II

(Mitteilungen)

MITTEILUNGEN DER ORGANE, EINRICHTUNGEN UND SONSTIGEN STELLEN DER EUROPÄISCHEN UNION

EUROPÄISCHES PARLAMENT

BESCHLUSS DES PRÄSIDIUMS DES EUROPÄISCHEN PARLAMENTS

vom 15. April 2013

über die Regeln zur Behandlung vertraulicher Informationen durch das Europäische Parlament

(2014/C 96/01)

DAS PRÄSIDIUM DES EUROPÄISCHEN PARLAMENTS —

gestützt auf Artikel 23 Absatz 12 der Geschäftsordnung,

in Erwägung folgender Gründe:

(1) Angesichts der am 20. Oktober 2010 unterzeichneten Rahmenvereinbarung über die Beziehungen zwischen dem Europäischen Parlament und der Europäischen Kommission [1] („Rahmenvereinbarung“) und der am 12. März 2014 unterzeichneten Interinstitutionellen Vereinbarung zwischen dem Europäischen Parlament und dem Rat über die Übermittlung an und die Bearbeitung durch das Europäische Parlament von im Besitz des Rates befindlichen Verschlusssachen in Bezug auf Angelegenheiten, die nicht unter die Gemeinsame Außen- und Sicherheitspolitik fallen [2] („Interinstitutionelle Vereinbarung“), müssen gezielte Vorschriften über die Behandlung vertraulicher Informationen durch das Europäische Parlament festgelegt werden.

(2) Mit dem Vertrag von Lissabon erhält das Europäische Parlament neue Aufgaben, und damit es seine Tätigkeit in den Bereichen, die ein bestimmtes Maß an Vertraulichkeit erfordern, entfalten kann müssen Grundsätze, Sicherheitsmindeststandards und geeignete Verfahren für die Behandlung vertraulicher Informationen, einschließlich Verschlusssachen, durch das Europäische Parlament festgelegt werden.

(3) Mit den in diesem Beschluss niedergelegten Regeln soll für gleiche Sicherheitsstandards und die Vereinbarkeit mit den Regeln gesorgt werden, die von anderen durch die Verträge oder auf deren Grundlage eingerichteten Organen, Einrichtungen und sonstigen Stellen oder von Mitgliedstaaten zwecks eines reibungslosen Ablaufs der Entscheidungsprozesse der Europäischen Union eingeführt wurden.

(4) Die Bestimmungen dieses Beschlusses berühren nicht die derzeitigen und künftigen Vorschriften über den Zugang zu Dokumenten, die nach Artikel 15 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV) erlassen worden sind.

[1] ABl. L 304 vom 20.11.2010, S. 47.
[2] ABl. C 95 vom 1.4.2014, S. 1.

(5) Die Bestimmungen dieses Beschlusses berühren nicht die derzeitigen und künftigen Vorschriften über den Schutz personenbezogener Daten, die nach Artikel 16 AEUV erlassen worden sind. —

BESCHLIESST:

Artikel 1

Ziel

Dieser Beschluss regelt die Verwaltung und Behandlung vertraulicher Informationen durch das Europäische Parlament, einschließlich Erstellung, Erhalt, Übermittlung und Aufbewahrung solcher Informationen durch das Europäische Parlament, mit dem Ziel, dass die Informationen angemessen geschützt werden. Er setzt die Interinstitutionelle Vereinbarung und die Rahmenvereinbarung, insbesondere deren Anhang II, um.

Artikel 2

Begriffsbestimmungen

Für die Zwecke dieses Beschlusses bezeichnet der Ausdruck

a) „Informationen“ alle Informationen in schriftlicher oder mündlicher Form, ungeachtet des Mediums, in dem sie vorliegen, und ungeachtet des Verfassers;

b) „vertrauliche Informationen“ „Verschlusssachen“, und „sonstige vertrauliche Informationen“, die nicht als Verschlusssache eingestuft sind;

c) „Verschlusssachen“ „EU-Verschlusssachen“ und „gleichwertige Verschlusssachen“;

d) „EU-Verschlusssachen“ (EUCI) alle Informationen und Materialien, die als TRES SECRET UE/EU TOP SECRET, SECRET UE/EU SECRET, CONFIDENTIEL UE/EU CONFIDENTIAL oder RESTREINT UE/EU RESTRICTED eingestuft werden und deren unbefugte Weitergabe den Interessen der Union oder eines oder mehrerer ihrer Mitgliedstaaten in unterschiedlichem Maß schaden könnte, unabhängig davon, ob die Informationen von durch die Verträge oder auf deren Grundlage eingerichteten Organen, Einrichtungen und sonstigen Stellen kommen; in diesem Zusammenhang bezeichnen Informationen und Materialien auf folgender Stufe:

— „TRÈS SECRET UE/EU TOP SECRET“: Informationen und Materialien, deren unbefugte Weitergabe den wesentlichen Interessen der Union oder eines oder mehrerer Mitgliedstaaten außerordentlich schweren Schaden zufügen könnte;

— „SECRET UE/EU SECRET“: Informationen und Materialien, deren unbefugte Weitergabe den wesentlichen Interessen der Union oder eines oder mehrerer Mitgliedstaaten schweren Schaden zufügen könnte;

— „CONFIDENTIEL UE/EU CONFIDENTIAL“: Informationen und Materialien, deren unbefugte Weitergabe den wesentlichen Interessen der Union oder eines oder mehrerer Mitgliedstaaten Schaden zufügen könnte;

— „RESTREINT UE/EU RESTRICTED“: Informationen und Materialien, deren unbefugte Weitergabe für die wesentlichen Interessen der Union oder eines oder mehrerer Mitgliedstaaten nachteilig sein könnte;

e) „gleichwertige Verschlusssachen“ Verschlusssachen, die von Mitgliedstaaten, Drittstaaten oder internationalen Organisation erstellt worden sind, deren Verschlusssachenkennzeichnung einer der Verschlusssachenkennzeichnungen für EUCI gleichwertig ist und die der Rat oder die Kommission dem Europäischen Parlament übermittelt hat;

f) „sonstige vertrauliche Informationen“ alle sonstigen nicht als Verschlusssache eingestuften vertraulichen Informationen, darunter Informationen, die unter Datenschutzbestimmungen oder das Berufsgeheimnis fallen und die vom Europäischen Parlament erstellt oder ihm von anderen durch die Verträge oder auf deren Grundlage eingerichteten Organen, Einrichtungen und sonstigen Stellen oder von Mitgliedstaaten übermittelt worden sind;

g) „Dokument“ aufgezeichnete Informationen aller Art, ungeachtet ihrer physischen Form oder Eigenschaften;

h) „Materialien“ alle Dokumente oder hergestellte bzw. in der Herstellung befindliche Geräte oder Ausrüstungen;

i) „berechtigtes Informationsinteresse“ das Bedürfnis einer Person, Zugang zu vertraulichen Informationen zu erhalten, um eine amtliche Funktion ausüben oder einen Auftrag ausführen zu können;

j) „Ermächtigung“ bei Mitgliedern des Europäischen Parlaments eine Entscheidung des Präsidenten und bei Beamten des Europäischen Parlaments und sonstigen Parlamentsbediensteten, die für die Fraktionen tätig sind, eine Entscheidung des Generalsekretärs, mit der diesen Personen auf der Grundlage eines positiven Ergebnisses einer Sicherheitsüberprüfung, die von einer nationalen Sicherheitsbehörde nach einzelstaatlichem Recht und gemäß den in Anlage I Teil 2 aufgeführten Bestimmungen durchgeführt wird, individueller Zugang zu Verschlusssachen bis zu einer bestimmten Stufe gewährt wird;

k) „Herabstufung“ eine Einstufung mit einem niedrigeren Geheimhaltungsgrad;

l) „Freigabe“ die Aufhebung sämtlicher Geheimhaltungsgrade;

m) „Kennzeichnung“ ein auf „sonstigen vertraulichen Informationen“ angebrachtes Zeichen, das für zuvor festgelegte spezifische Anweisungen bezüglich der Behandlung der Informationen oder des von einem bestimmten Dokument abgedeckten Bereichs steht; die Kennzeichnung kann auch auf Verschlusssachen angebracht werden, um zusätzliche Anforderungen an die Behandlung deutlich zu machen;

n) „Aufhebung der Kennzeichnung“ die Beseitigung von Kennzeichnungen;

o) „Urheber“ den ordnungsgemäß ermächtigten Verfasser vertraulicher Informationen;

p) „Sicherheitshinweise“ die in Anlage II festgelegten Durchführungsmaßnahmen;

q) „Behandlungsanweisungen“ die technischen Anweisungen an die Dienststellen des Parlaments hinsichtlich der Verwaltung vertraulicher Informationen.

Artikel 3

Grundsätze und Mindeststandards

1. Bei der Behandlung vertraulicher Informationen durch das Europäische Parlament sind die in Anlage I Teil 1 aufgeführten Grundsätze und Mindeststandards zu beachten.

2. Das Europäische Parlament richtet gemäß diesen Grundsätzen und Mindeststandards ein Managementsystem für Informationssicherheit (ISMS) ein. Das ISMS besteht aus den Sicherheitshinweisen, den Behandlungsanweisungen und den anwendbaren Bestimmungen der Geschäftsordnung. Es zielt darauf ab, die parlamentarische und administrative Arbeit zu erleichtern und dabei den Schutz aller vom Europäischen Parlament behandelten vertraulichen Informationen unter uneingeschränkter Einhaltung der vom Urheber der Informationen aufgestellten und in den Sicherheitshinweisen vermerkten Regeln sicherzustellen.

Die Verarbeitung vertraulicher Informationen durch automatisierte Kommunikations- und Informationssysteme (CIS) des Europäischen Parlaments erfolgt im Einklang mit dem Konzept der Informationssicherung, wie sie in Sicherheitshinweis 3 festgelegt sind.

3. Mitglieder des Europäischen Parlaments dürfen Verschlusssachen bis einschließlich Geheimhaltungsgrad CONFIDENTIEL UE/EU CONFIDENTIAL einsehen, ohne eine Sicherheitsüberprüfung absolviert zu haben.

4. Fallen die betreffenden Informationen unter die Einstufung CONFIDENTIEL UE/EU CONFIDENTIAL oder eine gleichwertige Einstufung, wird Zugang nur den Mitgliedern des Europäischen Parlaments gewährt, die gemäß Absatz 5 vom Präsidenten dazu ermächtigt wurden oder die eine förmliche Erklärung über die Geheimhaltung des Inhalts der Informationen, über die Einhaltung der Verpflichtung zum Schutz von Informationen des Geheimhaltungsgrads CONFIDENTIEL UE/EU CONFIDENTIAL und über die Kenntnisnahme von den Konsequenzen der Nichteinhaltung unterzeichnet haben.

5. Fallen die betreffenden Informationen unter die Einstufung SECRET UE/EU SECRET oder TRÈS SECRET UE/EU TOP SECRET oder eine gleichwertige Einstufung, wird Zugang nur den Mitgliedern des Europäischen Parlaments gewährt, die vom Präsidenten dazu ermächtigt wurden,

a) nachdem sie eine Sicherheitsüberprüfung gemäß Anlage I Teil 2 dieses Beschlusses absolviert haben oder

b) nach Erhalt einer Mitteilung einer zuständigen nationalen Behörde, dass die betreffenden Mitglieder aufgrund ihrer Aufgaben gemäß dem nationalen Recht ordnungsgemäß ermächtigt sind.

6. Bevor ihnen Zugang zu Verschlusssachen gewährt wird, werden die Mitglieder des Europäischen Parlaments gemäß Anlage I über ihre Verantwortlichkeiten hinsichtlich des Schutzes derartiger Informationen belehrt und erkennen diese an. Sie werden zudem über die Mittel zur Sicherstellung des Schutzes belehrt.

7. Beamte des Europäischen Parlaments und sonstige Parlamentsbedienstete, die für die Fraktionen tätig sind, dürfen vertrauliche Informationen einsehen, wenn sie erwiesenermaßen ein „berechtigtes Informationsinteresse“ haben, und dürfen Informationen eines höheren Geheimhaltungsgrads als RESTREINT UE/EU RESTRICTED einsehen, wenn sie die entsprechende Stufe der Sicherheitsüberprüfung aufweisen. Der Zugang zu Verschlusssachen wird nur gewährt, wenn diese Personen über ihre Verantwortlichkeiten hinsichtlich des Schutzes solcher Informationen und über die Mittel zur Sicherstellung dieses Schutzes belehrt worden sind und hierzu schriftliche Weisungen erhalten haben und eine Erklärung unterzeichnet haben, mit der sie den Erhalt dieser Weisungen bestätigen und sich verpflichten, sie entsprechend den derzeitigen Sicherheitsvorschriften zu befolgen.

Artikel 4

Erstellung vertraulicher Informationen und ihre administrative Behandlung durch das Europäische Parlament

1. Der Präsident des Europäischen Parlaments, die Vorsitze der betroffenen Parlamentsausschüsse und der Generalsekretär bzw. eine von ihm schriftlich dazu ermächtigte Person dürfen entsprechend den Sicherheitshinweisen vertrauliche Informationen erstellen und/oder Informationen einstufen.

2. Bei der Erstellung von Verschlusssachen beachtet der Urheber den jeweils angemessenen Geheimhaltungsgrad nach Maßgabe der internationalen Standards und Definitionen nach Anlage I. Außerdem legt der Urheber in der Regel die Adressaten fest, die entsprechend dem Geheimhaltungsgrad ermächtigt werden sollen, die Informationen einzusehen. Diese Festlegung wird dem Referat Verschlusssachen (CIU) mitgeteilt, wenn das Dokument dort abgelegt wird.

3. „Sonstige vertrauliche Informationen“, die dem Berufsgeheimnis unterliegen, sind nach Maßgabe der Anlagen I und II und der Behandlungsanweisungen zu behandeln.

Artikel 5

Entgegennahme vertraulicher Informationen durch das Europäische Parlament

1. Beim Europäischen Parlament eingegangene Informationen werden wie folgt weitergeleitet:

a) Informationen mit dem Geheimhaltungsgrad RESTREINT UE/EU RESTRICTED oder einem gleichwertigen Geheimhaltungsgrad und „sonstige vertrauliche Informationen“ an das Sekretariat des parlamentarischen Organs bzw. Amtsträgers, von dem der Geheimhaltungsgrad beantragt wurde, oder unmittelbar an das CIU;

b) Informationen mit dem Geheimhaltungsgrad CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET oder TRÈS SECRET UE/EU TOP SECRET oder einem gleichwertigen Geheimhaltungsgrad an das CIU.

2. Für die Registrierung, die Aufbewahrung und die Rückverfolgbarkeit von vertraulichen Informationen sorgt entweder das Sekretariat des parlamentarischen Organs bzw. Amtsträgers, bei dem die Informationen eingegangen sind, oder das CIU.

3. Im Fall von vertraulichen Informationen, die von der Kommission gemäß Anhang II Nummer 3.2 der Rahmenvereinbarung übermittelt werden, bzw. im Fall von Verschlusssachen, die vom Rat gemäß Artikel 5 Absatz 4 der Interinstitutionellen Vereinbarung übermittelt werden, wird die einvernehmlich festzulegende Regelung, mit der die Vertraulichkeit der Informationen gewahrt werden soll, zusammen mit den vertraulichen Informationen beim Sekretariat des parlamentarischen Organs bzw. Amtsträgers oder beim CIU hinterlegt.

4. Die Regelung nach Absatz 3 kann sinngemäß auch bei der Übermittlung vertraulicher Informationen durch andere durch die Verträge oder auf deren Grundlage eingerichteten Organen, Einrichtungen und sonstigen Stellen oder durch die Mitgliedstaaten angewandt werden.

5. Damit ein Schutzniveau erreicht wird, das dem Geheimhaltungsgrad TRÈS SECRET UE/EU TOP SECRET oder einem gleichwertigen Geheimhaltungsgrad angemessen ist, setzt die Konferenz der Präsidenten einen Kontrollausschuss ein. Informationen mit dem Geheimhaltungsgrad TRÈS SECRET UE/EU TOP SECRET oder einem gleichwertigen Geheimhaltungsgrad sind dem Europäischen Parlament unter Anwendung zusätzlicher Vorkehrungen zu übermitteln, die zwischen dem Europäischen Parlament und dem Organ der Union, von dem die Informationen stammen, zu vereinbaren sind.

Artikel 6

Übermittlung von Verschlusssachen durch das Europäische Parlament an Dritte

Das Europäische Parlament kann vorbehaltlich der vorherigen schriftlichen Zustimmung des Urhebers oder gegebenenfalls des Organs der Union, das dem Europäischen Parlament Verschlusssachen übermittelt hat, die Verschlusssachen Dritten unter der Voraussetzung übermitteln, dass sie sicherstellen, dass bei der Behandlung der Verschlusssachen in ihren Dienststellen und Räumlichkeiten Bestimmungen eingehalten werden, die den in diesem Beschluss festgelegten Bestimmungen gleichwertig sind.

Artikel 7

Gesicherte Einrichtungen

1. Das Europäische Parlament richtet für den Umgang mit vertraulichen Informationen einen gesicherten Bereich und gesicherte Leseräume ein.

2. Der gesicherte Bereich umfasst Einrichtungen zur Registrierung von Verschlusssachen, zur Einsichtnahme in sie sowie zu ihrer Archivierung, Übermittlung und Behandlung. Zu dem Bereich gehören unter anderem ein Leseraum und ein Sitzungsraum zur Einsichtnahme in Verschlusssachen, und der Bereich wird vom CIU verwaltet.

3. Außerhalb des gesicherten Bereichs können gesicherte Leseräume für die Einsichtnahme in Informationen, die als RESTREINT UE/EU RESTRICTED oder auf einer gleichwertigen Stufe eingestuft sind oder für die Einsichtnahme in „sonstige vertrauliche Information" eingerichtet werden. Diese gesicherten Leseräume sind von den zuständigen Dienststellen der Sekretariate der parlamentarischen Gremien bzw. Amtsträger oder vom CIU zu verwalten. In ihnen darf es keine Fotokopiergeräte, Telefone, Faxgeräte, Scanner oder sonstige Ausrüstungen zur Vervielfältigung oder Weiterleitung von Dokumenten geben.

Artikel 8

Registrierung, Bearbeitung und Speicherung vertraulicher Informationen

1. Informationen, die als RESTREINT UE/EU RESTRICTED oder auf einer gleichwertigen Stufe oder als „sonstige vertrauliche Information" eingestuft sind, werden von den zuständigen Dienststellen der Sekretariate der parlamentarischen Gremien bzw. Amtsträger oder vom CIU, je nachdem, bei welcher Stelle die Informationen eingegangen sind, registriert und gespeichert.

2. Für die Behandlung von Informationen, die als RESTREINT UE/EU RESTRICTED oder auf einer gleichwertigen Stufe oder als „sonstige vertrauliche Information" eingestuft sind, gelten folgende Bedingungen:

a) Die Dokumente werden dem Leiter des Sekretariats persönlich ausgehändigt, der sie registriert und eine Empfangsbestätigung ausstellt;

b) die Dokumente werden in einem abgeschlossenen Raum unter der Verantwortung des Sekretariats aufbewahrt, wenn sie gerade nicht verwendet werden;

c) die Informationen dürfen auf keinen Fall auf einem anderen Medium gespeichert oder anderen Personen übermittelt werden. Entsprechende Dokumente dürfen nur mit ordnungsgemäß akkreditierten Geräten, die der Definition in den Sicherheitshinweisen entsprechen, vervielfältigt werden;

d) der Zugang zu den Informationen ist auf die Personen beschränkt, die vom Urheber oder von dem Organ der Union, das dem Europäischen Parlament die Informationen übermittelt hat, gemäß den in Artikel 4 Absatz 2 bzw. Artikel 5 Absätze 3, 4 und 5 genannten Regelungen benannt worden sind;

e) das Sekretariat des parlamentarischen Organs bzw. Amtsträgers führt Aufzeichnungen über die Personen, die Einsicht in die Dokumente genommen haben, und über das Datum und die Uhrzeit der Einsichtnahme. Die Sekretariate der parlamentarischen Organe bzw. Amtsträger übermitteln dem CIU die Aufzeichnungen zum Zeitpunkt der Hinterlegung der Informationen beim CIU.

3. Informationen, die als CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET oder TRÈS SECRET UE/EU TOP SECRET oder gleichwertig eingestuft sind, werden vom CIU entsprechend der jeweiligen Geheimhaltungsstufe und den Festlegungen in den Sicherheitshinweisen im gesicherten Bereich registriert, behandelt und gespeichert.

4. Im Fall eines Verstoßes gegen die Regeln der Absätze 1 bis 3 unterrichtet der zuständige Beamte des Sekretariats des parlamentarischen Gremiums bzw. Amtsträgers oder des CIU den Generalsekretär, der die Angelegenheit an den Präsidenten weiterleitet, falls der Regelverstoß von einem Mitglied des Europäischen Parlaments begangen wurde.

Artikel 9

Zugang zu gesicherten Einrichtungen

1. Zugang zum gesicherten Bereich haben nur

a) Personen, die gemäß Artikel 3 Absätze 4 bis 7 berechtigt sind, die dort bereitgehaltenen Informationen einzusehen, und die einen Antrag nach Artikel 10 Absatz 1 gestellt haben;

b) Personen, die gemäß Artikel Absatz 1 berechtigt sind, Verschlusssachen zu erstellen, und die einen Antrag nach Artikel 10 Absatz 1 gestellt haben;

c) die Beamten des Europäischen Parlaments, die zum CIU gehören;

d) die für die Verwaltung des Kommunikations- und Informationssystems zuständigen Beamten des Europäischen Parlaments;

e) erforderlichenfalls die für Sicherheit und Brandschutz zuständigen Beamten des Europäischen Parlaments;

f) Reinigungspersonal, jedoch nur im Beisein und unter strenger Aufsicht eines Beamten des CIU.

2. Das CIU ist befugt, allen Personen den Zutritt zum gesicherten Bereich zu verwehren, die nicht zugangsberechtigt sind. Einsprüche gegen eine solche Zugangsverwehrung sind im Fall von Mitgliedern des Europäischen Parlaments, die Zugang beantragen, an den Präsidenten und in anderen Fällen an den Generalsekretär zu richten.

3. Der Generalsekretär kann eine Sitzung einer begrenzten Zahl von Personen im Sitzungsraum im gesicherten Bereich genehmigen.

