schutz von EU-Verschlusssachen durch.

▼M1

Das ►M3 Direktion Sicherheit 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 ►M3 Direktion Sicherheit der Kommission ◄ und in gegenseitigem Einvernehmen eine Inspektion von EU-Verschlusssachen durchführen.

16. GEHEIMHALTUNGSGRADE, SICHERHEITSKENNUNGEN UND KENNZEICHNUNGEN

16.1. **Geheimhaltungsgrade** ([2])

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

„►M2 TRES SECRET UE/EU TOP SECRET ◄“: 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.

„►M2 SECRET UE ◄“: 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.

„►M2 CONFIDENTIEL UE ◄“: 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.

„►M2 RESTREINT UE ◄“: 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.

([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.

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

▼M1

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

Der Hinweis auf den Geheimhaltungsgrad wird wie folgt angebracht:

a) bei Dokumenten, die als „►M2 RESTREINT UE ◄“ eingestuft werden, mit mechanischen oder elektronischen Mitteln;

b) bei Dokumenten, die als „►M2 CONFIDENTIEL UE ◄“ eingestuft werden, mit mechanischen Mitteln, von Hand oder durch Druck auf vorgestempeltem, registriertem Papier;

c) auf Dokumenten, die als „►M2 SECRET UE ◄“ oder „►M2 TRES SECRET UE/EU TOP SECRET ◄“ 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.

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 „►M2 TRES SECRET UE/EU TOP SECRET ◄“ in Umlauf zu bringen, ist möglichst klein zu halten, und ihre Namen sind in einer Liste zu verzeichnen, die vom ►M3 Direktion Sicherheit 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 „►M2 TRES SECRET UE/EU TOP SECRET ◄“.

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.

▼M1

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 „►M2 CONFIDENTIEL UE ◄“ 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 „►M2 CONFIDENTIEL UE ◄“ 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;

▼**M1**

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 „►**M2** CONFIDENTIEL UE ◄“ 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 „►**M2** CONFIDENTIEL UE ◄“ 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 „►**M2** RESTREINT UE ◄“ 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 „►**M2** TRES SECRET UE/EU TOP SECRET ◄“ eingestuften Verschlusssachen in Sicherheitsbereichen der Kategorie I oder II auf nationaler Ebene zugelassen sind;

▼**M1**

— Typ B: Behältnisse, die zur Aufbewahrung von als „►**M2** SECRET UE ◄“ und „►**M2** CONFIDENTIEL UE ◄“ eingestuften Verschlusssachen in Sicherheitsbereichen der Kategorie I oder II auf nationaler Ebene zugelassen sind;

— Typ C: Büromöbel, die ausschließlich für die Aufbewahrung von als „►**M2** RESTREINT UE ◄“ 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 „►**M2** CONFIDENTIEL UE ◄“ 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 ►**M3** Direktion Sicherheit 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 ►**M3** Direktion Sicherheit der Kommission ◄ unterhält diese Verzeichnisse unter anderem auf der Grundlage der von den nationalen Sicherheitsbehörden mitgeteilten Informationen.

▼**M1**

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 „►**M2** SECRET UE ◄“ und höher eingestufte Verschlusssachen gesprochen wird, sind bei entsprechendem Risiko gegen Ab- und Mithören zu schützen. Für die Einschätzung des Risikos ist das ►**M3** Direktion Sicherheit 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 ►**M3** Direktion Sicherheit 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 „►**M2** SECRET UE ◄“ und höher verwendet werden, auf Ersuchen des ►**M3** Direktor der Direktion Sicherheit 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-SICHERHEITSÜBERPRÜFUNG 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 „►**M2** TRES SECRET UE/EU TOP SECRET ◄“, „►**M2** SECRET UE ◄“ und „►**M2** CONFIDENTIEL UE ◄“ eingestuften Verschlusssachen wird nur Personen gestattet, die der entsprechenden Sicherheitsüberprüfung unterzogen worden sind.

▼**M1**

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 „►M2 TRES SECRET UE/EU TOP SECRET ◄“ eingestuften Verschlusssachen**

Alle Personen, die Zugang zu als „►**M2** TRES SECRET UE/EU TOP SECRET ◄“ eingestuften Verschlusssachen benötigen, müssen zunächst einer Sicherheitsüberprüfung in Bezug auf den Zugang zu den betreffenden Verschlusssachen unterzogen werden.

Alle Personen, die Zugang zu als „►**M2** TRES SECRET UE/EU TOP SECRET ◄“ eingestuften Verschlusssachen benötigen, sind von dem für Sicherheitsfragen zuständigen Mitglied der Kommission zu benennen, und ihre Namen sind in das einschlägige „►**M2** TRES SECRET UE/EU TOP SECRET ◄“-Register einzutragen. Dieses Register wird vom ►**M3** Direktion Sicherheit der Kommission ◄ angelegt und geführt.

Bevor diesen Personen der Zugang zu als „►**M2** TRES SECRET UE/EU TOP SECRET ◄“ 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 „►**M2** TRES SECRET UE/EU TOP SECRET ◄“ 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 „►**M2** TRES SECRET UE/EU TOP SECRET ◄“ 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 „►**M2** TRES SECRET UE/EU TOP SECRET ◄“ eingestuften Verschlusssachen verfügen müssen, werden aus dem „►**M2** TRES SECRET UE/EU TOP SECRET ◄“-Verzeichnis gestrichen. Ferner werden alle betreffenden Personen erneut auf ihre besondere Verantwortung für den Schutz von als „►**M2** TRES SECRET UE/EU TOP SECRET ◄“ eingestuften Verschlusssachen belehrt. Sie haben ferner eine Erklärung zu unterzeichnen, wonach sie ihre Kenntnisse über als „►**M2** TRES SECRET UE/EU TOP SECRET ◄“ eingestufte Verschlusssachen weder verwenden noch weitergeben werden.

▼M1

19.3. **Besondere Vorschriften für den Zugang zu als „►M2 SECRET UE ◄“ und „►M2 CONFIDENTIEL UE ◄“ eingestuften Verschlusssachen**

Alle Personen, die Zugang zu als „►M2 SECRET UE ◄“ oder „►M2 CONFIDENTIEL UE ◄“ eingestuften Verschlusssachen benötigen, müssen zunächst einer Sicherheitsüberprüfung in Bezug auf den geeigneten Geheimhaltungsgrad unterzogen werden.

Alle Personen, die Zugang zu als „►M2 SECRET UE ◄“ oder „►M2 CONFIDENTIEL UE ◄“ 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 „►M2 SECRET UE ◄“ oder „►M2 CONFIDENTIEL UE ◄“ 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 „►M2 RESTREINT UE ◄“ eingestuften Verschlusssachen**

Alle Personen, die Zugang zu als „►M2 RESTREINT UE ◄“ 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 ►M3 Direktion Sicherheit der Kommission ◄ wird jedoch die Beamten und sonstigen Bediensteten, für die es zuständig ist, über Reiseregelungen unterrichten, denen sie möglicherweise unterliegen.

▼M1

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 „►M2 TRES SECRET UE/EU TOP SECRET ◄“, „►M2 SECRET UE ◄“ und „►M2 CONFIDENTIEL UE ◄“ 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 ►M3 Direktor der Direktion Sicherheit 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 ►M3 Direktion Sicherheit 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 ►M3 Direktor der Direktion Sicherheit der Kommission ◄ entzogen, wenn seiner Ansicht nach hierzu Grund besteht. Die Entzugsverfügung wird der betreffenden Person, die beantragen kann, vom ►M3 Direktor der Direktion Sicherheit der Kommission ◄ gehört zu werden, sowie der zuständigen nationalen Behörde mitgeteilt.

i) Die Sicherheitsüberprüfung wird unter Mitwirkung der betreffenden Person auf Ersuchen des ►M3 Direktor der Direktion Sicherheit 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 ►M3 Direktor der Direktion Sicherheit 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 ►M3 Direktor der Direktion Sicherheit 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 ►M3 Direktor der Direktion Sicherheit der Kommission ◄ 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 ►M3 Direktor der Direktion Sicherheit der Kommission ◄ gehört zu werden. Der ►M3 Direktor der Direktion Sicherheit 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.

▼**M1**

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 ►**M3** Direktor der Direktion Sicherheit 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 ►**M3** Direktor der Direktion Sicherheit 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 „►**M2** TRES SECRET UE/EU TOP SECRET ◄“ 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 „►**M2** TRES SECRET UE/EU TOP SECRET ◄“ erhalten sollen, vorläufig und befristet zum Zugang zu als „►**M2** SECRET UE ◄“ 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 „►**M2** CONFIDENTIEL UE ◄“ 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 „►**M2** TRES SECRET UE/EU TOP SECRET ◄“ und „►**M2** SECRET UE ◄“ 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 „►**M2** CONFIDENTIEL UE ◄“ oder höher eingestuft werden.

2. Dokumente, die als „►**M2** CONFIDENTIEL UE ◄“ 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 „►**M2** TRES SECRET UE/EU TOP SECRET ◄“ werden über Registraturen verteilt, die den Vermerk „►**M2** TRES SECRET UE/EU TOP SECRET ◄“ tragen (siehe Abschnitt 22.2). Im Falle von Mitteilungen, die als „►**M2** TRES SECRET UE/EU TOP SECRET ◄“ eingestuft sind, kann die zuständige Registratur dem Leiter des Kommunikationszentrums gestatten, die in der Liste der Empfänger angegebene Anzahl von Ausfertigungen zu erstellen.

▼M1

3. Als „►M2 SECRET UE ◄“ 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 „►M2 CONFIDENTIEL UE ◄“ 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 „►M2 CONFIDENTIEL UE ◄“ 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 „►M2 CONFIDENTIEL UE ◄“ 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 „►M2 TRES SECRET UE/EU TOP SECRET ◄“ nur unter Zuhilfenahme offizieller Kurierdienste oder durch Personen übermittelt werden, die eine Zugangsermächtigung zu als „►M2 TRES SECRET UE/EU TOP SECRET ◄“ eingestuften Verschlusssachen haben.

2. Wird zur Übermittlung eines als „►M2 TRES SECRET UE/EU TOP SECRET ◄“ 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 ►M2 TRES SECRET UE/EU TOP SECRET ◄ eingestuften Dokumenten jederzeit unter der direkten Aufsicht eines verantwortlichen Beamten befinden.

3. In Ausnahmefällen können Beamte, die nicht Boten sind, als „►M2 TRES SECRET UE/EU TOP SECRET ◄“ 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 „►M2 TRES SECRET UE/EU TOP SECRET ◄“ eingestuften Dokumenten ermächtigt ist;

▼M1

b) die Form der Beförderung den Vorschriften für die Übermittlung von Dokumenten des Geheimhaltungsgrades „►M2 TRES SECRET UE/EU TOP SECRET ◄“ entspricht;

c) der Beamte die Dokumente des Geheimhaltungsgrades „►M2 TRES SECRET UE/EU TOP SECRET ◄“ unter keinen Umständen unbeaufsichtigt lässt;

d) Vorkehrungen getroffen werden, damit die Liste der Dokumente, die mitgenommen werden, in der „►M2 TRES SECRET UE/EU TOP SECRET ◄“-Registratur verwahrt, in einem Dienstbuch vermerkt und bei Rückkehr anhand dieses Eintrags kontrolliert wird.

4. Innerhalb ein und desselben Landes dürfen als „►M2 SECRET UE ◄“ oder „►M2 CONFIDENTIEL UE ◄“ 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 ►M3 Direktion Sicherheit 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 „►M2 CONFIDENTIEL UE ◄“ oder höher eingestuftes Material ist durch diplomatische oder militärische Kurierdienste zu befördern.

2. Eine persönliche Beförderung von als „►M2 SECRET UE ◄“ oder „►M2 CONFIDENTIEL UE ◄“ 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 ►M3 Direktion Sicherheit der Kommission ◄ arbeitet Anweisungen über die zwischenstaatliche persönliche Beförderung von Material des Geheimhaltungsgrades „►M2 SECRET UE ◄“ 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;

▼**M1**

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 „►**M2** RESTREINT UE ◄“*

Für die Beförderung von als „►**M2** RESTREINT UE ◄“ 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 „►**M2** SECRET UE ◄“ und „►**M2** CONFIDENTIEL UE ◄“ 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 „►**M2** CONFIDENTIEL UE ◄“ oder „►**M2** SECRET UE ◄“ 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 „►**M2** TRES SECRET UE/EU TOP SECRET ◄“-Dokumenten kann ausschließlich der Urheber gestatten.

2. Fordern Personen, die nicht über eine „►**M2** TRES SECRET UE/EU TOP SECRET ◄“-Sicherheitsermächtigung verfügen, Informationen an, die zwar in einem „►**M2** TRES SECRET UE/EU TOP SECRET ◄“-Dokument enthalten, aber nicht als solche eingestuft sind, so kann der Leiter der „►**M2** TRES SECRET UE/EU TOP SECRET ◄“-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 „►**M2** SECRET UE ◄“ 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.

▼**M1**

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 „►**M2** SECRET UE ◄“ und „►**M2** CONFIDENTIEL UE ◄“ 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.

▼M1

22.2. **Die „►M2 TRES SECRET UE/EU TOP SECRET ◄“-Registratur**

22.2.1. *Allgemeines*

1. Durch eine „►M2 TRES SECRET UE/EU TOP SECRET ◄“-Zentralregistratur wird die Registrierung, Handhabung und Verteilung von „►M2 TRES SECRET UE/EU TOP SECRET ◄“-Dokumenten gemäß den Sicherheitsvorschriften gewährleistet. Die „►M2 TRES SECRET UE/EU TOP SECRET ◄“-Registratur wird von dem Kontrollbeauftragten für die „►M2 TRES SECRET UE/EU TOP SECRET ◄“-Registratur geleitet.

2. Die „►M2 TRES SECRET UE/EU TOP SECRET ◄“-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 „►M2 TRES SECRET UE/EU TOP SECRET ◄“-Dokumenten zuständig sind; sie führen ein Register der von ihnen aufbewahrten Dokumente, das stets auf dem neuesten Stand gehalten wird.

4. „►M2 TRES SECRET UE/EU TOP SECRET ◄“-Unterregistraturen werden nach Maßgabe des Abschnitts 22.2.3 eingerichtet, damit längerfristigen Notwendigkeiten entsprochen werden kann; sie werden einer zentralen „►M2 TRES SECRET UE/EU TOP SECRET ◄“-Registratur zugeordnet. Müssen „►M2 TRES SECRET UE/EU TOP SECRET ◄“-Dokumente nur zeitweilig und gelegentlich konsultiert werden, so können sie ohne Einrichtung einer „►M2 TRES SECRET UE/EU TOP SECRET ◄“-Unterregistratur weitergeleitet werden, sofern Vorschriften festgelegt wurden, die gewährleisten, dass diese Dokumente unter der Kontrolle der entsprechenden „►M2 TRES SECRET UE/EU TOP SECRET ◄“-Registratur verbleiben und alle materiellen und personenbezogenen Sicherheitsmaßnahmen eingehalten werden.

