



Beschluss Nr. 041-2021 des Rechnungshofs über die Sicherheitsvorschriften für den Schutz von EU-Verschlussachen (EU-VS)

DER RECHNUNGSHOF DER EUROPÄISCHEN UNION —

- GESTÜTZT AUF Artikel 13 des Vertrags über die Europäische Union,
- GESTÜTZT AUF Artikel 287 des Vertrags über die Arbeitsweise der Europäischen Union,
- GESTÜTZT AUF Artikel 257 der Verordnung (EU, Euratom) 2018/1046 des Europäischen Parlaments und des Rates vom 18. Juli 2018 über die Haushaltsordnung für den Gesamthaushaltsplan der Union,
- GESTÜTZT AUF Artikel 1 Absatz 6 der Durchführungsbestimmungen zur Geschäftsordnung des Rechnungshofs (Beschluss Nr. 21-2021 des Rechnungshofs),
- GESTÜTZT AUF die Sicherheitsvorschriften für den Schutz von EU-Verschlussachen der anderen Organe, Agenturen und Einrichtungen der EU,
- GESTÜTZT AUF die Informationssicherheitspolitik des Rechnungshofs (DEC 127/15 FINAL) und die Politik zur Einstufung von Informationen (Personalmitteilung 123/2020),
- IN DER ERWÄGUNG, dass der Rechnungshof gemäß Artikel 287 Absatz 3 AEUV das Recht auf Zugang zu allen relevanten Dokumenten und Informationen, einschließlich zu EU-Verschlussachen (EU-VS), hat, die seiner Ansicht nach für die Ausführung seines Auftrags erforderlich sind, der unter uneingeschränkter Wahrung des Grundsatzes der loyalen Zusammenarbeit zwischen den Organen und des Grundsatzes der begrenzten Einzelermächtigung auszuführen ist; dass das durch den AEUV garantierte Recht auf Zugang zu EU-VS vom Herausgeber der EU-VS nicht in Frage gestellt werden kann, der Rechnungshof jedoch aufgefordert werden kann, bestimmte Sicherheitsmaßnahmen zu ergreifen und einzuhalten, wie im Folgenden näher ausgeführt wird;
- IN DER ERWÄGUNG, dass die Mitglieder des Rechnungshofs sowie seine Beamten und sonstigen Bediensteten auch nach ihrem Ausscheiden aus dem Dienst gemäß Artikel 339 AEUV, Artikel 17 des Statuts und den diesbezüglich erlassenen Rechtsakten zur Vertraulichkeit verpflichtet sind;
- IN DER ERWÄGUNG, dass die Bearbeitung der EU-VS in Anbetracht ihres sensiblen Charakters erfordert, dass die Einhaltung der Vertraulichkeitsverpflichtung durch geeignete Sicherheitsmaßnahmen sichergestellt wird, die ein hohes Schutzniveau für diese Informationen gewährleisten können und die denjenigen gleichwertig sind, die in den von den anderen Organen, Agenturen und Einrichtungen der EU erlassenen Vorschriften für den Schutz von EU-VS festgelegt sind, wobei sich der Rechnungshof für den Fall, dass er der Auffassung ist, dass derartige Sicherheitsmaßnahmen in Anbetracht der Art

und des Typs der EU-VS nicht gerechtfertigt sind, das Recht vorbehält, unter Beachtung des Geheimhaltungsgrades der EU-VS alle ihm angemessen erscheinenden Bemerkungen vorzubringen;

IN DER ERWÄGUNG, dass die Sicherheitsmaßnahmen für den Schutz der Vertraulichkeit, Integrität und Verfügbarkeit der an den Rechnungshof übermittelten Informationen für die Art und den Typ der betreffenden Informationen angemessen sein müssen;

IN DER ERWÄGUNG, dass der Zugang zu Verschlussachen dem Rechnungshof nach dem Grundsatz "Kenntnis nur, wenn nötig" gewährt werden muss, damit er die Aufgaben, die ihm durch die Verträge und die auf der Grundlage der Verträge erlassenen Rechtsakte übertragen wurden, wahrnehmen kann;

IN DER ERWÄGUNG, dass es angesichts der Art und des sensiblen Inhalts bestimmter Informationen angezeigt ist, ein besonderes Verfahren für die Bearbeitung von Dokumenten, die EU-VS enthalten, durch den Rechnungshof festzulegen;

IN DER ERWÄGUNG, dass das Organ sicherstellen muss, dass dieser Beschluss im Einklang mit allen geltenden Vorschriften umgesetzt wird, insbesondere mit den Bestimmungen über den Schutz personenbezogener Daten, die physische Sicherheit von Personen, Gebäuden und IT sowie den Zugang der Öffentlichkeit zu Dokumenten —

HAT FOLGENDEN BESCHLUSS ERLASSEN:

Artikel 1 Gegenstand und Anwendungsbereich

- 1) Dieser Beschluss legt die Grundprinzipien und die Mindestsicherheitsstandards für den Schutz von Verschlussachen fest, die der Rechnungshof in Ausübung seines Auftrags bearbeitet.
- 2) Im Sinne dieses Beschlusses bezeichnet der Ausdruck "Verschlussachen" eine oder alle der folgenden Arten von Informationen:
 - a) "EU-Verschlussachen" (EU-VS) gemäß der Begriffsbestimmung in den Sicherheitsvorschriften der anderen Organe, Agenturen, Einrichtungen oder Ämter der EU, die mit einem der folgenden Geheimhaltungsgrade gekennzeichnet sind:
 - TRÈS SECRET UE/EU TOP SECRET: Informationen und Materialien, deren unbefugte Weitergabe den wesentlichen Interessen der Europäischen Union oder eines oder mehrerer Mitgliedstaaten äußerst schweren Schaden zufügen könnte;
 - SECRET UE/EU SECRET: Informationen und Materialien, deren unbefugte Weitergabe den wesentlichen Interessen der Europäischen Union oder eines oder mehrerer Mitgliedstaaten schweren Schaden zufügen könnte;
 - CONFIDENTIEL UE/EU CONFIDENTIAL: Informationen und Materialien, deren unbefugte Weitergabe den wesentlichen Interessen der Europäischen Union oder eines oder mehrerer Mitgliedstaaten Schaden zufügen könnte;
 - RESTREINT UE/EU RESTRICTED: Informationen und Materialien, deren unbefugte Weitergabe für die wesentlichen Interessen der Europäischen Union oder eines oder mehrerer Mitgliedstaaten nachteilig sein könnte.