4. Zugang zu einem gesicherten Leseraum haben nur

a) die Mitglieder des Europäischen Parlaments, Beamte des Europäischen Parlaments und sonstige, für Fraktionen tätige Parlamentsbedienstete, die zum Zweck der Einsichtnahme in vertrauliche Informationen oder der Erstellung solcher Informationen gebührend ausgewiesen sind;

b) die für die Verwaltung des Kommunikations- und Informationssystems zuständigen Beamten des Europäischen Parlaments, die Beamten des Sekretariats des parlamentarischen Organs bzw. Amtsträgers, bei dem die Informationen eingegangen sind, und Beamte des CIU;

c) erforderlichenfalls die für Sicherheit und Brandschutz zuständigen Beamten des Europäischen Parlaments;

d) Reinigungspersonal, jedoch nur im Beisein und unter strenger Aufsicht eines im Sekretariat des parlamentarischen Organs bzw. Amtsträgers oder im CIU tätigen Beamten.

5. Das zuständige Sekretariat des parlamentarischen Organs bzw. Amtsträgers oder das CIU ist befugt, allen Personen den Zutritt zu einem gesicherten Leseraum zu verwehren, die nicht zugangsberechtigt sind. Einsprüche gegen eine solche Zugangsverwehrung sind im Fall von Mitgliedern des Europäischen Parlaments, die Zugang beantragen, an den Präsidenten und in anderen Fällen an den Generalsekretär zu richten.

Artikel 10

Einsichtnahme in vertrauliche Informationen und Erstellung solcher Informationen in gesicherten Einrichtungen

1. Jede Person, die im gesicherten Bereich Einsicht in vertrauliche Informationen nehmen oder solche Informationen erstellen will, teilt dem CIU vorab ihren Namen mit. Das CIU prüft die Identität dieser Person und überprüft, ob sie gemäß Artikel 3 Absätze 3 bis 7, Artikel 4 Absatz 1 oder Artikel 5 Absätze 3, 4 und 5 zur Einsichtnahme bzw. zur Erstellung vertraulicher Informationen ermächtigt ist.

2. Jede Person, die nach Maßgabe von Artikel 3 Absätze 3 und 7 in einem gesicherten Leseraum Einsicht in vertrauliche Informationen, die als RESTREINT UE/EU RESTRICTED oder gleichwertig oder als „sonstige vertrauliche Informationen" eingestuft wurden, nehmen will, teilt ihren Namen vorab den zuständigen Dienststellen des Sekretariats des parlamentarischen Gremiums bzw. Amtsträgers oder dem CIU mit.

3. Mit Ausnahme von außergewöhnlichen Umständen (zum Beispiel zahlreiche Anträge auf Einsichtnahme innerhalb einer kurzen Zeitspanne) darf jeweils nur einer Person gestattet werden, einzeln vertrauliche Informationen in der gesicherten Einrichtung im Beisein eines Beamten des Sekretariats des parlamentarischen Gremiums bzw. Amtsträgers oder des CIU einzusehen.

4. Während der Einsichtnahme sind der Kontakt mit der Außenwelt (auch über Telefon oder andere technische Hilfsmittel), das Aufzeichnen von Notizen und das Fotokopieren oder Fotografieren der eingesehenen vertraulichen Informationen untersagt.

5. Bevor einer Person gestattet wird, die gesicherte Errichtung zu verlassen, überprüft der Beamte des Sekretariats des parlamentarischen Gremiums bzw. Amtsträgers oder des CIU, dass die eingesehenen vertraulichen Informationen weiterhin unversehrt und vollständig vorhanden sind.

6. Im Fall eines Verstoßes gegen die vorstehenden Regeln unterrichtet der zuständige Beamte des Sekretariats des parlamentarischen Gremiums bzw. Amtsträgers oder des CIU den Generalsekretär, der die Angelegenheit an den Präsidenten weiterleitet, falls es sich um ein Mitglied des Europäischen Parlaments handelt.

Artikel 11

Mindeststandards für die Einsichtnahme in vertrauliche Informationen in einer Sitzung unter Ausschluss der Öffentlichkeit außerhalb gesicherter Einrichtungen

1. Informationen, die als RESTREINT UE/EU RESTRICTED oder gleichwertig oder als „sonstige vertrauliche Informationen" eingestuft wurden, können von Mitgliedern der Ausschüsse des Parlaments oder anderer politischer und administrativer Einrichtungen des Europäischen Parlaments in einer Sitzung unter Ausschluss der Öffentlichkeit außerhalb der gesicherten Einrichtungen eingesehen werden.

2. Unter den in Absatz 1 vorgesehenen Umständen sorgt das Sekretariat des für die Sitzung zuständigen parlamentarischen Gremiums bzw. Amtsträgers dafür, dass folgende Bedingungen erfüllt werden:

a) Nur die vom Vorsitz des zuständigen Ausschusses bzw. der zuständigen Einrichtung zur Teilnahme an der Sitzung bestimmten Personen dürfen den Sitzungssaal betreten;

b) alle Dokumente sind nummeriert, werden zu Beginn der Sitzung ausgeteilt und am Ende wieder eingesammelt, und es werden keine Aufzeichnungen, Fotokopien oder Fotografien davon gemacht;

c) im Sitzungsprotokoll wird nicht auf den Inhalt der Erörterung der geprüften Informationen Bezug genommen. Nur der diesbezügliche Beschluss, sofern einer gefasst wurde, darf vermerkt werden;

d) für vertrauliche Informationen, die Empfängern beim Europäischen Parlament mündlich übermittelt werden, gilt dasselbe Schutzniveau wie für in schriftlicher Form bereitgestellte vertrauliche Informationen;

e) in den Sitzungssälen werden keine zusätzlichen Dokumentbestände bereitgehalten;

f) Exemplare der Dokumente werden den Teilnehmern und den Dolmetschern zu Sitzungsbeginn nur in der notwendigen Anzahl ausgehändigt;

g) zu Sitzungsbeginn gibt der Sitzungsvorsitz deutlich den Status der Dokumente in Bezug auf Einstufung/Kennzeichnung bekannt;

h) die Teilnehmer nehmen keine Dokumente aus dem Sitzungssaal mit;

i) das Sekretariat des parlamentarischen Gremiums bzw. Amtsträgers sammelt sämtliche Exemplare der Dokumente am Ende der Sitzung ein und führt über sie Buch; und

j) elektronische Kommunikationsmittel oder andere elektronische Geräte werden nicht in den Sitzungssaal mitgenommen, in dem die vertrauliche Information eingesehen oder erörtert wird.

3. Wenn Informationen, die als CONFIDENTIEL UE/EU CONFIDENTIAL oder gleichwertig eingestuft worden sind, in Übereinstimmung mit den in Anhang II Nummer 3.2.2 der Rahmenvereinbarung und in Artikel 6 Absatz 5 der Interinstitutionellen Vereinbarung festgelegten Ausnahmen in einer Sitzung unter Ausschluss der Öffentlichkeit erörtert werden, sorgt das Sekretariat des für die Sitzung zuständigen parlamentarischen Gremiums bzw. Amtsträgers neben der Sicherstellung der Einhaltung der Bestimmungen des Absatzes 2 dafür, dass die zur Teilnahme an der Sitzung bestimmten Personen den Anforderungen des Artikels 3 Absätze 4 und 7 genügen.

4. In dem in Absatz 3 vorgesehenen Fall stellt das CIU dem Sekretariat des für die Sitzung unter Ausschluss der Öffentlichkeit zuständigen parlamentarischen Gremiums bzw. Amtsträgers die benötigte Anzahl an Exemplaren der zu erörternden Dokumente zur Verfügung, und diese werden nach der Sitzung dem CIU zurückgegeben.

Artikel 12

Archivierung vertraulicher Informationen

1. Im gesicherten Bereich werden Einrichtungen für eine gesicherte Archivierung geschaffen. Das CIU ist für die Führung des gesicherten Archivs entsprechend den auf die Archivierung bezogenen Standardkriterien zuständig.

2. Verschlusssachen, die endgültig beim CIU hinterlegt sind, und Informationen, die als CONFIDENTIEL UE/EU CONFIDENTIAL oder gleichwertig eingestuft worden sind und beim Sekretariat des parlamentarischen Organs bzw. Amtsträgers hinterlegt wurden, sind sechs Monate nach der letzten Einsichtnahme und spätestens ein Jahr, nachdem sie hinterlegt wurden, in die gesicherte Archivierung im gesicherten Bereich zu verbringen. „Sonstige vertrauliche Informationen" werden vom Sekretariat des betreffenden parlamentarischen Organs bzw. Amtsträgers nach den allgemeinen Bestimmungen über die Dokumentenverwaltung archiviert, sofern sie nicht beim CIU hinterlegt worden sind.

3. Im gesicherten Archiv aufbewahrte vertrauliche Informationen können unter folgenden Bedingungen eingesehen werden:

a) Nur namentlich oder durch ihre Funktion oder ihr Amt in dem Begleitdokument, das bei der Aufnahme der vertraulichen Informationen in das Archiv erstellt wurde, gekennzeichnete Personen sind zur Einsichtnahme in diese Informationen befugt;

b) der Antrag auf Einsichtnahme in die vertraulichen Informationen ist dem CIU vorzulegen, das das betreffende Dokument dann in den gesicherten Leseraum verbringt; und

c) die in Artikel 10 festgelegten Verfahren und Bedingungen bezüglich der Einsichtnahme in vertrauliche Informationen finden Anwendung.

Artikel 13

Herabstufung, Freigabe und Aufhebung der Kennzeichnung von vertraulichen Informationen

1. Vertrauliche Informationen dürfen nur mit vorheriger Genehmigung des Urhebers und erforderlichenfalls nach Rücksprache mit anderen Beteiligten herabgestuft, freigegeben oder von der Kennzeichnung befreit werden.

2. Die Herabstufung bzw. die Freigabe ist schriftlich zu bestätigen. Dem Urheber obliegt es, die Empfänger des Dokuments über die Änderung der Einstufung zu informieren, und diesen obliegt es ihrerseits, die weiteren Empfänger, denen sie das Original oder eine Kopie des Dokuments zugeleitet haben, von der Änderung zu unterrichten. Soweit möglich, gibt der Urheber auf als Verschlusssache eingestuften Dokumenten den Zeitpunkt oder ein Ereignis, ab dem — oder eine Zeitspanne, in der — die in dem Dokument enthaltenen Informationen herabgestuft oder freigegeben werden können. Andernfalls überprüft er die betroffenen Dokumente in Abständen von höchstens fünf Jahren, um sich zu vergewissern, dass die ursprüngliche Einstufung nach wie vor erforderlich ist.

3. In den gesicherten Archiven aufbewahrte vertrauliche Informationen werden rechtzeitig, spätestens am 25. Jahrestag nach ihrer Erstellung, darauf hin überprüft, ob sie freigegeben oder herabgestuft werden sollen bzw. ob ihre Kennzeichnung aufgehoben werden soll. Die Überprüfung und Veröffentlichung solcher Informationen erfolgt gemäß den Bestimmungen der Verordnung (EWG, Euratom) Nr. 354/83 des Rates vom 1. Februar 1983 über die Freigabe der historischen Archive der Europäischen Wirtschaftsgemeinschaft und der Europäischen Atomgemeinschaft ([1]). Die Freigabe erfolgt gemäß Anlage I Teil 1 Abschnitt 10 durch den Urheber der vertraulichen Informationen oder durch die zu dem Zeitpunkt zuständige Dienststelle.

4. Nach der Freigabe werden die zuvor als Verschlusssache eingestuften und im gesicherten Archiv aufbewahrten Informationen dem historischen Archiv des Europäischen Parlaments zum Zweck der ständigen Aufbewahrung und der Weiterbehandlung nach den geltenden Bestimmungen zugeführt.

5. Nach der Aufhebung der Kennzeichnung unterliegen die zuvor als „sonstige vertrauliche Informationen" eingestuften Informationen den beim Europäischen Parlament geltenden Bestimmungen über die Dokumentenverwaltung.

Artikel 14

Verletzung der Sicherheit, Verlust der vertraulichen Information oder Kenntnisnahme durch Unbefugte

1. Ein Verstoß gegen die Geheimhaltungspflicht im Allgemeinen und gegen diesen Beschluss im Besonderen, zieht im Fall von Mitgliedern des Europäischen Parlaments die Anwendung der in der Geschäftsordnung des Europäischen Parlaments festgelegten einschlägigen Bestimmungen über Sanktionen nach sich.

2. Ein Verstoß durch einen Bediensteten des Europäischen Parlaments führt zur Anwendung der Verfahren und Sanktionen, die im Statut der Beamten der Europäischen Union und in den Beschäftigungsbedingungen für die sonstigen Bediensteten der Europäischen Union, festgelegt durch die Verordnung (EWG, Euratom, EGKS) Nr. 259/68 ([2]) („Beamtenstatut") vorgesehen sind.

([1]) ABl. L 43 vom 15.2.1983, S. 1.
([2]) ABl. L 56 vom 4.3.1968, S. 1.

3. Bei einem Verstoß gemäß der Definition in Sicherheitshinweis 6 veranlasst der Präsident und/oder der Generalsekretär die erforderlichen Untersuchungen.

4. Wurden die vertraulichen Informationen dem Europäischen Parlament durch ein Organ der Union oder einen Mitgliedstaat übermittelt, unterrichten der Präsident und/oder der Generalsekretär das Organ der Union bzw. den betroffenen Mitgliedstaat über einen erwiesenen oder mutmaßlichen Verlust einer Verschlusssache oder eine erwiesene oder mutmaßliche Kenntnisnahme von einer Verschlusssache durch Unbefugte sowie über die Ergebnisse der Untersuchung und die Maßnahmen gegen eine Wiederholung des Vorfalls.

Artikel 15

Anpassung dieses Beschlusses und der Durchführungsbestimmungen sowie jährliche Berichterstattung über die Anwendung dieses Beschlusses

1. Der Generalsekretär arbeitet Vorschläge für gegebenenfalls notwendige Anpassungen dieses Beschlusses und seiner in den Anlagen festgelegten Durchführungsbestimmungen aus und legt sie dem Präsidium zur Entscheidung vor.

2. Der Generalsekretär ist für die Durchführung dieses Beschlusses durch die Dienststellen des Europäischen Parlaments verantwortlich und gibt in Übereinstimmung mit den Grundsätzen dieses Beschlusses die Behandlungsanweisungen in Bezug auf die unter das Managementsystem für Informationssicherheit (ISMS) fallenden Angelegenheiten heraus.

3. Der Generalsekretär legt dem Präsidium einen Jahresbericht über die Anwendung dieses Beschlusses vor.

Artikel 16

Übergangs- und Schlussbestimmungen

1. Nicht als Verschlusssache eingestufte Informationen, die beim CIU oder in einem anderen Archiv des Europäischen Parlaments vorliegen, als vertraulich gelten und vor dem 1. April 2014 datiert wurden, gelten für die Zwecke dieses Beschlusses als „sonstige vertrauliche Informationen". Deren Urheber kann ihren Geheimhaltungsgrad jederzeit einer Überprüfung unterziehen.

2. Abweichend von Artikel 5 Absatz 1 Buchstabe a und Artikel 8 Absatz 1 dieses Beschlusses sind Informationen, die aufgrund der in der Interinstitutionellen Vereinbarung vom Rat zur Verfügung gestellt und als RESTREINT UE/EU RESTRICTED oder gleichwertig eingestuft sind, während 12 Monaten ab dem 1. April 2014 beim CIU zu hinterlegen und von ihm zu registrieren und aufzubewahren. Derartige Informationen können nach Maßgabe von Artikel 4 Absatz 2 Buchstaben a und c sowie Artikel 5 Absatz 4 der Interinstitutionellen Vereinbarung eingesehen werden.

3. Der Beschluss des Präsidiums des Europäischen Parlaments vom 6. Juni 2011 über die Regeln zur Behandlung vertraulicher Informationen durch das Europäische Parlament wird aufgehoben.

Artikel 17

Inkrafttreten

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

ANLAGE I

Teil 1

GRUNDSÄTZE UND SICHERHEITSMINDESTSTANDARDS FÜR DEN SCHUTZ VERTRAULICHER INFORMATIONEN

1. **EINLEITUNG**

Die vorliegenden Bestimmungen enthalten die Grundsätze und Sicherheitsmindeststandards zum Schutz von vertraulichen Informationen, die vom Europäischen Parlament an sämtlichen Dienstorten sowie von allen Empfängern von Verschlusssachen und „sonstigen vertraulichen Informationen" einzuhalten sind, damit die Sicherheit gewährleistet ist und alle betroffenen Personen darauf vertrauen können, dass ein einheitliches Schutzniveau vorgegeben ist. Die Bestimmungen werden ergänzt durch die Sicherheitshinweise in Anlage II und sonstige Bestimmungen über die Behandlung vertraulicher Informationen durch die Ausschüsse des Parlaments und andere parlamentarische Organe bzw. Amtsträger.

2. **GRUNDSÄTZE**

Die Sicherheitsstrategie des Europäischen Parlaments ist integraler Bestandteil seines Gesamtkonzepts für die interne Verwaltung und beruht damit auf den Grundsätzen dieses Gesamtkonzepts. Zu diesen Grundsätzen zählen Rechtmäßigkeit, Transparenz, Rechenschaftspflicht, Subsidiarität und Verhältnismäßigkeit.

Der Begriff der Rechtmäßigkeit umfasst die Notwendigkeit, bei der Ausübung von Sicherheitsfunktionen voll und ganz innerhalb des rechtlichen Rahmens zu bleiben und die geltenden rechtlichen Anforderungen einzuhalten. Zudem müssen die Verantwortlichkeiten im Sicherheitsbereich auf angemessenen Rechtsvorschriften beruhen. Das Beamtenstatut, insbesondere Artikel 17 (Verpflichtung der Bediensteten, sich jeder nicht genehmigten Verbreitung von Informationen zu enthalten, von denen sie im Rahmen ihrer Aufgaben Kenntnis erhalten) und Titel VI (Disziplinarmaßnahmen) finden uneingeschränkt Anwendung. Schließlich müssen Verstöße gegen die Sicherheitsbestimmungen, die in der Zuständigkeit des Europäischen Parlaments liegen, im Einklang mit seiner Geschäftsordnung und seinen Grundsätzen in Bezug auf Disziplinarmaßnahmen behandelt werden.

Der Begriff der Transparenz umfasst das Erfordernis der Klarheit in Bezug auf alle Sicherheitsvorschriften, des Gleichgewichts zwischen den Dienststellen und dienstlichen Bereichen (physische Sicherheit gegenüber Schutz von Informationen usw.) und einer in sich schlüssigen und strukturierten Strategie für das Sicherheitsbewusstsein. Er umfasst außerdem das Erfordernis klarer schriftlicher Leitlinien für die Durchführung von Sicherheitsmaßnahmen.

Der Begriff der Rechenschaftspflicht bedeutet, dass die Verantwortlichkeiten im Sicherheitsbereich eindeutig festgelegt werden müssen. Zudem umfasst er das Erfordernis, in regelmäßigen Abständen festzustellen, ob die Verantwortlichkeiten ordnungsgemäß wahrgenommen worden sind.

Der Begriff der Subsidiarität bedeutet, dass die Sicherheit auf der niedrigstmöglichen Ebene und möglichst nahe bei den einzelnen Generaldirektionen und Dienststellen des Europäischen Parlaments organisiert werden muss. Verhältnismäßigkeit bedeutet, dass sicherheitsbezogene Tätigkeiten streng auf das absolut notwendige Maß beschränkt werden und dass Sicherheitsmaßnahmen in einem angemessenen Verhältnis zu den zu schützenden Interessen und zu der tatsächlichen oder potenziellen Bedrohung dieser Interessen stehen müssen, damit die Interessen in einer Weise geschützt werden können, die mit möglichst geringen Beeinträchtigungen verbunden ist.

3. **GRUNDLAGEN DER INFORMATIONSSICHERHEIT**

Die Grundlagen solider Informationssicherheit sind

a) solide Kommunikations- und Informationssysteme (CIS). Diese fallen unter die Verantwortlichkeit des Sicherheitsorgans des Europäischen Parlaments (wie im Sicherheitshinweis 1 definiert);

b) intern beim Europäischen Parlament die Informationssicherungsstelle (wie im Sicherheitshinweis 1 definiert), die dafür zuständig ist, in Zusammenarbeit mit dem Sicherheitsorgan Informationen und Beratung über technische Bedrohungen der Kommunikations- und Informationssysteme (CIS) und die Mittel zum Schutz vor diesen Bedrohungen bereitzustellen;

c) eine enge Zusammenarbeit zwischen den zuständigen Dienststellen des Europäischen Parlaments und den Sicherheitsdiensten der anderen Unionsorgane;

4. **GRUNDSÄTZE DER INFORMATIONSSICHERHEIT**

4.1. ***Ziele***

Die Hauptziele im Bereich der Informationssicherheit sind:

a) Schutz von vertraulichen Informationen vor Spionage, Kenntnisnahme durch Unbefugte oder unerlaubter Weitergabe;

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

c) Schutz der Gebäude des Parlaments, in denen Verschlusssachen aufbewahrt werden, vor Sabotage und vorsätzlicher Beschädigung;

d) im Fall des Versagens der Sicherheitsvorkehrungen: Bewertung des entstandenen Schadens, Begrenzung der Folgen, Durchführung sicherheitsbezogener Nachforschungen und Festlegung von zur Behebung des Schadens erforderlichen Maßnahmen.

4.2. ***Einstufung***

4.2.1. Im Bereich der Vertraulichkeit muss bei der Auswahl der schutzbedürftigen Informationen und Materialien und bei der Bewertung des Umfangs des erforderlichen Schutzes mit Sorgfalt vorgegangen und auf Erfahrungen zurückgegriffen werden. Es ist von entscheidender Bedeutung, dass der Umfang des Schutzes der Sicherheitsrelevanz der jeweils zu schützenden Informationen und Materialien entspricht. Im Interesse eines reibungslosen Informationsflusses müssen sowohl eine zu hohe als auch eine zu niedrige Einstufung vermieden werden.

4.2.2. Das Einstufungssystem ist das Instrument, mit dem die in diesem Abschnitt genannten Grundsätze umgesetzt werden. Ein entsprechendes Einstufungssystem ist bei der Planung und Durchführung von Maßnahmen zur Bekämpfung von Spionage, Sabotage, Terrorismus und anderen Arten der Bedrohung anzuwenden, damit die wichtigsten Gebäude, in denen Verschlusssachen aufbewahrt werden, und die empfindlichsten Stellen in diesen Gebäuden den größtmöglichen Schutz erhalten.

4.2.3. Die Verantwortung für die Festlegung des Geheimhaltungsgrads einer Information liegt allein bei dem Urheber der betreffenden Information.

4.2.4. Der Geheimhaltungsgrad hängt allein vom Inhalt der betreffenden Information ab.

4.2.5. Werden mehrere Informationen zu einem Ganzen zusammengestellt, muss ihre Einstufung mindestens so hoch sein wie der Geheimhaltungsgrad des am höchsten eingestuften Bestandteils. Eine Zusammenstellung von Informationen kann indessen höher eingestuft werden als ihre Bestandteile.