5. Unterregistraturen ist es nicht gestattet, ohne ausdrückliche Zustimmung ihrer „►M2 TRES SECRET UE/EU TOP SECRET ◄“-Zentralregistratur „►M2 TRES SECRET UE/EU TOP SECRET ◄“-Dokumente unmittelbar an andere Unterregistraturen derselben Zentralregistratur zu übermitteln.

6. Der Austausch von „►M2 TRES SECRET UE/EU TOP SECRET ◄“-Dokumenten zwischen Unterregistraturen, die nicht derselben Zentralregistratur zugeordnet sind, muss über die „►M2 TRES SECRET UE/EU TOP SECRET ◄“-Zentralregistraturen abgewickelt werden.

22.2.2. *Die „►M2 TRES SECRET UE/EU TOP SECRET ◄“-Zentralregistratur*

In seiner Eigenschaft als Kontrollbeauftragter ist der Leiter der „►M2 TRES SECRET UE/EU TOP SECRET ◄“-Zentralregistratur zuständig für

a) die Übermittlung von „►M2 TRES SECRET UE/EU TOP SECRET ◄“-Dokumenten gemäß den in Abschnitt 21.3 festgelegten Vorschriften;

b) die Führung einer Liste aller ihm unterstehenden „►M2 TRES SECRET UE/EU TOP SECRET ◄“-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 „►M2 TRES SECRET UE/EU TOP SECRET ◄“-Dokumente;

▼**M1**

d) die Führung eines Registers aller aufbewahrten und verteilten „►**M2** TRES SECRET UE/EU TOP SECRET ◄“-Dokumente;

e) die Führung einer aktuellen Liste aller „►**M2** TRES SECRET UE/EU TOP SECRET ◄“-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 „►**M2** TRES SECRET UE/EU TOP SECRET ◄“-Dokumente gemäß den Vorschriften des Abschnitts 18.

22.2.3. *„►**M2** TRES SECRET UE/EU TOP SECRET ◄“-Unterregistraturen*

In seiner Eigenschaft als Kontrollbeauftragter ist der Leiter einer „►**M2** TRES SECRET UE/EU TOP SECRET ◄“-Unterregistratur zuständig für

a) die Übermittlung von „►**M2** TRES SECRET UE/EU TOP SECRET ◄“-Dokumenten gemäß den in Abschnitt 21.3 festgelegten Vorschriften;

b) die Führung einer aktuellen Liste aller Personen, die befugt sind, Zugang zu den „►**M2** TRES SECRET UE/EU TOP SECRET ◄“-Informationen zu erhalten, welche seiner Aufsicht unterliegen;

c) die Verteilung von „►**M2** TRES SECRET UE/EU TOP SECRET ◄“-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 „►**M2** TRES SECRET UE/EU TOP SECRET ◄“-Dokumente, die seiner Aufsicht unterliegen oder die an andere „►**M2** TRES SECRET UE/EU TOP SECRET ◄“-Registraturen weitergeleitet wurden, und Aufbewahrung aller entsprechenden Empfangsbescheinigungen;

e) die Führung einer aktuellen Liste der „►**M2** TRES SECRET UE/EU TOP SECRET ◄“-Registraturen, mit denen er „►**M2** TRES SECRET UE/EU TOP SECRET ◄“-Dokumente austauschen darf, mit Name und Unterschrift ihrer Kontrollbeauftragten und bevollmächtigten Stellvertreter;

f) den materiellen Schutz aller in der Unterregistratur aufbewahrten „►**M2** TRES SECRET UE/EU TOP SECRET ◄“-Dokumente gemäß den Vorschriften des Abschnitts 18.

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

1. Alljährlich führt jede „►**M2** TRES SECRET UE/EU TOP SECRET ◄“-Registratur im Sinne dieses Abschnitts eine detaillierte Bestandsaufnahme der „►**M2** TRES SECRET UE/EU TOP SECRET ◄“-Dokumente durch. Als nachgewiesen gilt jedes Dokument, das in der Registratur materiell vorhanden ist oder für das die Empfangsbescheinigung einer „►**M2** TRES SECRET UE/EU TOP SECRET ◄“-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 „►**M2** TRES SECRET UE/EU TOP SECRET ◄“-Unterregistraturen übermitteln die Ergebnisse ihrer jährlichen Bestandsaufnahme der Zentralregistratur, der sie unterstehen, zu einem von dieser festgelegten Datum.

▼M1

3. EU-Verschlusssachen mit einer niedrigeren Einstufung als „►M2 TRES SECRET UE/EU TOP SECRET ◄“ 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, „►M2 TRES SECRET UE/EU TOP SECRET ◄“, „►M2 SECRET UE ◄“ und „►M2 CONFIDENTIEL UE ◄“-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 „►M2 TRES SECRET UE/EU TOP SECRET ◄“-Dokuments wird dem Urheber mitgeteilt;

   d) die Filmrollen oder sonstigen Träger enthalten nur Dokumente der gleichen „►M2 TRES SECRET UE/EU TOP SECRET ◄“, „►M2 SECRET UE ◄“ oder „►M2 CONFIDENTIEL UE ◄“-Einstufung;

   e) das Mikrofilmen/die Speicherung eines „►M2 TRES SECRET UE/EU TOP SECRET ◄“ oder „►M2 SECRET UE ◄“-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) „►M2 TRES SECRET UE/EU TOP SECRET ◄“-Dokumente werden nur von der für diese Dokumente zuständigen Zentralregistratur vernichtet. Jedes der Vernichtung zugeführte Dokument wird auf einer Vernichtungsbescheinigung eingetragen, die vom „►M2 TRES SECRET UE/EU TOP SECRET ◄“-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.

▼**M1**

c) „►**M2** TRES SECRET UE/EU TOP SECRET ◄“-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 „►**M2** TRES SECRET UE/EU TOP SECRET ◄“-Kontrollbeauftragten durch Verbrennen, Einstampfen, Zerkleinern oder andere geeignete Verfahren so vernichtet, dass der Inhalt weder erkennbar ist noch erkennbar gemacht werden kann.

2. „►**M2** SECRET UE ◄“-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 „►**M2** SECRET UE ◄“-Dokumente werden auf einer unterzeichneten Vernichtungsbescheinigung eingetragen, die von der Registratur zusammen mit den Verteilungsunterlagen mindestens drei Jahre lang aufbewahrt wird.

3. „►**M2** CONFIDENTIEL UE ◄“-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. „►**M2** RESTREINT UE ◄“-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 „►**M2** SECRET UE ◄“- und „►**M2** CONFIDENTIEL UE ◄“-Unterlagen im Krisenfall dürfen auf keinen Fall den Schutz oder die Vernichtung von „►**M2** TRES SECRET UE/EU TOP SECRET ◄“-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.

▼**M1**

23.2. **Zuständigkeiten**

23.2.1. ►**M3** *Direktion Sicherheit der Kommission* ◄

Das ►**M3** Direktion Sicherheit 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 ►**M3** Direktion Sicherheit 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 ►**M3** Direktion Sicherheit 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 ►**M3** Direktion Sicherheit 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;

▼M1

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.

▼**M1**

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.

▼**M1**

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 ►**M3** Direktion Sicherheit der Kommission ◄ zu benachrichtigen.

Fälle, in denen es um als „►**M2** RESTREINT UE ◄“ 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 „►**M2** CONFIDENTIEL UE ◄“ 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 „►**M2** RESTREINT UE ◄“ 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.

▼**M1**

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 ►**M3** Direktion Sicherheit 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 „►**M2** CONFIDENTIEL UE ◄“ 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 ►**M3** Direktion Sicherheit 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 „►**M2** RESTREINT UE ◄“ 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.

▼**M1**

25.1.5. *Sicherheitsmodus*

Alle Systeme, in denen als „►**M2** CONFIDENTIEL UE ◄“ 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.

▼**M1**

„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.

▼**M1**

„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.

▼M1

(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.

▼**M1**

Das ►**M3** Direktion Sicherheit 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 ►**M3** Direktion Sicherheit der Kommission ◄ sofort tätig.

Das ►**M3** Direktion Sicherheit der Kommission ◄ hat ein INFOSEC-Referat.

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

Der ►**M3** Direktor der Direktion Sicherheit 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.

▼**M1**

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 „►**M2** CONFIDENTIEL UE ◄“ 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.

▼**M1**

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 „►**M2** SECRET UE ◄“ 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 „►**M2** SECRET UE ◄“ oder höher eingestuft sind, beinhalten diese Verfahren besondere Anweisungen für die Nachvollziehbarkeit in Bezug auf diese Informationen.

▼**M1**

25.5.3. *Behandlung und Kontrolle von austauschbaren elektronischen Datenträgern*

Alle austauschbaren elektronischen Datenträger, die als „►**M2** CONFIDENTIEL UE ◄“ 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 „►**M2** TRES SECRET UE/EU TOP SECRET ◄“ 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 ►**M3** Direktor der Direktion Sicherheit 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 „►**M2** SECRET UE ◄“ 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 „►**M2** CONFIDENTIEL UE ◄“ oder „►**M2** RESTREINT UE ◄“ 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 ►**M3** Direktion Sicherheit der Kommission ◄ nach Konsultation der Beratenden Gruppe für das Sicherheitskonzept der Kommission erlässt.

Unter außergewöhnlichen Betriebsbedingungen können Informationen der Geheimhaltungsgrade „►**M2** RESTREINT UE ◄“, „►**M2** CONFIDENTIEL UE ◄“ und „►**M2** SECRET UE ◄“ 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

▼**M1**

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 „►**M2** CONFIDENTIEL UE ◄“ 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.

▼M1

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.

▼**M1**

Alle Systeme, die Sicherheitseigenschaften aufweisen, werden regelmäßig von der SAA kontrolliert oder überprüft. Bei Systemen, die Informationen des Geheimhaltungsgrades „►**M2** TRES SECRET UE/EU TOP SECRET ◄“ 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 ►**M3** Direktor der Direktion Sicherheit 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 ►**M3** Direktor der Direktion Sicherheit 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.

▼**M1**

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 „►**M2** RESTREINT UE ◄“ 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.

▼**M1**

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.

▼**M4**

27. GEMEINSAME MINDESTNORMEN FÜR INDUSTRIELLE SICHERHEIT

27.1. **Einleitung**

Dieser Abschnitt behandelt die besonderen Sicherheitsaspekte von Industrietätigkeiten im Zusammenhang mit der Aushandlung und Vergabe von Aufträgen und mit Finanzhilfevereinbarungen, bei denen industrielle oder andere Einrichtungen mit Aufgaben betraut werden, bei denen EU-Verschlusssachen herangezogen werden, gebraucht werden und/oder mit eingeschlossen sind, wozu auch die Weitergabe von und der Zugang zu EU-Verschlusssachen während des Verfahrens für die Vergabe öffentlicher Aufträge und von Aufrufen zur Einreichung von Vorschlägen (Ausschreibungsfrist und Verhandlungen vor dem Vertragsabschluss) gehören.

27.2. **Begriffsbestimmungen**

Für die Zwecke dieser gemeinsamen Mindestnormen bezeichnet der Ausdruck

a) „als Verschlusssache eingestufter Auftrag“ einen Vertrag oder eine Finanzhilfevereinbarung über die Lieferung von Waren, die Durchführung von Arbeiten, die Bereitstellung von Gebäuden oder die Erbringung von Dienstleistungen, dessen bzw. deren Ausführung den Zugang oder die Erstellung von EU-Verschlusssachen erfordert oder mit sich bringt;

b) „als Verschlusssache eingestufter Unterauftrag“ einen Vertrag zwischen einem Auftragnehmer oder dem Empfänger einer Finanzhilfe und einem anderen Auftragnehmer (Nachunternehmer) über die Lieferung von Waren, die Durchführung von Arbeiten, die Bereitstellung von Gebäuden oder die Erbringung von Dienstleistungen, dessen Ausführung den Zugang oder die Erstellung von EU-Verschlusssachen erfordert oder mit sich bringt;

c) „Auftragnehmer“ einen Wirtschaftsteilnehmer oder eine juristische Person, die geschäftsfähig ist oder Finanzhilfen erhalten kann;

d) „Beauftragte Sicherheitsbehörde (DSA)“ eine Behörde, die gegenüber der Nationalen Sicherheitsbehörde (NSA) eines EU-Mitgliedstaats für die Unterrichtung industrieller oder anderer Einrichtungen über die nationale Politik in allen Fragen der industriellen Sicherheit und für Weisungen und Unterstützung bei ihrer Umsetzung verantwortlich ist. Die Funktion der Beauftragen Sicherheitsbehörde kann von der Nationalen Sicherheitsbehörde wahrgenommen werden;

e) „Sicherheitsbescheid für Einrichtungen (FSC)“ die verwaltungsrechtliche Feststellung durch eine Nationale Sicherheitsbehörde/Beauftragte Sicherheitsbehörde, dass eine Einrichtung unter dem Gesichtspunkt der Sicherheit ausreichenden Schutz für EU-Verschlusssachen eines festgelegten Geheimhaltungsgrades bietet, und dass ihr Personal, das Zugang zu EU-Verschlusssachen haben muss, ordnungsgemäß sicherheitsüberprüft ist und über die für den Zugang zu und den Schutz von EU-Verschlusssachen erforderlichen einschlägigen Sicherheitsanforderungen informiert wurde;

f) „industrielle oder andere Einrichtung“ einen Auftragnehmer oder Nachunternehmer, der an der Lieferung von Waren, der Durchführung von Arbeiten oder der Erbringung von Dienstleistungen beteiligt ist; dabei kann es sich um Industrie-, Handels-, Dienstleistungs-, Wissenschafts-, Forschungs-, Bildungs- oder Entwicklungseinrichtungen handeln;

g) „industrielle Sicherheit“ die Anwendung von Schutzmaßnahmen und Verfahren zur Verhütung oder Erkennung des Verlustes oder der Preisgabe von EU-Verschlusssachen oder zur Sicherstellung im Zusammenhang damit, mit denen ein Auftragnehmer oder Nachunternehmer während der Verhandlungen vor der Auftragsvergabe und im Rahmen des als Verschlusssache eingestuften Auftrags zu tun hat;

▼M4

h) „Nationale Sicherheitsbehörde (NSA)“ die staatliche Behörde eines EU-Mitgliedstaats, bei der die Endverantwortung für den Schutz von EU-Verschlusssachen in dem betreffenden Mitgliedstaat liegt;

i) „globaler Geheimhaltungsgrad eines Auftrags“ den Geheimhaltungsgrad, der für den gesamten Auftrag oder die gesamte Finanzhilfevereinbarung auf der Grundlage der Einstufung von Informationen und/oder Materialien, die im Rahmen einer beliebigen Komponente des Gesamtauftrags oder der gesamten Finanzhilfevereinbarung erstellt, weitergegeben oder eingesehen werden müssen oder können, festgelegt wird. Der globale Geheimhaltungsgrad eines Auftrags darf nicht niedriger sein als der höchste Einstufungsgrad jeder einzelnen Komponente; er kann aber aufgrund des Kumulierungseffekts höher sein;

j) „Geheimschutzklausel (SAL)“ besondere Auftragsbedingungen der Vergabebehörde, die fester Bestandteil eines als Verschlusssache eingestuften und mit dem Zugang zu oder der Erstellung von EU-Verschlusssachen verbundenen Auftrags sind, und in denen die Sicherheitsanforderungen oder die schutzbedürftigen Komponenten des Auftrags festgelegt sind;

k) „Einstufungsleitfaden für Verschlusssachen (SCG)“ ein Dokument, das die Komponenten eines als Verschlusssache eingestuften Vorhabens, Auftrags oder einer Finanzhilfevereinbarung beschreibt und in dem die anzuwendenden Geheimhaltungsgrade anzugeben sind. Der Einstufungsleitfaden für Verschlusssachen kann während der Laufzeit des Vorhabens, des Auftrags oder der Finanzhilfevereinbarung erweitert werden, und Teile der Informationen können neu eingestuft oder herabgestuft werden. Ein solcher Leitfaden muss Teil der Geheimschutzklausel sein.