- b) Verschlussachen, die von den Mitgliedstaaten zur Verfügung gestellt werden und die mit einem nationalen Geheimhaltungsgrad gekennzeichnet sind, der einer unter Buchstabe a aufgeführten Kennzeichnung des Geheimhaltungsgrades für EU-VS¹ entspricht;
- c) Verschlussachen, die gemäß den jeweiligen Geheimschutzabkommen oder Verwaltungsvereinbarungen dem Europäischen Rechnungshof von Drittstaaten oder internationalen Organisationen zur Verfügung gestellt werden und mit einem nationalen Geheimhaltungsgrad gekennzeichnet sind, der einer unter Buchstabe a aufgeführten Kennzeichnung des Geheimhaltungsgrades für EU-VS entspricht.
- 3) Der Rechnungshof bearbeitet als "RESTREINT UE/EU RESTRICTED" eingestufte Informationen in seinen Räumlichkeiten und ergreift zu diesem Zweck alle erforderlichen Schutzmaßnahmen. Es werden Vereinbarungen getroffen, damit das Personal des Rechnungshofs, das Zugang zu EU-VS höherer Geheimhaltungsgrade benötigt, diesen Zugang in geeigneten Räumlichkeiten anderer Organe, Einrichtungen oder Agenturen der EU erhält.
- 4) Dieser Beschluss findet auf alle Dienststellen und Räumlichkeiten des Rechnungshofs Anwendung.
- 5) Sofern eine Bestimmung nicht bestimmte Gruppen von Mitarbeitern betrifft, gilt dieser Beschluss für die Mitglieder des Rechnungshofs, die Bediensteten des Rechnungshofs, die dem Personalstatut und den Beschäftigungsbedingungen für die sonstigen Bediensteten der Europäischen Union unterliegen², die zum Rechnungshof abgeordneten nationalen Sachverständigen (ANS), die Dienstleister und ihr Personal, die Praktikanten sowie alle Personen, die Zugang zu den Gebäuden und sonstigen Objekten des Rechnungshofs oder zu den vom Rechnungshof verwalteten Informationen haben.
- 6) Sofern nichts anderes bestimmt ist, gelten die Bestimmungen über EU-VS in gleicher Weise für die in Absatz 2 Buchstaben b und c des vorliegenden Artikels genannten Verschlussachen.

Artikel 2 **Begriffsbestimmungen**

Für die Zwecke dieses Beschlusses gelten folgende Begriffsbestimmungen:

- a) "Ermächtigung für den Zugang zu EU-VS": Entscheidung des Direktors für Personal, Finanzen und Allgemeine Dienste des Rechnungshofs auf der Grundlage der von einer zuständigen Behörde eines Mitgliedstaats getroffenen Feststellung, dass einem Beamten des Rechnungshofs, einem sonstigen Bediensteten oder einem abgeordneten nationalen Sachverständigen bis zu einem bestimmten Zeitpunkt und bis zu einem bestimmten Geheimhaltungsgrad ("CONFIDENTIEL UE/EU CONFIDENTIAL" oder höher) Zugang zu EU-VS gewährt werden kann, sofern die betreffende Person nachweislich Kenntnis von Verschlussachen haben muss und sie über ihre Verantwortlichkeiten angemessen belehrt worden ist; diese Person wird als "sicherheitsermächtigt" bezeichnet.

¹ Siehe Übereinkommen zwischen den im Rat vereinigten Mitgliedstaaten der Europäischen Union über den Schutz von Verschlussachen, die im Interesse der Europäischen Union ausgetauscht werden, vom 4. Mai 2011 und dessen Anhang ([ABl. 2011/C 202/13](#)).

² Verordnung Nr. 31 (EWG) zur Festlegung des Statuts der Beamten und der Beschäftigungsbedingungen für die sonstigen Bediensteten in ihrer geänderten Fassung, ABl. 01962R0031-01.01.2020-019.003-1 ([https://eur-lex.europa.eu/eli/reg/1962/31\(1\)/2020-01-01](https://eur-lex.europa.eu/eli/reg/1962/31(1)/2020-01-01)).

- b) "Einstufung": die Zuweisung eines Geheimhaltungsgrades zu Informationen auf der Grundlage des Grades des Schadens, der durch ihre unbefugte Weitergabe verursacht werden könnte;
- c) "kryptografisches Material": kryptografische Algorithmen, kryptografische Hardware- und Softwaremodule und Produkte, die Implementierungsdetails enthalten, und die dazugehörige Dokumentation sowie das Verschlüsselungsmaterial;
- d) "Aufhebung des Geheimhaltungsgrades": Löschung jeder Geheimhaltungskennzeichnung;
- e) "Dokument": jede aufgezeichnete Information, unabhängig von ihrer materiellen Form oder ihren Merkmalen;
- f) "Herabstufung": Einstufung in einen niedrigeren Geheimhaltungsgrad;
- g) "Sicherheitsbescheid für Unternehmen" (Facility Security Clearance, FSC): verwaltungsrechtliche Feststellung durch eine zuständige Sicherheitsstelle, dass ein Unternehmen unter dem Gesichtspunkt der Sicherheit ein angemessenes Schutzniveau für EU-VS bis zu einem bestimmten Geheimhaltungsgrad bieten kann;
- h) "Bearbeitung" von EU-VS: alle möglichen Handlungen, denen EU-VS während ihres gesamten Lebenszyklus unterliegen können. Sie umfasst die Erstellung, Registrierung, Verarbeitung, Beförderung, Herabstufung, Freigabe und Vernichtung. In Bezug auf Kommunikations- und Informationssysteme umfasst sie ferner die Sammlung, Darstellung, Übermittlung und Speicherung;
- i) "Besitzer": ordnungsgemäß ermächtigte Person, die nachweislich Kenntnis von Verschlussachen haben muss und die im Besitz einer EU-VS ist und dementsprechend für deren Schutz verantwortlich zeichnet;
- j) "Informationssicherheitsstelle": der Informationssicherheitsbeauftragte des Rechnungshofs, der die in diesem Beschluss vorgesehenen Aufgaben ganz oder teilweise übertragen kann;
- k) "Information": jede Information in schriftlicher oder mündlicher Form, unabhängig vom Trägermedium und davon, von wem sie stammt;
- l) "Material": Medien, Datenträger, Geräte oder Ausrüstungsgegenstände jeder Art;
- m) "Herausgeber": ein Organ, eine Einrichtung oder eine Agentur der EU, ein Mitgliedstaat, ein Drittstaat oder eine internationale Organisation, unter dessen/deren Aufsicht die Informationen erstellt und/oder in Strukturen der EU eingebracht wurden;
- n) "Erklärung über die Sicherheitsüberprüfung von Personal" (Personnel Security Clearance, PSC): Erklärung einer zuständigen Behörde eines Mitgliedstaats, die nach Abschluss einer Sicherheitsüberprüfung durch die zuständigen Behörden eines Mitgliedstaats abgegeben und mit der bescheinigt wird, dass einer Person, die nachweislich Kenntnis von Verschlussachen haben muss und die über ihre Verantwortlichkeiten angemessen belehrt worden ist, bis zu einem bestimmten Datum und bis zu einem bestimmten Geheimhaltungsgrad ("CONFIDENTIEL UE/EU CONFIDENTIAL" oder höher) Zugang zu EU-VS gewährt werden kann;
- o) "Sicherheitsüberprüfungsbescheinigung" (Personnel Security Clearance Certificate, PSCC): vom Direktor für Personal, Finanzen und Allgemeine Dienste des Rechnungshofs ausgestellte Bescheinigung, in der festgestellt wird, dass eine Person sicherheitsüberprüft ist oder eine gültige Sicherheitsermächtigung besitzt, aus der der Geheimhaltungsgrad ("CONFIDENTIEL UE/EU CONFIDENTIAL" oder höher), bis zu dem der Person Zugang zu EU-VS gewährt werden kann, das Gültigkeitsdatum der betreffenden Sicherheitsüberprüfung oder -ermächtigung und das Ablaufdatum der Bescheinigung selbst hervorgehen;