4.2.6 Eine Einstufung erfolgt nur dann, wenn sie erforderlich ist, und nur für den Zeitraum, in dem sie erforderlich ist.

4.3. ***Ziele von Sicherheitsmaßnahmen***

Sicherheitsmaßnahmen

a) erstrecken sich auf alle Personen, die Zugang zu Verschlusssachen, Medien mit Verschlusssachen und „sonstigen vertraulichen Informationen“ haben, sowie auf alle Gebäude, in denen sich derartige Informationen und wichtige Einrichtungen befinden;

b) sind so ausgelegt, dass Personen, die aufgrund ihrer Stellung (Zugangsmöglichkeiten, Verbindungen oder andere Gesichtspunkte) die Sicherheit solcher Informationen und wichtiger Einrichtungen, in denen solche Informationen aufbewahrt werden, gefährden könnten, erkannt und vom Zugang ausgeschlossen oder fern gehalten werden;

c) müssen verhindern, dass unbefugte Personen Zugang zu solchen Informationen oder zu Einrichtungen, in denen sie aufbewahrt werden, erhalten;

d) müssen sicherstellen, dass solche Informationen nur unter Beachtung des für alle Aspekte der Sicherheit grundlegenden Grundsatzes des berechtigten Informationsinteresses verbreitet werden;

e) müssen die Integrität (d. h. Unterbindung von Verfälschungen, unbefugten Änderungen oder unbefugten Löschungen) und die Verfügbarkeit (für Personen, die Zugang benötigen und dazu ermächtigt sind) von vertraulichen Informationen sicherstellen, insbesondere wenn die Informationen in elektromagnetischer Form gespeichert, verarbeitet oder übermittelt werden.

5. GEMEINSAME MINDESTSTANDARDS

Das Europäische Parlament sorgt dafür, dass gemeinsame Mindeststandards für die Sicherheit von allen Empfängern von Verschlusssachen eingehalten werden, sowohl innerhalb des Organs als auch in seinem Zuständigkeitsbereich, d. h. von allen Dienststellen und Auftragnehmern, damit bei der Weitergabe der Informationen darauf vertraut werden kann, dass sie mit derselben Sorgfalt behandelt werden. Diese Mindeststandards umfassen Kriterien für die Sicherheitsüberprüfung von Beamten des Europäischen Parlaments und sonstigen Parlamentsbediensteten, die für die Fraktionen tätig sind, sowie Verfahren zum Schutz von vertraulichen Informationen.

Das Europäische Parlament gewährt Dritten nur dann Zugang zu derartigen Informationen, wenn sie gewährleisten, dass beim Umgang mit den Informationen Bestimmungen eingehalten werden, die diesen gemeinsamen Mindeststandards mindestens gleichwertig sind.

Solche gemeinsamen Mindeststandards sind auch anzuwenden, wenn das Parlament aufgrund eines Vertrags oder einer Finanzhilfevereinbarung juristischen Personen in der Wirtschaft oder anderen Personen Aufgaben überträgt, die mit vertraulichen Informationen verbunden sind.

6. SICHERHEITSBESTIMMUNGEN IN BEZUG AUF BEAMTE DES EUROPÄISCHEN PARLAMENTS UND SONSTIGE PARLAMENTSBEDIENSTETE, DIE FÜR DIE FRAKTIONEN TÄTIG SIND

6.1. *Sicherheitsanweisungen in Bezug auf Beamte des Europäischen Parlaments und sonstige Parlamentsbedienstete, die für die Fraktionen tätig sind*

Beamte des Europäischen Parlaments und sonstige, für die Fraktionen tätige Parlamentsbedienstete, die Stellen bekleiden, in deren Rahmen sie Zugang zu Verschlusssachen erhalten könnten, sind bei Aufnahme ihrer Tätigkeit und danach in regelmäßigen Abständen eingehend über die Notwendigkeit von Sicherheitsbestimmungen und sicherheitsbezogenen Verfahren zu unterrichten. Diese Personen haben schriftlich zu bestätigen, dass sie die geltenden Sicherheitsbestimmungen gelesen haben und in vollem Umfang verstehen.

6.2. *Verantwortung der Führungskräfte*

Es muss zu den Pflichten von Führungskräften gehören, sich Kenntnis darüber zu verschaffen, welche ihrer Mitarbeiter mit Verschlusssachen zu tun haben oder Zugang zu gesicherten Kommunikations- oder Informationssystemen haben, und alle Vorfälle oder offenkundigen Schwachpunkte, die sicherheitsrelevant sein könnten, festzuhalten und zu melden.

6.3. *Sicherheitsstatus von Beamten und sonstigen Parlamentsbediensteten, die für die Fraktionen tätig sind*

Es sind Verfahren vorzusehen, durch die bei Bekanntwerden nachteiliger Informationen über einen Beamten des Europäischen Parlaments oder einen sonstigen Parlamentsbediensteten, der für eine Fraktion tätig ist, sichergestellt wird, dass Maßnahmen ergriffen werden um festzustellen, ob diese Person in ihrer Arbeit mit Verschlusssachen zu tun hat oder Zugang zu gesicherten Kommunikations- oder Informationssystemen hat, und dass der zuständige Dienst des Europäischen Parlaments in Kenntnis gesetzt wird. Gibt die zuständige nationale Sicherheitsbehörde Hinweise darauf, dass die fragliche Person ein Sicherheitsrisiko darstellt, ist diese von Aufgaben, bei denen sie die Sicherheit gefährden könnte, auszuschließen oder fern zu halten.

7. PHYSISCHER GEHEIMSCHUTZ

„Physischer Geheimschutz“ bedeutet die Anwendung von physischen und technischen Schutzmaßnahmen, um unbefugten Zugang zu Verschlusssachen zu verhindern.

7.1. ***Schutzbedarf***

Der Umfang der anzuwendenden Maßnahmen des physischen Geheimschutzes zum Schutz von Verschlusssachen muss in angemessenem Verhältnis zum Geheimhaltungsgrad, zum Umfang und zur Bedrohung der entsprechenden Informationen und Materialien stehen. Alle Personen, die Verschlusssachen verwahren, haben eine einheitliche Praxis bei der Einstufung solcher Informationen anzuwenden und gemeinsame Schutzstandards für die Verwahrung, Übermittlung und Beseitigung schutzbedürftiger Informationen und Materialien zu beachten.

7.2. ***Überprüfung***

Personen, die Bereiche, in denen sich ihnen anvertraute 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 Dienstschluss durchzuführen.

7.3. ***Gebäudesicherheit***

Gebäude, in denen sich Verschlusssachen oder gesicherte Kommunikations- und Informationssysteme befinden, sind gegen unerlaubten Zutritt zu schützen.

Die Art der Schutzmaßnahmen für Verschlusssachen (z. B. Vergitterung von Fenstern, Türschlösser, 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 Informationen und Materialien befinden, und

c) Beschaffenheit und Lage des Gebäudes.

Die Art der Schutzmaßnahmen für Kommunikations- und Informationssysteme hängt von folgenden Faktoren ab: Beurteilung des Wertes der betreffenden Vermögenswerte und der Höhe des im Fall einer Kenntnisnahme durch Unbefugte entstehenden Schadens, Beschaffenheit und Lage des Gebäudes, in dem das System untergebracht ist, und Ort seiner Unterbringung im Gebäude.

7.4. ***Notfallpläne***

Für den Schutz vertraulicher Informationen in Notfällen müssen vorab detaillierte Pläne bereitgehalten werden.

8. **SICHERHEITSKENNUNGEN, KENNZEICHNUNGEN, ANBRINGUNG UND REGELN FÜR DIE EINSTUFUNG ALS VERSCHLUSSSACHE**

8.1. ***Sicherheitskennungen***

Andere Geheimhaltungsgrade als die in Artikel 2 Buchstabe d dieses Beschlusses genannten sind nicht zugelassen.

Eine vereinbarte Sicherheitskennung darf verwendet werden, um die Geltungsdauer eines Geheimhaltungsgrades zu begrenzen (was bei Verschlusssachen automatische Herabstufung des Geheimhaltungsgrades oder Freigabe bedeutet).

Sicherheitskennungen sind nur in Verbindung mit einem Geheimhaltungsgrad zu verwenden.

Sicherheitskennungen sind in Sicherheitshinweis 2 im Einzelnen geregelt und in den Behandlungsanweisungen festgelegt.

8.2. ***Kennzeichnungen***

Kennzeichnungen werden benutzt, um vorab festgelegte spezifische Anweisungen zum Umgang mit vertraulichen Informationen deutlich zu machen. Kennzeichnungen können außerdem den von einem bestimmten Dokument abgedeckten Bereich, eine besondere Verbreitung auf der Grundlage des berechtigten Informationsinteresses oder (bei Dokumenten, die nicht als Verschlusssache eingestuft sind) den Ablauf einer Sperrfrist angeben.

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

Kennzeichnungen sind in Sicherheitshinweis 2 im Einzelnen geregelt und in den Behandlungsanweisungen festgelegt.

8.3. ***Anbringung von Hinweisen auf den Geheimhaltungsgrad und von Sicherheitskennungen***

Die Anbringung von Hinweisen auf den Geheimhaltungsgrad, Sicherheitskennungen und Kennzeichnungen muss nach Maßgabe des Sicherheitshinweises 2 Abschnitt E und der Behandlungsanweisungen vorgenommen werden.

8.4. ***Organisation der Einstufung***

8.4.1 *Allgemeines*

Informationen sind nur dann als Verschlusssache einzustufen, wenn es 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 Freigabe liegt allein beim Urheber der Information.

Beamte des Europäischen Parlaments nehmen auf Anweisung des Generalsekretärs oder in dessen Auftrag Einstufungen, Herabstufungen des Geheimhaltungsgrades oder Freigaben von Informationen vor.

Die Einzelheiten der Verfahren für die Behandlung von als Verschlusssache eingestuften Dokumenten müssen so angelegt sein, dass die Gewissheit besteht, dass die Dokumente den ihrem Inhalt angemessenen Schutz erhalten.

Die Zahl der Personen, die dazu ermächtigt sind, Informationen des Geheimhaltungsgrades TRÈS SECRET UE/EU TOP SECRET in Umlauf zu bringen, ist möglichst klein zu halten, und ihre Namen sind in einer Liste zu verzeichnen, die von dem CIU geführt wird.

8.4.2 *Anwendung der Geheimhaltungsgrade*

Bei der Festlegung des Geheimhaltungsgrades eines Dokuments wird das Niveau der Schutzbedürftigkeit seines Inhalts entsprechend den Begriffsbestimmungen in Artikel 2 Buchstabe d zugrunde gelegt. Es ist wichtig, dass die Einstufung korrekt vorgenommen und sparsam mit ihr umgegangen wird.

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

Der Urheber eines Dokuments, dem ein Geheimhaltungsgrad zugeordnet werden soll, muss die vorstehend genannten Vorschriften befolgen und eine zu hohe oder zu niedrige Einstufung vermeiden.

Einzelne Seiten, Absätze, Abschnitte, Anhänge und sonstige Anlagen eines Dokuments können unterschiedliche Geheimhaltungsgrade erfordern und sind entsprechend einzustufen. Der Geheimhaltungsgrad des Gesamtdokuments muss der Geheimhaltungsgrad seines am höchsten eingestuften Teils sein.

9. **INSPEKTIONEN**

Regelmäßige interne Inspektionen der Sicherheitsvorkehrungen zum Schutz von Verschlusssachen sind von der Direktion Sicherheit und Risikobewertung des Europäischen Parlaments durchzuführen, die die Sicherheitsorgane des Rates oder der Kommission um Unterstützung ersuchen kann.

Die Sicherheitsorgane und die zuständigen Stellen bei den Organen der Union können im Rahmen eines von einem der Organe eingeleiteten einvernehmlichen Prozesses gegenseitige Begutachtungen der Sicherheitsvorkehrungen zum Schutz von aufgrund der einschlägigen interinstitutionellen Vereinbarungen ausgetauschten Verschlusssachen vornehmen.

10. **VERFAHREN ZUR FREIGABE UND ZUR AUFHEBUNG DER KENNZEICHNUNG**

10.1. Das CIU prüft die vertraulichen Informationen in ihrem Register und ersucht den Urheber eines Dokuments spätestens bis zum 25. Jahrestag der Erstellung des Dokuments um Zustimmung zur Freigabe oder zur Aufhebung der Kennzeichnung. Dokumente, die bei der ersten Prüfung nicht freigegeben wurden oder deren Kennzeichnung nicht aufgehoben wurde, sind regelmäßig und mindestens alle fünf Jahre erneut zu prüfen. Das Verfahren der Aufhebung der Kennzeichnung kann, abgesehen von den Dokumenten, die sich in den gesicherten Archiven im gesicherten Bereich befinden und gebührend eingestuft sind, auch sonstige vertrauliche Informationen betreffen, die sich entweder bei dem parlamentarischen Organ bzw. Amt oder der für die historischen Archive des Parlaments zuständigen Dienststelle befinden.

10.2 Die Entscheidung über die Freigabe oder die Aufhebung der Kennzeichnung ist generell ausschließlich vom Urheber oder ausnahmsweise in Zusammenarbeit mit dem parlamentarischen Organ bzw. Amtsträger, das bzw. der die Informationen aufbewahrt, zu treffen, bevor die betreffenden Informationen an die für die historischen Archive des Parlaments zuständige Dienststelle weitergeleitet werden. Die Freigabe oder die Aufhebung der Kennzeichnung von Verschlusssachen darf nur nach schriftlicher Zustimmung des Urhebers vorgenommen werden. Im Fall der „sonstigen vertraulichen Informationen" entscheidet das Sekretariat des parlamentarischen Organs bzw. der Amtsträger, das bzw. der die Informationen aufbewahrt, in Zusammenarbeit mit dem Urheber darüber, ob die Kennzeichnung des Dokuments aufgehoben werden kann.

10.3. Das CIU ist dafür zuständig, im Namen des Urhebers die Empfänger des Dokuments über die Änderung der Einstufung oder der Kennzeichnung zu informieren, wobei letztere wiederum die weiteren Empfänger, denen sie das Original oder eine Kopie des Dokuments zugeleitet haben, von der Änderung zu unterrichten haben.

10.4. Die Freigabe berührt nicht die Sicherheitskennungen oder Kennzeichnungen, die möglicherweise auf dem Dokument angebracht sind.

10.5. Bei Freigabe ist der Hinweis auf den ursprünglichen Geheimhaltungsgrad, der am oberen und unteren Ende jeder Seite vermerkt ist, durchzustreichen. Die erste Seite (Titelseite) des Dokuments ist mit einem Stempel und der Referenznummer des CIU zu versehen. Bei Aufhebung der Kennzeichnung ist die ursprüngliche Kennzeichnung am oberen Ende jeder Seite durchzustreichen.

10.6. Der Text des freigegebenen Dokuments oder des Dokuments mit aufgehobener Kennzeichnung ist dem elektronischen Datenblatt oder einem gleichwertigen System, in dem es registriert wurde, beizufügen.

10.7. Im Fall von Dokumenten, die unter die Ausnahmen bezüglich der Privatsphäre und der Integrität der persönlichen oder der geschäftlichen Interessen einer natürlichen oder juristischen Person fallen, und im Fall von sensiblen Dokumenten findet Artikel 2 der Verordnung (EWG, Euratom) Nr. 354/83 des Rates Anwendung.

10.8. Zusätzlich zu den in den Nummern 10.1 bis 10.7 enthaltenen Bestimmungen gelten folgende Bestimmungen:

a) Bei Dokumenten von Dritten befragt das CIU die jeweiligen Dritten, bevor es eine Freigabe oder Aufhebung der Kennzeichnung vornimmt.

b) Im Fall der Ausnahme, die die Privatsphäre und die Integrität des Einzelnen betrifft, ist im Verfahren der Freigabe oder der Aufhebung der Kennzeichnung insbesondere die Zustimmung der betroffenen Person zu berücksichtigen oder gegebenenfalls der Umstand, dass diese nicht ermittelt werden kann.

c) Im Fall der Ausnahme, die die geschäftlichen Interessen einer natürlichen oder juristischen Person betrifft, kann die betroffene Person durch Veröffentlichung im *Amtsblatt der Europäischen Union* unterrichtet werden, wobei für mögliche Anmerkungen eine Frist von vier Wochen ab dem Tag der Veröffentlichung vorzusehen ist.

Teil 2

VERFAHREN DER SICHERHEITSÜBERPRÜFUNG

11. **VERFAHREN DER SICHERHEITSÜBERPRÜFUNG BEI MITGLIEDERN DES EUROPÄISCHEN PARLAMENTS**

11.1. Um Zugang zu den als CONFIDENTIEL UE/EU CONFIDENTIAL oder gleichwertig eingestuften Verschlusssachen zu erhalten, müssen Mitglieder des Europäischen Parlaments hierzu entweder nach dem Verfahren der Nummern 11.3 und 11.4 dieses Anhangs oder auf der Grundlage einer förmlichen Geheimhaltungserklärung gemäß Artikel 3 Absatz 4 dieses Beschlusses ermächtigt worden sein.

11.2 Um Zugang zu als TRÈS SECRET UE/EU TOP SECRET und SECRET UE/EU SECRET oder gleichwertig eingestuften Verschlusssachen zu erhalten, müssen Mitglieder des Europäischen Parlaments nach dem Verfahren der Nummern 11.3 und 11.14 ermächtigt worden sein.

11.3. Die Ermächtigung wird nur Mitgliedern des Europäischen Parlaments erteilt, die durch die zuständigen nationalen Behörden der Mitgliedstaaten gemäß dem Verfahren der Nummern 11.9 bis 11.14 einer Sicherheitsüberprüfung unterzogen worden sind. Die Ermächtigung für Mitglieder fällt in die Zuständigkeit des Präsidenten.

11.4 Der Präsident kann die schriftliche Ermächtigung nach Einholung der Stellungnahme der zuständigen Behörden der Mitgliedstaaten auf der Grundlage der gemäß den Nummern 11.8 bis 11.13 durchgeführten Sicherheitsüberprüfung erteilen.

11.5. Die für Sicherheit zuständige Direktion Sicherheit und Risikobewertung des Europäischen Parlaments führt ein fortlaufend aktualisiertes Verzeichnis aller Mitglieder des Europäischen Parlaments, denen eine Ermächtigung erteilt wurde; dies gilt auch für vorläufige Ermächtigungen im Sinn der Nummer 11.15.

11.6. Die Ermächtigung gilt für eine Dauer von fünf Jahren oder für die Dauer der Aufgaben, wegen denen sie erteilt wurde, wobei der kürzere der beiden Zeiträume zugrunde gelegt wird. Sie kann gemäß dem Verfahren der Nummer 11.4 verlängert werden.

11.7. Ermächtigungen sind vom Präsidenten zu entziehen, wenn er dies für begründet hält. Die Entscheidung über den Entzug der Ermächtigung wird dem betroffenen Mitglied des Europäischen Parlaments mitgeteilt, das beantragen kann, vom Präsidenten gehört zu werden, bevor der Entzug wirksam wird, und der zuständigen nationalen Behörde mitgeteilt.

11.8. Die Sicherheitsüberprüfung wird unter Mitwirkung des betroffenen Mitglieds des Europäischen Parlaments und auf Ersuchen des Präsidenten vorgenommen. Die für die Überprüfung zuständige nationale Behörde ist die Behörde des Mitgliedstaats, dessen Staatsangehörigkeit das betroffene Mitglied besitzt.

11.9. Das betroffene Mitglied des Europäischen Parlaments hat im Zuge der Sicherheitsüberprüfung ein Auskunftsformular auszufüllen.

11.10. Der Präsident benennt in seinem Ersuchen an die zuständige nationale Behörde den Geheimhaltungsgrad der Informationen, zu denen das betroffene Mitglied des Europäischen Parlaments Zugang erhalten soll, damit die zuständige nationale Behörde das Sicherheitsüberprüfungsverfahren entsprechend durchführen kann.

11.11 Der gesamte Ablauf und die Ergebnisse des von der nationalen Behörde durchgeführten Verfahrens der Sicherheitsüberprüfung stehen im Einklang mit den einschlägigen Vorschriften und Regelungen des betroffenen Mitgliedstaats, einschließlich der Vorschriften und Regelungen über Rechtsbehelfe.

11.12. Bei befürwortender Stellungnahme der zuständigen nationalen Behörde kann der Präsident dem betroffenen Mitglied des Europäischen Parlaments die Ermächtigung erteilen.

11.13. Eine ablehnende Stellungnahme der zuständigen nationalen Behörde wird dem betroffenen Mitglied des Europäischen Parlaments mitgeteilt, das beantragen kann, vom Präsidenten gehört zu werden. Der Präsident kann, wenn er es für erforderlich hält, bei der zuständigen nationalen Behörde um weitere Auskünfte nachsuchen. Bei Bestätigung der ablehnenden Stellungnahme darf die Ermächtigung nicht erteilt werden.

11.14. Alle nach Nummer 11.3 ermächtigten Mitglieder des Europäischen Parlaments erhalten zum Zeitpunkt der Erteilung der Ermächtigung und danach in regelmäßigen Abständen die notwendigen Leitlinien über den Schutz von Verschlusssachen und über die Mittel zur Sicherstellung dieses Schutzes. Diese Mitglieder unterzeichnen eine Erklärung, mit der sie den Erhalt dieser Leitlinien bestätigen.

11.15. Ausnahmsweise kann der Präsident, nachdem er die zuständige nationale Behörde hiervon unterrichtet hat und von dieser Behörde binnen eines Monats dazu nicht Stellung genommen wurde, einem Mitglied des Europäischen Parlaments eine vorläufige Ermächtigung für höchstens sechs Monate erteilen, bis ihm das Ergebnis der Sicherheitsüberprüfung nach Nummer 11.11 vorliegt. Die so erteilten vorläufigen Ermächtigungen berechtigen nicht zum Zugang zu als TRÈS SECRET UE/EU TOP SECRET oder gleichwertig eingestuften Verschlusssachen.

12. VERFAHREN DER SICHERHEITSÜBERPRÜFUNG VON BEAMTEN DES EUROPÄISCHEN PARLAMENTS UND SONSTIGEN PARLAMENTSBEDIENSTETEN, DIE FÜR DIE FRAKTIONEN TÄTIG SIND

12.1. Nur Beamte des Europäischen Parlaments und sonstige für Fraktionen tätige Parlamentsbedienstete, die aufgrund ihrer Aufgabenbereiche und dienstlicher Erfordernisse von Verschlusssachen Kenntnis nehmen müssen oder sie benutzen müssen, dürfen Zugang zu solchen Verschlusssachen erhalten.