27.3. **Organisation**

a) Die Kommission kann industrielle oder andere Einrichtungen, die in einem Mitgliedstaat eingetragen sind, durch einen als Verschlusssache eingestuften Auftrag mit Aufgaben betrauen, bei denen EU-Verschlusssachen herangezogen werden, gebraucht werden und/oder mit eingeschlossen sind.

b) Die Kommission trägt dafür Sorge, dass bei der Vergabe von als Verschlusssache eingestuften Aufträgen alle sich aus den vorliegenden Mindestnormen ergebenden Anforderungen eingehalten werden.

c) Die Kommission zieht zur Anwendung der vorliegenden Mindestnormen für industrielle Sicherheit die zuständige(n) Nationale(n) Sicherheitsbehörde(n) hinzu. Die Nationalen Sicherheitsbehörden können eine oder mehrere Beauftragte Sicherheitsbehörden damit betrauen.

d) Die endgültige Verantwortung für den Schutz von EU-Verschlusssachen innerhalb von industriellen und anderen Einrichtungen liegt bei der Leitung dieser Einrichtungen.

e) Bei jeder Vergabe eines unter diese Mindestnormen fallenden Auftrags oder Unterauftrags verständigt die Kommission und/oder die Nationale Sicherheitsbehörde/die Beauftragte Sicherheitsbehörde — je nachdem, was zutrifft — unverzüglich die Nationale Sicherheitsbehörde/die Beauftragte Sicherheitsbehörde des Mitgliedstaats, in dem der Auftragnehmer oder Nachunternehmer eingetragen ist.

27.4. **Als Verschlusssache eingestufte Aufträge und Finanzhilfeentscheidungen**

a) Der Geheimhaltungsgrad von als Verschlusssache eingestuften Aufträgen oder Finanzhilfevereinbarungen muss sich nach folgenden Grundsätzen richten:

— Die Kommission legt gegebenenfalls die schutzbedürftigen Aspekte des Auftrags und den entsprechenden Geheimhaltungsgrad fest, und zwar unter Berücksichtigung des ursprünglichen Geheimhaltungsgrades, den der Urheber den vor der Auftragsvergabe entstandenen Informationen zugewiesen hat.

— Der globale Geheimhaltungsgrad des Auftrags darf nicht niedriger sein als der höchste Grad jeder einzelnen Auftragskomponente.

— Im Rahmen von vertraglichen Tätigkeiten entstandene EU-Verschlusssachen werden anhand des Einstufungsleitfadens für Verschlusssachen eingestuft.

▼M4

— In den Fällen, in denen es zweckmäßig ist, trägt die Kommission die Verantwortung für die Änderung des globalen Geheimhaltungsgrades des Auftrags oder des Geheimhaltungsgrades jeder einzelner seiner Komponenten, und zwar in Absprache mit dem Urheber und zur Unterrichtung aller Betroffenen.

— Verschlusssachen, die an den Auftragnehmer oder Nachunternehmer weitergegeben werden oder im Rahmen einer vertraglichen Tätigkeit erstellt werden, dürfen nicht für andere als die Zwecke verwendet werden, die in dem als Verschlusssache eingestuften Auftrag festgelegt sind; sie dürfen nicht ohne vorherige schriftliche Zustimmung des Urhebers an Dritte weitergegeben werden.

b) Die Kommission und die Nationalen Sicherheitsbehörden/Beauftragten Sicherheitsbehörden der betreffenden Mitgliedstaaten tragen dafür Sorge, dass Auftragnehmer und Nachunternehmer, die den Zuschlag für als Verschlusssache eingestufte Aufträge mit Informationen des Geheimhaltungsgrades CONFIDENTIEL UE oder darüber erhalten, alle geeigneten Maßnahmen zum Schutz solcher EU-Verschlusssachen treffen, die im Zuge der Ausführung des als Verschlusssache eingestuften Auftrags gemäß den einzelstaatlichen Gesetzen und Vorschriften an sie weitergegeben oder von ihnen erstellt werden. Die Nichteinhaltung der Sicherheitsanforderungen kann die Kündigung des als Verschlusssache eingestuften Auftrags zur Folge haben.

c) Alle industriellen und anderen Einrichtungen, die an als Verschlusssache eingestuften Aufträgen beteiligt sind, die mit dem Zugang zu Informationen des Geheimhaltungsgrades CONFIDENTIEL UE oder höher verbunden sind, müssen im Besitz eines einzelstaatlichen Sicherheitsbescheids für Einrichtungen sein. Dieser Bescheid wird von der Nationalen Sicherheitsbehörde/Beauftragten Sicherheitsbehörde eines Mitgliedstaats zur Bestätigung darüber ausgestellt, dass eine Einrichtung in der Lage ist, unter dem Gesichtspunkt der Sicherheit ausreichenden Schutz von EU-Verschlusssachen bis zu dem entsprechenden Geheimhaltungsgrad zu bieten und zu gewährleisten.

d) Bei der Vergabe eines als Verschlusssache eingestuften Auftrags beantragt ein vom Management des Auftragnehmers oder Nachunternehmers ernannter Sicherheitsbeauftragter (FSO) für alle Personen, die in einer in einem Mitgliedstaat eingetragenen industriellen oder anderen Einrichtung beschäftigt sind und die im Rahmen eines als Verschlusssache eingestuften Auftrags Zugang zu EU-Verschlusssachen mit dem Geheimhaltungsgrad CONFIDENTIEL EU oder darüber haben, eine Sicherheitsüberprüfung (Personnel Security Clearance — PSC); diese Sicherheitsüberprüfung wird von der Nationalen Sicherheitsbehörde/Beauftragten Sicherheitsbehörde des betreffenden Mitgliedstaats nach den einzelstaatlichen Bestimmungen durchgeführt.

e) Als Verschlusssache eingestufte Aufträge müssen die in Nummer 27.2 Buchstabe j festgelegte Geheimschutzklausel umfassen. Die Geheimschutzklausel muss den Einstufungsleitfaden für Verschlusssachen umfassen.

f) Vor Beginn der Verhandlungen über einen als Verschlusssache eingestuften Auftrag setzt sich die Kommission mit der jeweiligen Nationalen Sicherheitsbehörde/der Beauftragten Sicherheitsbehörde des Mitgliedstaats, in dem die betreffende industrielle oder andere Einrichtungen eingetragen ist (sind), in Verbindung, um die Bestätigung zu erhalten, dass diese Behörden im Besitz eines gültigen, dem Geheimhaltungsgrad des Auftrags entsprechenden Sicherheitsbescheids für Einrichtungen sind.

g) Die Vergabebehörde darf keinen als Verschlusssache eingestuften Auftrag an einen bevorzugten Wirtschaftsteilnehmer vergeben, bevor sie den gültigen Sicherheitsbescheid für die Einrichtungen erhalten hat.

h) Bei Aufträgen mit Informationen des Geheimhaltungsgrades RESTREINT UE ist ein Sicherheitsbescheid für Einrichtungen nicht erforderlich, es sei denn, die einzelstaatlichen Gesetze und Vorschriften schreiben einen solchen Bescheid vor.

i) Aufforderungen zur Angebotsabgabe im Zusammenhang mit als Verschlusssachen eingestuften Aufträgen müssen eine Klausel enthalten, die vorsieht, dass ein Wirtschaftsteilnehmer, der eine Angebotsabgabe unterlässt oder der nicht ausgewählt wird, alle Unterlagen innerhalb einer vorgegebenen Frist zurückgeben muss.

j) Gegebenenfalls muss ein Auftragnehmer auf verschiedenen Ebenen mit Nachunternehmern über als Verschlusssache eingestufte Unteraufträge verhandeln. Der Auftragnehmer hat dafür Sorge zu tragen, dass alle Tätigkeiten, die Unteraufträge betreffen, gemäß den gemeinsamen Mindestnormen nach diesem Abschnitt ausgeübt werden. Der Auftragnehmer darf einem Nachunternehmer jedoch nicht ohne vorherige schriftliche Zustimmung des Urhebers EU-Verschlusssachen oder als solche eingestufte Materialen übermitteln.

▼M4

k) Die Bedingungen, zu denen der Auftragnehmer Unteraufträge vergeben darf, müssen in der Ausschreibung oder in der Aufforderung zur Einreichung von Vorschlägen sowie in dem als Verschlusssache eingestuften Auftrag festgelegt sein. Die Vergabe von Unteraufträgen an Einrichtungen, die in einem EU-Nichtmitgliedstaat eingetragen sind, bedarf der vorherigen Zustimmung der Kommission.

l) Während der Dauer des als Verschlusssache eingestuften Auftrags überwacht die Kommission in Abstimmung mit der zuständigen Nationalen Sicherheitsbehörde/Beauftragten Sicherheitsbehörde die Einhaltung aller Sicherheitsanforderungen des Auftrags. Sicherheitsrelevante Zwischenfälle werden gemäß den in Teil II Abschnitt 24 dieser Sicherheitsvorschriften festgelegten Bestimmungen gemeldet. Bei Änderung des Sicherheitsbescheids für Einrichtungen oder bei Entzug dieses Bescheids wird die Kommission und jede andere Nationale Sicherheitsbehörde/Beauftragte Sicherheitsbehörde, der die Ausstellung des Bescheids notifiziert wurde, unverzüglich davon unterrichtet.

m) Bei Kündigung eines als Verschlusssache eingestuften Auftrags oder Unterauftrags benachrichtigt die Kommission und/oder die Nationale Sicherheitsbehörde/Beauftragte Sicherheitsbehörde — je nachdem, was zutrifft — umgehend die Nationale Sicherheitsbehörde/Beauftragte Sicherheitsbehörde des Mitgliedstaats, in dem der Auftragnehmer oder Nachunternehmer eingetragen ist.

n) Die gemeinsamen Mindestnormen dieses Abschnitts sind weiter einzuhalten; nach Kündigung oder Beendigung des als Verschlusssache eingestuften Auftrags oder Unterauftrags gewährleisten die Auftragnehmer und Nachunternehmer weiterhin die Vertraulichkeit der Verschlusssache.

o) Die besonderen Bestimmungen für die Vernichtung von Verschlusssachen bei Auftragsende werden in der Geheimschutzklausel oder in anderen einschlägigen Vorschriften unter Angabe der Sicherheitsanforderungen festgelegt.

p) Die in diesem Abschnitt genannten Pflichten und Bedingungen gelten entsprechend auch für Verfahren zur Gewährung von Finanzhilfen, insbesondere für die Empfänger solcher Finanzhilfen. Alle Pflichten des Finanzhilfeempfängers sind in der Entscheidung zur Gewährung der Finanzhilfe geregelt.

27.5. **Besuche**

Vorkehrungen für Besuche von Mitgliedern des Personals der Kommission bei industriellen oder anderen Einrichtungen in den Mitgliedstaaten, die als EU-Verschlusssachen eingestufte Aufträge ausführen, im Rahmen der Ausführung solcher Aufträge werden in Absprache mit der zuständigen Nationalen Sicherheitsbehörde/Beauftragten Sicherheitsbehörde getroffen. Vorkehrungen für Besuche von Mitgliedern des Personals industrieller oder anderer Einrichtungen im Rahmen eines als EU-Verschlusssache eingestuften Auftrags werden von den zuständigen Nationalen Sicherheitsbehörden/Beauftragten Sicherheitsbehörden untereinander getroffen. Die Nationalen Sicherheitsbehörden/Beauftragten Sicherheitsbehörden, die mit einem als EU-Verschlusssache eingestuften Auftrag befasst sind, können jedoch ein Verfahren vereinbaren, nach dem die Vorkehrungen für Besuche, die Mitglieder des Personals industrieller oder anderer Einrichtungen abstatten, direkt getroffen werden können.

27.6. **Übermittlung und Beförderung von EU-Verschlusssachen**

a) Für die Übermittlung von EU-Verschlusssachen gelten die Bestimmungen des Teils II Abschnitt 21 dieser Sicherheitsvorschriften. Ergänzend zu diesen Bestimmungen gelten die derzeit von den Mitgliedstaaten untereinander angewandten Verfahren.

b) Für die internationale Beförderung von als EU-Verschlusssachen eingestuften Materialien im Zusammenhang mit als Verschlusssachen eingestuften Aufträgen gelten die innerstaatlichen Verfahren der Mitgliedstaaten. Folgende Grundsätze werden angewandt, wenn sicherheitsbezogene Regelungen für die internationale Beförderung geprüft werden:

   — Die Sicherheit muss vom Ausgangsort bis zum endgültigen Bestimmungsort in allen Phasen der Beförderung und unter allen Umständen gewährleistet sein.

   — Das Schutzniveau für eine Sendung richtet sich nach dem höchsten Geheimhaltungsgrad der in der Sendung enthaltenen Materialien.

   — Für die Transportunternehmen ist gegebenenfalls ein Sicherheitsbescheid für Einrichtungen zu beschaffen. In solchen Fällen müssen die Personen, die die Lieferung bewerkstelligen, einer Sicherheitsüberprüfung gemäß den gemeinsamen Mindestnormen dieses Abschnitts unterzogen worden sein.