- p) "Sicherheitsstelle für den materiellen Geheimschutz": Leiter der Dienststelle "Sicherheit" des Rechnungshofs, der für die Durchführung der erforderlichen materiellen Geheimschutzmaßnahmen und -verfahren zum Schutz der EU-VS verantwortlich ist;
- q) Die "Erfassungsstelle" wird vom Sekretariat des Rechnungshofs verwaltet und ist in einem Verwaltungsbereich unter der Verantwortung des Direktors für Personal, Finanzen und Allgemeine Dienste des Rechnungshofs angesiedelt. Sie ist für den Ein- und Ausgang der als "RESTREINT UE/EU RESTRICTED" eingestuft oder diesem Geheimhaltungsgrad entsprechenden Informationen, die mit dem Rechnungshof ausgetauscht werden, zuständig.
- r) Die "Registratur für EU-VS" ist ein Bereich, der innerhalb eines besonders geschützten Bereichs eingerichtet wird. Diese Registratur wird von dem sicherheitsüberprüften und ermächtigten Registraturkontrollbeauftragten des Rechnungshofs geleitet. Sie ist für den Ein- und Ausgang der als "CONFIDENTIEL UE/EU CONFIDENTIAL" eingestuft oder diesem Geheimhaltungsgrad entsprechenden Informationen, die mit dem Rechnungshof ausgetauscht werden, zuständig.
- s) "Sicherheitsakkreditierungsstelle": der Direktor für Personal, Finanzen und Allgemeine Dienste des Rechnungshofs.

Artikel 3 Maßnahmen für den Schutz von EU-VS

- 1) Der Rechnungshof gewährleistet den Schutz aller ihm zur Verfügung gestellten Verschlussachen in einer Weise, die dem vom Herausgeber festgelegten Geheimhaltungsgrad entspricht und im Einklang mit diesem Beschluss steht.
- 2) Zu diesem Zweck unterwirft der Rechnungshof die Bearbeitung von EU-VS materiellen und gegebenenfalls personellen Geheimschutzmaßnahmen, einschließlich Zugangsermächtigungen für die benannten Personen, sowie Maßnahmen für den Schutz der Kommunikations- und Informationssysteme. Diese Maßnahmen sind in den Artikeln 4 bis 6 beschrieben und gelten für den gesamten Lebenszyklus der EU-VS. Sie müssen dem Geheimhaltungsgrad der EU-VS, der Form und dem Umfang der Informationen oder des Materials, dem Standort und der Beschaffenheit der Einrichtungen, in denen die EU-VS aufbewahrt werden, sowie der örtlichen Einschätzung der Bedrohung durch böswillige und/oder kriminelle Handlungen, einschließlich Spionage, Sabotage und Terrorismus, entsprechen.
- 3) EU-VS sind durch materielle Geheimschutzmaßnahmen zu schützen, und Informationen, die als "CONFIDENTIEL UE/EU CONFIDENTIAL" oder höher eingestuft sind, müssen zusätzlich durch personelle Geheimschutzmaßnahmen geschützt werden.
- 4) EU-VS dürfen nur an Personen weitergegeben werden, die innerhalb des Organs Kenntnis von ihnen haben müssen. Der Besitzer einer EU-Verschlussache muss diese gemäß den Forderungen in diesem Beschluss schützen.
- 5) EU-VS dürfen weder mündlich noch schriftlich weitergegeben werden. Vorläufige Bemerkungen, Berichte, Stellungnahmen, Pressemitteilungen und andere Produkte des Rechnungshofs, seine Website und sein Intranet, mündliche Beiträge, Antworten auf Anträge auf Zugang zu Dokumenten³ und Sprach- oder Videoaufzeichnungen dürfen keine EU-VS oder Auszüge daraus enthalten oder auf sie verweisen. Hat der Herausgeber jedoch Dokumente

³ Gemäß dem Beschluss Nr. 12-2005 des Rechnungshofs über den Zugang der Öffentlichkeit zu den Dokumenten des Hofes, geändert durch den Beschluss Nr. 14-2009 ([ABl. 2009/C 67/1](#)).

oder Informationen veröffentlicht, die einen Verweis auf EU-VS enthalten, kann dieser Verweis erwähnt werden.

- 6) Ungeachtet des Absatzes 5 können der Rechnungshof und der Herausgeber vereinbaren, dass der Rechnungshof im Fall einer speziellen Prüfung Elemente der EU-VS in einem Dokument reproduzieren oder verwenden darf. In diesem Fall ist das entsprechende Dokument des Rechnungshofs vor oder während des kontradiktorischen Verfahrens zunächst an den Herausgeber der betreffenden EU-VS zu richten. Der Rechnungshof und der Herausgeber einigen sich in dieser Situation darauf, ob das vom Rechnungshof ausgestellte Dokument als Verschlussache eingestuft werden soll. Hält es ein berichtendes Mitglied des Rechnungshofs für erforderlich, einen ganz oder teilweise als Verschlussache eingestuften Prüfungsbericht – unter Berücksichtigung aller mit dem vorliegenden Beschluss verbundenen Sicherheitsmaßnahmen – an bestimmte Adressaten im Europäischen Parlament oder im Rat zu übermitteln, bedarf dies der Zustimmung des Herausgebers der Verschlussache. Der Rechtsrahmen und das Verfahren für den Austausch solcher Dokumente ist in Artikel 7 festgelegt.
- 7) Ist es für die Ausübung des Auftrags des Rechnungshofs notwendig, dass bestimmte Elemente eines als Verschlussache eingestuften Dokuments oder einer als Verschlussache eingestuften Information in größerem Umfang weitergegeben werden, konsultiert der Rechnungshof unter gebührender Berücksichtigung des Geheimhaltungsgrades, mit dem das Dokument oder die Information gekennzeichnet ist, den Herausgeber, bevor der Rechnungshof beschließt, diese Elemente oder Informationen zu verwenden, wenn der Rechnungshof der Auffassung ist, dass ein überwiegendes öffentliches Interesse daran besteht. Die Informationen dürfen in dem Bericht nur so verwendet werden, dass die Interessen des Herausgebers nicht beeinträchtigt werden. Dies lässt sich entsprechend sicherstellen, indem der Herausgeber um Stellungnahme gebeten wird, damit eine Einigung über die Art und Weise der Anonymisierung, Verkürzung oder Verallgemeinerung der Informationen usw. erzielt wird und gleichzeitig die Interessen derjenigen gewahrt werden, die in erster Linie von den veröffentlichten Informationen betroffen sind.
- 8) Der Rechnungshof darf EU-VS nur nach vorheriger Konsultation und ausdrücklicher schriftlicher Zustimmung des Herausgebers an ein anderes Organ, eine Agentur, eine Einrichtung oder ein Amt der EU, einen Mitgliedstaat, einen Drittstaat oder eine internationale Organisation weitergeben.
- 9) Sofern der Herausgeber eines als "SECRET UE / EU SECRET" oder niedriger eingestuften Dokuments keine Beschränkungen für dessen Vervielfältigung oder Übersetzung auferlegt hat, können solche Dokumente auf Ersuchen des Besitzers und unter Einhaltung der praktischen Arbeitsanweisungen der Informationssicherheitsstelle beim Rechnungshof vervielfältigt oder übersetzt werden. Die für das Originaldokument geltenden Geheimschutzmaßnahmen finden auch auf Kopien und Übersetzungen dieses Dokuments Anwendung.
- 10) Ist es für den Rechnungshof erforderlich, dass der Geheimhaltungsgrad eines als Verschlussache eingestuften Dokuments, das er erhalten oder zu dem er Zugang erhalten hat, herabgestuft oder aufgehoben wird, nimmt der Rechnungshof mit dem Herausgeber Rücksprache, ob dieser eine herabgestufte Fassung des Dokuments oder eine Fassung ohne Geheimhaltungsgrad bereitstellen kann.