12.2. Um Zugang zu den als CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET oder TRÈS SECRET UE/EU TOP SECRET oder gleichwertig eingestuften Verschlusssachen zu erhalten, müssen die Beamten des Europäischen Parlaments bzw. die für eine Fraktion tätigen sonstigen Parlamentsbediensteten hierzu nach dem Verfahren der Nummern 12.3 und 12.4 ermächtigt worden sein.

12.3. Die Ermächtigung wird nur Personen nach Nummer 12.1 erteilt, die durch die zuständigen Behörden der Mitgliedstaaten gemäß dem Verfahren der Nummern 12.9 bis 12.14 einer Sicherheitsüberprüfung unterzogen worden sind. Die Ermächtigung für Beamte des Parlaments und sonstige Parlamentsbedienstete, die bei den Fraktionen tätig sind, fällt in die Zuständigkeit des Generalsekretärs.

12.4. Der Generalsekretär erteilt die schriftliche Ermächtigung nach Einholung der Stellungnahme der zuständigen Behörden der Mitgliedstaaten auf der Grundlage der gemäß den Nummern 12.8 bis 12.13 durchgeführten Sicherheitsüberprüfung.

12.5. Die für Sicherheit zuständige Direktion Sicherheit und Risikobewertung des Europäischen Parlaments führt ein fortlaufend aktualisiertes Verzeichnis aller mit der Notwendigkeit einer Sicherheitsüberprüfung verbundenen Stellen, die ihr von den einschlägigen Dienststellen des Parlaments gemeldet werden, und von allen Personen, denen eine Ermächtigung, einschließlich einer vorläufigen Ermächtigung im Sinn der Nummer 12.15, erteilt worden ist.

12.6. Die Ermächtigung gilt für eine Dauer von fünf Jahren oder für die Dauer der Aufgaben, wegen denen sie erteilt wurde, wobei der kürzere der beiden Zeiträume zugrunde gelegt wird. Sie kann gemäß dem Verfahren der Nummer 12.4 verlängert werden.

12.7. Ermächtigungen sind vom Generalsekretär zu entziehen, wenn er dies für begründet hält. Die Entscheidung über den Entzug der Ermächtigung wird dem betroffenen Beamten des Europäischen Parlaments bzw. dem für eine Fraktion tätigen sonstigen Parlamentsbediensteten mitgeteilt, der beantragen kann, vom Präsidenten gehört zu werden, bevor der Entzug wirksam wird, und der zuständigen nationalen Behörde mitgeteilt.

12.8. Die Sicherheitsüberprüfung wird unter Mitwirkung des betroffenen Beamten des Europäischen Parlaments bzw. des für eine Fraktion tätigen sonstigen Parlamentsbediensteten auf Ersuchen des Generalsekretärs vorgenommen. Die für die Überprüfung zuständige nationale Behörde ist die Behörde des Mitgliedstaats, dessen Staatsangehörigkeit die betroffene Person besitzt. Soweit dies aufgrund einzelstaatlicher Rechts- und Verwaltungsvorschriften zulässig ist, können die zuständigen nationalen Behörden Ermittlungen über Ausländer durchführen, die Zugang zu Verschlusssachen verlangen, die als CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET oder TRÈS SECRET UE/EU TOP SECRET eingestuft sind.

12.9. Der betroffene Beamte des Europäischen Parlaments bzw. der für eine Fraktion tätige sonstige Parlamentsbedienstete hat im Zuge der Sicherheitsüberprüfung ein Auskunftsformular auszufüllen.

12.10. Der Generalsekretär benennt in seinem Ersuchen an die zuständige nationale Behörde den Geheimhaltungsgrad der Verschlusssachen, zu denen der betroffene Beamte des Europäischen Parlaments bzw. der für eine Fraktion tätige sonstige Parlamentsbedienstete Zugang erhalten soll, damit die zuständige nationale Behörde das Sicherheitsüberprüfungsverfahren entsprechend durchführen und zu der der betroffenen Person zu erteilenden Ermächtigungsstufe Stellung nehmen kann.

12.11. Der gesamte Ablauf und die Ergebnisse des von der nationalen Behörde durchgeführten Verfahrens der Sicherheitsüberprüfung stehen im Einklang mit den einschlägigen Vorschriften und Regelungen des betroffenen Mitgliedstaats, einschließlich der Vorschriften und Regelungen über Rechtsbehelfe.

12.12. Bei befürwortender Stellungnahme der zuständigen nationalen Behörde kann der Generalsekretär dem betroffenen Beamten des Europäischen Parlaments bzw. dem für Fraktionen tätigen sonstigen Parlamentsbediensteten die Ermächtigung erteilen.

12.13. Eine ablehnende Stellungnahme der zuständigen nationalen Behörde wird dem betroffenen Beamten des Europäischen Parlaments bzw. dem für eine Fraktion tätigen sonstigen Parlamentsbediensteten mitgeteilt, der beantragen kann, vom Generalsekretär gehört zu werden. Der Generalsekretär kann, wenn er es für erforderlich hält, bei der zuständigen nationalen Behörde um weitere Auskünfte nachsuchen. Bei Bestätigung der ablehnenden Stellungnahme darf die Ermächtigung nicht erteilt werden.

12.14. Alle Beamten des Europäischen Parlaments und für die Fraktionen tätigen sonstigen Parlamentsbediensteten, denen eine Ermächtigung im Sinn der Nummern 12.4 und 12.5 erteilt wurde, erhalten zum Zeitpunkt der Erteilung der Ermächtigung und danach in regelmäßigen Abständen die gebotenen Anweisungen zum Schutz von Verschlusssachen und zu den Mitteln zur Sicherstellung dieses Schutzes. Diese Beamten und Bediensteten unterzeichnen eine Erklärung, mit der sie den Erhalt dieser Anweisungen bestätigen und sich zu ihrer Einhaltung verpflichten.

12.15. Ausnahmsweise kann der Generalsekretär, nachdem er die zuständige nationale Behörde hiervon unterrichtet hat und von dieser Behörde binnen eines Monats dazu nicht Stellung genommen wurde, einem Beamten des Europäischen Parlaments bzw. einem für eine Fraktion tätigen sonstigen Parlamentsbediensteten eine vorläufige Ermächtigung für höchstens sechs Monate erteilen, bis ihm das Ergebnis der Sicherheitsüberprüfung nach Nummer 12.11 vorliegt. Die so erteilten vorläufigen Ermächtigungen berechtigen nicht zum Zugang zu als TRÈS SECRET UE/EU TOP SECRET oder gleichwertig eingestuften Verschlusssachen.

ANLAGE II

EINLEITUNG

Durch diese Bestimmungen werden die Sicherheitshinweise festgelegt, die für die sichere Verarbeitung und Verwaltung vertraulicher Informationen durch das Europäische Parlament gelten und sorgen. Diese Sicherheitshinweise stellen zusammen mit den Behandlungsanweisungen das in Artikel 3 Absatz 2 dieses Beschlusses genannte Managementsystem für Informationssicherheit des Europäischen Parlaments dar.

SICHERHEITSHINWEIS 1

Die Organisation der Sicherheit im Europäischen Parlament zum Schutz vertraulicher Informationen

SICHERHEITSHINWEIS 2

Umgang mit vertraulichen Informationen

SICHERHEITSHINWEIS 3

Die Verarbeitung vertraulicher Informationen durch automatisierte Informationssysteme

SICHERHEITSHINWEIS 4

Materieller Geheimschutz

SICHERHEITSHINWEIS 5

Geheimschutz in der Wirtschaft

SICHERHEITSHINWEIS 6

Verletzung der Sicherheit, Verlust vertraulicher Informationen oder Kenntnisnahme von vertraulichen Informationen durch Unbefugte

SICHERHEITSHINWEIS 1

DIE ORGANISATION DER SICHERHEIT IM EUROPÄISCHEN PARLAMENT ZUM SCHUTZ VERTRAULICHER INFORMATIONEN

1. Für die allgemeine und kohärente Durchführung dieses Beschlusses ist der Generalsekretär zuständig.

Der Generalsekretär trifft die notwendigen Maßnahmen um sicherzustellen, dass für die Zwecke der Behandlung oder Aufbewahrung vertraulicher Informationen dieser Beschluss in den Räumlichkeiten des Parlaments durch die Mitglieder des Europäischen Parlaments, durch Beamte des Europäischen Parlaments oder sonstige für Fraktionen tätige Parlamentsbedienstete und durch Auftragnehmer angewandt wird.

2. Der Generalsekretär ist das Sicherheitsorgan. In dieser Eigenschaft ist der Generalsekretär zuständig für

2.1. die Koordinierung aller Sicherheitsfragen im Zusammenhang mit den Tätigkeiten des Parlaments mit Bezug auf den Schutz vertraulicher Informationen;

2.2. die Billigung der Einrichtung eines gesicherten Bereichs, gesicherter Leseräume und gesicherter Ausrüstung;

2.3. die Ausführung von Beschlüssen gemäß Artikel 6 dieses Beschlusses zur Genehmigung der Übermittlung von Verschlusssachen an Dritte durch das Parlament;

2.4. Ermittlungen oder die Anordnung von Ermittlungen bei unberechtigter Offenlegung vertraulicher Informationen, die dem ersten Anschein nach im Parlament erfolgt ist, in Absprache mit dem Präsidenten des Europäischen Parlaments, sofern ein Mitglied des Europäischen Parlaments betroffen ist;

2.5. die Aufrechterhaltung enger Kontakte mit den Sicherheitsorganen anderer Institutionen der Union und mit nationalen Sicherheitsbehörden in den Mitgliedstaaten im Hinblick auf die Sicherstellung einer optimalen Abstimmung der Sicherheitspolitik mit Bezug auf Verschlusssachen;

2.6. die ständige Überprüfung der Sicherheitspolitik und -verfahren des Parlaments und Erteilung angemessener Empfehlungen, die sich daraus ergeben;

2.7. die Meldung an die nationale Sicherheitsbehörde, die das Verfahren der Sicherheitsüberprüfung gemäß Anlage I Teil 2 Nummer 11.3 durchgeführt hat, in Fällen nachteiliger Informationen, die diese Behörde betreffen könnten.

3. Falls ein Mitglied des Europäischen Parlaments betroffen ist, nimmt der Generalsekretär seine Aufgaben in enger Abstimmung mit dem Präsidenten des Europäischen Parlaments wahr.

4. Bei der Wahrnehmung seiner Aufgaben nach den Absätzen 2 und 3 wird der Generalsekretär durch den stellvertretenden Generalsekretär, die Direktion Sicherheit und Risikobewertung, die Direktion Informationstechnologien (DIT) und das Referat Verschlusssachen unterstützt.

4.1. Die Direktion Sicherheit und Risikobewertung ist für persönliche Schutzmaßnahmen und insbesondere das Verfahren der Sicherheitsüberprüfung nach Anlage I Teil 2 zuständig. Die Direktion Sicherheit und Risikobewertung hat auch

a) der Kontaktpunkt für die Sicherheitsorgane der anderen Institutionen der Union und für die nationalen Sicherheitsbehörden in Angelegenheiten mit Bezug auf das Verfahren der Sicherheitsüberprüfung von Mitgliedern des Europäischen Parlaments, Beamten des Europäischen Parlaments und sonstigen für Fraktionen tätige Parlamentsbedienstete zu sein;

b) die notwendigen allgemeinen Informationsveranstaltungen zum Thema Sicherheit über die Pflichten zum Schutz von Verschlusssachen und die Konsequenzen von Verstößen dagegen durchzuführen;

c) den Betrieb des gesicherten Bereichs und der gesicherten Leseräume innerhalb der Räumlichkeiten des Parlaments gegebenenfalls in Zusammenarbeit mit den Sicherheitsdiensten der anderen Institutionen der Union und den nationalen Sicherheitsbehörden zu überwachen;

d) in Zusammenarbeit mit den Sicherheitsdiensten der anderen Institutionen der Union und den nationalen Sicherheitsbehörden die Verfahren für den Umgang mit Verschlusssachen und ihre Aufbewahrung, des gesicherten Bereichs und der gesicherten Leseräume innerhalb der Räumlichkeiten des Parlaments, wo Verschlusssachen behandelt werden, zu überprüfen;

e) dem Generalsekretär die angemessenen Behandlungsanweisungen vorzuschlagen.

4.2. Die DIT ist für die Behandlung von Verschlusssachen durch gesicherte IT-Systeme im Europäischen Parlament zuständig.

4.3. Das Referat Verschlusssachen ist für Folgendes zuständig:

a) Ermittlung des Sicherheitsbedarfs zum wirksamen Schutz vertraulicher Informationen in enger Zusammenarbeit mit der Direktion Sicherheit und Risikobewertung und der DIT sowie den Sicherheitsdiensten der anderen Institutionen der Union;

b) Ermittlung aller Aspekte des Umgangs mit vertraulichen Informationen und ihre Aufbewahrung innerhalb des Parlaments gemäß den Behandlungsanweisungen;

c) Betrieb des gesicherten Bereichs;

d) Umgang mit oder Einsichtnahme in vertrauliche(n) Informationen im gesicherten Bereich oder im Leseraum des Referats Verschlusssachen gemäß Artikel 7 Absätze 2 und 3 dieses Beschlusses;

e) Verwaltung des Registers des Referats Verschlusssachen;

f) Meldung an das Sicherheitsorgan von Verletzungen oder vermuteten Verletzungen der Sicherheit, Verlust oder Kenntnisnahme im Zusammenhang mit vertraulichen Informationen, die im Referat Verschlusssachen hinterlegt und im gesicherten Bereich oder im gesicherten Leseraum des Referats Verschlusssachen aufbewahrt werden.

5. Außerdem hat der Generalsekretär als Sicherheitsorgan die folgenden Stellen zu einzurichten:

a) eine Sicherheits-Akkreditierungsstelle (SAA);

b) eine für den Betrieb zuständige Stelle für Informationssicherung (IAOA);

c) eine Krypto-Verteilungsstelle (CDA);

d) eine TEMPEST-Stelle (TA);

e) eine Stelle für Informationssicherung (IAA).

Für die Wahrnehmung dieser Funktionen sind keine zentralen organisatorischen Einheiten erforderlich. Für die einzelnen Funktionen werden gesonderte Mandate erteilt. Diese Funktionen und die damit einhergehenden Verantwortlichkeiten können jedoch zusammengefasst oder der gleichen organisatorischen Einheit zugewiesen oder auf verschiedene organisatorische Einheiten aufgeteilt werden, sofern Interessenkonflikte und Überschneidungen von Aufgaben vermieden werden.

6. Die SAA berät in allen Sicherheitsfragen im Zusammenhang mit der Akkreditierung jedes IT-Systems und -Netzes innerhalb des Parlaments, indem sie

6.1. dafür sorgt, dass die Kommunikations- und Informationssysteme den Sicherheitskonzepten und Sicherheitsleitlinien entsprechen; hierfür erteilt sie eine Erklärung über die Zulassung für die Behandlung von Verschlusssachen bis zu einem bestimmten Geheimhaltungsgrad in dem betreffenden Betriebsumfeld durch das Kommunikations- und Informationssystem und gibt die Voraussetzungen für die Akkreditierung sowie die Kriterien an, unter denen eine erneute Zulassung erforderlich ist;

6.2. ein Verfahren für die Sicherheitsakkreditierung im Einklang mit den einschlägigen Konzepten unter genauer Angabe der Voraussetzungen für die Zulassung von Kommunikations- und Informationssystemen unter ihrer Leitung festlegt;

6.3. eine Strategie für die Sicherheitsakkreditierung entwirft, in der dargelegt wird, wie detailliert das Akkreditierungsverfahren entsprechend der geforderten Vertraulichkeit angelegt sein muss;

6.4. die sicherheitsbezogene Dokumentation — einschließlich der Erklärung zum Risikomanagement und der Erklärung zum Restrisiko, der Dokumentation über die Überprüfung der Sicherheitsimplementierung und der sicherheitsbezogenen Betriebsverfahren — prüft und zulässt sowie gewährleistet, dass sie mit den Sicherheitsvorschriften und -konzepten des Parlaments übereinstimmt;

6.5. die Implementierung der Sicherheitsmaßnahmen in Bezug auf das Kommunikations- und Informationssystem im Wege der Durchführung oder Förderung von Sicherheitsbewertungen, -kontrollen oder -überprüfungen kontrolliert;

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

6.7. die Zusammenschaltung eines bestimmten Kommunikations- und Informationssystems mit anderen Kommunikations- und Informationssystemen genehmigt — oder gegebenenfalls an der gemeinsamen Genehmigung mitwirkt;

6.8. die Sicherheitsnormen technischer Ausrüstungen genehmigt, die für die gesicherte Behandlung und den Schutz von Verschlusssachen eingesetzt werden sollen;

6.9. sicherstellt, dass kryptografische Produkte, die im Parlament benutzt werden, in die Liste der EU-weit zugelassenen Produkte aufgenommen sind;

6.10. den Systembetreiber, die Sicherheitsakteure und die Vertreter der Nutzer in Bezug auf das Sicherheitsrisikomanagement — insbesondere hinsichtlich des Restrisikos — und auf die Voraussetzungen für die Erklärung über die Zulassung konsultiert.

7. Die IAOA ist für Folgendes zuständig:

7.1. Ausarbeitung der Sicherheitsdokumentation im Einklang mit den Sicherheitskonzepten und Sicherheitsleitlinien; dies betrifft insbesondere auch die Erklärung zum Restrisiko, die sicherheitsbezogenen Betriebsverfahren und das Kryptokonzept im Rahmen des Akkreditierungsverfahrens für Kommunikations- und Informationssysteme;

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

7.3. Überwachung der Implementierung und Anwendung der sicherheitsbezogenen Betriebsverfahren und gegebenenfalls Übertragung der Verantwortung für die Betriebssicherheit an den Systemeigner, d.h. das Referat Verschlusssachen;

7.4. Umgang mit kryptografischen Produkten und ihre Handhabung, Gewährleistung der Aufbewahrung von verschlüsseltem Material und der Kontrolle unterliegendem Material sowie erforderlichenfalls Gewährleistung der Generierung kryptografischer Variablen;

7.5. Durchführung von Sicherheitsanalysen, -überprüfungen und -tests, insbesondere zum Zwecke der Erstellung der von der SAA verlangten einschlägigen Risikoberichte;

7.6. Durchführung von für das Kommunikations- und Informationssystem spezifischen Schulungen in Bezug auf Informationssicherung;

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

8. Die CDA ist für Folgendes zuständig:

8.1. Verwaltung und Rechenschaftspflicht in Bezug auf EU-Kryptomaterial;

8.2. in enger Zusammenarbeit mit der SAA Vorkehrungen dafür, dass für das gesamte EU-Kryptomaterial in Bezug auf Rechenschaftspflicht, sichere Behandlung, Speicherung und Verteilung geeignete Verfahren durchgesetzt und Pläne vorhanden sind;

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

9. Die TA hat sicherzustellen, dass die Kommunikations- und Informationssysteme den TEMPEST-Konzepten und -Behandlungsanweisungen entsprechen. Sie genehmigt TEMPEST-Schutzmaßnahmen für Installationen und Produkte, damit Verschlusssachen bis zu einem bestimmten Geheimhaltungsgrad in dem betreffenden Betriebsumfeld geschützt sind.

10. Die IAA ist für alle Aspekte des Umgangs mit vertraulichen Informationen und ihre Behandlung innerhalb des Parlaments zuständig und insbesondere für Folgendes:

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

10.2. Schutz und Verwaltung der technischen Informationen über kryptografische Produkte;

10.3. Vorkehrungen dafür, dass die für den Schutz von Verschlusssachen gewählten Informationssicherungsmaßnahmen den einschlägigen Regeln für ihre Eignung und Auswahl entsprechen;

10.4. Vorkehrungen dafür, dass die kryptografischen Produkte unter Einhaltung der Regeln für ihre Eignung und Auswahl gewählt werden;

10.5. Konsultation des Systembetreibers, der Sicherheitsverantwortlichen und der Vertreter der Nutzer in Bezug auf die Sicherheitskonzepte und Sicherheitsleitlinien für Informationssicherung;

SICHERHEITSHINWEIS 2

UMGANG MIT VERTRAULICHEN INFORMATIONEN

A. **VORBEMERKUNGEN**

1. In diesem Sicherheitshinweis werden die Bestimmungen für den Umgang des Parlaments mit vertraulichen Informationen dargelegt.

2. Wer Informationen als vertraulich einstuft, gibt ihren Geheimhaltungsgrad an und richtet sich bei seiner Entscheidung nach den in diesem Sicherheitshinweis aufgeführten Grundsätzen für die Einstufung oder Kennzeichnung vertraulicher Informationen.

B. **EINSTUFUNG ALS EU-VERSCHLUSSSACHE**

3. Die Entscheidung darüber, ob ein Dokument als Verschlusssache eingestuft wird, erfolgt vor dessen Erstellung. Als EU-Verschlusssache wird eine Information eingestuft, wenn ihr Urheber nach der Prüfung ihres Grads an Vertraulichkeit entscheidet, dass ihre unbefugte Weitergabe den Interessen der Europäischen Union oder eines oder mehrerer ihrer Mitgliedstaaten oder Bürger in bestimmtem Maße Schaden zufügen könnte.

4. Wird eine Information als Verschlusssache eingestuft, erfolgt eine zweite Prüfung im Vorfeld, bei der der geeignete Geheimhaltungsgrad festgelegt wird. Der Geheimhaltungsgrad eines Dokuments richtet sich nach der Schutzbedürftigkeit seines Inhalts.

5. Die Verantwortung für die Festlegung des Geheimhaltungsgrades einer Information liegt allein beim Urheber. Beamte des Parlaments nehmen auf Anweisung des Generalsekretärs oder in dessen Auftrag Einstufungen von Informationen vor.

6. Eine Einstufung als Verschlusssache wird korrekt vorgenommen und erfolgt nur bei wirklichem Bedarf. Der Urheber eines Dokuments, dem ein Geheimhaltungsgrad zugeordnet werden soll, muss eine zu hohe oder zu niedrige Einstufung vermeiden.

7. Der Geheimhaltungsgrad, der der Information zugewiesen wird, ist ausschlaggebend für das Schutzniveau, dem sie hinsichtlich der personen-, objekt- und verfahrensbezogenen Sicherheit und der Informationssicherung unterliegt.

8. Informationen, die einer Einstufung als Verschlusssache bedürfen, müssen ungeachtet ihrer materiellen Form als Verschlusssache gekennzeichnet und behandelt werden. Die Einstufung als Verschlusssache muss den Empfängern deutlich mitgeteilt werden, entweder durch die Kennzeichnung mit einem Geheimhaltungsgrad (falls die Information schriftlich übermittelt wird, sei es auf Papier oder über Kommunikations- und Informationssysteme) oder durch einen mündlichen Hinweis (falls die Information mündlich übermittelt wird, beispielsweise in einem Gespräch oder einer Sitzung unter Ausschluss der Öffentlichkeit). Als Verschlusssache eingestuftes Material ist materiell zu kennzeichnen, damit sein Geheimhaltungsgrad einfach zu erkennen ist.