   — Die Beförderung erfolgt nach Möglichkeit von Punkt zu Punkt und wird so rasch abgeschlossen, wie es die Umstände erlauben.

▼**M4**

— Nach Möglichkeit werden nur Beförderungsrouten gewählt, die durch die EU-Mitgliedstaaten führen. Beförderungsrouten, die durch EU-Nichtmitgliedstaaten führen, werden nur gewählt, wenn sie von der Nationalen Sicherheitsbehörde/Beauftragten Sicherheitsbehörde des Staates des Absenders wie auch des Empfängers genehmigt worden sind.

— Vor jeder Beförderung von als EU-Verschlusssachen eingestuften Materialen stellt der Absender einen Beförderungsplan auf, der von der betreffenden Nationalen Sicherheitsbehörde/Beauftragten Sicherheitsbehörde genehmigt werden muss.

▼M2

Anlage 1

GEGENÜBERSTELLUNG DER NATIONALEN GEHEIMHALTUNGSSTUFEN

EU-Einstufung	TRES SECRET UE/EU TOP SECRET	SECRET UE	CONFIDENTIEL UE	RESTREINT UE
WEU-Einstufung	FOCAL TOP SECRET	WEU SECRET	WEU CONFIDENTIAL	WEU RESTRICTED
Euratom-Einstufung	EURA TOP SECRET	EURA SECRET	EURA CONFIDENTIAL	EURA RESTRICTED
NATO-Einstufung	COSMIC TOP SECRET	NATO SECRET	NATO CONFIDENTIAL	NATO RESTRICTED
Belgien	Très Secret	Secret	Confidentiel	Diffusion restreinte
	Zeer Geheim	Geheim	Vertrouwelijk	Beperkte Verspreiding
Tschechische Republik	Přísn tajné	Tajné	Důvěrné	Vyhrazené
Dänemark	Yderst hemmeligt	Hemmeligt	Fortroligt	Til tjenestebrug
Deutschland	Streng geheim	Geheim	VS ([1]) — Vertraulich	VS — Nur für den Dienstgebrauch
Estland	Täiesti salajane	Salajane	Konfidentsiaalne	Piiratud
Griechenland	Άκρως Απόρρητο	Απόρρητο	Εμπιστευτικό	Περιορισμένης Χρήσης
	Abr: ΑΑΠ	Abr: (ΑΠ)	Abr: (ΕΜ)	Abr: (ΠΧ)
Spanien	Secreto	Reservado	Confidencial	Difusión Limitada
Frankreich	Très Secret Défense ([2])	Secret Défense	Confidentiel Défense	
Irland	Top Secret	Secret	Confidential	Restricted
Italien	Segretissimo	Segreto	Riservatissimo	Riservato
Zypern	Άκρως Απόρρητο	Απόρρητο	Εμπιστευτικό	Περιορισμένης Χρήσης
Lettland	Sevišķi slepeni	Slepeni	Konfidenciāli	Dienesta vajadzībām
Litauen	Visiškai slaptai	Slaptai	Konfidencialiai	Riboto naudojimo
Luxemburg	Très Secret	Secret	Confidentiel	Diffusion restreinte

▼M2

Ungarn	Szigorúan titkos !	Titkos !	Bizalmas !	Korlátozott terjesztésű !
Malta	L-Ghola Segretezza	Sigriet	Kunfidenzjali	Ristrett
Niederlande	Stg ([3]). Zeer Geheim	Stg. Geheim	Stg. Confidentieel	Departementaalvertrouwelijk
Österreich	Streng Geheim	Geheim	Vertraulich	Eingeschränkt
Polen	Ściśle Tajne	Tajne	Poufne	Zastrzeżone
Portugal	Muito Secreto	Secreto	Confidencial	Reservado
Slowenien	Strogo tajno	Tajno	Zaupno	SVN Interno
Slowakei	Prísne tajné	Tajné	Dôverné	Vyhradené
Finnland	Erittäin salainen	Erittäin salainen	Salainen	Luottamuksellinen
Schweden	Kvalificerat hemlig	Hemlig	Hemlig	Hemlig
Vereinigtes Königreich	Top Secret	Secret	Confidential	Restricted

([1]) VS = Verschlusssache.
([2]) Die Einstufung Très Secret Défense, die sich auf wichtigste staatliche Angelegenheiten bezieht, kann nur mit Genehmigung des Premierministers geändert werden.
([3]) Stg = staatsgeheim.

▼M1

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
►**M2** TRES SECRET UE/EU TOP SECRET ◄: 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 „►**M2** TRES SECRET UE/EU TOP SECRET ◄“ 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 „►**M2** TRES SECRET UE/EU TOP SECRET ◄“ 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]. „►**M2** TRES SECRET UE/EU TOP SECRET ◄“-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 „►**M2** TRES SECRET UE/EU TOP SECRET ◄“-Dokumente zuständigen Beamten und dem der Vernichtung als Zeuge beiwohnenden Beamten, der einer Sicherheitsüberprüfung für „►**M2** TRES SECRET UE/EU TOP SECRET ◄“-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]. „►**M2** TRES SECRET UE/EU TOP SECRET ◄“-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 „►**M2** TRES SECRET UE/EU TOP SECRET ◄“-ermächtigen 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].

▼M1

Einstufung	Wann	Wer	Anbringung	Herabstufung/Aufhebung des Geheimhaltungsgrades/Vernichtung	
				Wer	Wann
►M2 SECRET UE ◄: 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 „►M2 SECRET UE ◄“ 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 „►M2 SECRET UE ◄“ 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]. „►M2 SECRET UE ◄“-Dokumente werden von der für diese Dokumente zuständigen Registratur unter der Aufsicht einer sicherheitsüberprüften Person vernichtet. „►M2 SECRET UE ◄“-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]. „►M2 SECRET UE ◄“-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].

▼M1

Einstufung	Wann	Wer	Anbringung	Herabstufung/Aufhebung des Geheimhaltungsgrades/Vernichtung	
				Wer	Wann
►M2 CONFIDENTIEL UE ◄: 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 „►M2 CONFIDENTIEL UE ◄“ 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,	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 „►M2 CONFIDENTIEL UE ◄“ 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]. „►M2 CONFIDENTIEL UE ◄“-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 ►M3 des für Sicherheitsfragen zuständigen Kommissionsmitglieds ◄ zu dokumentieren [22.5].	Überzählige Exemplare und nicht länger benötigte Dokumente sind zu vernichten [22.5]. „►M2 CONFIDENTIEL UE ◄“-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].

▼M1

Einstufung	Wann	Wer	Anbringung	Herabstufung/Aufhebung des Geheimhaltungsgrades/Vernichtung	
				Wer	Wann
	— ernstliche Behinderung der Ausarbeitung oder Durchführung wichtiger EU-Politiken, — Abbruch oder erhebliche Unterbrechung wichtiger EU-Aktivitäten.				
►M2 RESTREINT UE ◄: 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 „►M2 RESTREINT UE ◄“ 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,	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 „►M2 RESTREINT UE ◄“ 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]. „►M2 RESTREINT UE ◄“-Dokumente werden von der für diese Dokumente zuständigen Registratur gemäß den Weisungen ►M3 des für Sicherheitsfragen zuständigen Kommissionsmitglieds ◄ vernichtet [22.5].	Überzählige Exemplare und nicht länger benötigte Dokumente sind zu vernichten [22.5].

▼M1

Einstufung	Wann	Wer	Anbringung	Herabstufung/Aufhebung des Geheimhaltungsgrades/Vernichtung	
				Wer	Wann
	— 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.				

▼**M1**

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 „►**M2** CONFIDENTIEL UE ◄“ 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.

▼M1

b) Umfassen die Verschlusssachen, deren Weitergabe von der Kommission genehmigt wird, Informationen der Stufe „►M2 TRES SECRET UE/EU TOP SECRET ◄“, 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 „►M2 CONFIDENTIEL UE ◄“ 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 „►M2 SECRET UE ◄“ und „►M2 TRES SECRET UE/EU TOP SECRET ◄“ 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 „►M2 CONFIDENTIEL UE ◄“ oder „►M2 SECRET UE ◄“ 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 „►M2 TRES SECRET UE/EU TOP SECRET ◄“ 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 ►M3 Direktion Sicherheit 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 ►M3 Direktion Sicherheit 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 ►M3 Direktion Sicherheit der Kommission ◄ empfohlenen Maßnahmen, damit sich der Vorfall nicht wiederholt.

▼**M1**

14. Inspektionen

Der ►**M3** Direktion Sicherheit 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.

▼**M1**

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 „►**M2** SECRET UE ◄“ 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.

▼**M1**

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 ►**M3** vom Direktor der Direktion Sicherheit der Kommission ◄ 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.

▼**M1**

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 „►**M2** CONFIDENTIEL UE ◄“ oder darüber eingestuften Dokumenten dürfen nur mit Genehmigung des ►**M3** Direktion Sicherheit der Kommission ◄ angefertigt werden.

d) Das Verfahren zur raschen und vollständigen Vernichtung der Dokumente im Notfall sollte im Benehmen mit dem ►**M3** Direktion Sicherheit 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 ►**M3** Direktion Sicherheit der Kommission ◄ oder an die nationale Sicherheitsbehörde des Mitgliedstaats, der die Initiative zur Übermittlung von Dokumenten ergriffen hat (mit einer Abschrift an das ►**M3** Direktion Sicherheit 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 ►**M3** Direktion Sicherheit 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.

▼**M1**

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 „►**M2** SECRET UE ◄“ 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. ►**M3** Das für Sicherheitsfragen zuständige Kommissionsmitglied ◄ legt der Kommission das Gutachten der Beratenden Gruppe für das Sicherheitskonzept der Kommission zur Entscheidung vor.

▼M1

8. Hat die Kommission die Weitergabe von EU-Verschlusssachen beschlossen und die praktischen Durchführungsverfahren festgelegt, knüpft das ►M3 Direktion Sicherheit 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 ►M3 Direktion Sicherheit 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 ►M3 Direktion Sicherheit 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 „►M2 CONFIDENTIEL UE ◄“ 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.

▼**M1**

15. Verwendung und Schutz von ausgetauschten Verschlusssachen

a) Der Umgang mit Verschlusssachen des Geheimhaltungsgrades „►**M2** SECRET UE ◄“ 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 „►**M2** SECRET UE ◄“ werden mit Diplomatenpost, sicheren Postdiensten und sicheren Telekommunikationsmitteln übermittelt. Ein „►**M2** SECRET UE ◄“-Dokument darf nur mit schriftlicher Genehmigung der herausgebenden Stelle kopiert werden. Alle Kopien werden registriert, und ihre Verteilung wird überwacht. Für alle Verrichtungen mit ►**M2** SECRET UE ◄-Dokumenten werden Empfangsbescheinigungen ausgestellt.

b) Der Umgang mit Verschlusssachen des Geheimhaltungsgrades „►**M2** CONFIDENTIEL UE ◄“ 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 „►**M2** CONFIDENTIEL UE ◄“ 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 „►**M2** RESTREINT UE ◄“ 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 „►**M2** RESTREINT UE ◄“ und „►**M2** CONFIDENTIEL UE ◄“ wird ein entsprechender Vermerk in die speziellen Register aufgenommen. Für „►**M2** SECRET UE ◄“-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 „►**M2** CONFIDENTIEL UE ◄“ oder „►**M2** SECRET UE ◄“ 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 ►**M3** Direktion Sicherheit 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.

▼M1

Anlage 6

ABKÜRZUNGSVERZEICHNIS

CrA	Kryptographische Stelle
CCAM	Vergabebeirat
CISO	Sicherheitsbeauftragter für die zentrale IT
COMPUSEC	Computersicherheit
COMSEC	Kommunikationssicherheit
CSD	►M3 Direktion Sicherheit der Kommission ◄

▼M4

DSA	Designated Security Authority = Beauftragte Sicherheitsbehörde

▼M1

ESVP	Europäische Sicherheits- und Verteidigungspolitik

▼M4

FSC	Facility Security Clearance = Sicherheitsbescheid für Einrichtungen
FSO	Facility Security Officer = Sicherheitsbeauftragter

▼M1

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

▼M4

PSC	Personnel Security Clearance = Sicherheitsüberprüfung

▼M1

RCO	Kontrollbeauftragter für die Registratur
SAA	Akkreditierungsstelle für Sicherheit

▼M4

SAL	Security Aspects Letter = Geheimschutzklausel
SCG	Security Classification Guide = Einstufungsleitfaden für Verschlusssachen

▼M1

SecOP	Sicherheitsbezogene Betriebsverfahren
SSRS	Systemspezifische Sicherheitsanforderungen
TA	TEMPEST-Stelle
TSO	Eigentümer des technischen Systems

▼M5

DURCHFÜHRUNGSBESTIMMUNGEN ZUR VERORDNUNG (EG) Nr. 1049/2001 DES EUROPÄISCHEN PARLAMENTS UND DES RATES ÜBER DEN ZUGANG DER ÖFFENTLICHKEIT ZU DOKUMENTEN DES EUROPÄISCHEN PARLAMENTS, DES RATES UND DER KOMMISSION

In Erwägung nachstehender Gründe:

(1) Gemäß Artikel 255 Absatz 2 EG-Vertrag haben das Europäische Parlament und der Rat die Verordnung (EG) Nr. 1049/2001 ([1]) über den Zugang der Öffentlichkeit zu Dokumenten des Europäischen Parlaments, des Rates und der Kommission angenommen,

(2) Gemäß Artikel 255 Absatz 3 EG-Vertrag legt diese Verordnung die allgemeinen Grundsätze und Beschränkungen dieses Zugangsrechts fest und sieht in Artikel 18 vor, dass jedes Organ seine Geschäftsordnung an die Bestimmungen dieser Verordnung anpasst.

Artikel 1

Zugangsberechtigte

Unionsbürger und natürliche oder juristische Personen mit Wohnsitz oder Sitz in einem Mitgliedstaat üben ihr Recht auf Zugang zu den Dokumenten der Kommission nach Artikel 255 Absatz 1 EG-Vertrag und Artikel 2 Absatz 1 der Verordnung (EG) Nr. 1049/2001 gemäß den in den nachfolgenden Bestimmungen genannten Verfahren aus. Dieses Zugangsrecht umfasst die Dokumente der Kommission, das heißt Dokumente die von ihr erstellt wurden oder bei ihr eingegangen sind und sich in ihrem Besitz befinden.

Gemäß Artikel 2 Absatz 2 der Verordnung (EG) Nr. 1049/2001 kann allen natürlichen oder juristischen Personen, die keinen Wohnsitz oder Sitz in einem Mitgliedstaat haben, Zugang zu den Dokumenten der Kommission unter den gleichen Voraussetzungen wie den in Artikel 255 Absatz 1 EG-Vertrag genannten Zugangsberechtigten gewährt werden.