Artikel 4 Personeller Geheimschutz

- 1) Die Mitglieder des Rechnungshofs sind aufgrund ihrer Tätigkeit ermächtigt, Zugang zu allen EU-VS zu haben und an Sitzungen teilzunehmen, in denen EU-VS behandelt werden. Die Mitglieder werden über ihre Sicherheitspflichten im Hinblick auf den Schutz der EU-VS

- unterrichtet und erkennen ihre Verantwortung für den Schutz dieser Informationen schriftlich an.
- 2) Den Mitarbeitern des Rechnungshofs, unabhängig davon, ob es sich um einen Beamten, einen Bediensteten, der den Beschäftigungsbedingungen für die sonstigen Bediensteten der Europäischen Union unterliegt, oder einen ANS handelt, darf der Zugang zu EU-VS nur gewährt, wenn
 - i. festgestellt wurde, dass sie Kenntnis von Verschlussachen haben müssen;
 - ii. sie über die Sicherheitsvorschriften für den Schutz der EU-VS und die einschlägigen Sicherheitsnormen und -leitlinien unterrichtet wurden und ihre Verantwortung für den Schutz solcher Informationen schriftlich anerkannt haben und
 - iii. sie im Fall von "CONFIDENTIEL UE/EU CONFIDENTIAL" oder höher eingestuft Informationen sicherheitsüberprüft und zum Zugang ermächtigt sind.
 - 3) Das Verfahren, mit dem ermittelt wird, ob ein Beamter oder sonstiger Bediensteter des Rechnungshofs unter Berücksichtigung seiner Loyalität, Integrität und Zuverlässigkeit und nach Einholung der in Artikel 2 Buchstabe n angegebenen Feststellung der zuständigen Behörden eines Mitgliedstaats für den Zugang zu Informationen, die als "CONFIDENTIEL UE/EU CONFIDENTIAL" oder höher eingestuft sind, ermächtigt werden kann, wird in einem delegierten Beschluss gemäß Artikel 10 Absatz 10 festgelegt. Die Entscheidung über die Erteilung der Zugangsermächtigung trifft der Direktor für Personal, Finanzen und Allgemeine Dienste des Rechnungshofs.
 - 4) Der Direktor für Personal, Finanzen und Allgemeine Dienste des Rechnungshofs kann Sicherheitsüberprüfungsbescheinigungen ausstellen, in denen der Geheimhaltungsgrad, für den Personen der Zugang zu EU-VS gewährt werden kann ("CONFIDENTIEL UE / EU CONFIDENTIAL" oder höher), die Gültigkeitsdauer der entsprechenden Zugangsermächtigung und das Ablaufdatum der Sicherheitsüberprüfungsbescheinigung angegeben sind.
 - 5) Nur die Personen, die über eine in Absatz 2 Ziffer iii) genannte Ermächtigung verfügen, und die Mitglieder des Rechnungshofs gemäß Absatz 1 dürfen an Sitzungen teilnehmen, in denen Informationen behandelt werden, die als "CONFIDENTIEL UE/EU CONFIDENTIAL" oder höher eingestuft sind. Der Rechnungshof und der Herausgeber treffen von Fall zu Fall die praktischen Modalitäten für diese Sitzungen.
 - 6) Die Dienststellen des Rechnungshofs, die für die Organisation von Sitzungen zuständig sind, in denen als "CONFIDENTIEL UE/EU CONFIDENTIAL" oder höher eingestufte Informationen behandelt werden sollen, informieren die Informationssicherheitsstelle rechtzeitig über die Termine, Uhrzeiten und Orte dieser Sitzungen sowie die Teilnehmerlisten.
 - 7) Jede Person, die im Besitz von EU-VS ist, ohne dass sie dazu ordnungsgemäß ermächtigt ist und/oder nachweislich Kenntnis benötigt, muss diesen Umstand so schnell wie möglich der Informationssicherheitsstelle melden und sicherstellen, dass die EU-VS gemäß den Vorschriften in diesem Beschluss geschützt werden.

Artikel 5 Maßnahmen des materiellen Geheimschutzes für Verschlussachen

- 1) "Materieller Geheimschutz" bedeutet den Einsatz von materiellen und technischen Schutzmaßnahmen, damit der unbefugte Zugang zu EU-VS verhindert wird.
- 2) Die Maßnahmen des materiellen Geheimschutzes zielen darauf ab, das heimliche oder gewaltsame Eindringen unbefugter Personen zu verhindern, von unbefugten Handlungen

abzuschrecken bzw. diese zu verhindern und aufzudecken und den Einsatz von Personal in Bezug auf den Zugang zu EU-VS nach dem Grundsatz „Kenntnis nur, wenn nötig“ zu ermöglichen. Diese Maßnahmen werden auf der Grundlage eines Risikomanagementprozesses im Einklang mit diesem Beschluss festgelegt.

