BESCHLUSS (EU) 2022/640 DER KOMMISSION

vom 7. April 2022

mit Durchführungsbestimmungen zu den Rollen und Zuständigkeiten der wichtigsten Sicherheitsakteure

DIE EUROPÄISCHE KOMMISSION —

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

gestützt auf den Beschluss (EU, Euratom) 2015/443 der Kommission vom 13. März 2015 über Sicherheit in der Kommission ([1]),

gestützt auf den Beschluss (EU, Euratom) 2015/444 der Kommission vom 13. März 2015 über die Sicherheitsvorschriften für den Schutz von EU-Verschlusssachen ([2]),

in Erwägung nachstehender Gründe:

(1) Die Beschlüsse (EU, Euratom) 2015/443 und (EU, Euratom) 2015/444 finden auf alle Dienststellen und Räumlichkeiten der Kommission Anwendung.

(2) Erforderlichenfalls werden zur Ergänzung oder Untermauerung des Beschlusses (EU, Euratom) 2015/444 im Einklang mit Artikel 60 jenes Beschlusses Durchführungsbestimmungen erlassen.

(3) Die Sicherheitsmaßnahmen zum Schutz von EU-Verschlusssachen während ihres gesamten Lebenszyklus müssen insbesondere dem Geheimhaltungsgrad entsprechen.

(4) Sicherheitsmaßnahmen zum Schutz der Kommunikations- und Informationssysteme in der Kommission sind im Beschluss (EU, Euratom) 2017/46 der Kommission ([3]) festgelegt, insbesondere in Artikel 3 über die Grundsätze für die IT-Sicherheit in der Kommission und in Artikel 9 über die Systemeigner.

(5) Mit den Durchführungsbestimmungen zu den Rollen und Zuständigkeiten der wichtigsten Sicherheitsakteure sollen Leitlinien zu den Voraussetzungen und Pflichten, die für diese Rollen in den Beschlüssen (EU, Euratom) 2015/443 und (EU, Euratom) 2015/444 festgelegt sind, breitgestellt werden.

(6) In Artikel 36 Absatz 7 des Beschlusses (EU, Euratom) 2015/444 sind eine Reihe zusätzlicher sicherheitsbezogener Funktionen festgelegt, die von der Sicherheitsstelle der Kommission wahrzunehmen sind. Die Aufgaben im Zusammenhang mit diesen Funktionen sind Gegenstand des vorliegenden Beschlusses.

(7) Gemäß dem Beschluss (EU, Euratom) 2015/444 haben lokale Sicherheitsbeauftragte (Local Security Officers — LSO) und Registraturkontrollbeauftragte (Registry Control Officers — RCO) besondere Zuständigkeiten im Zusammenhang mit dem Schutz von EU-Verschlusssachen in ihren Dienststellen.

(8) Am 4. Mai 2016 erließ die Kommission einen Beschluss ([4]), mit dem das für Sicherheitsfragen zuständige Mitglied der Kommission ermächtigt wurde, im Namen der Kommission und unter ihrer Verantwortung die in Artikel 60 des Beschlusses (EU, Euratom) 2015/444 der Kommission vorgesehenen Durchführungsbestimmungen zu erlassen; entsprechend erließ das für Sicherheitsfragen zuständige Mitglied der Kommission am 13. April 2021 im Namen der Kommission und unter ihrer Verantwortung einen Beschluss ([5]) über eine Weiterübertragung von Befugnissen bezüglich dieser Durchführungsbestimmungen an den Generaldirektor der Generaldirektion Humanressourcen und Sicherheit —

([1]) ABl. L 72 vom 17.3.2015, S. 41.
([2]) ABl. L 72 vom 17.3.2015, S. 53.
([3]) Beschluss (EU, Euratom) 2017/46 der Kommission vom 10. Januar 2017 über die Sicherheit von Kommunikations- und Informationssystemen in der Europäischen Kommission (ABl. L 6 vom 11.1.2017, S. 40).
([4]) Beschluss C(2016) 2797 final vom 4. Mai 2016 über eine Ermächtigung im Bereich der Sicherheit.
([5]) Beschluss C(2021) 2684 final vom 13. April 2021 über eine Weiterübertragung von Befugnissen gemäß dem Beschluss C(2016) 2797 der Kommission über eine Ermächtigung im Bereich der Sicherheit.