Gemäß Artikel 195 Absatz 1 EG-Vertrag haben diese Personen jedoch nicht die Möglichkeit, eine Beschwerde beim Europäischen Bürgerbeauftragten einzureichen. Verweigert die Kommission allerdings nach einem Zweitantrag ganz oder teilweise den Zugang, können sie entsprechend den Bestimmungen von Artikel 230 Absatz 4 EG-Vertrag vor dem Gericht erster Instanz der Europäischen Gemeinschaften Klage erheben.

Artikel 2

Anträge auf Zugang zu einem Dokument

Anträge auf Zugang zu einem Dokument sind per Post, Fax oder elektronische Post an das Generalsekretariat der Kommission, die zuständige Generaldirektion oder den zuständigen Dienst zu richten. Die entsprechenden Anschriften werden in dem in Artikel 8 dieser Bestimmungen genannten Leitfaden veröffentlicht.

Die Kommission beantwortet die Erst- und Zweitanträge auf Zugang zu einem Dokument innerhalb von fünfzehn Werktagen ab dem Datum der Registrierung des Antrags. Bei komplexen oder umfangreichen Anträgen kann diese Frist um fünfzehn Werktage verlängert werden. Jede Fristverlängerung muss begründet sein und dem Antragsteller vorher mitgeteilt werden.

([1]) ABl. L 145 vom 31.5.2001, S. 43.

▼M5

Bei einem Antrag, der, wie in Artikel 6 Absatz 2 der Verordnung (EG) Nr. 1049/2001 beschrieben, unpräzise formuliert ist, fordert die Kommission den Antragsteller auf, zusätzliche Informationen beizubringen, um die beantragten Schriftstücke ausfindig machen zu können; die Beantwortungsfrist beginnt erst zu dem Zeitpunkt, zu dem das Organ über diese Angaben verfügt.

Jeder, selbst teilweise, ablehnende Bescheid enthält eine Begründung der Ablehnung auf der Grundlage einer der in Artikel 4 der Verordnung (EG) Nr. 1049/2001 genannten Ausnahmen und unterrichtet den Antragsteller über die ihm zur Verfügung stehenden Rechtsmittel.

Artikel 3

Behandlung von Erstanträgen

Unbeschadet von Artikel 9 dieser Bestimmungen erhält der Antragsteller, sobald sein Antrag registriert wurde, eine Eingangsbestätigung, es sei denn, der Bescheid erging postwendend.

Die Eingangsbestätigung und der Bescheid werden schriftlich, eventuell per elektronische Post, versandt.

Der Antragsteller wird vom Generaldirektor oder dem Leiter des für den Antrag zuständigen Dienstes oder von einem zu diesem Zweck innerhalb des Generalsekretariats benannten Direktor bzw. von einem innerhalb des OLAF benannten Direktor, sofern sich der Antrag auf Dokumente im Zusammenhang mit in Artikel 2 Absätze 1 und 2 des Beschlusses 1999/352/EG, EGKS, Euratom der Kommission [1] zur Errichtung des OLAF vorgesehenen, von OLAF durchgeführten Maßnahmen bezieht, oder aber von dem Beamten, der zu diesem Zweck bestimmt wurde, darüber unterrichtet, wie sein Antrag beschieden wurde.

In jedem, selbst teilweise, ablehnenden Bescheid wird der Antragsteller über sein Recht informiert, innerhalb von 15 Werktagen nach Eingang des Bescheides einen Zweitantrag beim Generalsekretariat der Kommission oder beim Direktor des OLAF, sofern der Zweitantrag Dokumente im Zusammenhang mit in Artikel 2 Absätze 1 und 2 des Beschlusses 1999/352/EG, EGKS, Euratom vorgesehenen, von dem OLAF durchgeführten Maßnahmen betrifft, zu stellen.

Artikel 4

Behandlung von Zweitanträgen

Gemäß Artikel 14 der Geschäftsordnung der Kommission wird die Entscheidungsbefugnis über Zweitanträge dem Generalsekretär übertragen. Betrifft der Zweitantrag allerdings Dokumente im Zusammenhang mit in Artikel 2 Absätze 1 und 2 des Beschlusses 1999/352/EG, EGKS, Euratom vorgesehenen, von dem OLAF durchgeführten Maßnahmen, wird die Entscheidungsbefugnis dem Direktor des OLAF übertragen.

Die Generaldirektion oder der Dienst unterstützen das Generalsekretariat bei der Erarbeitung der Entscheidung.

Die Entscheidung wird durch den Generalsekretär oder den Direktor des OLAF nach Zustimmung des Juristischen Dienstes getroffen.

Der Bescheid wird dem Antragsteller schriftlich, gegebenenfalls in elektronischer Form, übermittelt und weist ihn auf sein Recht hin, beim Gericht erster Instanz Klage zu erheben oder beim Europäischen Bürgerbeauftragten Beschwerde einzulegen.

[1] ABl. L 136 vom 31.5.1999, S. 20.

▼M5

Artikel 5

Konsultationen

(1) Erhält die Kommission einen Antrag auf Zugang zu einem Dokument, in dessen Besitz sie zwar ist, das aber von einem Dritten stammt, prüft die Generaldirektion oder der Dienst, bei der bzw. dem sich das Dokument befindet, die Anwendbarkeit einer der in Artikel 4 der Verordnung (EG) Nr. 1049/2001 vorgesehenen Ausnahmen. Handelt es sich bei dem beantragten Dokument um eine Verschlusssache gemäß den Schutzvorschriften der Kommission, ist Artikel 6 dieser Bestimmungen anzuwenden.

(2) Gelangt die Generaldirektion oder der Dienst, bei der bzw. dem sich das Dokument befindet, nach dieser Prüfung zu der Auffassung, dass der Zugang zu dem beantragten Dokument entsprechend einer der in Artikel 4 der Verordnung (EG) Nr. 1049/2001 vorgesehenen Ausnahmen zu verweigern ist, wird die Ablehnung dem Antragsteller ohne Konsultation des Dritten zugestellt.

(3) Die Generaldirektion oder der Dienst, bei der bzw. dem sich das Dokument befindet, erteilt einen positiven Bescheid, ohne den externen Verfasser zu konsultieren, wenn:

a) das beantragte Dokument entweder durch seinen Verfasser bzw. aufgrund der Verordnung oder entsprechender Bestimmungen bereits verbreitet wurde;

b) die, möglicherweise auch teilweise Verbreitung seines Inhalts nicht wesentlich gegen eines der in Artikel 4 der Verordnung (EG) Nr. 1049/2001 vorgesehenen Interessen verstößt.

(4) In allen anderen Fällen wird der Urheber außerhalb der Organe konsultiert. Insbesondere in Fällen, in denen der Antrag auf Zugang zu einem Dokument eines Mitgliedstaates gestellt wird, konsultiert die Generaldirektion oder der Dienst, bei der bzw. dem sich das Dokument befindet, die Heimatbehörde, wenn:

a) das Dokument der Kommission vor dem Inkrafttreten der Verordnung (EG) Nr. 1049/2001 übermittelt wurde;

b) der Mitgliedstaat die Kommission ersucht hat, das Dokument gemäß den Bestimmungen von Artikel 4 Absatz 5 der Verordnung (EG) Nr. 1049/2001 nicht ohne seine vorherige Zustimmung zu verbreiten.

(5) Der konsultierte Dritte verfügt über eine Beantwortungsfrist, die mindestens fünf Werktage beträgt und es gleichzeitig der Kommission ermöglichen muss, ihre eigenen Beantwortungsfristen zu wahren. Geht innerhalb der festgesetzten Frist keine Antwort ein, oder ist der Dritte nicht auffindbar bzw. nicht feststellbar, entscheidet die Kommission entsprechend der Ausnahmeregelung von Artikel 4 der Verordnung (EG) Nr. 1049/2001 unter Berücksichtigung der berechtigten Interessen des Dritten auf der Grundlage der Angaben, über die sie verfügt.

(6) Sofern die Kommission beabsichtigt, gegen den ausdrücklichen Wunsch seines Verfassers den Zugang zu einem Dokument zu gewähren, unterrichtet sie den Verfasser über ihre Absicht, das Dokument nach einer Frist von zehn Werktagen freizugeben und verweist ihn auf die Rechtsmittel, die ihm zur Verfügung stehen, um diese Freigabe zu verhindern.

(7) Erhält ein Mitgliedstaat einen Antrag auf Zugang zu einem Dokument, das von der Kommission stammt, kann er sich zu Konsultationszwecken an das Generalsekretariat wenden, das die für das Dokument innerhalb der Kommission zuständige Generaldirektion oder den zuständigen Dienst benennt. Die Generaldirektion oder der Dienst, die bzw. der das Dokument verfasst hat, bearbeitet diesen Antrag nach Konsultation des Generalsekretariats.

▼M5

Artikel 6

Behandlung der Anträge auf Zugang zu Verschlusssachen

Betrifft der Antrag auf Zugang zu einem Dokument ein sensibles Dokument entsprechend der Definition in Artikel 9, Absatz 1 der Verordnung (EG) Nr. 1049/2001 oder eine andere Verschlusssache gemäß den Schutzvorschriften der Kommission, wird er von Beamten geprüft, die befugt sind, dieses Dokument einzusehen.

Wird der Antrag auf Zugang zu einer Verschlusssache ganz oder teilweise abschlägig beschieden, so ist dies auf der Grundlage der in Artikel 4 der Verordnung (EG) Nr. 1049/2001 genannten Ausnahmeregelungen zu begründen. Stellt sich heraus, dass der Zugang zu dem beantragten Dokument auf der Grundlage dieser Ausnahmeregelungen nicht abgelehnt werden kann, sorgt der Beamte, der diesen Antrag prüft, für die Freigabe des Dokumentes, bevor es dem Antragsteller übermittelt wird.

In jedem Fall ist für den Zugang zu einem sensiblen Dokument das Einverständnis der Heimatbehörde erforderlich.

Artikel 7

Ausübung des Zugangsrechts

Die Dokumente werden je nach Art des Antrags schriftlich, per Fax oder gegebenenfalls per E-Mail versandt. Bei umfangreichen oder schwer handzuhabenden Dokumenten kann der Antragsteller gebeten werden, die Dokumente vor Ort einzusehen. Diese Einsichtnahme ist kostenlos.

Ist das Dokument veröffentlicht worden, so sind in dem Bescheid Hinweise zur Veröffentlichung bzw. zu der Stelle zu geben, wo das Dokument verfügbar ist, sowie gegebenenfalls die Internet-Adresse des Dokumentes auf dem Server EUROPA.

Überschreitet der Umfang des beantragten Dokumentes 20 Seiten, kann dem Antragsteller eine Gebühr von 0,10 EUR je Seite zuzüglich Versandkosten in Rechnung gestellt werden. Über die Kosten im Zusammenhang mit anderen Hilfsmitteln wird von Fall zu Fall entschieden, ohne dass diese über einen angemessenen Betrag hinausgehen dürfen.

Artikel 8

Maßnahmen zur Erleichterung des Zugangs zu den Dokumenten

(1) Der Umfang des in Artikel 11 der Verordnung (EG) Nr. 1049/2001 vorgesehenen Registers wird schrittweise erweitert und auf der Startseite der EUROPA-Webseite angegeben.

Das Register enthält den Titel des Dokumentes (in den Sprachen, in denen es verfügbar ist), die Signatur und andere nützliche Hinweise, eine Angabe zu seinem Verfasser und das Datum seiner Erstellung oder seiner Verabschiedung.

Eine Hilfsseite (in allen Amtssprachen) unterrichtet die Öffentlichkeit darüber, wie das Dokument erhältlich ist. Handelt es sich um ein veröffentlichtes Dokument, erfolgt ein Verweis auf den Gesamttext.

(2) Die Kommission erarbeitet einen Leitfaden, der die Öffentlichkeit über ihre Rechte aufgrund der Verordnung (EG) Nr. 1049/2001 informiert. Dieser Leitfaden wird in allen Amtssprachen auf der EUROPA-Webseite sowie als Broschüre veröffentlicht.

▼M5

Artikel 9

Unmittelbar öffentlich zugängliche Dokumente

(1) Die Bestimmungen dieses Artikels finden nur auf solche Dokumente Anwendung, die nach Inkrafttreten der Verordnung (EG) Nr. 1049/2001 erstellt oder erhalten wurden.

(2) Folgende Dokumente werden auf Anfrage automatisch zur Verfügung gestellt und, soweit möglich, unmittelbar in elektronischer Form zugänglich gemacht:

a) Tagesordnungen der Kommissionssitzungen;

b) gewöhnliche Protokolle der Kommissionssitzungen nach ihrer Genehmigung;

c) von der Kommission verabschiedete Texte, die zur Veröffentlichung im Amtsblatt der Europäischen Gemeinschaften bestimmt sind;

d) Dokumente Dritter, die bereits vom Verfasser oder mit seiner Zustimmung veröffentlicht worden sind;

e) Dokumente, die bereits im Zusammenhang mit einem früheren Antrag veröffentlicht wurden.

(3) Sofern eindeutig feststeht, dass keine der in Artikel 4 der Verordnung (EG) Nr. 1049/2001 vorgesehenen Ausnahmen auf sie Anwendung findet, können folgende Dokumente, soweit möglich in elektronischer Form, verbreitet werden, vorausgesetzt, sie geben keine persönlichen Meinungen oder Stellungnahmen wieder:

a) nach Verabschiedung eines Vorschlags für einen Rechtsakt des Rates bzw. des Europäischen Parlaments und des Rates die vorbereitenden Dokumente zu diesen Vorschlägen, die dem Kollegium während des Verfahrens der Annahme vorgelegt wurden;

b) nach Verabschiedung eines Rechtsakts der Kommission aufgrund der ihr verliehenen Ausführungsbefugnisse die vorbereitenden Dokumente zu diesen Rechtsakten, die dem Kollegium während des Verfahrens der Annahme vorgelegt wurden;

c) nach Verabschiedung eines Rechtsakts aufgrund ihrer eigenen Befugnisse, einer Mitteilung, eines Berichts oder eines Arbeitsdokumentes durch die Kommission, die vorbereitenden Dokumente zu diesen Dokumenten, die dem Kollegium während des Verfahrens der Annahme vorgelegt wurden.

Artikel 10

Interne Organisation

Die Generaldirektoren und Leiter der Dienste entscheiden über die Erstanträge. Zu diesem Zweck benennen sie einen Beamten, der die Anträge auf Zugang zu einem Dokument prüft und die Stellungnahme seiner Generaldirektion oder seines Dienstes koordiniert.

Dem Generalsekretariat wird zur Kenntnisnahme mitgeteilt, wie die Erstanträge beschieden wurden.