- 3) Die zuständige Sicherheitsstelle des Rechnungshofs überprüft regelmäßig die Bereiche, in denen EU-VS bearbeitet oder aufbewahrt werden.
- 4) Für die Bearbeitung und die Speicherung von EU-VS dürfen nur Ausrüstungen oder Geräte verwendet werden, die den Vorschriften entsprechen, die innerhalb der Organe, Agenturen oder Einrichtungen der EU gelten.
- 5) Außerhalb der Räumlichkeiten des Rechnungshofs können die Mitarbeiter des Rechnungshofs auf EU-VS, die als "CONFIDENTIEL UE/EU CONFIDENTIAL "oder höher eingestuft sind, oder deren Entsprechungen in besonders geschützten Bereichen zugreifen.
- 6) Der Rechnungshof kann eine Dienstleistungsvereinbarung mit einem anderen EU-Organ in Luxemburg abschließen, um Informationen, die als "CONFIDENTIEL UE/EU CONFIDENTIAL" oder höher eingestuft sind, in einem besonders geschützten Bereich dieses Organs bearbeiten und aufbewahren bzw. speichern zu können. Ohne eine ausdrückliche Zustimmung des Herausgebers dürfen diese EU-VS in den Räumlichkeiten des Rechnungshofs nicht bearbeitet oder aufbewahrt bzw. gespeichert und vom Rechnungshof nicht vervielfältigt oder übersetzt werden.
- 7) Der Rechnungshof erfasst den Eingang von als "RESTREINT UE/EU RESTRICTED" eingestuften Informationen. Einsichtnahmen in Informationen, die als "CONFIDENTIEL UE/EU CONFIDENTIAL" oder höher eingestuft sind, oder deren Entsprechungen außerhalb der Räumlichkeiten des Rechnungshofs sind zu Sicherheitszwecken zu registrieren.
- 8) EU-VS des Geheimhaltungsgrades "RESTREINT UE/EU RESTRICTED" können in geeigneten, verschließbaren Büromöbeln in einem Verwaltungsbereich oder einem besonders geschützten Bereich aufbewahrt werden. EU-VS des Geheimhaltungsgrades "CONFIDENTIEL UE/EU CONFIDENTIAL" oder "SECRET UE/EU SECRET" müssen im Rahmen einer Dienstleistungsvereinbarung in einem Sicherheitsbehältnis in einem besonders geschützten Bereich eines anderen EU-Organs in Luxemburg aufbewahrt werden.
- 9) Außerhalb der Registratur werden EU-VS zwischen Dienststellen und Räumlichkeiten wie folgt befördert:
 - a) In der Regel werden EU-VS elektronisch übermittelt und dabei durch kryptografische Produkte geschützt, die gemäß Artikel 6 Absatz 8 zugelassen wurden.
 - b) Erfolgt die Übermittlung nicht wie unter Buchstabe a beschrieben, werden die EU-VS unter Verwendung eines Datenträgers (z. B. USB-Speicherstick, CD, Festplattenlaufwerk), der durch kryptografische Produkte geschützt ist, welche gemäß Artikel 6 Absatz 8 zugelassen wurden, oder als Papierfassung in einem undurchsichtigen, versiegelten Umschlag befördert.
- 10) Informationen des Geheimhaltungsgrades "RESTREINT UE/EU RESTRICTED" können vorbehaltlich der beim Rechnungshof geltenden Archivierungsvorschriften vom Besitzer vernichtet werden. Informationen, die als "CONFIDENTIEL UE/EU CONFIDENTIAL" oder höher eingestuft sind, dürfen nur auf Anweisung des Besitzers oder einer zuständigen Stelle im Einklang mit den beim Rechnungshof geltenden Archivierungsvorschriften vom Registraturkontrollbeauftragten vernichtet werden. Dokumente, die als "SECRET UE/EU SECRET" eingestuft sind, werden in Anwesenheit eines Zeugen vernichtet, dessen Sicherheitsüberprüfung mindestens dem Geheimhaltungsgrad des Dokuments entspricht, das

vernichtet werden soll Der Registraturkontrollbeauftragte und der Zeuge, sofern die Anwesenheit eines solchen erforderlich ist, unterzeichnen ein Protokoll über die Vernichtung, das in der Registratur abgelegt wird. Der Registraturkontrollbeauftragte bewahrt die Protokolle über die Vernichtung von Dokumenten der Geheimhaltungsgrade "CONFIDENTIEL UE/EU CONFIDENTIAL" und "SECRET UE/EU SECRE" mindestens fünf Jahre auf.

- 11) Die Sicherheitsstelle für den materiellen Geheimschutz und die Informationssicherheitsstelle erarbeiten unter Berücksichtigung der örtlichen Gegebenheiten einen gemeinsamen Plan für die Sicherung von EU-VS in Krisenzeiten, der, wenn dies erforderlich sein sollte, auch Pläne für deren Vernichtung oder Evakuierung in einem Notfall beinhaltet. Sie erteilen die Anweisungen, die sie für geeignet halten, um zu verhindern, dass EU-VS in die Hände Unbefugter gelangen.
- 12) Müssen EU-VS physisch befördert werden, befolgt der Rechnungshof die Maßnahmen, die von dem Herausgeber auferlegt werden, um sie vor unbefugter Offenlegung während des Transports zu schützen.
- 13) Die Maßnahmen des materiellen Geheimschutzes, die in den Verwaltungsbereichen gelten, in denen Informationen des Geheimhaltungsgrades "RESTREINT UE/EU-RESTRICTED" bearbeitet und aufbewahrt bzw. gespeichert werden, sind im Anhang festgelegt.

Artikel 6 Schutz von EU-VS in Kommunikations- und Informationssystemen

- 1) Im Sinne dieses Artikels bezeichnet der Ausdruck "Kommunikations- und Informationssystem" jedes System, das die Bearbeitung von Verschlussachen in elektronischer Form ermöglicht. Zu einem Kommunikations- und Informationssystem gehören sämtliche für seinen Betrieb benötigten Voraussetzungen, einschließlich der Infrastruktur, der Organisation, des Personals und der Informationsressourcen.
- 2) "Rechtmäßiger Nutzer" bezeichnet ein Mitglied des Rechnungshofs, einen Beamten, einen sonstigen Bediensteten oder einen ANS, der nachweislich und anerkanntermaßen Zugang zu einem bestimmten Informationssystem benötigt.
- 3) Der Rechnungshof gewährleistet, dass seine Systeme die mit ihnen bearbeiteten Informationen in geeigneter Weise schützen und dass diese Systeme unter der Kontrolle rechtmäßiger Nutzer jederzeit ordnungsgemäß funktionieren. Dazu müssen sie Folgendes in angemessenem Umfang sicherstellen:
 - Authentizität: Es ist sichergestellt, dass die Informationen echt sind und von in gutem Glauben handelnden Quellen stammen.
 - Verfügbarkeit: Die Informationen sind auf Anfrage einer befugten Stelle verfügbar und nutzbar.
 - Vertraulichkeit: Die Informationen werden nicht gegenüber unbefugten Personen, Stellen oder Verarbeitungsprozessen offengelegt.
 - Integrität: Die Genauigkeit und die Vollständigkeit der Informationen und Vermögenswerte sind gewährleistet.
 - Beweisbarkeit: Es kann nachgewiesen werden, dass ein Vorgang oder ein Ereignis stattgefunden hat, sodass dieser Vorgang oder dieses Ereignis nicht nachträglich abgestritten werden kann.

Diese Sicherung stützt sich auf einen Risikomanagementprozess. "Risiko" bezeichnet die Möglichkeit, dass bei einer bestimmten Bedrohung die internen und externen Schwachstellen einer Organisation oder eines der von ihr verwendeten Systeme ausgenutzt und dadurch die Organisation und ihre materiellen und immateriellen Werte geschädigt werden. Gemessen wird das Risiko als die Kombination der Wahrscheinlichkeit des Eintretens von Bedrohungen und ihrer Auswirkungen. Der Risikomanagementprozess

besteht aus den folgenden Schritten: Bedrohungs- und Anfälligkeitsermittlung, Risikobewertung, Risikobehandlung, Risikoakzeptanz und Risikokommunikation.