9. Elektronische Verschlusssachen dürfen ausschließlich in einem akkreditierten Kommunikations- und Informationssystem erstellt werden. Die Verschlusssache selbst sowie der Dateiname und der Datenträger (dies gilt für externe Träger, beispielsweise CD-ROM und USB-Speicherstifte) ist mit der betreffenden Verschlusssachenkennzeichnung zu versehen.

10. Informationen werden als Verschlusssache eingestuft, sobald sie Form annehmen. Zum Beispiel müssen persönliche Notizen, Entwürfe oder E-Mails, die Informationen enthalten, die einer Einstufung als EU-Verschlusssache bedürfen, von Beginn an als Verschlusssache gekennzeichnet und gemäß den materiellen und technischen Anforderungen dieses Beschlusses erstellt und behandelt werden. Diese Informationen können dann in die Form eines offiziellen Dokuments gebracht werden, das seinerseits entsprechend gekennzeichnet und behandelt wird. Während der Abfassung eines offiziellen Dokuments kann es erforderlich sein, seine ursprüngliche Einstufung zu überprüfen und ihm entsprechend seiner weiteren Ausgestaltung einen höheren oder niedrigeren Geheimhaltungsgrad zuzuweisen.

11. Die Urheber können entscheiden, dass bestimmten Kategorien von Informationen, die sie regelmäßig erstellen, ein Standard-Geheimhaltungsgrad zugewiesen wird. Ist dies der Fall, müssen sie jedoch dafür Sorge tragen, bestimmte Informationen nicht systematisch zu hoch oder zu niedrig einzustufen.

12. Als EU-Verschlusssache eingestufte Informationen müssen immer eine Verschlusssachenkennzeichnung tragen, die dem jeweiligen Geheimhaltungsgrad entspricht.

B.1. ***Geheimhaltungsgrade***

13. EU-Verschlusssachen werden in einen der folgenden Geheimhaltungsgrade eingestuft:

— TRÈS SECRET UE/EU TOP SECRET, gemäß der Begriffsbestimmung in Artikel 2 Buchstabe d dieses Beschlusses, sofern durch ihre unbefugte Weitergabe aller Wahrscheinlichkeit nach

a) die innere Sicherheit der Union oder eines oder mehrerer ihrer Mitgliedstaaten oder die innere Sicherheit von Drittstaaten oder internationalen Organisationen unmittelbar gefährdet würde,

b) die Beziehungen zu Drittstaaten oder internationalen Organisationen außerordentlich schwerwiegend geschädigt würden,

c) unmittelbar zahlreiche Menschen ums Leben kämen,

d) die Einsatzfähigkeit oder Sicherheit von Einsatzpersonal der Mitgliedstaaten oder anderer Partner bzw. die andauernde Wirksamkeit äußerst wertvoller Sicherheitseinsätze oder Erkenntnisgewinnungsverfahren außerordentlich schwerwiegend beeinträchtigt würde, oder

e) die Wirtschaft der Union oder ihrer Mitgliedstaaten schwer und langfristig geschädigt würde,

— SECRET UE/EU SECRET, gemäß der Begriffsbestimmung in Artikel 2 Buchstabe d dieses Beschlusses, sofern durch ihre unbefugte Weitergabe aller Wahrscheinlichkeit nach

a) erhebliche internationale Spannungen entstünden,

b) Beziehungen zu Drittstaaten und internationalen Organisationen schwerwiegend geschädigt würden,

c) unmittelbar Leben gefährdet würden oder die öffentliche Ordnung oder die individuelle Sicherheit oder Freiheit schwerwiegend beeinträchtigt würde,

d) wichtige Verhandlungen über handelspolitische oder allgemein politische Fragen beeinträchtigt würden und der Union oder den Mitgliedstaaten dadurch erhebliche operationelle Probleme entstünden,

e) die operative Sicherheit der Mitgliedstaaten oder die Wirksamkeit sehr wertvoller Sicherheitseinsätze oder Erkenntnisgewinnungsverfahren schwerwiegend beeinträchtigt würde,

f) die finanziellen, monetären, wirtschaftlichen und handelspolitischen Interessen der Union oder ihrer Mitgliedstaaten erheblich materiell geschädigt würden,

g) die finanzielle Tragfähigkeit wichtiger Organisationen oder Akteure wesentlich beeinträchtigt würde, oder

h) die Ausarbeitung oder Durchführung von Strategien der Union so behindert würde, dass erhebliche wirtschaftliche, handelspolitische oder finanzielle Folgen drohen;

— CONFIDENTIEL UE/EU CONFIDENTIAL, gemäß der Begriffsbestimmung in Artikel 2 Buchstabe d dieses Beschlusses, sofern durch ihre unbefugte Weitergabe aller Wahrscheinlichkeit nach

a) die diplomatischen Beziehungen erheblichen Schaden nähmen und beispielsweise ein förmlicher Protest oder andere Sanktionen die Folge wären,

b) individuelle Sicherheit oder Freiheit gefährdet würden,

c) die Ergebnisse von Verhandlungen über handelspolitische oder allgemein politische Fragen ernsthaft gefährdet würden, die Union oder die Mitgliedstaaten vor operative Probleme gestellt würden,

d) die operative Sicherheit der Mitgliedstaaten oder die Wirksamkeit von Sicherheitseinsätzen oder Erkenntnisgewinnungsverfahren beeinträchtigt würde,

e) die finanzielle Tragfähigkeit wichtiger Organisationen oder Akteure wesentlich beeinträchtigt würde,

f) Ermittlungstätigkeiten behindert würden oder das Begehen von Straftaten oder Terrorhandlungen erleichtert würde,

g) den finanziellen, monetären, wirtschaftlichen und handelspolitischen Interessen der Union oder der Mitgliedstaaten in erheblichem Maße entgegengewirkt würde, oder

h) die Ausarbeitung oder Durchführung von Strategien der EU so behindert würde, dass erhebliche wirtschaftliche, handelspolitische oder finanzielle Folgen drohen;

— RESTREINT UE/EU RESTRICTED, gemäß der Begriffsbestimmung in Artikel 2 Buchstabe d dieses Beschlusses, sofern durch ihre unbefugte Weitergabe aller Wahrscheinlichkeit nach

a) die allgemeinen Interessen der Union beeinträchtigt würden,

b) die diplomatischen Beziehungen ungünstig beeinflusst würden,

c) Einzelpersonen erhebliche Unannehmlichkeiten erführen,

d) der Union oder den Mitgliedstaaten bei Verhandlungen über handelspolitische oder allgemein politische Fragen Nachteile erwüchsen,

e) die Aufrechterhaltung der Sicherheit in der Union oder den Mitgliedstaaten erschwert würde,

f) die Ausarbeitung oder Durchführung von Strategien der Union behindert würde,

g) die sachgerechte Verwaltung der EU und ihre Tätigkeitsbereiche beeinträchtigt würde,

h) Verpflichtungen des Parlaments gebrochen würden, nach denen von dritter Seite erteilte und als Verschlusssache eingestufte Informationen ihren Status behalten müssen,

i) gegen gesetzlich begründete Einschränkungen der Weitergabe von Informationen verstoßen würde,

j) Einzelpersonen oder Unternehmen finanzielle Verluste entstünden oder ungerechtfertigte Gewinne oder Vorteile erleichtert würden, oder

k) Ermittlungstätigkeiten behindert würden oder das Begehen von Straftaten erleichtert würde.

B.2. ***Geheimhaltungsgrad von Zusammenstellungen, Deckblättern und Auszügen***

14. Ein Begleitschreiben oder ein Übermittlungsvermerk ist so hoch einzustufen wie die am höchsten eingestufte Anlage. Der Urheber gibt klar an, welcher Geheimhaltungsgrad für das Begleitschreiben bzw. den Übermittlungsvermerk gilt, wenn ihm seine Anlagen nicht beigefügt sind. Übermittlungsvermerke bzw. Begleitschreiben, die nicht eingestuft werden müssen, enthalten folgenden Schlusssatz: „Ohne beigefügte Anlagen gilt für diesen Übermittlungsvermerk bzw. dieses Begleitschreiben kein Geheimhaltungsgrad."

15. Dokumente oder Dateien, die Teile mit unterschiedlichen Geheimhaltungsgraden umfassen, müssen möglichst so untergliedert werden, dass Teile mit unterschiedlichen Geheimhaltungsgraden leicht zu erkennen sind und gegebenenfalls abgetrennt werden können. Der Geheimhaltungsgrad des Gesamtdokuments oder der Datei entspricht mindestens dem Geheimhaltungsgrad seines/ihres am höchsten eingestuften Teils.

16 Einzelne Seiten, Absätze, Abschnitte, Anhänge oder sonstige Anlagen eines Dokuments können unterschiedliche Geheimhaltungsgrade erfordern und sind entsprechend einzustufen. In Dokumenten, die EU-Verschlusssachen enthalten, können Standardabkürzungen verwendet werden, um den Geheimhaltungsgrad von Textabschnitten oder Textteilen von weniger als einer Seite anzugeben.

17. Werden Informationen aus verschiedenen Quellen in einem Dokument zusammengestellt, so wird die endgültige Fassung durchgesehen, um den grundsätzlichen Geheimhaltungsgrad zu bestimmen, da sie einen höheren Geheimhaltungsgrad als für die einzelnen Bestandteile nötig erfordern kann.

C. **SONSTIGE VERTRAULICHE INFORMATIONEN**

18. Sonstige vertrauliche Informationen werden gemäß Abschnitt E dieses Sicherheitshinweises und den Behandlungsanweisungen gekennzeichnet.

D. **ERSTELLUNG VERTRAULICHER INFORMATIONEN**

19. Die Erstellung vertraulicher Informationen ist Personen vorbehalten, die durch diesen Beschluss oder durch das Sicherheitsorgan dazu ermächtigt werden.

20. Vertrauliche Informationen dürfen nicht in Internet- bzw. Intranet-Dokumentenverwaltungssystemen erfasst werden.

D.1. ***Erstellung von EU-Verschlusssachen***

21. Wer eine EU-Verschlusssache mit dem Geheimhaltungsgrad CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET oder TRÈS SECRET UE/EU TOP SECRET erstellen möchte, bedarf der Ermächtigung durch diesen Beschluss oder zunächst einer Genehmigung gemäß Artikel 4 Absatz 1 dieses Beschlusses.

22. EU-Verschlusssachen mit dem Geheimhaltungsgrad CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET oder TRÈS SECRET UE/EU TOP SECRET werden ausschließlich im abgesicherten Bereich erstellt.

23. Für die Erstellung einer EU-Verschlusssache gelten folgende Vorschriften:

a) Der geltende Geheimhaltungsgrad ist auf jeder Seite eindeutig zu vermerken.

b) Jede Seite ist zu nummerieren, und auf jeder Seite ist die Gesamtseitenzahl anzugeben.

c) Das Dokument ist auf der ersten Seite mit einem Aktenzeichen und einem Betreff zu versehen, der selbst keine Verschlusssache sein darf, es sei denn er ist an dem Dokument als solche gekennzeichnet.

d) Das Dokument ist auf der ersten Seite zu datieren.

e) Auf der ersten Seite von Dokumenten mit dem Geheimhaltungsgrad CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET oder TRÈS SECRET UE/EU TOP SECRET sind sämtliche Anhänge und Anlagen aufzulisten.

f) Dokumente mit dem Geheimhaltungsgrad CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET oder TRÈS SECRET UE/EU TOP SECRET sind auf jeder Seite mit einer eigenen Exemplarnummer zu versehen, sofern sie in mehreren Exemplaren verteilt werden sollen. Auf der ersten Seite jedes Exemplars ist die Gesamtzahl der Exemplare und Seiten anzugeben.

g) Wird in dem Dokument auf andere Dokumente verwiesen, die von anderen Unionsorganen erhaltene und als Verschlusssache eingestufte Informationen enthalten, oder enthält das Dokument als Verschlusssache eingestufte und aus diesen Dokumenten stammende Informationen, so ist es auf den gleichen Geheimhaltungsgrad wie diese Dokumente einzustufen und darf ohne vorherige schriftliche Zustimmung des Urhebers nicht an Personen verteilt werden, die nicht in der Verteilungsliste des Dokuments bzw. der Dokumente, aus dem bzw. denen die als Verschlusssache eingestuften Informationen stammen, aufgeführt sind.

24. Der Urheber behält die Kontrolle über die von ihm erstellte EU-Verschlusssache. Seine Zustimmung ist einzuholen, bevor die EU-Verschlusssache

a) herabgestuft oder ihr Geheimhaltungsgrad aufgehoben wird,

b) für andere als die vom Urheber festgelegten Zwecke verwandt wird,

c) an Drittstaaten oder internationale Organisationen weitergegeben wird,

d) an Personen, Institutionen, Staaten oder internationale Organisationen weitergegeben wird, die nicht zum Kreis derjenigen gehören, denen der Urheber selbst Einsicht in die Informationen gewährt hat,

e) an Auftragnehmer oder potenzielle Auftragnehmer mit Sitz in einem Drittstaat weitergegeben wird,

f) vervielfältigt oder übersetzt wird, falls es sich um Informationen mit dem Geheimhaltungsgrad TRES SECRET UE/EU TOP SECRET handelt,

g) vernichtet wird.

D.2. ***Erstellung sonstiger vertraulicher Informationen***

25. Über die Genehmigung der Erstellung sonstiger vertraulicher Informationen durch Funktionsbereiche, Dienste und/oder Einzelpersonen kann der als Sicherheitsorgan fungierende Generalsekretär entscheiden.

26. Sonstige vertrauliche Informationen werden gemäß den Behandlungsanweisungen gekennzeichnet.

27. Für die Erstellung sonstiger vertraulicher Informationen gelten folgende Vorschriften:

a) Die Kennzeichnung ist oben auf der ersten Seite des Dokuments anzubringen.

b) Jede Seite ist zu nummerieren, und auf jeder Seite ist die Gesamtseitenzahl anzugeben.

c) Das Dokument ist auf der ersten Seite mit einem Aktenzeichen und einem Betreff zu versehen.

d) Das Dokument ist auf der ersten Seite zu datieren.

e) Auf der letzten Seite des Dokuments sind sämtliche Anhänge und Anlagen aufzulisten.

28. Die Erstellung sonstiger vertraulicher Informationen erfolgt nach besonderen Vorschriften und Verfahren, die in den Behandlungsanweisungen festgelegt sind.

E. **SICHERHEITSKENNUNGEN UND KENNZEICHNUNGENSICHERHEIT**

29. Die Sicherheitskennungen und Kennzeichnungen auf Dokumenten dienen dazu, den Informationsfluss zu kontrollieren und den Zugang zu vertraulichen Informationen nach dem Grundsatz des berechtigten Informationsinteresses zu beschränken.

30. Wenn Sicherheitskennungen und/oder Kennzeichnungen verwendet oder angebracht werden, ist darauf zu achten, dass eine Verwechslung mit den Verschlusssachenkennzeichnungen für EU-Verschlussachen — RESTREINT UE/EU RESTRICTED, CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET, TRES SECRET UE/EU TOP SECRET — vermieden wird.

31. Für den Gebrauch von Sicherheitskennungen und Kennzeichnungen werden in den Behandlungsanweisungen, zusammen mit einer Liste der Sicherheitskennzeichnungen des Europäischen Parlaments, besondere Regeln festgelegt.

E.1. ***Sicherheitskennungen***

32. Sicherheitskennungen dürfen nur in Verbindung mit einer Verschlusssachenkennzeichnung verwendet werden; sie dürfen nicht separat auf Dokumenten angebracht werden. Auf EU-Verschlusssachen kann eine Sicherheitskennung angebracht werden,

a) um die Geltungsdauer eines Geheimhaltungsgrades zu begrenzen (was bei Verschlusssachen eine automatische Herabstufung des Geheimhaltungsgrades oder Freigabe bedeutet),

b) um die Verbreitung der betreffenden EU-Verschlusssache zu begrenzen,

c) um über die mit dem Geheimhaltungsgrad verbundenen Vorschriften hinaus besondere Regelungen für den Umgang mit der Verschlusssache festzulegen.

33. Die zusätzlichen Einschränkungen, die für die Handhabung und Aufbewahrung von Dokumenten mit EU-Verschlusssachen gelten, sind für die Beteiligten mit einem zusätzlichen Aufwand verbunden. Um den Arbeitsauswand in diesem Zusammenhang zu minimieren, hat es sich bewährt, bei der Erstellung solcher Dokumente eine Frist oder ein Ereignis festzulegen, nach deren Ablauf bzw. dessen Eintreten die Einstufung automatisch ungültig wird und der Geheimhaltungsgrad der im Dokument enthaltenen Informationen herabgestuft oder aufgehoben wird.

34. Wenn ein Dokument sich auf einen konkreten Arbeitsbereich bezieht und seine Verbreitung begrenzt werden muss und/oder für den Umgang mit dem Dokument besondere Regelungen gelten, kann der Einstufung eine diesbezügliche Erklärung beigefügt werden, damit der betreffende Empfängerkreis leichter zu erkennen ist.

E.2. *Kennzeichnungen*

35. Kennzeichnungen gelten nicht als Geheimhaltungseinstufung. Sie dienen lediglich als Hinweis auf konkrete Anweisungen für den Umgang mit einem Dokument und werden nicht dazu verwendet, den Inhalt des betreffenden Dokuments zu beschreiben.

36. Kennzeichnungen können separat auf Dokumenten angebracht oder in Verbindung mit einer Geheimhaltungseinstufung verwendet werden.

37. Grundsätzlich gilt, dass Kennzeichnungen bei Informationen angebracht werden, die dem Berufsgeheimnis gemäß Artikel 287 des EG-Vertrags und Artikel 17 des Beamtenstatuts unterliegen oder die aus rechtlichen Gründen durch das Parlament zu schützen sind, aber nicht als Verschlusssache behandelt werden müssen oder können.

E.3. *Gebrauch von Kennzeichnungen im Rahmen des Kommunikations- und Informationssystems*

38. Die Vorschriften für den Gebrauch von Kennzeichnungen gelten auch im Rahmen des akkreditierten Informations- und Kommunikationssystems.

39. Die SAA legt für den Gebrauch von Kennzeichnungen im Rahmen des akkreditierten Informations- und Kommunikationssystems besondere Regeln fest.

F. **EMPFANG VON INFORMATIONEN**

40. Im Parlament ist nur das Referat Verschlusssachen zum Empfang von Informationen berechtigt, die von Dritten als CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET oder TRÈS SECRET UE/EU TOP SECRET oder gleichwertig eingestuft wurden.

41. Bei Informationen, die als RESTREINT UE/EU RESTRICTED oder gleichwertig oder als sonstige vertrauliche Informationen eingestuft wurden, kann die Verantwortung für die Entgegennahme der Informationen von Dritten sowie für die Einhaltung der in diesem Sicherheitshinweis aufgeführten Grundsätze beim Referat Verschlusssachen oder aber bei dem zuständigen parlamentarischen Organ bzw. Amtsträger liegen.

G. **REGISTRIERUNG**

42. Als Registrierung wird die Anwendung der Verfahren zur Aufzeichnung des Umlaufs vertraulicher Informationen, einschließlich ihrer Verbreitung, der Einsichtnahme in die vertraulichen Informationen und deren Vernichtung, bezeichnet.

43. Für die Zwecke dieses Sicherheitshinweises ist das „Dienstbuch“ das Register, in dem vor allem Datum und Uhrzeit des Zeitpunkts erfasst werden, zu dem

a) die vertraulichen Informationen bei dem Sekretariat des betreffenden parlamentarischen Organs bzw. Amtsträgers oder gegebenenfalls beim Referat Verschlusssachen eingehen oder dieses Sekretariat bzw. Referat verlassen,

b) eine sicherheitsüberprüfte Person auf die vertraulichen Informationen zugreift oder diese weiterleitet und

c) die vertraulichen Informationen vernichtet werden.

44. Der Urheber der Verschlusssache ist im Zuge der Erstellung des Dokuments, das die Verschlusssache enthält, dafür verantwortlich, die erste Erklärung mit einer Kennzeichnung zu versehen. Diese Erklärung wird bei Erstellung des Dokuments dem Referat Verschlusssachen übermittelt.

45. Informationen, die als CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET oder TRÈS SECRET UE/EU TOP SECRET oder gleichwertig eingestuft werden, können beim Referat Verschlusssachen nur zu Sicherheitszwecken registriert werden. Informationen, die als RESTREINT UE/EU RESTRICTED oder gleichwertig eingestuft wurden, und von Dritten eingehende, als sonstige vertrauliche Informationen eingestufte Informationen werden aus verwaltungstechnischen Gründen bei der Dienststelle registriert, die für den offiziellen Empfang des Dokuments verantwortlich ist, das heißt entweder vom Referat Verschlusssachen oder von dem Sekretariat des betreffenden parlamentarischen Organs bzw. Amtsträgers. Im Parlament erstellte sonstige vertrauliche Informationen werden aus verwaltungstechnischen Gründen vom Urheber registriert.

46. Informationen, die als CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET oder TRÈS SECRET UE/EU TOP SECRET oder gleichwertig eingestuft wurden, werden insbesondere registriert

a) bei der Erstellung,

b) bei ihrem Eingang beim Referat Verschlusssachen oder beim Verlassen dieses Referats und

c) bei ihrem Eingang im Kommunikations- und Informationssystem oder beim Verlassen dieses Systems.

47. Informationen, die als RESTREINT UE/EU RESTRICTED oder gleichwertig eingestuft wurden, werden insbesondere registriert

a) bei der Erstellung,

b) bei ihrem Eingang bei dem Sekretariat des betreffenden parlamentarischen Organs bzw. Amtsträgers oder beim Referat Verschlusssachen oder beim Verlassen dieses Sekretariats bzw. Referats und

c) bei ihrem Eingang im Kommunikations- und Informationssystem oder beim Verlassen dieses Systems.

48. Die Registrierung vertraulicher Informationen kann in Papierform oder in elektronischen Dienstbüchern bzw. im Kommunikations- und Informationssystem erfolgen.