HAT FOLGENDEN BESCHLUSS ERLASSEN:

KAPITEL 1

Allgemeine Bestimmungen

Artikel 1

Gegenstand und Geltungsbereich

(1) In diesem Beschluss werden die Rollen und Zuständigkeiten der wichtigsten Sicherheitsakteure, die nach Maßgabe der Beschlüsse (EU, Euratom) 2015/443 und (EU, Euratom) 2015/444 für den Schutz von EU-Verschlusssachen in der Kommission zuständig sind, festgelegt.

(2) Dieser Beschluss findet auf alle Kommissionsdienststellen und in allen Räumlichkeiten der Kommission Anwendung.

KAPITEL 2

Generaldirektion Humanressourcen und Sicherheit

Artikel 2

Sicherheitsstelle der Kommission (Commission Security Authority — CSA)

(1) Der Direktor der Direktion Sicherheit der Generaldirektion Humanressourcen und Sicherheit ist die Sicherheitsstelle der Kommission gemäß Artikel 7 des Beschlusses (EU, Euratom) 2015/444.

(2) Im Einklang mit den Artikeln 3 bis 7 des vorliegenden Beschlusses nimmt die Sicherheitsstelle der Kommission ihre Funktionen gemäß dem Beschluss (EU, Euratom) 2015/444 in folgenden Bereichen wahr:

a) personeller Geheimschutz;

b) physische Sicherheit;

c) Verwaltung von EU-VS;

d) Akkreditierung aller Kommunikations- und Informationssysteme, in denen EU-VS bearbeitet werden;

e) Geheimschutz in der Wirtschaft und

f) Austausch von Verschlusssachen.

(3) Die Sicherheitsstelle der Kommission führt die verpflichtende Schulung der LSO, der stellvertretenden LSO, der RCO und der stellvertretenden RCO zu ihren jeweiligen Zuständigkeiten und Aufgaben durch.

Artikel 3

Stelle für Informationssicherung (Information Assurance Authority)

Die Stelle für die Informationssicherung ist im Zusammenhang mit dem Schutz von EU-VS für folgende Tätigkeiten zuständig:

a) Entwicklung von Sicherheitskonzepten und Sicherheitsleitlinien für Informationssicherung sowie Überwachung ihrer Wirksamkeit und Angemessenheit;

b) Schutz und Verwaltung der technischen Informationen über kryptografische Produkte;

c) Sicherstellen, dass Informationssicherungsmaßnahmen der Sicherheits- und Beschaffungspolitik der Kommission entsprechen;

d) Gewährleistung, dass die kryptografischen Produkte unter Einhaltung der Regeln für ihre Eignung und Auswahl gewählt werden;

e) Konsultation der Systemeigner, Systembetreiber, Sicherheitsverantwortlichen und Vertreter von Nutzern in Bezug auf die Sicherheitskonzepte und Sicherheitsleitlinien für Informationssicherung.

Artikel 4

Sicherheitsakkreditierungsstelle (Security Accreditation Authority — SAA)

(1) Die Sicherheitsstelle der Kommission ist für die Akkreditierung besonders geschützter Bereiche, die die Anforderungen des Artikels 18 des Beschlusses 2015/444 erfüllen, sowie für die Akkreditierung von Kommunikations- und Informationssystemen für die Bearbeitung von EU-VS zuständig.

(2) Die Dienststellen der Kommission konsultieren die Sicherheitsakkreditierungsstelle in Abstimmung mit ihrem LSO und ihrem Beauftragten für die lokale IT-Sicherheit (LISO), wenn eine Dienststelle beabsichtigt,

a) einen besonders geschützten Bereich zu schaffen;

b) ein Kommunikations- und Informationssystem für die Bearbeitung von EU-VS einzurichten;

c) sonstige Ausrüstungen zur Bearbeitung von Verschlusssachen zu installieren, einschließlich der Anbindung an ein Kommunikations- und Informationssystem Dritter.