- Die "Risikobewertung" umfasst die Ermittlung von Bedrohungen und Schwachstellen sowie die Durchführung der entsprechenden Risikoanalyse, d. h. die Bewertung der Eintrittswahrscheinlichkeit und der Auswirkungen.
 - Die "Risikobehandlung" beinhaltet die Minderung, Beseitigung, Verringerung (durch eine geeignete Kombination von technischen, physischen, organisatorischen oder verfahrenstechnischen Maßnahmen), Übertragung oder Überwachung des Risikos.
 - Die "Risikoakzeptanz" ist die Hinnahme der Möglichkeit, dass nach der Risikobehandlung ein Restrisiko bleibt.
 - Das "Restrisiko" bedeutet das Risiko, das nach dem Ergreifen von Sicherheitsmaßnahmen verbleibt, falls nicht alle Bedrohungen erfasst werden und nicht alle Schwachstellen beseitigt werden können.
 - Die "Risikokommunikation" besteht darin, die Nutzer eines Kommunikations- und Informationssystems für Risiken zu sensibilisieren sowie die Zulassungsstellen über diese Risiken zu informieren und die für den Betrieb zuständigen Stellen entsprechend zu unterrichten.
- 4) Alle elektronischen Geräte und Ausrüstungen, die für die Bearbeitung von EU-VS verwendet werden, müssen den Vorschriften entsprechen, die für den Schutz von EU-VS gelten. Zu bevorzugen sind elektronische Geräte und Ausrüstungen, die bereits von einem anderen Organ, einer anderen Agentur oder einer anderen Einrichtung der EU zugelassen wurden. Die Sicherheit der Geräte muss während ihres gesamten Lebenszyklus gewährleistet sein.
- 5) Das Kommunikations- und Informationssystem des Rechnungshofs für die Bearbeitung von EU-VS bedarf der Akkreditierung durch eine zuständige Behörde. Zu diesem Zweck bemüht sich der Rechnungshof um den Abschluss einer Dienstleistungsvereinbarung (Service Level Agreement, SLA) mit einer Sicherheitsakkreditierungsstelle eines EU-Organs, die in der Lage ist, Kommunikations- und Informationssysteme, in denen EU-VS bearbeitet werden, zu akkreditieren, um für die Informationen des Geheimhaltungsgrades "RESTREINT UE/EU RESTRICTED", die im Kommunikations- und Informationssystem des Rechnungshofs verarbeitet werden sollen, und die entsprechenden Betriebsbedingungen eine Akkreditierungserklärung zu erhalten. Die Dienstleistungsvereinbarung soll außerdem die Standards, die für den Akkreditierungsprozess Anwendung finden, enthalten und wird gemäß dem in Artikel 10 Absatz 3 festgelegten Verfahren geschlossen.
- 6) Für den Fall, dass der Rechnungshof einen eigenen Akkreditierungsprozess für sein Kommunikations- und Informationssystem einrichten muss, wird dieser Prozess in einem delegierten Beschluss gemäß Artikel 10 Absatz 10 des vorliegenden Beschlusses im Einklang mit den Standards festgelegt, die für den Akkreditierungsprozess für Kommunikations- und Informationssysteme gelten, in denen EU-VS in anderen Organen, Agenturen und Einrichtungen der EU bearbeitet werden.
- 7) Die alleinige Verantwortung für die Erstellung der Akkreditierungsdateien und -unterlagen in Übereinstimmung mit den geltenden Standards trägt der Systemeigentümer des betreffenden Kommunikations- und Informationssystems.
- 8) Werden EU-VS durch kryptografische Produkte geschützt, gibt der Rechnungshof den Produkten den Vorzug, die vom Rat oder vom Generalsekretär des Rates in dessen Funktion als Krypto-Zulassungsstelle oder andernfalls von anderen Organen, Agenturen und Einrichtungen der EU für den Schutz von EU-VS zugelassen wurden.
- 9) Informationen des Geheimhaltungsgrades "RESTREINT UE/EU-RESTRICTED" dürfen nur auf solchen elektronischen Geräten (z. B. Arbeitsplatzrechnern, Druckern, Kopierern) bearbeitet

werden, die sich in einem Verwaltungsbereich oder in einem besonders geschützten Bereich befinden. Elektronische Geräte, mit denen Informationen des Geheimhaltungsgrades "RESTREINT UE/EU RESTRICTED" bearbeitet werden, müssen von anderen Computernetzwerken getrennt und durch geeignete physische oder technische Maßnahmen geschützt sein.

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

Artikel 7 Verfahren für den Austausch von Verschlusssachen und die Ermöglichung des Zugangs zu ihnen

- 1) Die Organe, Agenturen, Einrichtungen und Ämter der EU sowie die nationalen Behörden gewähren dem Rechnungshof, wenn sie aufgrund der Verträge oder der auf der Grundlage der Verträge erlassenen Rechtsakte rechtlich dazu verpflichtet sind, von sich aus oder auf schriftlichen Antrag des Präsidenten, des berichterstattenden Mitglieds bzw. der berichterstattenden Mitglieder oder des Generalsekretärs Zugang zu den EU-VS nach dem im Folgenden beschriebenen Verfahren.
- 2) Die Zugangsanträge werden über die Erfassungsstelle des Rechnungshofs an die betreffenden Organe übermittelt.
- 3) Erforderlichenfalls schließt der Rechnungshof eine Verwaltungsvereinbarung, in der die praktischen Modalitäten für den Austausch von EU-VS oder gleichwertigen Informationen geregelt werden.
- 4) Zum Zwecke des Abschlusses solcher Verwaltungsvereinbarungen stellt der Rechnungshof dem Herausgeber alle erforderlichen Informationen über sein Informationssicherheitssystem zur Verfügung. Bei entsprechender Notwendigkeit kann ein Begutachtungsbesuch organisiert werden.
- 5) Diese Verwaltungsvereinbarungen werden unter uneingeschränkter Wahrung der Grundsätze der begrenzten Einzelermächtigung und der loyalen Zusammenarbeit gemäß Artikel 13 des Vertrags über die Europäische Union geschlossen. Ihr Abschluss erfolgt gemäß dem in Artikel 10 Absatz 4 festgelegten Verfahren.
- 6) Besteht mit einem bestimmten Organ, einer Einrichtung oder einer Agentur der EU, einem Drittstaat oder einer internationalen Organisation keine Verwaltungsvereinbarung über die Bereitstellung von Verschlusssachen an den Rechnungshof, unterzeichnet der Rechnungshof eine Verpflichtungserklärung für den Schutz der ihm zugehenden Verschlusssachen.

Artikel 8 Verletzung der Sicherheit, Verlust der Verschlusssache oder Kenntnisnahme durch Unbefugte

- 1) Eine Sicherheitsverletzung bedeutet eine Handlung oder Unterlassung einer Person, die den in diesem Beschluss und den Durchführungsbestimmungen festgelegten Sicherheitsvorschriften zuwiderläuft.