49. Für als RESTREINT UE/EU RESTRICTED oder gleichwertig eingestufte Informationen und sonstige vertrauliche Informationen sind mindestens die folgenden Angaben zu erfassen:

a) Datum und Uhrzeit des Zeitpunkts, zu dem die Informationen bei dem Sekretariat des betreffenden parlamentarischen Organs bzw. Amtsträgers oder gegebenenfalls beim Referat Verschlusssachen eingehen oder zu dem sie dieses Sekretariat bzw. Referat verlassen,

b) Titel des Dokuments, Geheimhaltungsgrad oder Kennzeichnung des Dokuments, Ablauf der Geheimhaltungsfrist bzw. der Geltungsdauer der Kennzeichnung des Dokuments sowie alle ihm zugewiesenen Nummern.

50. Für als CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET oder TRÈS SECRET UE/EU TOP SECRET oder gleichwertig eingestufte Informationen sind mindestens die folgenden Angaben zu erfassen:

a) Datum und Uhrzeit des Zeitpunkts, zu dem die Informationen beim Referat Verschlusssachen eingehen bzw. dieses Referat verlassen,

b) Titel des Dokuments, Geheimhaltungsgrad oder Kennzeichnung des Dokuments, alle ihm zugewiesenen Nummern sowie Ablauf der Geheimhaltungsfrist bzw. der Geltungsdauer der Kennzeichnung des Dokuments,

c) Detailangaben zum Urheber,

d) ein Vermerk über die Identität der Personen, denen Zugang zu dem Dokument gewährt wird, und die Zeitpunkte, zu denen von diesen Personen jeweils auf das Dokument zugegriffen wurde,

e) ein Vermerk über etwaige Kopien oder Übersetzungen des Dokuments,

f) Datum und Uhrzeit des Zeitpunkts, zu dem etwaige Kopien oder Übersetzungen des Dokuments das Referat Verschlusssachen verlassen oder dort wieder eintreffen, und Detailangaben dazu, an wen sie gesendet wurden und wer sie zurückgegeben hat,

g) Datum und Uhrzeit des Zeitpunkts, zu dem das Dokument vernichtet wird, sowie — gemäß den Sicherheitsvorschriften des Parlaments für die Vernichtung von Dokumenten — die Person, die das Dokument vernichtet hat, und

h) ein Vermerk über die Aufhebung oder Herabstufung des Geheimhaltungsgrades des Dokuments.

51. Die Dienstbücher erhalten eine angemessene Einstufung oder Kennzeichnung. Dienstbücher für Informationen, die als TRES SECRET UE/EU TOP SECRET oder gleichwertig eingestuft wurden, werden mit demselben Geheimhaltungsgrad registriert.

52. Verschlusssachen können registriert werden

a) in einem einzigen Dienstbuch oder

b) in gesonderten Dienstbüchern, in denen sie jeweils nach ihrem Geheimhaltungsgrad, aufgrund der Einstufung als eingehende oder ausgehende Informationen oder nach ihrem Herkunfts- oder Bestimmungsort erfasst werden.

53. Im Falle der elektronischen Erfassung im Rahmen eines Kommunikations- und Informationssystems (CIS) können die Registrierungsverfahren durch Prozesse im CIS selbst erfolgen, wobei diese Prozesse Vorgaben genügen müssen, die den vorstehend genannten Anforderungen gleichwertig sind. Sobald EU-Verschlusssachen das Kommunikations- und Informationssystem verlassen, findet das vorstehend beschriebene Registrierungsverfahren Anwendung.

54. Das Referat Verschlusssachen führt Aufzeichnungen über alle Verschlusssachen, die vom Parlament für Dritte freigegeben wurden, sowie über alle Verschlusssachen, die das Parlament von Dritten erhalten hat.

55. Sobald die Registrierung von als CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET oder TRÈS SECRET UE/EU TOP SECRET oder gleichwertig eingestuften Informationen abgeschlossen ist, überprüft das Referat Verschlusssachen, ob der Empfänger im Besitz einer gültigen Sicherheitsermächtigung ist. Ist das der Fall, so wird der Empfänger vom Referat Verschlusssachen entsprechend unterrichtet. Verschlusssachen dürfen erst eingesehen werden, wenn das Dokument, in dem sie enthalten sind, registriert ist.

H. **VERBREITUNG**

56. Der Urheber legt die erste Verteilungsliste für die von ihm erstellte EU-Verschlusssachen an.

57. Als RESTREINT UE/EU RESTRICTED eingestufte Informationen und sonstige vom Parlament erstellte vertrauliche Informationen werden vom Urheber gemäß den einschlägigen Behandlungsanweisungen und nach dem Grundsatz des berechtigten Informationsinteresses im Parlament verteilt. Bei Informationen, die als CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET oder TRÈS SECRET UE/EU TOP SECRET eingestuft und vom Parlament im gesicherten Bereich erstellt wurden, ist die Verteilungsliste (sowie jegliche weiteren Anweisungen für die Verbreitung der Informationen) dem Referat Verschlusssachen vorzulegen, das für die Führung dieser Liste verantwortlich ist.

58. Vom Parlament erstellte EU-Verschlusssachen dürfen nur vom Referat Verschlusssachen und nach dem Grundsatz des berechtigten Informationsinteresses an Dritte weitergegeben werden.

59. Vertrauliche Informationen, die beim Referat Verschlusssachen oder bei dem parlamentarischen Organ bzw. Amtsträger eingehen, das bzw. der den betreffenden Antrag gestellt hat, werden nach den vom Urheber erhaltenen Anweisungen verteilt.

I. **BEHANDLUNG, AUFBEWAHRUNG UND EINSICHTNAHME**

60. Für die Behandlung und Aufbewahrung vertraulicher Informationen und die Einsichtnahme in vertrauliche Informationen gelten Sicherheitshinweis 4 sowie die Behandlungsanweisungen.

J. **KOPIEREN, ÜBERSETZEN UND DOLMETSCHEN VON VERSCHLUSSSACHEN**

61. Dokumente, die als TRES SECRET UE/EU TOP SECRET oder gleichwertig eingestufte Informationen enthalten, dürfen nur mit vorheriger schriftlicher Zustimmung des Urhebers kopiert oder übersetzt werden. Dokumente, die als SECRET UE/EU SECRET oder gleichwertig oder als CONFIDENTIEL UE/EU CONFIDENTIAL oder gleichwertig eingestufte Informationen enthalten, dürfen auf Anweisung des Besitzers kopiert oder übersetzt werden, sofern der Urheber dies nicht untersagt hat.

62. Jede Kopie eines Dokuments, das als TRES SECRET UE/EU TOP SECRET, SECRET UE/EU SECRET oder CONFIDENTIEL UE/EU CONFIDENTIAL oder gleichwertig eingestufte Informationen enthält, muss zu Sicherheitszwecken registriert werden.

63. Die für das Verschlusssachen enthaltende Originaldokument geltenden Sicherheitsmaßnahmen finden auch auf Kopien und Übersetzungen dieses Dokuments Anwendung.

64. Vom Rat eingehende Dokumente sollten in allen Amtssprachen der Union eingehen.

65. Kopien und/oder Übersetzungen von Dokumenten, die Verschlusssachen enthalten, können vom Urheber oder vom Besitzer einer Kopie angefordert werden. Kopien von Dokumenten, die als CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET oder TRÈS SECRET UE/EU TOP SECRET oder gleichwertig eingestufte Informationen enthalten, dürfen nur innerhalb des gesicherten Bereichs und auf Kopiermaschinen angefertigt werden, die Teil eines akkreditierten Kommunikations- und Informationssystems sind. Kopien von Dokumenten, die als RESTREINT UE/EU RESTRICTED oder gleichwertig eingestufte Informationen oder sonstige vertrauliche Informationen enthalten, werden innerhalb der Räumlichkeiten des Parlaments mit einem akkreditierten Vervielfältigungsgerät angefertigt.

66. Kopien und Übersetzungen von Dokumenten oder von Teilen von Dokumentkopien, die vertrauliche Informationen enthalten, werden entsprechend gekennzeichnet, nummeriert und registriert.

67. Es werden grundsätzlich nur so viele Kopien angefertigt, wie unbedingt notwendig. Nach Ablauf des Zeitraums für die Einsichtnahme werden alle Kopien gemäß den Behandlungsanweisungen vernichtet.

68. Nur Dolmetscher und Übersetzer, bei denen es sich um Beamte des Parlaments handelt, dürfen Zugang zu Verschlusssachen haben.

69. Dolmetscher und Übersetzer, die Zugang zu Dokumenten mit Informationen haben, die als CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET oder TRÈS SECRET UE/EU TOP SECRET oder gleichwertig eingestuft wurden, müssen der entsprechenden Sicherheitsüberprüfung unterzogen worden sein.

70. Die Dolmetscher und Übersetzer, die Dokumente mit als CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET oder TRÈS SECRET UE/EU TOP SECRET oder gleichwertig eingestuften Informationen behandeln, müssen im gesicherten Bereich arbeiten.

K. HERABSETZUNG ODER AUFHEBUNG DER EINSTUFUNG BZW. AUFHEBUNG DER KENNZEICHNUNG ALS VERTRAULICHE INFORMATION

K.1. *Allgemeine Grundsätze*

71. Wenn eine Information nicht mehr gemäß der bisherigen Geheimhaltungsstufe oder überhaupt nicht mehr geschützt werden muss, wird die Einstufung als vertrauliche Information aufgehoben bzw. herabgesetzt oder die betreffende Kennzeichnung aufgehoben.

72. Die Entscheidung, die Einstufung von Informationen in vom Parlament erstellten Dokumenten herabzusetzen oder aufzuheben oder die betreffende Kennzeichnung aufzuheben, muss unter Umständen ad hoc getroffen werden — beispielsweise, wenn einem Antrag auf Zugang der Öffentlichkeit oder eines anderen EU-Organs oder auf Initiative des Referats Verschlusssachen oder des parlamentarischen Organs bzw. Amtsträgers stattgegeben werden soll.

73. Gleichzeitig teilen die Urheber von EU-Verschlusssachen möglichst mit, ob die betreffende EU-Verschlusssache zu einem bestimmten Zeitpunkt oder im Anschluss an ein bestimmtes Ereignis herabgestuft oder freigegeben werden kann. Wenn eine solche Auskunft nicht erteilt werden kann, wird der Geheimhaltungsgrad der EU-Verschlusssache mindestens alle fünf Jahre durch den Urheber, das Referat Verschlusssachen oder das parlamentarische Organ bzw. den Amtsträger überprüft, das bzw. der Besitzer der Information ist. In jedem Fall kann die Einstufung der EU-Verschlusssache nur mit vorheriger schriftlicher Zustimmung des Urhebers herabgesetzt oder aufgehoben werden.

74. Wenn der Urheber von EU-Verschlusssachen hinsichtlich eines im Parlament erstellten Dokuments nicht festgestellt oder ermittelt werden kann, überprüft das Sicherheitsorgan den Geheimhaltungsgrad der entsprechenden EU-Verschlusssache gestützt auf einen entsprechenden Vorschlag des parlamentarischen Organs bzw. Amtsträgers, das bzw. der Besitzer der Information ist; das Organ bzw. der Amtsträger kann das Referat Verschlusssachen in dieser Sache konsultieren.

75. Das Referat Verschlusssachen oder das parlamentarische Organ bzw. der Amtsträger, das bzw. der Besitzer der Information ist, ist dafür verantwortlich, den oder die Empfänger über die Aufhebung oder Herabsetzung der Einstufung der Information in Kenntnis zu setzen, und der oder die betreffenden Empfänger sind ihrerseits dafür verantwortlich, etwaige weitere Empfänger darüber zu informieren, denen sie das Original oder eine Kopie des Dokuments zugeleitet haben.

76. Die Aufhebung oder Herabsetzung der Einstufung oder Aufhebung der Kennzeichnung von Informationen in einem Dokument wird aufgezeichnet.

K.2. *Freigabe*

77. EU-Verschlusssachen können ganz oder in Teilen freigegeben werden. Sie können teilweise freigegeben werden, wenn der Schutz bei einem bestimmten Teil des Dokuments, das die Verschlusssache enthält, nicht länger für notwendig erachtet wird, während der Schutz in Bezug auf das übrige Dokument weiterhin als gerechtfertigt gilt.

78. Wenn im Zuge der Überprüfung einer EU-Verschlusssache, die in einem vom Parlament erstellten Dokument enthalten ist, entschieden wird, die Verschlusssache freizugeben, muss geklärt werden, ob das Dokument veröffentlicht werden kann oder ob es mit einer Verteilungskennzeichnung versehen werden soll (und also nicht veröffentlicht wird).

79. Wenn eine EU-Verschlusssache freigegeben wird, wird die Freigabe im Dienstbuch zusammen mit den folgenden Angaben erfasst: Datum der Freigabe, Name der Person, die die Freigabe beantragt hat, und der Person, die die Freigabe genehmigt hat, Nummer des freigegebenen Dokuments und dessen Endbestimmung.

80. Die alten Verschlusssachenkennzeichnungen auf dem freigegebenen Dokument und den Kopien dieses Dokuments werden durchgestrichen. Das Original und die Kopien des Dokuments werden entsprechend aufbewahrt.

81. Bei teilweiser Freigabe von Verschlusssachen ist der freigegebene Teil als Auszug anzulegen und entsprechend aufzubewahren. Die zuständige Dienststelle registriert

a) das Datum der teilweisen Freigabe,

b) den Namen der Person, die die Freigabe beantragt hat, und der Person, die die Freigabe genehmigt hat, und

c) die Nummer des freigegebenen Auszugs.

K.3. ***Herabstufung***

82. Nach der Herabstufung einer Verschlusssache wird das diese Verschlusssache enthaltende Dokument in den Dienstbüchern für den alten wie auch den neuen Geheimhaltungsgrad registriert. Zu vermerken sind das Datum der Herabstufung sowie der Name der Person, die diese genehmigt hat.

83. Das Dokument, das die herabgestuften Informationen enthält, und alle Kopien dieses Dokuments werden nach dem neuen Geheimhaltungsgrad eingestuft und entsprechend aufbewahrt.

L. **VERNICHTUNG VERTRAULICHER INFORMATIONEN**

84. Vertrauliche Informationen (als Papierfassung oder in elektronischer Form), die nicht mehr benötigt werden, sind gemäß den Behandlungsanweisungen und den einschlägigen Archivierungsvorschriften zu vernichten oder zu löschen.

85. Als TRES SECRET UE/EU TOP SECRET oder SECRET UE/EU SECRET oder gleichwertig eingestufte Informationen werden vom Referat Verschlusssachen vernichtet. Ihre Vernichtung erfolgt in Anwesenheit eines Zeugen, der mindestens der Sicherheitsüberprüfung unterzogen wurde, die dem für die vernichteten Informationen geltenden Geheimhaltungsgrad entspricht.

86. Als TRES SECRET UE/EU TOP SECRET oder gleichwertig eingestufte Informationen werden nur mit vorheriger schriftlicher Zustimmung des Urhebers vernichtet.

87. Als CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET oder TRÈS SECRET UE/EU TOP SECRET oder gleichwertig eingestufte Informationen werden auf Anweisung des Urhebers oder einer zuständigen Behörde vom Referat Verschlusssachen vernichtet und entsorgt. Die Dienstbücher und sonstigen Register werden entsprechend aktualisiert. Als RESTREINT UE/EU RESTRICTED oder gleichwertig eingestufte Informationen werden vom Referat Verschlusssachen oder von dem betreffenden parlamentarischen Organ bzw. Amtsträger vernichtet und entsorgt.

88. Der für die Vernichtung verantwortliche Beamte und die die Vernichtung bezeugende Person unterschreiben eine Vernichtungsbescheinigung, die im Referat Verschlusssachen abgelegt und archiviert wird. Das Referat Verschlusssachen bewahrt die Vernichtungsbescheinigungen bei als TRES SECRET UE/EU TOP SECRET oder gleichwertig eingestuften Informationen mindestens zehn Jahre lang und bei als SECRET UE/EU SECRET oder gleichwertig und CONFIDENTIEL UE/EU CONFIDENTIAL oder gleichwertig eingestuften Informationen mindestens fünf Jahre lang zusammen mit den Verteilungsunterlagen auf.

89. Dokumente, die Verschlusssachen enthalten, werden nach Verfahren vernichtet, die den einschlägigen EU-Normen oder gleichwertigen Normen entsprechen, damit einer vollständigen oder teilweisen Wiederherstellung vorgebeugt wird.

90. Die Vernichtung elektronischer Datenträger, die für Verschlusssachen verwendet wurden, erfolgt gemäß den entsprechenden Behandlungsanweisungen.

91. Die Vernichtung von Verschlusssachen wird in dem entsprechenden Dienstbuch zusammen mit den folgenden Angaben erfasst:

a) Datum und Uhrzeit der Vernichtung,

b) Name des für die Vernichtung zuständigen Beamten,

c) Identifizierung des vernichteten Dokuments bzw. der vernichteten Kopien,

d) ursprüngliche materielle Form der vernichteten EU-Verschlusssache,

e) Art der Vernichtung und

f) Ort der Vernichtung.

M. **ARCHIVIERUNG**

92. Verschlusssachen, auch Übermittlungsvermerke oder Begleitschreiben, Anlagen, Empfangsbestätigungen und/oder andere Teile des Dossiers, sind sechs Monate nach der letzten Einsichtnahme oder spätestens ein Jahr, nachdem sie abgelegt wurden, in das gesicherte Archiv im gesicherten Bereich zu verbringen. Die Vorschriften, die für die Archivierung von Verschlusssachen im Einzelnen gelten, werden in den Behandlungsanweisungen festgelegt.

93. Für sonstige vertrauliche Informationen gelten unbeschadet etwaiger anderer Sonderbestimmungen für den Umgang mit diesen Informationen die allgemeinen Bestimmungen für die Verwaltung von Dokumenten.

SICHERHEITSHINWEIS 3

DIE VERARBEITUNG VERTRAULICHER INFORMATIONEN DURCH AUTOMATISIERTE KOMMUNIKATIONS- UND INFORMATIONSSYSTEME

A. **INFORMATIONSSICHERUNG VON VERSCHLUSSSACHEN, DIE IN INFORMATIONSSYSTEMEN BEHANDELT WERDEN**

1. Informationssicherung (Information Assurance, IA) im Bereich von Informationssystemen beinhaltet das Vertrauen darauf, dass die in diesen Systemen behandelten Verschlusssachen geschützt sind und dass diese Systeme unter der Kontrolle rechtmäßiger Nutzer jederzeit ordnungsgemäß funktionieren. Eine effektive Informationssicherung stellt ein angemessenes Niveau der Vertraulichkeit, Integrität, Verfügbarkeit, Beweisbarkeit und Authentizität sicher. Die Informationssicherung stützt sich auf einen Risikomanagementprozess.

2. Bei einem Kommunikations- und Informationssystem für die Behandlung von Verschlusssachen handelt es sich um ein System, das die Handhabung von Verschlusssachen in elektronischer Form ermöglicht. Zu einem solchen Informationssystem gehören sämtliche für seinen Betrieb benötigten Voraussetzungen, einschließlich der Infrastruktur, der Organisation, des Personals und der Informationsressourcen.

3. Mit einem Kommunikations- und Informationssystem werden Verschlusssachen im Einklang mit dem Konzept der Informationssicherung behandelt.

4. Kommunikations- und Informationssysteme werden einem Akkreditierungsverfahren unterzogen. Mit der Akkreditierung wird bezweckt, Gewissheit darüber zu erlangen, dass alle angemessenen Sicherheitsmaßnahmen durchgeführt worden sind und dass ein ausreichender Schutz der Verschlusssachen und der Kommunikations- und Informationssysteme gemäß diesem Sicherheitshinweis erreicht wird. In der Akkreditierungserklärung wird festgelegt, bis zu welchem Geheimhaltungsgrad und unter welchen Voraussetzungen Verschlusssachen in Kommunikations- und Informationssystemen behandelt werden dürfen.

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

a) Authentizität: die Garantie, dass die Informationen echt sind und aus Bona-fide-Quellen stammen;

b) Verfügbarkeit: der Umstand, dass die Informationen auf Anfrage einer befugten Stelle verfügbar und nutzbar sind;

c) Vertraulichkeit: der Umstand, dass die Informationen nicht gegenüber unbefugten Personen, Stellen oder Verarbeitungsprozessen offengelegt werden darf;

d) Integrität: der Umstand, dass die Genauigkeit und die Vollständigkeit der Informationen und Werte gewährleistet sind;

e) Beweisbarkeit: die Möglichkeit des Nachweises, dass ein Vorgang oder ein Ereignis stattgefunden hat, um die Möglichkeit auszuschließen, dass dieser Vorgang oder dieses Ereignis nachträglich abgestritten werden kann.

B. **GRUNDSÄTZE DER INFORMATIONSSICHERUNG**

6. Die nachstehenden Bestimmungen sind Ausgangsbasis für die Sicherheit von Kommunikations- und Informationssystemen, in denen Verschlusssachen behandelt werden. Detaillierte Anforderungen zur Durchführung dieser Bestimmungen werden in Sicherheitskonzepten und Sicherheitsleitlinien für Informationssicherung festgelegt.

B.1. ***Sicherheitsrisikomanagement***

7. Sicherheitsrisikomanagement ist ein integraler Bestandteil der Konzeption, der Entwicklung, des Betriebs und der Wartung von Kommunikations- und Informationssystemen. Das Risikomanagement (Bewertung, Behandlung, Akzeptanz und Kommunikation) wird als fortlaufender Prozess gemeinsam von den in Sicherheitshinweis 1 festgelegten Vertretern der Systemeigner, den für ein Projekt zuständigen Stellen, den für den Betrieb zuständigen Stellen und den Sicherheits-Zulassungsstellen durchgeführt; dabei wird ein bewährtes, transparentes und verständliches Risikobewertungsverfahren durchgeführt. Der Umfang des Kommunikations- und Informationssystems und seine Werte müssen gleich zu Beginn des Risikomanagementprozesses klar umrissen sein.

8. Die in Sicherheitshinweis 1 festgelegten zuständigen Stellen müssen die potenziellen Bedrohungen für Kommunikations- und Informationssysteme überprüfen und über stets aktuelle und genaue Risikobewertungen entsprechend dem jeweiligen betrieblichen Umfeld verfügen. Sie halten ihre Kenntnisse über potenzielle Schwachstellen stets auf dem neuesten Stand und überprüfen regelmäßig die Bewertung der Schwachstellen, um den sich ändernden IT-Gegebenheiten Rechnung zu tragen.

9. Das Ziel bei der Sicherheitsrisikobehandlung muss darin bestehen, ein Paket von Sicherheitsmaßnahmen anzuwenden, die zu einer zufriedenstellenden Ausgewogenheit zwischen den Anforderungen der Nutzer, den Kosten und dem Sicherheitsrestrisiko führen.