Der für den Erstantrag verantwortlichen Generaldirektion oder dem hierfür verantwortlichen Dienst wird mitgeteilt, dass ein Zweitantrag gestellt wurde.

Das Generalsekretariat sorgt für die reibungslose Koordinierung und einheitliche Anwendung dieser Vorschriften durch die Generaldirektionen und Kommissionsdienste. Hierzu stellt es alle notwendigen Leitlinien und Verhaltensmaßregeln zur Verfügung.

▼M6

BESTIMMUNGEN ZUR VERWALTUNG VON DOKUMENTEN

In Erwägung nachstehender Gründe:

(1) Die Maßnahmen und Beschlüsse der Kommission in den Bereichen Politik, Gesetzgebung, Technik, Finanzen und Verwaltung führen alle irgendwann zur Erstellung von Dokumenten.

(2) Diese Dokumente müssen gemäß den für alle Generaldirektionen und gleichgestellten Dienste geltenden Vorschriften verwaltet werden, da sie gleichzeitig eine direkte Verbindung zu den laufenden Maßnahmen und ein Abbild der abgeschlossenen Maßnahmen der Kommission in ihrer doppelten Funktion als europäisches Organ und europäische öffentliche Verwaltung darstellen.

(3) Diese einheitlichen Vorschriften müssen gewährleisten, dass die Kommission jederzeit Rechenschaft über das ablegen kann, dessen sie rechenschaftspflichtig ist. Deshalb müssen die Dokumente und Akten, die sich bei einer Generaldirektion bzw. einem gleichgestellten Dienst befinden, die Arbeit des Organs nachvollziehbar machen, den Informationsaustausch erleichtern, erfolgte Tätigkeiten belegen und den rechtlichen Verpflichtungen, denen die Dienste unterliegen, entsprechen.

(4) Die Umsetzung der zuvor genannten Vorschriften erfordert die Einrichtung einer adäquaten und soliden Organisationsstruktur sowohl auf Ebene der einzelnen Generaldirektionen bzw. gleichgestellten Dienste, als auch dienstübergreifend und auf Ebene der Kommission.

(5) Die Erstellung und Einführung eines Aktenplans, gestützt auf eine Nomenklatur, die allen Kommissionsdiensten im Rahmen des maßnahmenbezogenen Managements (MBM) des Organs gemeinsam sein wird, ermöglichen eine Strukturierung der Dokumente in Akten und erleichtern den Zugang dazu sowie die Transparenz.

(6) Eine effiziente Verwaltung der Dokumente ist für eine effiziente Politik des öffentlichen Zugangs zu den Dokumenten der Kommission unerlässlich; die Ausübung dieses Zugangsrechts durch den Bürger wird erleichtert durch die Einrichtung von Registern mit Verweisen auf die Dokumente, die von der Kommission erstellt wurden oder bei ihr eingegangen sind.

Artikel 1

Begriffsbestimmungen

Im Sinne dieser Bestimmungen bedeutet:

— *Dokument*: Inhalte, die von der Europäischen Kommission erstellt wurden oder bei ihr eingegangen sind, und die einen Sachverhalt im Zusammenhang mit den Politiken, Maßnahmen und Entscheidungen aus dem Zuständigkeitsbereich des Organs im Rahmen seines offiziellen Auftrags betreffen, unabhängig von der Form des Datenträgers (auf Papier oder in elektronischer Form, Ton-, Bild- oder audiovisuelles Material)

— *Akte*: der Kern, um den die Dokumente entsprechend der Geschäftstätigkeit des Organs zu Nachweis-, Rechtfertigungs- oder Informationszwecken sowie zur Gewährleistung der Arbeitseffizienz organisiert werden.

Artikel 2

Gegenstand

Diese Bestimmungen legen die Grundsätze der Verwaltung von Dokumenten fest.

Die Verwaltung von Dokumenten muss Folgendes gewährleisten:

— die Erstellung, den Empfang und die Aufbewahrung der Dokumente in vorschriftsmäßiger Form;

▼M6

— die Kennzeichnung jedes Dokuments mit Hilfe angemessener Kennzeichen, die seine einfache Zuordnung und Suche sowie Verweise auf dasselbe ermöglichen;

— die Bewahrung des Gedächtnisses des Organs, die Erhaltung der Nachweise über durchgeführte Maßnahmen und die Beachtung der rechtlichen Verpflichtungen, denen die Dienste unterliegen;

— den einfachen Informationsaustausch;

— die Beachtung der Verpflichtung zur Transparenz des Organs.

Artikel 3

Einheitliche Vorschriften

Dokumente unterliegen folgenden Arbeitsgängen:

— Registrierung,

— Ablage,

— Aufbewahrung,

— Abgabe der Akten an das Historische Archiv.

Diese Arbeitsgänge werden im Rahmen der für alle Generaldirektionen und gleichgestellten Dienste der Kommission einheitlichen Vorschriften durchgeführt.

Artikel 4

Registrierung

Vom Zeitpunkt seines Eingangs oder seiner formalen Erstellung durch einen Dienst unterliegt ein Dokument, unabhängig von der Form des Datenträgers, einer Analyse, die das weitere Verfahren bestimmt, welches dem Dokument vorbehalten ist, mithin die Verpflichtung, es zu registrieren oder nicht.

Ein Dokument, das von einem Kommissionsdienst erstellt wurde oder bei diesem eingegangen ist, muss registriert werden, wenn es wichtige dauerhafte Informationen enthält und/oder zu einem Tätigwerden oder zu Folgemaßnahmen der Kommission bzw. einem ihrer Dienste führen kann. Handelt es sich um ein erstelltes Dokument, erfolgt die Registrierung durch den ausfertigenden Dienst in dem System, dem es entstammt. Handelt es sich um ein eingegangenes Dokument, wird die Registrierung von dem Dienst vorgenommen, an den es gerichtet wurde. Bei jeder weiteren Bearbeitung dieses auf diese Weise registrierten Dokuments muss auf die ursprüngliche Registrierung verwiesen werden.

Die Registrierung muss die deutliche und sichere Identifikation der von der Kommission oder einem ihrer Dienste erstellten oder bei diesen eingegangenen Dokumente erlauben, in einer Weise, die die Rückverfolgbarkeit der betreffenden Dokumente während ihres vollständigen Lebenszyklus gewährleistet.

Die Registrierung gibt Anlass zur Anlegung von Registern die Angaben zu den Dokumenten enthalten.

Artikel 5

Ablage

Die Generaldirektionen und gleichgestellten Dienste erstellen einen Aktenplan, der ihren spezifischen Erfordernissen entspricht.

Dieser Aktenplan, der mit Mitteln der Informationstechnik zugänglich sein wird, ist auf eine vom Generalsekretariat für alle Kommissionsdienste definierte gemeinsame Nomenklatur gestützt. Diese Nomenklatur fügt sich in den Rahmen des maßnahmenbezogenen Managements (MBM) der Kommission ein.

▼M6

Die registrierten Dokumente werden in Akten organisiert. Für jeden Vorgang, der in die Zuständigkeit der Generaldirektion oder des gleichgestellten Dienstes fallt, wird eine einzige offizielle Akte angelegt. Jede offizielle Akte muss vollständig sein und der Geschäftstätigkeit des jeweiligen Dienstes in Bezug auf den Vorgang entsprechen.

Das Anlegen einer Akte und ihre Eingliederung in den Aktenplan einer Generaldirektion oder eines gleichgestellten Dienstes obliegt dem für den jeweiligen Bereich zuständigen Dienst entsprechend den anzuwendenden Modalitäten, die in den einzelnen Generaldirektionen oder gleichgestellten Diensten festzulegen sind.

Artikel 6

Aufbewahrung

Jede Generaldirektion bzw. gleichgestellter Dienst stellt den materiellen Schutz der Dokumente, die sich in deren Zuständigkeit befinden sowie den kurz- und mittelfristigen Zugang zu diesen Dokumenten sicher. Sie müssen ferner in der Lage sein, die dazugehörigen Akten bereitzustellen oder zu rekonstruieren.

Die Verwaltungsvorschriften und die rechtlichen Verpflichtungen bestimmen die Mindestaufbewahrungsdauer eines Dokuments.

Jede Generaldirektion bzw. gleichgestellter Dienst legt ihre interne Organisationsstruktur im Hinblick auf die Aufbewahrung ihrer Akten fest. Die Mindestaufbewahrungsdauer innerhalb ihrer Dienste richtet sich nach einer gemeinsamen Liste, die entsprechend den in Artikel 12 genannten Anwendungsmodalitäten erstellt wurde und für die gesamte Kommission gilt.

Artikel 7

Vorauswahl und Abgabe an das Historische Archiv

Unbeschadet der in Artikel 6 genannten Mindestaufbewahrungsfristen treffen die in Artikel 9 genannten Registraturen in regelmäßigen Abständen gemeinsam mit den für die Akten zuständigen Diensten eine Vorauswahl der Dokumente und Akten im Hinblick auf ihre Archivwürdigkeit und eine mögliche Abgabe an das Historische Archiv der Kommission. Nach Prüfung der Vorschläge kann das Historische Archiv die Abgabe ablehnen. Jede ablehnende Entscheidung wird begründet und den betreffenden Diensten mitgeteilt.

Akten und Dokumente, deren Aufbewahrung durch die Dienste sich als nicht mehr notwendig erweist, werden spätestens fünfzehn Jahre nach ihrer Erstellung über die Registraturen und unter der Verantwortung des Generaldirektors an das Historische Archiv der Kommission abgegeben. Danach werden diese Akten und Dokumente einer Bewertung entsprechend den Regeln, die in den in Artikel 12 genannten Anwendungsmodalitäten festgelegt sind, unterzogen. Diese Bewertung dient dazu, diejenigen Akten und Dokumente, die aufbewahrt werden müssen, von denen zu trennen, die weder von administrativem noch von historischem Interesse sind.

Das Historische Archiv verfügt über besondere Magazine für die Aufbewahrung dieser übernommenen Akten und Dokumente. Auf Anfrage werden sie für die Generaldirektion bzw. gleichgestellten Dienst, aus der sie stammen, bereitgestellt.

Artikel 8

Verschlusssachen

Als Verschlusssache eingestufte Dokumente werden entsprechend den geltenden Schutzvorschriften behandelt.

▼M6

Artikel 9

Registraturen

Jede Generaldirektion bzw. gleichgestellter Dienst richtet unter Berücksichtigung ihrer Struktur und ihrer Sachzwänge eine oder mehrere Registraturen ein.

Die Registraturen haben zu gewährleisten, dass die in ihrer Generaldirektion bzw. Dienst erstellten oder dort eingegangenen Dokumente entsprechend den festgelegten Vorschriften verwaltet werden.

Artikel 10

Beauftragte für die Verwaltung von Dokumenten

Jeder Generaldirektor oder Dienstleiter benennt einen Beauftragten für die Verwaltung von Dokumenten.

Im Zuge der Einrichtung eines modernen und leistungsfähigen Verwaltungs- und Archivierungssystems der Dokumente kontrolliert dieser Beauftragte folgende Aufgaben:

— Identifizierung der verschiedenen für die Aufgabenfelder seiner Generaldirektion oder seines gleichgestellten Dienstes spezifischen Arten von Dokumenten und Akten;

— Erstellung eines Inventars der bestehenden Datenbanken und Informationssysteme sowie dessen Aktualisierung;

— Erstellung des Aktenplans seiner Generaldirektion bzw. gleichgestellten Dienstes;

— Festlegung besonderer Vorschriften und Verfahren seiner Generaldirektion oder seines gleichgestellten Dienstes für die Verwaltung der Dokumente und Akten sowie Kontrolle ihrer Anwendung;

— Organisation von Schulungen der Mitarbeiter, die mit der Durchführung, der Überwachung und den Folgemaßnahmen der in diesen Bestimmungen festgelegten Verwaltungsvorschriften in seiner Generaldirektion oder seinem gleichgestellten Dienst betraut sind.

Der Beauftragte gewährleistet die horizontale Koordinierung zwischen der oder den Registraturen und den übrigen beteiligten Dienststellen.

Artikel 11

Dienstübergreifende Gruppe von Beauftragten für die Verwaltung von Dokumenten

Es wird eine dienstübergreifende Gruppe von Beauftragten für die Verwaltung von Dokumenten unter Vorsitz des Generalsekretariats eingerichtet, die folgende Aufgaben wahrnimmt:

— Kontrolle der korrekten und einheitlichen Anwendung dieser Bestimmungen in den Dienststellen;

— Behandlung eventueller Fragen bei der Anwendung derselben;

— Beteiligung an der Erarbeitung der in Artikel 12 genannten Anwendungsmodalitäten;

— Weiterleitung des Schulungsbedarfs sowie des Bedarfs an Unterstützungsmaßnahmen der Generaldirektionen und gleichgestellten Dienste.

Die Gruppe wird von ihrem Vorsitzenden auf dessen Initiative oder auf Anfrage einer Generaldirektion bzw. eines gleichgestellten Dienstes einberufen.

▼M6

Artikel 12

Anwendungsmodalitäten

Die Anwendungsmodalitäten dieser Bestimmungen werden vom Generalsekretär im Einvernehmen mit dem Generaldirektor für Personal und Verwaltung auf Vorschlag der dienstübergreifenden Gruppe von Beauftragten für die Verwaltung von Dokumenten erlassen und regelmäßig aktualisiert.

Bei der Aktualisierung sind insbesondere folgende Aspekte zu berücksichtigen:

— Entwicklung neuer Technologien im Bereich der Information und Kommunikation;

— Weiterentwicklung der Dokumentationswissenschaften sowie Forschungsergebnisse auf Gemeinschafts- und internationaler Ebene einschließlich der Entwicklung von Normen in diesem Bereich;

— Verpflichtungen der Kommission im Hinblick auf Transparenz und öffentlichen Zugang zu den Dokumenten und zu den Dokumentenregistern;

— Entwicklungen im Hinblick auf Standardisierung und formalen Aufbau der Dokumente der Kommission und ihrer Dienste;

— Definition der anzuwendenden Vorschriften im Hinblick auf den Beweiswert elektronischer Dokumente.

Artikel 13

Umsetzung innerhalb der Dienste

Jeder Generaldirektor bzw. Dienstleiter schafft die organisatorischen, administrativen, materiellen und personellen Voraussetzungen für die praktische Umsetzung dieser Bestimmungen und ihrer Anwendungsmodalitäten durch seine Dienststellen.

Artikel 14

Information, Schulung und Unterstützung

Das Generalsekretariat und die Generaldirektion für Personal und Verwaltung stellen Informations-, Schulungs- und Unterstützungsmaßnahmen bereit, die für die erfolgreiche Umsetzung und Durchführung dieser Bestimmungen in den Generaldirektionen und gleichgestellten Diensten notwendig sind.