- 2) Eine Kompromittierung liegt vor, wenn eine EU-VS infolge einer Verletzung der Sicherheit ganz oder teilweise an unbefugte Personen weitergegeben wurde.
- 3) Jede erfolgte oder vermutete Verletzung der Sicherheit ist der Informationssicherheitsstelle des Rechnungshofs unverzüglich zu melden.
- 4) Ist bekannt oder besteht guter Grund zu der Annahme, dass EU-VS kompromittiert wurden oder verloren gegangen sind, informiert die Informationssicherheitsstelle den Direktor für Personal, Finanzen und Allgemeine Dienste und den Generalsekretär des Rechnungshofs. Der Direktor für Personal, Finanzen und Allgemeine Dienste informiert unverzüglich die entsprechende Sicherheitsstelle des Herausgebers. Der genannte Direktor des Rechnungshofs führt eine Ermittlung durch und teilt dem Generalsekretär des Rechnungshofs und der Sicherheitsstelle des Herausgebers die Ergebnisse und die Maßnahmen mit, die getroffen wurden, um ein wiederholtes Auftreten einer solchen Situation zu verhindern. Ist ein Mitglied des Rechnungshofs betroffen, trägt der Präsident des Rechnungshofs die Verantwortung, in Zusammenarbeit mit dem Generalsekretär des Rechnungshofs tätig zu werden.
- 5) Jeder Beamte oder sonstige Bedienstete des Rechnungshofs, der für einen Verstoß gegen die in diesem Beschluss und seinen Durchführungsbestimmungen festgelegten Sicherheitsvorschriften verantwortlich ist, unterliegt den Sanktionen, die im Statut und in den Beschäftigungsbedingungen für die sonstigen Bediensteten der Europäischen Union vorgesehen sind.
- 6) Jedes Mitglied des Rechnungshofs, das den Bestimmungen dieses Beschlusses nicht nachkommt, ist den in Artikel 286 Absatz 6 des Vertrags vorgesehenen Maßnahmen und Sanktionen unterworfen.
- 7) Gegen jede Person, die für den Verlust oder die Kompromittierung von EU-VS verantwortlich ist, können gemäß den geltenden Rechtsvorschriften Disziplinarmaßnahmen ergriffen und/oder rechtliche Schritte unternommen werden.

Artikel 9 Sicherheit bei Eingriffen durch Außenstehende

- 1) Der Rechnungshof kann Auftragnehmer, die in einem Mitgliedstaat registriert sind, auf vertraglicher Grundlage mit der Ausführung von Aufgaben beauftragen, die den Zugang zu EU-VS beinhalten oder erfordern. Dieser Fall kann insbesondere im Zusammenhang mit der Wartung von Kommunikations- und Informationssystemen und dem Computernetzwerk eintreten.
- 2) Bei Eingriffen durch Außenstehende trifft der Rechnungshof alle erforderlichen Sicherheitsmaßnahmen gemäß Absatz 3 dieses Artikels, einschließlich der Vorlage eines Sicherheitsbescheids für Unternehmen (Facility Security Clearance, FSC), um den Schutz von EU-VS durch Bewerber und Bieter während der gesamten Dauer eines Ausschreibungs- und Vergabeverfahrens sowie durch Auftragnehmer und Unterauftragnehmer während der gesamten Laufzeit eines Vertrags sicherzustellen. Der Auftraggeber stellt sicher, dass die in diesem Beschluss vorgesehenen Mindestsicherheitsstandards in den Verträgen genannt werden, um die Auftragnehmer zur Einhaltung dieser Standards zu verpflichten.
- 3) Die Sicherheitsvorschriften, die Vergabeverfahren sowie die Vorlagen und Muster für Verträge und Unterverträge, die den Zugang zu EU-VS beinhalten, die Bekanntmachungen, die Leitlinien für Fälle, in denen Sicherheitsbescheide für Unternehmen und Sicherheitsüberprüfungsbescheinigungen für Personal erforderlich sind, Projektsicherheitsanweisungen, die Geheimschutzklauseln, die Besuche sowie die Übermittlung und Beförderung von EU-VS im Rahmen solcher Verträge und Unterverträge

müssen den Vorschriften, Vorlagen und Mustern entsprechen, die von der Europäischen Kommission für als Verschlussache eingestufte Aufträge im Beschluss (EU, Euratom) 2015/444 der Kommission vom 13. März 2015 über die Sicherheitsvorschriften für den Schutz von EU-Verschlussachen festgelegt wurden.

Artikel 10 Durchführung des Beschlusses und damit verbundene Verantwortlichkeiten

- 1) Die Dienststellen des Rechnungshofs treffen alle erforderlichen Maßnahmen, die in ihre Zuständigkeit fallen, um sicherzustellen, dass sie bei der Bearbeitung oder Aufbewahrung bzw. Speicherung von EU-VS oder anderen Verschlussachen diesen Beschluss und die einschlägigen Durchführungsbestimmungen anwenden.
- 2) Der Generalsekretär ist Anstellungs- und Einstellungsbehörde für alle Beamten und sonstigen Bediensteten. Der Generalsekretär kann dem Direktor für Personal, Finanzen und Allgemeine Dienste die Zuständigkeit für die Erteilung von Zugangsberechtigungen für Beamte und sonstige Bedienstete zu Informationen, die als "CONFIDENTIEL UE/EU CONFIDENTIAL" oder höher eingestuft sind, für die Ausübung seiner Funktion als Sicherheitsakkreditierungsstelle und für die Überwachung des Sekretariats des Rechnungshofs in Bezug auf die Bearbeitung der EU-VS übertragen.
- 3) Der Generalsekretär ist zuständig für den Abschluss von Dienstleistungsvereinbarungen über die Akkreditierung der Kommunikations- und Informationsausrüstung und -systeme des Rechnungshofs, über die Nutzung eines besonders geschützten Bereichs in einem anderen EU-Organ und über das Verfahren für Anträge auf Erklärungen über die Sicherheitsüberprüfungen von Personal für den Zugang zu EU-VS.
- 4) Der Direktor für Personal, Finanzen und Allgemeine Dienste ist befugt, mit den Organen, Agenturen und anderen Einrichtungen der EU Verwaltungsvereinbarungen über den Austausch von EU-VS zu schließen, die der Rechnungshof benötigt, um seinen Auftrag erfüllen zu können. Der genannte Direktor kann auch mit Drittstaaten oder internationalen Organisationen Verwaltungsvereinbarungen über den Schutz der erhaltenen Verschlussachen schließen.
- 5) Der Direktor für Personal, Finanzen und Allgemeine Dienste ist befugt, eine Verpflichtungserklärung für den Schutz der EU-VS, die im Rahmen einer außerordentlichen Ad-hoc-Freigabe zur Verfügung gestellt werden sollen, zu unterzeichnen.
- 6) Der Informationssicherheitsbeauftragte des Rechnungshofs fungiert als Informationssicherheitsstelle. Der Informationssicherheitsbeauftragte und die Personen, denen er seine Aufgaben ganz oder teilweise überträgt, müssen entsprechend sicherheitsüberprüft sein. Die Informationssicherheitsstelle nimmt ihre Aufgaben in enger Zusammenarbeit mit der Direktion "Personal, Finanzen und Allgemeine Dienste", der Direktion "Information, Arbeitsplatz und Innovation" und der Direktion des Ausschusses für Qualitätskontrolle im Prüfungsbereich wahr (siehe insbesondere Artikel 4, 6 und 8). Die Informationssicherheitsstelle ist auch für Schulungs- und Sensibilisierungsveranstaltungen für die Informationssicherheit sowie für die regelmäßigen Inspektionen zur Überprüfung der Einhaltung dieses Beschlusses, auch bei Eingriffen durch Außenstehende, und etwaiger Maßnahmen zuständig, die zu ergreifen sind, um die Einhaltung sicherzustellen.
- 7) Der Leiter der Dienststelle "Sicherheit" ist für die Maßnahmen des materiellen Geheimschutzes (insbesondere Artikel 5) verantwortlich.
- 8) Eine im Sekretariat des Rechnungshofs eingerichtete Erfassungsstelle ist die Eingangs- und Ausgangsstelle für als "RESTREINT UE/EU RESTRICTED" eingestufte Informationen, die der