10. Zur Akkreditierung eines Kommunikations- und Informationssystems gehören eine förmliche Erklärung zum Restrisiko und die Akzeptanz des Restrisikos durch eine zuständige Stelle. Die spezifischen Anforderungen, der Maßstab und Grad der Detaillierung, die von der einschlägigen SAA zur Akkreditierung eines Kommunikations- und Informationssystems festgelegt werden, müssen dem festgestellten Risiko entsprechen; dabei ist allen relevanten Faktoren Rechnung zu tragen, darunter dem Geheimhaltungsgrad der Verschlusssachen, die in dem Kommunikations- und Informationssystem behandelt werden.

B.2. ***Sicherheit während des gesamten Lebenszyklus eines Kommunikations- und Informationssystems***

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

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

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

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

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

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

B.3. ***Optimale Vorgehensweisen***

17. Die IAA entwickelt optimale Vorgehensweisen für den Schutz von Verschlusssachen, die von einem Kommunikations- und Informationssystem behandelt werden. Leitlinien zu optimalen Vorgehensweisen enthalten Sicherheitsmaßnahmen in den Bereichen Technik, materieller Geheimschutz, Organisation und Verfahren für Kommunikations- und Informationssysteme, deren Effizienz bei der Abwehr von Bedrohungen und der Behebung von Schwachstellen belegt ist.

18. Für den Schutz von Verschlusssachen, die von Kommunikations- und Informationssystemen behandelt werden, sind die Erfahrungen derjenigen Stellen, die im Bereich Informationssicherung tätig sind, heranzuziehen.

19. Die Verbreitung und anschließende Anwendung optimaler Vorgehensweisen soll dazu beitragen, dass ein gleichwertiges Sicherheitsniveau für die verschiedenen, vom Sekretariat des Parlaments betriebenen Kommunikations- und Informationssysteme erreicht wird, in denen Verschlusssachen behandelt werden.

B.4. ***Mehrschichtige Sicherheit***

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

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

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

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

d) Widerstandsfähigkeit: Sicherheitsmaßnahmen, mit denen darauf abgezielt wird, die Auswirkungen eines Angriffes auf möglichst wenige Informationen oder Werte eines Kommunikations- und Informationssystems zu begrenzen und weiteren Schaden zu verhindern, und

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

Wie streng diese Sicherheitsmaßnahmen zu sein haben, wird durch eine Risikobewertung bestimmt.

21. Die in Sicherheitshinweis 1 festgelegten zuständigen Behörden tragen dafür Sorge, dass sie auf Zwischenfälle, die die Grenzen einer Organisation überschreiten können, dahingehend reagieren können, dass sie die Reaktionen koordinieren und Informationen über diese Zwischenfälle und damit zusammenhängende Risikokonstellationen austauschen (Computer-Notfall-Reaktionsfähigkeit).

B.5. ***Minimalitätsprinzip und Prinzip der minimalen Zugriffsrechte***

22. Um unnötige Risiken zu vermeiden werden nur die für die operativen Anforderungen unbedingt notwendigen Funktionen, Geräte und Dienste implementiert.

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

B.6. ***Sensibilisierung in Bezug auf Informationssicherung***

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

a) Sicherheitslücken können Kommunikations- und Informationssystemen, in denen Verschlusssachen behandelt werden, erheblich schaden;

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

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

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

B.7. ***Evaluierung und Zulassung von IT-Sicherheitsprodukten***

26. Kommunikations- und Informationssysteme, in denen als CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET oder TRÈS SECRET UE/EU TOP SECRET oder gleichwertig eingestufte Verschlusssachen behandelt werden, werden so geschützt, dass von Informationen nicht über unbeabsichtigte elektromagnetische Abstrahlung unbefugt Kenntnis genommen werden kann („TEMPEST-Sicherheitsvorkehrungen“).

27. Wird der Schutz von Verschlusssachen mit kryptografischen Produkten sichergestellt, so sind diese Produkte von der SAA als unter die EU-weit zugelassenen kryptografischen Produkte fallend zu zertifizieren.

28. Bei der Übermittlung von Verschlusssachen auf elektronischem Wege werden EU-weit zugelassene kryptografische Produkte verwendet. Ungeachtet dieser Anforderung können in Notsituationen nach Maßgabe der Nummern 41 bis 44 spezielle Verfahren oder spezielle technische Konfigurationen angewendet werden.

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

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

31. Die SAA billigt Sicherheitsleitlinien in Bezug auf die Eignung und Zulassung von nicht-kryptografischen IT-Sicherheitsprodukten.

B.8. ***Übermittlung innerhalb abgesicherter Bereiche***

32. Wenn Verschlusssachen innerhalb abgesicherter Bereiche übermittelt werden, kann eine nicht verschlüsselte Verteilung oder eine Verschlüsselung auf einer niedrigeren Stufe unter Zugrundelegung der Ergebnisse eines Risikomanagementprozesses und vorbehaltlich der Zustimmung der SAA erfolgen.

B.9. ***Sichere Zusammenschaltung von Kommunikations- und Informationssystemen***

33. Eine Systemzusammenschaltung ist die direkte Verbindung von zwei oder mehr IT-Systemen für die gemeinsame Nutzung von Daten und anderen Informationsressourcen; die Verbindung kann unidirektional oder multidirektional sein.

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

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

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

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

c) Dienste für den Schutz von Systemübergängen werden an der Peripherie von Kommunikations- und Informationssystemen implementiert.

36. Es darf keine Zusammenschaltung zwischen einem akkreditierten Kommunikations- und Informationssystem und einem ungeschützten oder öffentlichen Netz geben, außer wenn das Kommunikations- und Informationssystem über zugelassene Dienste für den Schutz von Systemübergängen verfügt, die zu diesem Zweck zwischen dem Kommunikations- und Informationssystem und dem ungeschützten oder öffentlichen Netz installiert wurden. Die Sicherheitsmaßnahmen für eine derartige Zusammenschaltung werden von der zuständigen Stelle für Informationssicherung überprüft und von der zuständigen SAA genehmigt.

37. Wenn das ungeschützte oder öffentliche Netz lediglich als Träger verwendet wird und die Daten durch ein gemäß Nummer 27 EU-weit zertifiziertes kryptografisches Produkt verschlüsselt werden, gilt eine derartige Verbindung nicht als Zusammenschaltung.

38. Die direkte oder kaskadierte Zusammenschaltung eines Kommunikations- und Informationssystems, das für die Behandlung von Verschlusssachen des Geheimhaltungsgrads TRES SECRET UE/EU TOP SECRET oder eines gleichwertigen Geheimhaltungsgrads und Verschlusssachen des Geheimhaltungsgrads SECRET UE/EU SECRET oder eines gleichwertigen Geheimhaltungsgrads akkreditiert ist, mit einem ungeschützten oder öffentlichen Netz ist untersagt.

B.10. ***Elektronische Datenträger***

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

40. Elektronische Datenträger werden nach Maßgabe der Behandlungsanweisungen wiederverwendet, herabgestuft oder freigegeben.

B.11. ***Notsituationen***

41. In einer Notsituation wie beispielsweise drohenden oder bereits eingetretenen Krisen-, Konflikt- oder Kriegssituationen oder im Fall besonderer operativer Umstände können die nachstehend beschriebenen besonderen Verfahren angewandt werden.

42. Verschlusssachen können mit Zustimmung der zuständigen Behörde mit Hilfe kryptografischer Produkte, die für einen niedrigeren Geheimhaltungsgrad zugelassen sind, oder unverschlüsselt übermittelt werden, wenn eine Verzögerung einen Schaden verursachen würde, der deutlich größer wäre als der Schaden, der durch eine Preisgabe des als Verschlusssache eingestuften Materials entstehen würde, und wenn

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

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

43. Verschlusssachen, die unter den unter Nummer 41 erläuterten Umständen übermittelt werden, sind nicht mit Kennzeichnungen oder Angaben zu versehen, die sie von nicht als Verschlusssache eingestuften Informationen oder solchen unterscheiden, die mit einem zur Verfügung stehenden kryptografischen Produkt geschützt werden können. Die Empfänger werden auf anderem Weg unverzüglich über den Geheimhaltungsgrad unterrichtet.

44. Wird gemäß Nummer 41 oder Nummer 42 Buchstabe a vorgegangen, ist der zuständigen Behörde und dem Sicherheitsausschuss anschließend Bericht zu erstatten.

SICHERHEITSHINWEIS 4

MATERIELLER GEHEIMSCHUTZ

A. **EINLEITUNG**

Dieser Sicherheitshinweis legt die Sicherheitsgrundsätze für die Schaffung eines sicheren Umfelds für die Gewährleistung der korrekten Behandlung vertraulicher Informationen im Europäischen Parlament fest. Diese Grundsätze, einschließlich derjenigen, die sich auf die technische Sicherheit beziehen, werden durch die Behandlungsanweisungen ergänzt.

B. **SICHERHEITSRISIKOMANAGEMENT**

1. Risiken für Verschlusssachen sind als Verfahren zu behandeln. Dieses Verfahren zielt auf die Bestimmung bekannter Sicherheitsrisiken, auf die Festlegung von Sicherheitsmaßnahmen zur Verringerung solcher Risiken auf ein hinnehmbares Niveau in Übereinstimmung mit den Grundprinzipien und Mindeststandards dieses Sicherheitshinweises und auf die Anwendung dieser Maßnahmen entsprechend dem Konzept der mehrschichtigen Sicherheit gemäß Sicherheitshinweis 3. Die Wirksamkeit solcher Maßnahmen wird fortlaufend bewertet.

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

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

4. In Kontinuitätsplänen sind Präventions- und Wiederherstellungsmaßnahmen vorzusehen, damit die Auswirkungen größerer Störungen oder Zwischenfälle auf die Behandlung und Aufbewahrung von Verschlusssachen so gering wie möglich gehalten werden.

C. **ALLGEMEINE GRUNDSÄTZE**

5. Der Geheimhaltungsgrad oder die Kennzeichnung die den Informationen zugewiesen werden, sind ausschlaggebend für das Schutzniveau, dem sie hinsichtlich des materiellen Geheimschutzes unterliegen.

6. Informationen, die einer Einstufung als Verschlusssache bedürfen, müssen ungeachtet ihrer materiellen Form als Verschlusssache gekennzeichnet und behandelt werden. Die Einstufung als Verschlusssache muss den Empfängern deutlich mitgeteilt werden, entweder durch die Kennzeichnung mit einem Geheimhaltungsgrad (falls die Information schriftlich übermittelt wird, sei es auf Papier oder über Informations- und Kommunikationssysteme) oder durch einen mündlichen Hinweis (falls die Information mündlich übermittelt wird, beispielsweise in einem Gespräch oder einem Vortrag). Als Verschlusssache eingestuftes Material ist materiell zu kennzeichnen, damit sein Geheimhaltungsgrad einfach zu erkennen ist.

7. Vertrauliche Informationen dürfen unter keinen Umständen in der Öffentlichkeit gelesen werden, wo sie von einer Person ohne die Einstufung „Kenntnis notwendig“ eingesehen werden könnten, etwa in Zügen, Flugzeugen, Cafés, Bars u. ä. Sie sind nicht in Hotelsafes oder -räumen zu lassen bzw. dürfen in der Öffentlichkeit nicht unbeaufsichtigt gelassen werden.

D. **ZUSTÄNDIGKEITEN**

8. Das Referat Verschlusssachen ist für die Gewährleistung des materiellen Geheimschutzes bei der Verwaltung vertraulicher Informationen, die in seinen gesicherten Einrichtungen hinterlegt sind, zuständig. Das Referat Verschlusssachen ist auch für die Verwaltung seiner gesicherten Einrichtungen zuständig.

9. Der materielle Geheimschutz bei der Verwaltung von Informationen, die als RESTREINT UE/EU RESTRICTED oder gleichwertig eingestuft wurden, und von „sonstigen vertraulichen Informationen" liegt in der Zuständigkeit des jeweiligen parlamentarischen Organs bzw. Amtsträgers.

10. Die Direktion Sicherheit und Risikobewertung ist für den persönlichen Geheimschutz und die Sicherheitsüberprüfung, die für die Gewährleistung der sicheren Behandlung vertraulicher Information im Europäischen Parlament notwendig ist, zuständig.

11. Die Direktion für Informationstechnologien (DIT) berät mit der Zielstellung und trägt dafür Sorge, dass alle erstellten oder verwendeten Kommunikations- und Informationssysteme vollständig dem Sicherheitshinweis 3 und den entsprechenden Behandlungsanweisungen entsprechen.

E. **GESICHERTE EINRICHTUNGEN**

12. Gesicherte Einrichtungen können nach den technischen Sicherheitsstandards und entsprechend dem Niveau, der der vertraulichen Information gemäß Artikel 7 zugewiesen wird, eingerichtet werden.

13. Die gesicherten Einrichtungen werden von der Sicherheits-Akkreditierungsstelle (SAA) zertifiziert und von dem Sicherheitsorgan (SA) validiert.

F. **EINSICHTNAHME IN VERTRAULICHE INFORMATIONEN**

14. Ist eine als RESTREINT UE/EU RESTRICTED oder gleichwertig oder als „sonstige vertrauliche Information" eingestufte Information im Referat Verschlusssachen hinterlegt, in die außerhalb des gesicherten Bereichs Einsicht genommen werden muss, übermittelt das Referat Verschlusssachen eine Kopie an die entsprechende befugte Dienststelle, die dafür sorgt, dass die Einsichtnahme und Behandlung der jeweiligen Information mit Artikel 8 Absatz 2 und Artikel 10 dieses Beschlusses und den entsprechenden Behandlungsanweisungen vereinbar ist.

15. Ist eine als RESTREINT UE/EU RESTRICTED oder gleichwertig oder als „sonstige vertrauliche Information" eingestufte Information in einem parlamentarischen Organ bzw. bei einem Amtsträger außerhalb des Referats Verschlusssachen hinterlegt, sorgt das Sekretariat dieses parlamentarischen Organs bzw. Amtsträgers dafür, dass die Einsichtnahme und Behandlung der jeweiligen Information mit Artikel 7 Absatz 3, Artikel 8 Absätze 1, 2 und 4, Artikel 9 Absatz 3, 4 und 5, Artikel 10 Absätze 2 bis 6 und Artikel 11 dieses Beschlusses und den entsprechenden Behandlungsanweisungen vereinbar ist.

16. Muss in eine als CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET oder TRÈS SECRET UE/EU TOP SECRET oder gleichwertig eingestufte Information im gesicherten Bereich Einsicht genommen werden, sorgt das Referat Verschlusssachen dafür, dass die Einsichtnahme und Behandlung der jeweiligen Information mit Artikel 9 und Artikel 10 dieses Beschlusses und den entsprechenden Behandlungsanweisungen vereinbar ist.

G. **TECHNISCHER GEHEIMSCHUTZ**

17. Für den technischen Geheimschutz ist die Sicherheits-Akkreditierungsstelle (SAA) zuständig, die in den entsprechenden Behandlungsanweisungen die anzuwendenden spezifischen technischen Sicherheitsmaßnahmen festlegt.

18. Gesicherte Leseräume für die Einsichtnahme in Informationen, die als RESTREINT UE/EU RESTRICTED oder gleichwertig oder als „sonstige vertrauliche Information" eingestuft sind, müssen den spezifischen technischen Sicherheitsmaßnahmen der Behandlungsanweisungen entsprechen.

19. Der gesicherte Bereich umfasst die folgenden Einrichtungen:

a) einen Raum für die Zugangs-Sicherheitsüberprüfung (SAS), der den in den Behandlungsanweisungen festgelegten technischen Sicherheitsmaßnahmen entsprechend einzurichten ist. Der Zugang zu dieser Einrichtung wird registriert. Der Raum für die Zugangs-Sicherheitsüberprüfung entspricht hohen Standards in Bezug auf die Identifizierung von Personen, die Zugang haben, die Videoaufzeichnung und den sicheren Ort für das Hinterlegen von persönlichen Gegenständen, die nicht in den gesicherten Räumen erlaubt sind (Telefone, Stifte usw.);

b) ein Gesprächszimmer für die Übermittlung und den Empfang von Verschlusssachen, einschließlich verschlüsselten Verschlusssachen entsprechend Sicherheitshinweis 3 und den entsprechenden Behandlungsanweisungen.

c) ein gesichertes Archiv, in dem zugelassene oder zertifizierte Behälter gesondert für Informationen, die als RESTREINT UE/EU RESTRICTED, als CONFIDENTIEL UE/EU CONFIDENTIAL und/oder als SECRET EU/EU SECRET oder gleichwertig eingestuft wurden, verwendet werden. Informationen, die als TRES SECRET UE/EU TOP SECRET oder gleichwertig eingestuft wurden, befinden sich in einem getrennten Raum in einem speziell zertifizierten Behälter. Das einzig zusätzliche Material, das in diesem Raum verfügbar ist, ist ein Tisch zur Unterstützung für den Umgang mit dem Archiv durch das Referat Verschlusssachen.

d) einen Registrierungsraum, in dem die benötigten Instrumente bereitgestellt werden, damit die Registrierung auf Papier oder elektronisch durchgeführt werden kann und daher mit den gesicherten Einrichtungen auszustatten ist, die benötigt werden, um die entsprechenden Kommunikations- und Informationssysteme einzurichten. Zugelassene und akkreditierte Vervielfältigungsgeräte (zur Erstellung von Kopien in Papier oder elektronischer Form) dürfen sich nur im Registrierungsraum befinden. Die Behandlungsanweisungen legen fest, welche Vervielfältigungsgeräte zugelassen und akkreditiert werden. Im Registrierungsraum werden auch die benötigten Räumlichkeiten bereitgestellt, damit akkreditiertes Material aufbewahrt und behandelt werden kann, um das Kennzeichnen, Kopieren und Verschicken der Verschlusssachen in materieller Form je nach Geheimhaltungsgrad zu ermöglichen. Das gesamte akkreditierte Material wird vom Referat Verschlusssachen definiert und durch die Sicherheits-Akkreditierungsstelle entsprechend der Beratung durch die für den Betrieb zuständige Stelle für Informationssicherung (IAOA) akkreditiert. Der Registrierungsraum ist gemäß der Beschreibung in den Behandlungsanweisungen auch mit den akkreditierten Vernichtungsgeräten, die für den höchsten Geheimhaltungsgrad zugelassen sind, ausgestattet. Die Übersetzung der Verschlusssachen mit dem Geheimhaltungsgrad CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET oder TRÈS SECRET UE/EU TOP SECRET oder gleichwertig erfolgt im Registrierungsraum, in dem entsprechenden und akkreditierten System. Der Registrierungsraum verfügt über Arbeitsplätze für bis zu zwei Übersetzer gleichzeitig für das gleiche Dokument. Ein Angehöriger des Personals des Referats Verschlusssachen ist anwesend.

e) einen Leseraum zur individuellen Einsichtnahme in Verschlusssachen durch entsprechend befugte Personen. Der Leseraum soll bietet genügend Platz für zwei Personen, einschließlich eines Angehörigen des Personals des Referats Verschlusssachen, der während der gesamten Dauer jeder Einsichtnahme anwesend ist. Der Geheimhaltungsgrad dieses Raumes ist der Einsichtnahme von als CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET oder TRÈS SECRET UE/EU TOP SECRET oder gleichwertig eingestuften Informationen angemessen. Der Leseraum kann mit TEMPEST-Instrumenten ausgerüstet sein, um gegebenenfalls je nach Geheimhaltungsgrad der betreffenden Information die elektronische Einsichtnahme zu ermöglichen.

f) ein Sitzungsraum, in dem bis zu 25 Personen Platz finden, um die als CONFIDENTIEL UE/EU CONFIDENTIAL und SECRET EU/EU SECRET oder gleichwertig eingestuften Verschlusssachen zu besprechen. Der Sitzungsraum ist mit den notwendigen technischen gesicherten und zertifizierten Einrichtungen für das Dolmetschen nach und aus bis zu zwei Sprachen ausgestattet. Wird der Sitzungsraum nicht für Sitzungen benötigt, kann er auch als zusätzlicher Leseraum für individuelle Einsichtnahmen genutzt werden. In Ausnahmefällen kann das Referat Verschlusssachen mehr als einer befugten Person gestatten, in Verschlusssachen Einsicht zu nehmen, solange die Sicherheitsüberprüfung und die Einstufung „Kenntnis notwendig" für alle Personen im Raum die gleiche ist. Nicht mehr als vier Personen wird die gleichzeitige Einsichtnahme in Verschlusssachen gestattet. Die Anwesenheit der Beamten des Referats Verschlusssachen wird verstärkt.

g) technisch gesicherte Räume für die gesamte technische Ausrüstung, die mit dem Geheimschutz im gesamten gesicherten Bereich und den gesicherten IT-Servern verbunden ist.

20. Der gesicherte Bereich entspricht den anwendbaren internationalen Geheimschutzstandards und wird von der Direktion Sicherheit und Risikobewertung zertifiziert. Der gesicherte Bereich verfügt über die folgende Mindestausrüstung hinsichtlich des technischen Geheimschutzes:

a) Alarm- und Überwachungssysteme;

b) Sicherheitsvorrichtungen und Notfallsysteme (Zwei-Wege-Warnsystem);

c) Videoüberwachungssystem;

d) Einbruchsmeldeanlage;

e) Zugangskontrolle (einschließlich biometrischer Sicherheitssysteme);

f) Behälter;

g) Schließfächer;

h) Antielektromagnetischer Schutz.

21. Soweit zusätzliche technische Geheimschutzmaßnahmen notwendig sind, können diese von der Sicherheits-Akkreditierungsstelle (SAA) in enger Zusammenarbeit mit dem Referat Verschlusssachen und mit der Zustimmung des Sicherheitsorgans (SA) hinzugefügt werden.

22. Die Infrastrukturausrüstungen können mit den allgemeinen Verwaltungssystemen des Gebäudes, in dem der gesicherte Bereich liegt, verbunden werden. Die Sicherheitsausrüstung, die der Zugangskontrolle und den Kommunikations- und Informationssystemen dient, ist jedoch unabhängig von allen anderen derartigen bestehenden Systemen im Europäischen Parlament.

H. **INPEKTIONEN DES GESICHERTEN BEREICHS**

23. Inspektionen des gesicherten Bereichs werden auf Antrag des Referats Verschlusssachen regelmäßig von der Sicherheits-Akkreditierungsstelle (SAA) durchgeführt.

24. Die Sicherheits-Akkreditierungsstelle erstellt eine Prüfliste für Sicherheitsinspektionen mit den entsprechend der Behandlungsanweisungen während der Inspektion zu prüfenden Gegenständen und aktualisiert diese Liste.

I. **TRANSPORT VERTRAULICHER INFORMATIONEN**

25. Beim Transport werden vertrauliche Informationen blickgeschützt und geben keinen Hinweis auf die Vertraulichkeit des Inhalts, entsprechend den Behandlungsanweisungen transportiert.