Bei der Festlegung der Schulungsmaßnahmen berücksichtigen sie sorgfältig den von der dienstübergreifenden Gruppe von Beauftragten für die Verwaltung von Dokumenten festgestellten Schulungs- und Unterstützungsbedarf der Generaldirektionen und gleichgestellten Dienste.

Artikel 15

Durchführung der Bestimmungen

Das Generalsekretariat sorgt in Absprache mit den Generaldirektoren und Dienstleitern für die Durchführung der vorliegenden Bestimmungen.

▼M11

▼M8

BESTIMMUNGEN DER KOMMISSION ÜBER ELEKTRONISCHE UND NUMMERISIERTE DOKUMENTE

In Erwägung nachstehender Gründe:

(1) Die allgemeine Verwendung der neuen Informations- und Kommunikationstechnologien durch die Kommission für ihre interne Tätigkeit und beim Austausch von Dokumenten mit externen Stellen, insbesondere den gemeinschaftlichen Verwaltungen einschließlich den Einrichtungen, die für die Durchführung bestimmter Gemeinschaftspolitiken zuständig sind, und den nationalen Verwaltungen hat zur Folge, dass das Dokumentationssystem der Kommission immer mehr elektronische und nummerisierte Dokumente enthält.

(2) Entsprechend dem Weißbuch über die Reform der Kommission ([1]), dessen Maßnahmen 7, 8 und 9 den Übergang zur elektronischen Kommission sicherstellen sollen, und der Mitteilung „Auf dem Weg zur elektronischen Kommission: Umsetzungsstrategie 2001 — 2005 (Maßnahmen 7, 8 und 9 des Reformweißbuches)“ ([2]) hat die Kommission im Rahmen ihrer internen Tätigkeit und der Beziehungen zwischen den Dienststellen die Entwicklung von Informatiksystemen für die elektronische Verwaltung von Dokumenten und elektronische Verfahren verstärkt.

(3) Mit Beschluss 2002/47/EG, EGKS, Euratom ([3]) hat die Kommission Bestimmungen zur Verwaltung von Dokumenten im Anhang zu ihrer Geschäftsordnung angefügt, damit sie insbesondere jederzeit Rechenschaft über Handlungen ablegen kann, für die sie rechenschaftspflichtig ist. Die Kommission hat sich in ihrer Mitteilung über die Vereinfachung und Modernisierung der Verwaltung ihrer Dokumente ([4]) mittelfristig das Ziel gesetzt, eine auf gemeinsamen Bestimmungen und Verfahren beruhende, für alle Dienststellen geltende elektronische Archivierung von Dokumenten einzurichten.

(4) Die Verwaltung von Dokumenten muss unter Einhaltung der für die Kommission gebotenen Sicherheitsregeln insbesondere im Bereich der Klassifizierung von Dokumenten gemäß dem Beschluss 2001/844/EG, EGKS, Euratom ([5]), des Schutzes von Informationssystemen gemäß dem Beschluss K(95) 1510 und des Schutzes personenbezogener Daten gemäß der Verordnung (EG) Nr. 45/2001 des Europäischen Parlaments und des Rates ([6]) erfolgen. Der Dokumentationsraum der Kommission muss so gestaltet sein, dass die Informationssysteme sowie die Übertragungsnetze und -mittel, die ihn speisen, durch geeignete Sicherheitsmaßnahmen geschützt sind.

(5) Es ist erforderlich, Bestimmungen über die Bedingungen für die Gültigkeit elektronischer und nummerisierter oder auf elektronischem Wege übermittelter Dokumente in Bezug auf die Kommission anzunehmen, sofern diese Bedingungen nicht bereits anderweitig festgelegt sind, sowie auch Bedingungen für die Aufbewahrung der Dokumente anzunehmen, die die Unverfälschtheit und Lesbarkeit dieser Dokumente und der begleitenden Metadaten im Laufe der Zeit für die gesamte geforderte Aufbewahrungsdauer garantieren —

BESCHLIESST:

Artikel 1

Zweck

Diese Bestimmungen legen die Bedingungen für die Gültigkeit elektronischer und nummerisierter Dokumente in Bezug auf die Kommission fest. Sie stellen ebenfalls darauf ab, die Echtheit, Unverfälschtheit und Lesbarkeit dieser Dokumente und der begleitenden Metadaten im Laufe der Zeit zu garantieren.

([1]) K(2000) 200.
([2]) SEK(2001) 924.
([3]) ABl. L 21 vom 24.1.2002, S. 23.
([4]) K(2002) 99 endg.
([5]) ABl. L 317 vom 3.12.2001, S. 1.
([6]) ABl. L 8 vom 12.1.2001, S. 1.

▼**M8**

Artikel 2

Anwendungsbereich

Diese Bestimmungen gelten für elektronische und nummerisierte Dokumente, die von der Kommission erstellt wurden oder bei ihr eingegangen sind und sich in ihrem Besitz befinden.

Sie können im Wege einer Vereinbarung auf elektronische und nummerisierte Dokumente im Besitz anderer Stellen, die für die Durchführung bestimmter Gemeinschaftspolitiken zuständig sind, oder auf Dokumente erweitert werden, die im Rahmen von Telematiknetzen, an denen die Kommission teilnimmt, zwischen Verwaltungen ausgetauscht werden.

Artikel 3

Begriffsbestimmungen

Im Sinne dieser Bestimmung bedeutet:

1. *„Dokument":* ein Dokument im Sinne von Artikel 3 Buchstabe a) der Verordnung (EG) Nr. 1049/2001 des Europäischen Parlaments und des Rates ([1]) und Artikel 1 der Bestimmungen zur Verwaltung von Dokumenten im Anhang zur Geschäftsordnung der Kommission, nachstehend als „Bestimmungen zur Verwaltung von Dokumenten" bezeichnet;

2. *„elektronisches Dokument":* ein Datensatz, der auf jedwedem Träger durch ein Informatiksystem oder ein ähnliches Mittel erfasst oder aufbewahrt wird und von Personen oder solchen Systemen oder Mitteln gelesen oder wahrgenommen werden kann, sowie Aufzeichnung und Ausgang dieser Daten in Druckform oder auf andere Weise;

3. *„Nummerisierung von Dokumenten":* das Verfahren, mit dem Papierdokumente oder andere traditionelle Träger in elektronische Bilder umgewandelt werden. Die Nummerisierung betrifft alle Dokumentenarten und kann ausgehend von verschiedenen Trägern wie Papier, Fax, Mikroformen (Mikrofiche, Mikrofilm), Fotos, Video- oder Audiokassetten und Filmen erfolgen;

4. *„Lebensdauer eines Dokuments":* sämtliche Abschnitte oder Perioden des Bestehens eines Dokuments vom Zeitpunkt seines Eingangs oder seiner formalen Erstellung im Sinne von Artikel 4 der Bestimmungen zur Verwaltung von Dokumenten bis zu seiner Abgabe an das Historische Archiv der Kommission und seiner Öffnung für die Bürger oder seiner Zerstörung im Sinne von Artikel 7 dieser Bestimmungen;

5. *„Dokumentationssystem der Kommission":* alle Dokumente, Akten und Metadaten, die von der Kommission erstellt, empfangen, registriert, zugeordnet und aufbewahrt werden;

6. *„Unverfälschtheit":* die Tatsache, dass die in dem Dokument enthaltenen Informationen und die begleitenden Metadaten vollständig (alle Daten sind vorhanden) und richtig (alle Daten sind unverändert) sind;

7. *„Lesbarkeit im Laufe der Zeit":* die Tatsache, dass die in den Dokumenten enthaltenen Informationen und die begleitenden Metadaten für alle Personen, die dazu Zugang haben müssen oder können, während der gesamten Lebensdauer dieser Dokumente ab ihrer formalen Erstellung oder ihrem Eingang bis zu ihrer Abgabe an das Historische Archiv der Kommission und ihrer Öffnung für die Bürger oder ihrer genehmigten Zerstörung nach Maßgabe der geforderten Aufbewahrungsdauer leicht lesbar bleiben;

([1]) ABl. L 145 vom 31.5.2001, S. 43.

▼M8

8. *„Metadaten“:* Daten, die den Zusammenhang, Inhalt und Aufbau der Dokumente sowie ihre Verwaltung im Laufe der Zeit beschreiben, wie sie in den Anwendungsmodalitäten der Bestimmungen zur Verwaltung von Dokumenten festgelegt sind und durch Anwendungsmodalitäten dieser Bestimmungen ergänzt werden;

9. *„elektronische Signatur“:* die elektronische Signatur im Sinne von Artikel 2 Nummer 1 der Richtlinie 1999/93/EG des Europäischen Parlaments und des Rates ([1]);

10. *„fortgeschrittene elektronische Signatur“:* die elektronische Signatur im Sinne von Artikel 2 Nummer 2 der Richtlinie 1999/93/EG.

Artikel 4

Gültigkeit elektronischer Dokumente

(1) Verlangt eine anwendbare gemeinschaftsrechtliche oder nationale Bestimmung das unterzeichnete Original eines Dokuments, so erfüllt ein elektronisches Dokument, das von der Kommission erstellt wurde oder bei ihr eingegangen ist, dieses Erfordernis, wenn das betreffende Dokument eine fortgeschrittene elektronische Signatur, die auf einem qualifizierten Zertifikat beruht und von einer sicheren Signaturerstellungseinheit erstellt worden ist, oder eine elektronische Signatur enthält, die gleichwertige Garantien in Bezug auf die einer Signatur zugewiesen Funktionen bietet.

(2) Verlangt eine anwendbare gemeinschaftsrechtliche oder nationale Bestimmung die schriftliche Erstellung eines Dokuments, nicht aber das unterzeichnete Original, so erfüllt ein elektronisches Dokument, das von der Kommission erstellt wurde oder bei ihr eingegangen ist, dieses Erfordernis, wenn die Person, von der es stammt, hinreichend identifiziert ist und das Dokument unter Bedingungen erstellt wird, die die Unverfälschtheit seines Inhalts und der begleitenden Metadaten garantieren und es unter den in Artikel 7 dargelegten Bedingungen aufbewahrt wird.

(3) Dieser Artikel ist ab dem auf die Annahme der Anwendungsmodalitäten nach Artikel 9 folgenden Tag anwendbar.

Artikel 5

Gültigkeit elektronischer Verfahren

(1) Ist nach einem internen Verfahren der Kommission die Signatur einer ermächtigten Person oder die Zustimmung einer Person zu einem oder mehreren Abschnitten dieses Verfahrens erforderlich, so kann es rechnergestützt verwaltet werden, sofern alle Personen sicher und eindeutig identifiziert werden und das betreffende System Garantien für die Unveränderbarkeit des Inhalts sowie auch der Verfahrensschritte bietet.

(2) Umfasst ein Verfahren die Kommission und andere Stellen und ist die Signatur einer ermächtigten Person oder die Zustimmung einer Person zu einem oder mehreren Abschnitten dieses Verfahrens erforderlich, so kann es rechnergestützt verwaltet werden, wobei die Bedingungen und technischen Garantien in einer Vereinbarung geregelt werden.

Artikel 6

Elektronische Übermittlung

(1) Die Übermittlung von Dokumenten durch die Kommission an einen internen oder externen Empfänger kann über die für den betreffenden Fall geeignetsten Kommunikationsmittel erfolgen.

(2) Die Übermittlung von Dokumenten an die Kommission kann über alle Kommunikationsmittel, einschließlich auf elektronischem Weg mittels Kopie, E-Mail, elektronischem Formular oder Internet erfolgen.

([1]) ABl. L 13 vom 19.1.2000, S. 12.

▼M8

(3) Die Absätze 1 und 2 finden keine Anwendung, wenn eine gemäß einem Abkommen oder einer Vereinbarung zwischen den Parteien anwendbare gemeinschaftsrechtliche oder nationale Bestimmung besondere Übermittlungsarten oder besondere Förmlichkeiten in Bezug auf die Übermittlung vorschreibt.

Artikel 7

Aufbewahrung

(1) Die Aufbewahrung elektronischer und nummerisierter Dokumente durch die Kommission muss während der gesamten erforderlichen Dauer unter folgenden Bedingungen sichergestellt werden:

a) Das Dokument wird in der Form aufbewahrt, in der es erstellt, abgesandt oder empfangen wurde bzw. in einer Form, die die Unverfälschtheit des Inhalts des Dokuments sowie der begleitenden Metadaten wahrt.

b) Der Inhalt des Dokuments und der begleitenden Metadaten ist während der gesamten Aufbewahrungsdauer von allen lesbar, die zugangsberechtigt sind.

c) Bei einem auf elektronischem Weg abgesandten oder empfangenen Dokument gehören jene Informationen, die die Feststellung seiner Herkunft und Bestimmung ermöglichen, sowie das Datum und die Uhrzeit der Absendung oder des Empfangs zu den Metadaten, die jedenfalls aufbewahrt werden müssen.

d) Bei elektronischen Verfahren, die von Informatiksystemen gestützt werden, müssen die Angaben über die förmlichen Abschnitte des Verfahrens in einer Weise aufbewahrt werden, dass diese Abschnitte sowie der Urheber und Beteiligte erkennbar sind.

(2) Für die Zwecke von Absatz 1 richtet die Kommission ein elektronisches Aufbewahrungssystem ein, das die gesamte Lebensdauer der elektronischen und nummerisierten Dokumente umfasst.

Die technischen Erfordernisse des elektronischen Aufbewahrungssystems werden in den Anwendungsmodalitäten nach Artikel 9 geregelt.

Artikel 8

Sicherheit

Die Verwaltung der elektronischen und nummerisierten Dokumente erfolgt unter Einhaltung der für die Kommission gebotenen Sicherheitsregeln. Dazu werden die Informationssysteme sowie die Übertragungsnetze und -mittel, die das Dokumentationssystem der Kommission speisen, durch geeignete Sicherheitsmaßnahmen im Bereich der Zuordnung von Dokumenten, des Schutzes von Informationssystemen und des Schutzes personenbezogener Daten geschützt.

Artikel 9

Anwendungsmodalitäten

Die Anwendungsmodalitäten dieser Bestimmungen werden in Absprache mit den Generaldirektionen und gleichgestellten Diensten erstellt und vom Generalsekretär der Kommission im Einvernehmen mit dem auf Ebene der Kommission für Informatik zuständigen Generaldirektor erlassen.

Sie werden nach Maßgabe der Entwicklung neuer Technologien im Bereich der Information und Kommunikation und neuer Verpflichtungen, die sich für die Kommission ergeben könnten, regelmäßig aktualisiert.