Rechnungshof mit anderen Organen, Agenturen und Einrichtungen der EU sowie den Mitgliedstaaten gegebenenfalls austauscht. Sie ist auch die Eingangs- und Ausgangsstelle für vergleichbare Informationen von Drittstaaten und internationalen Organisationen. Die Erfassungsstelle wird gemäß den Festlegungen in einem delegierten Beschluss organisiert. Der Erfassungsbeauftragte übernimmt die folgenden Hauptaufgaben:

- a) Erfassung von Ein- und Ausgängen von Informationen, die als "RESTREINT UE/EU RESTRICTED" eingestuft sind;
 - b) Verwaltung spezieller Verwaltungsbereiche für die Erfassung, Bearbeitung, Aufbewahrung von und Einsichtnahme in EU-VS, die als "RESTREINT UE/EU RESTRICTED" eingestuft sind.
- 9) Im Rahmen einer Dienstleistungsvereinbarung wird eine Registratur für die Nutzung des besonders geschützten Bereichs eines anderen EU-Organs eingerichtet. Diese vom Sekretariat des Rechnungshofs unter der Verantwortung des Direktors für Personal, Finanzen und Allgemeine Dienste des Rechnungshofs eingerichtete Registratur ist die Eingangs- und Ausgangsstelle für Informationen, die als "CONFIDENTIEL UE/EU CONFIDENTIAL" oder höher eingestuft sind und die der Rechnungshof mit anderen Organen, Agenturen und Einrichtungen der EU sowie den Mitgliedstaaten gegebenenfalls austauscht. Sie ist auch die Eingangs- und Ausgangsstelle für vergleichbare Informationen von Drittstaaten und internationalen Organisationen. Sie ist mit geeigneten Panzerschranken und anderen Sicherheitseinrichtungen ausgestattet, die für den Schutz von Informationen des Geheimhaltungsgrades "CONFIDENTIEL UE/EU CONFIDENTIAL" oder höher geeignet sind. Die Organisation der Registratur wird in einem delegierten Beschluss festgelegt. Der Registraturkontrollbeauftragte muss sicherheitsüberprüft sein und übernimmt die folgenden Hauptaufgaben:
- a) Verwaltung von Vorgängen im Zusammenhang mit der Registrierung, Einsichtnahme, Aufbewahrung, Vervielfältigung, Übersetzung, Übermittlung, Versendung und gegebenenfalls Vernichtung von EU-VS;
 - b) Wahrnehmung aller sonstigen Aufgaben im Zusammenhang mit dem Schutz von EU-VS, die in einem delegierten Beschluss festgelegt sind.
- 10) Der Verwaltungsausschuss erlässt einen delegierten Beschluss zur Festlegung der Durchführungsbestimmungen zu diesem Beschluss. Der Informationssicherheitsbeauftragte legt Leitlinien für die Informationssicherheit fest. Der Ausschuss für Qualitätskontrolle im Prüfungsbereich erstellt Leitlinien für den Prüfungsbereich.

Artikel 11 Inkrafttreten des Beschlusses

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

Geschehen zu Luxemburg am 3. Juni 2021

Für den Rechnungshof

Klaus-Heiner Lehne
Präsident

Anhang: MASSNAHMEN DES MATERIELLEN GEHEIMSCHUTZES VON VERWALTUNGSBEREICHEN
 FÜR EU-VS

ANHANG

MASSNAHMEN DES MATERIELLEN GEHEIMSCHUTZES VON VERWALTUNGSBEREICHEN FÜR EU-VS

- 1) Dieser Anhang enthält die Vorschriften zur Anwendung von Artikel 5 des Beschlusses. In ihm sind die Mindestanforderungen an den materiellen Schutz von Verwaltungsbereichen für Informationen des Geheimhaltungsgrades "RESTREINT UE/EU RESTRICTED" beim Rechnungshof festgelegt, d. h. Bereiche, die für die Erfassung und Aufbewahrung von sowie die Einsichtnahme in Informationen mit der Einstufung "RESTREINT UE/EU RESTRICTED" ausgewiesen sind.
- 2) Die Maßnahmen des materiellen Geheimschutzes in Verwaltungsbereichen zielen darauf ab, den Zugang unbefugter Personen zu diesen Bereichen wie folgt zu verhindern:
 - a) Es wird eine sichtbare äußere Abgrenzung eingerichtet, die die Kontrolle von Personen ermöglicht.
 - b) Unbegleiteter Zugang wird nur Personen gewährt, die von der Informationssicherheitsstelle des Rechnungshofs oder einer anderen zuständigen Stelle entsprechend ermächtigt wurden.
 - c) Bei allen anderen Personen ist eine ständige Begleitung oder eine gleichwertige Kontrolle sicherzustellen.
- 3) Die Informationssicherheitsstelle des Rechnungshofs kann in Ausnahmefällen unbefugten Personen Zugang gewähren, auch für Arbeiten in einem Verwaltungsbereich, sofern dies nicht den Zugang zu EU-VS – die unter Verschluss bleiben müssen – zur Folge hat. Diese Personen dürfen Bereiche nur in Begleitung und unter ständiger Aufsicht der Informationssicherheitsstelle oder des Erfassungskontrollbeauftragten betreten.
- 4) Die Informationssicherheitsstelle legt Verfahren für die Verwaltung der Schlüssel und/oder Kombinationseinstellungen für alle Verwaltungsbereiche und das gesicherte Mobiliar fest. Der Zweck dieser Verfahren ist der Schutz vor unbefugtem Zugang.
- 5) Der Kreis der Personen, denen die Kombinationen zur Kenntnis gegeben werden, ist auf die kleinstmögliche Anzahl von Personen, die Kenntnis davon haben müssen, zu begrenzen. Die Kombinationseinstellungen für gesichertes Mobiliar, das zur Aufbewahrung von Informationen des Geheimhaltungsgrades "RESTREINT UE/EU RESTRICTED" verwendet wird, sind zu ändern:
 - bei Zugang eines neuen Sicherheitsmöbels;
 - bei Wechsel des Personals, das die Kombination kennt;
 - wenn die Einstellung kompromittiert wurde oder der Verdacht besteht, dass sie kompromittiert wurde;
 - wenn ein Schloss gewartet oder repariert wurde;
 - mindestens alle 12 Monate.
- 6) Die Informationssicherheitsstelle und der Leiter der Dienststelle "Sicherheit" sind für die Einhaltung dieser Vorschriften verantwortlich.