Die Sicherheitsakkreditierungsstelle berät in Bezug auf diese Tätigkeiten sowohl beim Planungs-, Bau- und Entwicklungsprozess.

(3) EU-VS dürfen erst in einem besonders geschützten Bereich oder einem Kommunikations- und Informationssystem bearbeitet werden, wenn die Sicherheitsakkreditierungsstelle für den entsprechenden EU-VS-Geheimhaltungsgrad eine Akkreditierung erteilt hat.

(4) Die Voraussetzungen für die Akkreditierung eines besonders geschützten Bereichs umfassen Folgendes:

a) die Genehmigung der Pläne für den besonders geschützten Bereich;

b) die Genehmigung aller Verträge über Arbeiten, die von externen Auftragnehmern ausgeführt werden, unter Berücksichtigung der Bestimmungen über den Geheimschutz in der Wirtschaft, wie etwa der Anforderungen an die Sicherheitsüberprüfungen der Auftragnehmer und ihres Personals;

c) die Bereitstellung aller erforderlichen Konformitätserklärungen und -bescheinigungen;

d) die physische Inspektion des besonders geschützten Bereichs zur Überprüfung, ob die Baumaterialien und -methoden, die Zugangskontrollen, die Sicherheitsausrüstung und alle anderen Gegenstände den von der Sicherheitsstelle der Kommission festgelegten Anforderungen entsprechen;

e) die Validierung der Schutzmaßnahmen gegen elektromagnetische Abstrahlung für jeden technisch abgesicherten Bereich;

f) die Genehmigung der sicherheitsbezogenen Betriebsverfahren (security operating procedures — SecOPs) für den besonders geschützten Bereich.

(5) Für die Akkreditierung eines Kommunikations- und Informationssystems, in dem EU-VS bearbeitet werden, ist Folgendes erforderlich:

a) die Ausarbeitung einer Akkreditierungsstrategie für das System;

b) die Validierung des Sicherheitsplans des Kommunikations- und Informationssystems auf der Grundlage eines Risikomanagementansatzes;

c) die Validierung der sicherheitsbezogenen Betriebsverfahren für das Kommunikations- und Informationssystem;

d) die Validierung aller sonstigen von der Sicherheitsakkreditierungsstelle festgelegten erforderlichen Sicherheitsdokumente;

e) die Genehmigung jeglicher Verwendung von Verschlüsselungstechnologien;

f) die Validierung der Schutzmaßnahmen gegen elektromagnetische Abstrahlung für ein Kommunikations- und Informationssystem, in dem als „CONFIDENTIEL UE/EU CONFIDENTIAL“ oder höher eingestufte Informationen bearbeitet werden;

g) eine Inspektion des Kommunikations- und Informationssystems zur Überprüfung, ob die dokumentierten Sicherheitsmaßnahmen korrekt umgesetzt werden.

(6) Sind die Voraussetzungen für die Akkreditierung erfüllt, so erteilt die Sicherheitsakkreditierungsstelle entsprechend dem Geheimhaltungsgrad der zu bearbeitenden EU-VS und den damit verbundenen Risiken eine förmliche Genehmigung für die Bearbeitung von EU-VS im besonders geschützten Bereich oder im Kommunikations- und Informationssystem für den festgelegten höchsten Geheimhaltungsgrad der EU-VS und für einen Zeitraum von bis zu fünf Jahren.

(7) Wird eine Sicherheitsverletzung oder eine wesentliche Änderung bezüglich der Gestaltung oder der Sicherheitsmaßnahmen des besonders geschützten Bereichs oder des Kommunikations- und Informationssystems gemeldet, so überprüft die Sicherheitsakkreditierungsstelle die Genehmigung für die Bearbeitung von EU-VS und kann diese erforderlichenfalls widerrufen, bis alle festgestellten Probleme behoben sind.