▼**M8**

Artikel 10

Durchführung in den Dienststellen

Die Generaldirektoren bzw. Dienstleiter ergreifen die erforderlichen Maßnahmen, damit die Dokumente, Verfahren und elektronischen Systeme, für die sie verantwortlich sind, den Erfordernissen dieser Bestimmungen und ihrer Anwendungsmodalitäten entsprechen.

Artikel 11

Durchführung der Bestimmungen

Das Generalsekretariat sorgt in Absprache mit den Generaldirektionen und gleichgestellten Diensten, insbesondere mit der in der Kommission für Informatik zuständigen Generaldirektion, für die Durchführung dieser Bestimmungen.

▼M10

KOMMISSIONSBESTIMMUNGEN ZUR EINRICHTUNG DES ALLGEMEINEN FRÜHWARNSYSTEMS ARGUS

In Erwägung nachstehender Gründe:

(1) Um auf Krisen gleich welcher Ursache, die mehrere Sektoren und Politikbereiche betreffen und Maßnahmen auf Gemeinschaftsebene erfordern, in ihren Zuständigkeitsbereichen rascher, wirksamer und koordinierter reagieren zu können, sollte die Kommission ein allgemeines Frühwarnsystem („ARGUS“) einrichten.

(2) Das System sollte sich zunächst auf ein internes Kommunikationsnetz gründen, über das die Generaldirektionen und Dienste der Kommission im Krisenfall Informationen austauschen können.

(3) Das System sollte im Lichte der gewonnenen Erfahrungen und des technologischen Fortschritts überprüft werden, um die Verknüpfung und die Koordinierung der bestehenden spezialisierten Netze sicherzustellen.

(4) Es ist erforderlich, ein geeignetes Koordinierungsverfahren für die Beschlussfassung und eine rasche, koordinierte und kohärente Reaktion der Kommission auf schwere, mehrere Sektoren betreffende Krisen festzulegen. Dieses Verfahren muss flexibel gestaltet werden und auf die besonderen Anforderungen und Umstände einer gegebenen Krise zugeschnitten werden können. Dabei ist den bestehenden politischen Instrumenten für die Bewältigung spezifischer Krisensituationen Rechnung zu tragen.

(5) Das System sollte die spezifischen Eigenheiten, Fachkenntnisse, Verfahrensvorschriften und Zuständigkeitsbereiche der bestehenden sektorspezifischen Frühwarnsysteme der Kommission, welche die Kommissionsdienststellen in die Lage versetzen, auf spezifische Krisen in verschiedenen Tätigkeitsbereichen der Gemeinschaft zu reagieren, ebenso berücksichtigen wie den Subsidiaritätsgrundsatz.

(6) Da die Kommunikation von zentraler Bedeutung für die Krisenbewältigung ist, sollte besonderes Gewicht auf die Information der Öffentlichkeit und die wirksame Kommunikation mit den Bürgern über die Presse und verschiedene Kommunikationsmittel und -stellen der Kommission in Brüssel und/oder an geeigneter Stelle gelegt werden.

Artikel 1

Das ARGUS-System

(1) Damit die Kommission auf Krisen gleich welcher Ursache, die mehrere Sektoren und Politikbereiche betreffen und Maßnahmen auf Gemeinschaftsebene erfordern, in ihren Zuständigkeitsbereichen rascher, wirksamer und kohärenter reagieren kann, wird ein allgemeines System zur Frühwarnung und raschen Reaktion („ARGUS“) eingerichtet.

(2) ARGUS umfasst

a) ein internes Kommunikationsnetz;

b) ein spezifisches Koordinierungsverfahren, das im Fall einer schweren Krise, die mehrere Sektoren betrifft, eingeleitet wird.

(3) Diese Bestimmungen lassen den Beschluss 2003/246/EG der Kommission über operationelle Verfahren für die Bewältigung von Krisensituationen unberührt.

Artikel 2

Das ARGUS-Informationsnetz

(1) Das interne Kommunikationsnetz wird als ein ständig verfügbares Instrument eingerichtet, das den Generaldirektionen und Diensten der Kommission den zeitnahen Austausch von sachdienlichen Informationen über entstandene, mehrere Sektoren betreffende Krisen oder absehbare bzw. unmittelbar bevorstehende derartige Bedrohungen und die Koordinierung einer geeigneten Reaktion in den Zuständigkeitsbereichen der Kommission ermöglicht.

▼**M10**

(2) Den Kern des Netzes bilden folgende Dienststellen: Generalsekretariat, GD Presse und Information einschließlich Dienst des Sprechers, GD Umwelt, GD Gesundheit und Verbraucherschutz, GD Justiz, Freiheit und Sicherheit, GD Außenbeziehungen, GD Humanitäre Hilfe, GD Personal und Verwaltung, GD Handel, GD Informatik, GD Steuern und Zollunion, Gemeinsame Forschungsstelle und Juristischer Dienst.

(3) Weitere Generaldirektionen oder Dienste der Kommission können auf Antrag in das Netz eingebunden werden, wenn sie die in Absatz 4 genannten Mindestanforderungen erfüllen.

(4) Die in dem Netz mitwirkenden Generaldirektionen und Dienste ernennen einen ARGUS-Korrespondenten und führen eine geeignete Bereitschaftsregelung ein, damit sie im Fall einer ihr Eingreifen erforderlich machenden Krise jederzeit erreichbar sind und rasch tätig werden können. Das System wird so gestaltet, dass dies mit dem vorhandenen Personal möglich ist.

Artikel 3

Koordinierungsverfahren bei schweren Krisen

(1) Im Fall einer schweren, mehrere Sektoren betreffenden Krise oder einer absehbaren bzw. unmittelbar bevorstehenden derartigen Bedrohung kann der Präsident von sich aus nach einer Warnung oder auf Ersuchen eines Mitglieds der Kommission beschließen, ein spezifisches Koordinierungsverfahren in die Wege zu leiten. Der Präsident entscheidet zudem über die Zuweisung der politischen Verantwortung für die Krisenbewältigungsmaßnahmen der Kommission. Er kann die Verantwortung selbst übernehmen oder sie einem Mitglied der Kommission übertragen.

(2) Die Verantwortung erstreckt sich auf die Leitung und Koordinierung der Krisenbewältigungsmaßnahmen, die Vertretung der Kommission gegenüber den anderen Organen und Einrichtungen und die Kommunikation mit der Öffentlichkeit. Die bestehende Aufgaben- und Kompetenzverteilung in der Kommission bleibt davon unberührt.

(3) Das Generalsekretariat ruft im Auftrag des Präsidenten bzw. des Kommissionsmitglieds, dem die Verantwortung übertragen wurde, das in Artikel 4 beschriebene, spezifische operative Krisenbewältigungsgremium („Krisenkoordinierungsausschuss“) zusammen.

Artikel 4

Krisenkoordinierungsausschuss

(1) Der Krisenkoordinierungsausschuss ist ein spezifisches operatives Krisenbewältigungsgremium, das zur Leitung und Koordinierung der Krisenbewältigungsmaßnahmen eingesetzt wird und sich aus Vertretern aller zuständigen Generaldirektionen und Dienste der Kommission zusammensetzt. In der Regel sind im Krisenkoordinierungsausschuss die in Artikel 2 Absatz 2 genannten Generaldirektionen und Dienste sowie weitere, durch die spezifische Krise betroffene Generaldirektionen und Dienste vertreten. Der Krisenkoordinierungsausschuss greift auf die vorhandenen Ressourcen und Mittel der Dienste zurück.

(2) Den Vorsitz im Krisenkoordinierungsausschuss führt der für die politische Koordinierung zuständige stellvertretende Generalsekretär.

(3) Der Krisenkoordinierungsausschuss hat insbesondere die Aufgabe, die Entwicklung der Krisensituation zu überwachen und zu bewerten, Fragen sowie Entscheidungs- und Vorgehensmöglichkeiten zu prüfen und dafür zu sorgen, dass Beschlüsse und Maßnahmen umgesetzt werden und die Krisenbewältigungsmaßnahmen kohärent und konsequent sind.

▼**M10**

(4) Die Annahme der im Krisenkoordinierungsausschuss vereinbarten Maßnahmen erfolgt auf dem Wege der normalen Beschlussfassungsverfahren der Kommission; die Umsetzung erfolgt durch die Generaldirektionen und über die Frühwarnsysteme.

(5) Die Kommissionsdienste tragen dafür Sorge, dass die in ihre Zuständigkeit fallenden Aufgaben im Zusammenhang mit der Krisenbewältigung ordnungsgemäß erfüllt werden.

Artikel 5

Verfahrenshandbuch

Es wird ein Verfahrenshandbuch mit ausführlichen Bestimmungen zur Durchführung dieses Beschlusses erstellt.

Artikel 6

Die Kommission überprüft diesen Beschluss spätestens ein Jahr nach seinem Inkrafttreten im Lichte der gewonnenen Erfahrungen und des technologischen Fortschritts und erlässt erforderlichenfalls weitere Maßnahmen in Bezug auf die Funktionsweise des ARGUS-Systems.

▼M12

DURCHFÜHRUNGSBESTIMMUNGEN ZUR VERORDNUNG (EG) Nr. 1367/2006 DES EUROPÄISCHEN PARLAMENTS UND DES RATES ÜBER DIE ANWENDUNG DER BESTIMMUNGEN DES ÜBEREINKOMMENS VON ÅRHUS ÜBER DEN ZUGANG ZU INFORMATIONEN, DIE ÖFFENTLICHKEITSBETEILIGUNG AN ENTSCHEIDUNGSVERFAHREN UND DEN ZUGANG ZU GERICHTEN IN UMWELTANGELEGENHEITEN AUF ORGANE UND EINRICHTUNGEN DER GEMEINSCHAFT

Artikel 1

Zugang zu Umweltinformationen

Die Frist von 15 Werktagen nach Artikel 7 der Verordnung (EG) Nr. 1367/2006 beginnt am Tag der Registrierung des Antrags durch die zuständige Dienststelle in der Kommission.

Artikel 2

Öffentlichkeitsbeteiligung

Zur Durchführung des Artikels 9 Absatz 1 der Verordnung (EG) Nr. 1367/2006 sorgt die Kommission für eine Beteiligung der Öffentlichkeit gemäß der Mitteilung „Allgemeine Grundsätze und Mindeststandards für die Konsultation betroffener Parteien“ ([1]).

Artikel 3

Anträge auf interne Überprüfung

Anträge auf interne Überprüfung eines Verwaltungsakts oder einer Unterlassung sind auf dem Postweg, per Fax oder per E-Mail an die Dienststelle zu richten, die für die Anwendung der Bestimmung, auf deren Grundlage der Verwaltungsakt erlassen wurde oder bezüglich deren die Unterlassung behauptet wird, zuständig ist.

Die entsprechenden Kontaktadressen werden der Öffentlichkeit durch alle geeigneten Mittel bekannt gegeben.

Richtet sich der Antrag an eine andere als die für die Überprüfung zuständige Dienststelle, so wird er von der erstgenannten an die zuständige Dienststelle weitergeleitet.

Handelt es sich bei der für die Überprüfung zuständigen Dienststelle nicht um die Generaldirektion „Umwelt“, so ist Letztere über den Antrag zu unterrichten.

Artikel 4

Entscheidungen über die Zulässigkeit von Anträgen auf interne Überprüfung

(1) Nach der Registrierung des Antrags auf interne Überprüfung wird umgehend — gegebenenfalls auf elektronischem Weg — eine Empfangsbestätigung an die Nichtregierungsorganisation gesandt, die den Antrag gestellt hat.

(2) Die betreffende Kommissionsdienststelle stellt fest, ob die Nichtregierungsorganisation befugt ist, einen Antrag auf interne Überprüfung nach dem Beschluss 2008/50/EG der Kommission ([2]) zu stellen.

([1]) KOM(2002) 704 endg.
([2]) ABl. L 13 vom 16.1.2008, S. 24.

▼M12

(3) Die Befugnis, über die Zulässigkeit eines Antrags auf interne Überprüfung zu entscheiden, wird gemäß Artikel 14 der Geschäftsordnung an den betreffenden Generaldirektor oder Dienststellenleiter übertragen.

Entscheidungen über die Zulässigkeit des Antrags umfassen alle Entscheidungen über die Befugnis der den Antrag stellenden Nichtregierungsorganisation gemäß Absatz 2, den fristgerechten Eingang des Antrags nach Artikel 10 Absatz 1 Unterabsatz 2 der Verordnung (EG) Nr. 1367/2006 und bezüglich der genannten, näher ausgeführten Gründe für den Antrag nach Artikel 1 Absätze 2 und 3 der Entscheidung 2008/50/EG.

(4) Kommt der Generaldirektor oder Dienststellenleiter nach Absatz 3 zu dem Ergebnis, dass der Antrag auf interne Überprüfung ganz oder teilweise unzulässig ist, wird die den Antrag stellende Nichtregierungsorganisation schriftlich — gegebenenfalls auf elektronischem Weg — unter Angabe von Gründen darüber unterrichtet.

Artikel 5

Entscheidungen über den Sachverhalt von Anträgen auf interne Überprüfung

(1) Die Kommission entscheidet, ob der zu überprüfende Verwaltungsakt oder die behauptete Unterlassung gegen das Umweltrecht verstoßen.

(2) Das Mitglied der Kommission, das für die Anwendung der Bestimmungen zuständig ist, auf deren Grundlage der betreffende Verwaltungsakt angenommen wurde oder auf die sich die behauptete Unterlassung bezieht, ist gemäß Artikel 13 der Geschäftsordnung befugt, zu entscheiden, dass der Verwaltungsakt, dessen Überprüfung beantragt wurde, oder die behauptete Unterlassung nicht gegen das Umweltrecht verstößt.

Eine Weiterübertragung von nach Absatz 1 übertragenen Befugnissen ist unzulässig.

(3) Die Nichtregierungsorganisation, die den Antrag gestellt hat, wird — gegebenenfalls auf elektronischem Weg — schriftlich über das Ergebnis der Überprüfung und dessen Gründe unterrichtet.

Artikel 6

Rechtsbehelfe

Gegen eine Antwort, in der der Nichtregierungsorganisation mitgeteilt wird, dass ihr Antrag ganz oder teilweise unzulässig ist oder dass der Verwaltungsakt, dessen Überprüfung beantragt wird oder die behauptete Unterlassung nicht gegen das Umweltrecht verstoßen, kann die Nichtregierungsorganisation unter den Bedingungen der Artikel 230 und 195 des EG-Vertrags die ihr offen stehenden Rechtsbehelfe — Klage gegen die Kommission, Beschwerde beim Bürgerbeauftragten oder beides — einlegen.

Artikel 7

Unterrichtung der Öffentlichkeit

Die Öffentlichkeit wird in einem Leitfaden über ihre Rechte nach der Verordnung (EG) Nr. 1367/2006 unterrichtet.