26. Nur Boten oder Bedienstete mit der entsprechender Einstufung der Geheimschutzbefugnis können Informationen, die als CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET oder TRÈS SECRET UE/EU TOP SECRET oder gleichwertig eingestuft sind, transportieren.

27. Vertrauliche Informationen dürfen nur entsprechend der Bedingungen der Behandlungsanweisungen in Form von externem Schriftverkehr oder als Handgepäck außerhalb eines Gebäudes versandt werden.

28. Informationen, die als CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET oder TRÈS SECRET UE/EU TOP SECRET oder gleichwertig eingestuft sind, werden in keinem Fall mit E-Mail oder Fax versandt, selbst wenn ein „sicheres" E-Mail-System oder ein verschlüsseltes Fax-Gerät vorhanden ist. Informationen, die als RESTREINT UE/EU RESTRICTED oder gleichwertig eingestuft sind, und sonstige vertrauliche Informationen können unter Verwendung eines akkreditierten Verschlüsselungssystems mit E-Mail versandt werden.

J. **AUFBEWAHRUNG VERTRAULICHER INFORMATIONEN**

29. Der Geheimhaltungsgrad oder die Kennzeichnung der vertraulichen Information bestimmt das ihr zugewiesene Geheimschutzniveau in Bezug auf ihre Aufbewahrung. Sie wird in der für diesen Zweck zertifizierten Ausrüstung entsprechend der Behandlungsanweisungen aufbewahrt.

30. Informationen, die als RESTREINT UE/EU RESTRICTED oder gleichwertig eingestuft wurden und „sonstige vertrauliche Informationen" werden:

a) in einem verschlossenen Stahlschrank nach Standardausrüstung aufbewahrt, entweder in einem Büro oder in einem Arbeitsbereich, wenn sie aktuell nicht verwendet werden;

b) nicht unbeaufsichtigt gelassen, es sei denn, sie sind ordnungsgemäß weggeschlossen und aufbewahrt;

c) nicht auf einem Schreibtisch, Tisch usw. gelassen, so dass eine unbefugte Person, z. B. Besucher, Reinigungspersonal, Wartungspersonal usw. diese lesen oder entfernen können;

d) unbefugten Personen weder gezeigt noch mit ihnen darüber gesprochen.

31. Informationen, die als RESTREINT UE/EU RESTRICTED oder gleichwertig eingestuft sind und „sonstige vertrauliche Informationen" werden nur innerhalb des Sekretariats des parlamentarischen Organs bzw. Amtsträgers oder im Referat Verschlusssachen nach Maßgabe der Behandlungsanweisungen aufbewahrt.

32. Informationen, die als CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET oder TRÈS SECRET UE/EU TOP SECRET oder gleichwertig eingestuft wurden, werden:

a) im gesicherten Bereich, in einem Sicherheitsbehälter oder in einem Tresorraum aufbewahrt. In Ausnahmefällen, etwa wenn das Referat Verschlusssachen geschlossen ist, können sie in einem zugelassenen und zertifizierten Tresorfach innerhalb der Sicherheitsdienste aufbewahrt werden;

b) werden zu keiner Zeit im gesicherten Bereich unbeaufsichtigt gelassen, solange sie nicht in einem zugelassenen Tresor weggeschlossen werden (selbst bei kürzesten Abwesenheiten);

c) nicht auf einem Schreibtisch, Tisch usw. gelassen, so dass eine unbefugte Person diese lesen oder entfernen können, selbst wenn das verantwortliche Mitglied des Personals des Referats Verschlusssachen im Raum bleibt.

Wird ein Dokument, das Verschlusssachen enthält, in elektronischer Form im gesicherten Bereich erstellt, wird der Computer gesichert und der Bildschirm unzugänglich gemacht, wenn der Urheber oder das verantwortliche Mitglied des Personals des Referats Verschlusssachen den Raum verlässt (selbst bei kürzesten Abwesenheiten). Eine automatische Sicherheitsverriegelung, die nach einigen Minuten erfolgt, ist nicht als ausreichende Sicherheitsmaßnahme zu betrachten.

SICHERHEITSHINWEIS 5

GEHEIMSCHUTZ IN DER WIRTSCHAFT

A. **EINLEITUNG**

1. Dieser Sicherheitshinweis betrifft nur Verschlusssachen.

2. Er enthält Bestimmungen über die Umsetzung der in Teil 1 von Anlage I dieses Beschlusses geregelten gemeinsamen Mindeststandards.

3. Der „Geheimschutz in der Wirtschaft" beinhaltet die Anwendung von Maßnahmen, die darauf abzielen, den Schutz von Verschlusssachen durch Auftragnehmer oder Subauftragnehmer während der Verhandlungen vor der Auftragsvergabe und während der gesamten Laufzeit eines als Verschlusssache eingestuften Auftrags zu gewährleisten. Solche Aufträge beinhalten nicht den Zugang zu als TRÈS SECRET UE/EU TOP SECRET eingestuften Verschlusssachen.

4. Das Europäische Parlament stellt als Vergabebehörde sicher, dass die in diesem Beschluss festgelegten und in dem Auftrag genannten Mindeststandards für den Geheimschutz in der Wirtschaft eingehalten werden, wenn als Verschlusssache eingestufte Aufträge von ihm an industrielle oder andere Unternehmen vergeben werden.

B. **SICHERHEITSBESTIMMUNGEN BEI ALS VERSCHLUSSSACHE EINGESTUFTEN AUFTRÄGEN**

B.1. ***Einstufungsliste für Verschlusssachen***

5. Vor der Ausschreibung oder der Vergabe eines als Verschlusssache eingestuften Auftrags bestimmt das Europäische Parlament als Vergabebehörde den Geheimhaltungsgrad für Informationen, die Bietern oder Auftragnehmern zur Verfügung gestellt werden, sowie den Geheimhaltungsgrad für Informationen, die vom Auftragnehmer herauszugeben sind. Zu diesem Zweck erstellt es eine Einstufungsliste für Verschlusssachen (VS-Einstufungsliste), die bei der Erfüllung des Vertrags heranzuziehen ist.

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

a) bei der Erstellung einer VS-Einstufungsliste berücksichtigt das Europäische Parlament alle relevanten Sicherheitsaspekte, unter anderem den Geheimhaltungsgrad, den der Urheber der Information, deren Nutzung für den Auftrag er gebilligt hat, dieser zugewiesen hat;

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

B.2. ***Geheimschutzklausel***

7. Die vertragsspezifischen Sicherheitsanforderungen werden in einer Geheimschutzklausel festgelegt. Die Geheimschutzklausel enthält gegebenenfalls die VS-Einstufungsliste und ist fester Bestandteil eines als Verschlusssache eingestuften Auftrags oder Subauftrags.

8. Die Geheimschutzklausel enthält die Bestimmungen, mit denen der Auftragnehmer und/oder Subauftragnehmer verpflichtet wird, die Mindeststandards dieses Beschlusses einzuhalten. Die Nichteinhaltung dieser Mindeststandards kann einen ausreichenden Grund für die Kündigung des Auftrags darstellen.

B.3. ***Sicherheitsanweisungen für ein Programm/Projekt***

9. Abhängig vom Umfang von Programmen oder Projekten, die mit dem Zugang zu oder dem Umgang mit oder der Aufbewahrung von EU-VS verbunden sind, kann eine spezifische Sicherheitsanweisung für ein Programm/Projekt (Programme/Project Security Instructions, PSI) von der mit der Verwaltung des betreffenden Programms oder Projekts beauftragten Vergabebehörde ausgearbeitet werden.

C. **SICHERHEITSBESCHEID FÜR UNTERNEHMEN**

10. Ein Sicherheitsbescheid für Unternehmen wird von der Nationalen Sicherheitsbehörde oder einem sonstigen zuständigen Sicherheitsorgan eines Mitgliedstaats ausgestellt und gibt gemäß den innerstaatlichen Rechtsvorschriften Auskunft darüber, dass ein industrielles oder anderes Unternehmen in der Lage ist, EU-Verschlusssachen bis zu dem Geheimhaltungsgrad CONFIDENTIEL UE/EU CONFIDENTIAL oder SECRET UE/EU SECRET oder gleichwertig in seinen Anlagen zu schützen. Ein Nachweis der Ausstellung des Sicherheitsbescheids ist dem Europäischen Parlament als der Vergabebehörde vorzulegen, bevor einem Auftragnehmer oder Subauftragnehmer bzw. einem möglichen Auftragnehmer oder Subauftragnehmer EU-Verschlusssachen zur Verfügung gestellt werden können oder ihm Zugang zu diesen gewährt werden kann.

11. Ein Sicherheitsbescheid

a) bewertet die Integrität des industriellen oder anderen Unternehmens;

b) bewertet die Eigentums- und Kontrollverhältnisse und/oder die Möglichkeit einer unzulässigen Einflussnahme unter dem Aspekt eines eventuellen Sicherheitsrisikos;

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

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

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

12. Das Europäische Parlament als Vergabebehörde teilt der zuständigen Nationalen Sicherheitsbehörde oder einem sonstigen zuständigen Sicherheitsorgan gegebenenfalls mit, dass ein Sicherheitsbescheid für Unternehmen in der Phase vor der Auftragsvergabe oder für die Ausführung des Auftrags erforderlich ist. Ein Sicherheitsbescheid für Unternehmen oder eine Sicherheitsermächtigung ist in der Phase vor der Auftragsvergabe erforderlich, wenn als CONFIDENTIEL UE/EU CONFIDENTIAL oder SECRET UE/EU SECRET eingestufte Informationen während des Bietverfahrens zur Verfügung gestellt werden müssen.

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

14. Jede zuständige Sicherheitsbehörde, die einen Sicherheitsbescheid erteilt hat, teilt dem Europäischen Parlament als Vergabebehörde alle Änderungen mit, die diesen Sicherheitsbescheid betreffen. Bei Subaufträgen ist die zuständige Sicherheitsbehörde entsprechend zu informieren.

15. Die Aufhebung eines Sicherheitsbescheids für Unternehmen durch die jeweilige Nationale Sicherheitsbehörde oder das sonst zuständige Sicherheitsorgan stellt für das Europäische Parlament als Vergabebehörde einen ausreichenden Grund dar, den als Verschlusssache eingestuften Auftrag zu kündigen oder einen Bieter vom Vergabeverfahren auszuschließen.

D. **ALS VERSCHLUSSSACHE EINGESTUFTE AUFTRÄGE UND SUBAUFTRÄGE**

16. Werden Verschlusssachen einem möglichen Bieter in der Phase vor der Auftragsvergabe zur Verfügung gestellt, so enthält die Aufforderung zur Angebotsabgabe eine Klausel, wonach ein jeder, der kein Angebot abgibt oder der nicht ausgewählt wird, verpflichtet ist, alle als Verschlusssache eingestuften Dokumente innerhalb einer vorgegebenen Frist zurückzugeben.

17. Sobald der Zuschlag für einen als Verschlusssache eingestuften Auftrag oder Subauftrag erteilt wurde, teilt das Europäische Parlament als Vergabebehörde der Nationalen Sicherheitsbehörde des Auftragnehmers oder Subauftragnehmers und/oder einem sonstigen zuständigen Sicherheitsorgan die Sicherheitsvorschriften für den als Verschlusssache eingestuften Auftrag mit.

18. Bei Kündigung eines derartigen Auftrags informiert das Europäische Parlament als Vergabebehörde (und/oder gegebenenfalls die zuständige Sicherheitsbehörde bei Subaufträgen) unverzüglich die Nationale Sicherheitsbehörde oder ein sonstiges zuständiges Sicherheitsorgan des Mitgliedstaats, in dem der Auftragnehmer oder Subauftragnehmer eingetragen ist.

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

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

21. Wird dem Auftragnehmer oder Subauftragnehmer gestattet, Verschlusssachen nach der Kündigung eines Auftrags zu behalten, so gelten die in diesem Beschluss niedergelegten Mindeststandards weiterhin und die Geheimhaltung von EU-Verschlusssachen muss von dem Auftragnehmer oder Subauftragnehmer geschützt werden.

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

23. Der Auftragnehmer holt die Erlaubnis des Europäischen Parlaments als Vergabebehörde ein, bevor er für Teile eines als Verschlusssache eingestuften Auftrags Subaufträge vergibt. Subaufträge können nicht an industrielle oder andere Unternehmen vergeben werden, die in einem Drittstaat eingetragen sind, der mit der Union kein Geheimschutzabkommen geschlossen hat.

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

25. Für Verschlusssachen, die von einem Auftragnehmer oder Subauftragnehmer herausgegeben oder behandelt werden, werden die dem Urheber zugewiesenen Rechte von der Vergabebehörde ausgeübt.

E. **BESUCHE IM ZUSAMMENHANG MIT ALS VERSCHLUSSSACHE EINGESTUFTEN AUFTRÄGEN**

26. Benötigen das Europäische Parlament, die Auftragnehmer oder die Subauftragnehmer zur Ausführung eines als Verschlusssache eingestuften Auftrags Zugang zu als CONFIDENTIEL UE/EU CONFIDENTIAL oder SECRET UE/EU SECRET eingestuften Informationen in den Räumlichkeiten des jeweils anderen, werden im Benehmen mit der jeweiligen Nationalen Sicherheitsbehörde oder einem sonstigen zuständigen Sicherheitsorgan Besuche vereinbart. Im Zusammenhang mit speziellen Projekten können die Nationalen Sicherheitsbehörden jedoch auch ein Verfahren vereinbaren, nach dem Besuche unmittelbar verabredet werden können.

27. Alle Besucher müssen über eine entsprechende Sicherheitsermächtigung verfügen und im Hinblick auf den Zugang zu Verschlusssachen in Verbindung mit dem Auftrag des Europäischen Parlaments ein „berechtigtes Informationsinteresse“ haben.

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

F. **ÜBERMITTLUNG UND BEFÖRDERUNG VON VERSCHLUSSSACHEN**

29. Für die Übermittlung von Verschlusssachen auf elektronischem Wege gelten die einschlägigen Bestimmungen des Sicherheitshinweises 3.

30. Für die Beförderung von Verschlusssachen gelten die einschlägigen Bestimmungen des Sicherheitshinweises 4 und die einschlägigen Behandlungsanweisungen.

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

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

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

c) die Transportunternehmen benötigen einen Sicherheitsbescheid für Unternehmen des entsprechenden Geheimhaltungsgrads. In solchen Fällen müssen die für die Abwicklung der Versendung sorgenden Personen eine Sicherheitsüberprüfung gemäß Anlage I durchlaufen haben;

d) vor jeder grenzüberschreitenden Verbringung von als CONFIDENTIEL UE/EU CONFIDENTIAL oder SECRET UE/EU SECRET oder gleichwertig eingestuftem Material stellt der Absender einen Transportplan auf, der vom Generalsekretär zu genehmigen ist;

e) die Beförderung erfolgt soweit irgend möglich direkt von einem bestimmten Ausgangspunkt zu einem bestimmten Zielpunkt und wird so rasch abgeschlossen, wie es die Umstände erlauben;

f) die Transportrouten führen soweit irgend möglich durch das Territorium von Mitgliedstaaten.

G. **WEITERGABE VON VERSCHLUSSSACHEN AN AUFTRAGNEHMER IN DRITTSTAATEN**

32. Verschlusssachen werden an Auftragnehmer und Subauftragnehmer in Drittstaaten nach Maßgabe der Geheimschutzmaßnahmen weitergegeben, die zwischen dem Europäischen Parlament als Vergabebehörde und dem betreffenden Drittstaat, in dem der Auftragnehmer eingetragen ist, vereinbart wurden.

H. **UMGANG MIT UND AUFBEWAHRUNG VON ALS „RESTREINT UE/EU RESTRICTED“ EINGESTUFTEN INFORMATIONEN**

33. Gegebenenfalls im Benehmen mit der Nationalen Sicherheitsbehörde des betreffenden Mitgliedstaats ist das Europäische Parlament als Vergabebehörde berechtigt, Besuche in den Anlagen von Auftragnehmern/Subauftragnehmern auf der Grundlage vertraglicher Bestimmungen durchzuführen, um zu überprüfen, dass die nach dem Vertrag erforderlichen einschlägigen Sicherheitsmaßnahmen zum Schutz von EU-VS des Geheimhaltungsgrads RESTREINT UE/EU RESTRICTED getroffen wurden.

34. Soweit dies nach den innerstaatlichen Rechtsvorschriften erforderlich ist, werden die Nationalen Sicherheitsbehörden oder sonstige zuständige Sicherheitsorgane vom Europäischen Parlament als Vergabebehörde über Aufträge oder Subaufträge, die als RESTREINT UE/EU RESTRICTED eingestufte Informationen enthalten, unterrichtet.

35. Bei vom Europäischen Parlament vergebenen Aufträgen mit Informationen, die als RESTREINT UE/EU RESTRICTED eingestuft wurden, ist ein Sicherheitsbescheid für Unternehmen oder eine Sicherheitsermächtigung für Auftragnehmer und Subauftragnehmer und deren Personal nicht erforderlich.

36. Das Europäische Parlament als Vergabebehörde prüft die Antworten auf Ausschreibungen bei Aufträgen, die Zugang zu Informationen erfordern, die als RESTREINT UE/EU RESTRICTED eingestuft wurden, ungeachtet etwaiger Anforderungen in Bezug auf Sicherheitsbescheide für Unternehmen oder Sicherheitsermächtigungen, die nach Maßgabe der innerstaatlichen Rechtsvorschriften gegebenenfalls bestehen.

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

38. Ist mit einem Auftrag der Umgang mit als RESTREINT UE/EU RESTRICTED eingestuften Informationen in einem Kommunikations- und Informationssystem verbunden, das vom Auftragnehmer betrieben wird, so stellt das Europäische Parlament als Vergabebehörde sicher, dass in dem Auftrag und etwaigen Subaufträgen die notwendigen technischen und organisatorischen Anforderungen in Bezug auf die Akkreditierung des Kommunikations- und Informationssystems angegeben werden, die dem festgestellten Risiko entsprechen, wobei allen relevanten Faktoren Rechnung zu tragen ist. Der Umfang der Akkreditierung eines solchen Kommunikations- und Informationssystems ist von der Vergabebehörde mit der betreffenden Nationalen Sicherheitsbehörde/Beauftragten Sicherheitsbehörde zu vereinbaren.

SICHERHEITSHINWEIS 6

VERLETZUNG DER SICHERHEIT, VERLUST VERTRAULICHER INFORMATIONEN ODER KENNTNISNAHME VON VERTRAULICHEN INFORMATIONEN DURCH UNBEFUGTE

1. Eine Verletzung der Sicherheit liegt vor, wenn durch eine Handlung oder eine Unterlassung, die diesem Beschluss zuwiderläuft, vertrauliche Informationen in Gefahr geraten oder Unbefugten zur Kenntnis gelangen könnten.

2. Eine Kenntnisnahme von vertraulichen Informationen durch Unbefugte liegt vor, wenn diese ganz oder teilweise in die Hände unbefugter Personen, d. h. von Personen, die nicht die erforderliche Zugangsermächtigung bzw. kein berechtigtes Informationsinteresse haben, gelangt ist oder es wahrscheinlich ist, dass eine derartige Kenntnisnahme stattgefunden hat.

3. Die Kenntnisnahme von vertraulichen Informationen durch Unbefugte kann die Folge von Nachlässigkeit, Fahrlässigkeit oder Indiskretion, aber auch der Tätigkeit von Diensten, die in der Union Kenntnis davon erlangen wollen, oder von subversiven Organisationen sein.

4. Wenn der Generalsekretär eine nachweisliche oder vermutete Verletzung der Sicherheit bzw. den Verlust oder die Kenntnisnahme von vertraulichen Informationen durch Unbefugte entdeckt oder hiervon unterrichtet wird,

a) klärt er den Sachverhalt;

b) bewertet er den entstandenen Schaden und hält ihn möglichst gering;

c) ergreift er Maßnahmen, damit ein solcher Vorfall sich nicht wiederholt;

d) benachrichtigt er die zuständige Behörde des Drittstaates oder des Mitgliedstaates, aus dem die vertraulichen Informationen stammen bzw. der sie weitergeleitet hat.

Betrifft der Vorfall ein Mitglied des Europäischen Parlaments, so wird der Generalsekretär gemeinsam mit dem Präsidenten des Europäischen Parlaments tätig.

Gehen die Informationen von einem anderen Unionsorgan ein, handelt der Generalsekretär in Einklang mit den geeigneten Sicherheitsmaßnahmen für Verschlusssachen und den in der Rahmenvereinbarung mit der Kommission bzw. der Interinstitutionellen Vereinbarung mit dem Rat festgelegten Vorkehrungen.

5. Alle Personen, die mit vertraulichen Informationen umgehen müssen, werden eingehend über Sicherheitsverfahren, die Gefährdung durch indiskrete Gespräche sowie ihre Beziehungen zu den Medien unterrichtet und unterzeichnen gegebenenfalls eine Erklärung, dass sie den Inhalt vertraulicher Informationen nicht an Dritte weitergeben werden, dass sie die Verpflichtungen zum Schutz von Verschlusssachen einhalten und sich der Folgen jeglicher Zuwiderhandlung bewusst sind. Haben Personen, die nicht entsprechend unterrichtet wurden und die entsprechende Erklärung nicht unterzeichnet haben, Zugang zu Verschlusssachen oder nutzen diese Verschlusssachen, so gilt dies als Verletzung der Sicherheit.

6. Alle Mitglieder des Europäischen Parlaments, Beamte des Parlaments und sonstige für Fraktionen oder Auftragnehmer tätige Parlamentsbedienstete melden dem Generalsekretär unverzüglich alle Verletzungen der Sicherheit sowie jeglichen Verlust vertraulicher Informationen oder jegliche Kenntnisnahme von vertraulichen Informationen durch Unbefugte, von denen sie Kenntnis erlangen.

7. Gegen jede für die Kenntnisnahme von vertraulichen Informationen durch Unbefugte verantwortliche Person werden disziplinarische Maßnahmen aufgrund der geltenden Vorschriften und Regelungen ergriffen. Diese Maßnahmen lassen ein etwaiges gerichtliches Vorgehen nach geltendem Recht unberührt.

8. Unbeschadet eines weiteren gerichtlichen Vorgehens finden bei von Beamten des Parlaments und sonstigen für Fraktionen tätigen Parlamentsbediensteten begangenen Verstößen die in Titel VI des Beamtenstatuts festgelegten Verfahren und Sanktionen Anwendung.

9. Unbeschadet eines weiteren gerichtlichen Vorgehens wird bei von Mitgliedern des Europäischen Parlaments begangenen Verstößen nach Artikel 9 Absatz 2 sowie Artikel 152, 153 und 154 der Geschäftsordnung des Parlaments verfahren.