Artikel 5

TEMPEST-Stelle

(1) TEMPEST-Sicherheitsmaßnahmen sind zum Schutz von Kommunikations- und Informationssystemen, in denen Verschlusssachen des Geheimhaltungsgrades „CONFIDENTIEL UE/EU CONFIDENTIAL“ oder höher bearbeitet werden, zu treffen und können für Verschlusssachen des Geheimhaltungsgrades „RESTREINT UE/EU RESTRICTED“ getroffen werden.

(2) Die TEMPEST-Stelle ist für die Genehmigung der Maßnahmen zuständig, die zum Schutz vor Kompromittierungen von EU-VS durch unbeabsichtigte elektronische Abstrahlung ergriffen werden.

(3) Auf Ersuchen eines Systemeigners eines Kommunikations- und Informationssystems, in dem EU-VS bearbeitet werden, gibt die TEMPEST-Stelle Spezifikationen für TEMPEST-Sicherheitsmaßnahmen heraus, die für den Geheimhaltungsgrad der Informationen angemessen sind.

(4) Die TEMPEST-Stelle führt während der Akkreditierung von besonders geschützten Bereichen und von Kommunikations- und Informationssystemen für die Bearbeitung von EU-VS des Geheimhaltungsgrades „CONFIDENTIAL UE/EU CONFIDENTIAL“ oder höher entsprechende technische Überprüfungen durch und stellt nach erfolgreicher Überprüfung eine TEMPEST-Bescheinigung aus.

(5) Eine TEMPEST-Bescheinigung enthält mindestens folgende Angaben:

a) das Datum der Überprüfung;

b) eine Beschreibung der TEMPEST-Sicherheitsmaßnahmen, einschließlich der Pläne der Räumlichkeiten;

c) das Gültigkeitsdatum der Bescheinigung;

d) jegliche Änderungen, die die Bescheinigung außer Kraft setzen;

e) die Unterschrift der TEMPEST-Stelle.

(6) Ein LSO bzw. ein Organisator einer vertraulichen Sitzung in Abstimmung mit dem LSO kann die TEMPEST-Stelle auffordern, die Sitzungssäle zu überprüfen, um sicherzustellen, dass diese technisch abgesichert sind.

Artikel 6

Krypto-Zulassungsstelle (Crypto Approval Authority)

(1) Die Krypto-Zulassungsstelle ist für die Genehmigung der Verwendung von Verschlüsselungstechnologien zuständig.

(2) Die Krypto-Zulassungsstelle gibt Leitlinien zu den Anforderungen an die Verwendung und Genehmigung von Verschlüsselungstechnologien heraus.

(3) Die Krypto-Zulassungsstelle genehmigt die Verwendung von Verschlüsselungslösungen auf Antrag des Systemeigners. Die Genehmigung wird erteilt, wenn mindestens folgende Aspekte als zufriedenstellend bewertet wurden:

a) der Sicherheitsbedarf in Bezug auf die zu schützenden Informationen;

b) ein Überblick über das an der Lösung beteiligte Kommunikations- und Informationssystem;

c) eine Bewertung des inhärenten Risikos und des Restrisikos;

d) eine Beschreibung der vorgeschlagenen Lösung;

e) die sicherheitsbezogenen Betriebsverfahren für die Verschlüsselungslösung.

(4) Die Krypto-Zulassungsstelle führt ein Verzeichnis der genehmigten Verschlüsselungstechnologien.

Artikel 7

Krypto-Verteilungsstelle (Crypto Distribution Authority)

(1) Die Krypto-Verteilungsstelle ist dafür zuständig, das zum Schutz von EU-VS verwendete kryptografische Material (hauptsächlich Verschlüsselungsausrüstung, kryptografische Schlüssel, Zertifikate und zugehörige Authentifikatoren) an folgende Stellen zu verteilen:

a) Nutzer oder Dienststellen innerhalb der Kommission bei Kommunikations- und Informationssystemen, die von externen Parteien verwaltet werden;

b) Nutzer oder Organisationen außerhalb der Kommission bei Kommunikations- und Informationssystemen, die von der Kommission verwaltet werden.

(2) Die Krypto-Verteilungsstelle kann die Verteilung von kryptografischem Material an Dritte gemäß Artikel 17 Absatz 3 des Beschlusses 2015/443 an andere Dienststellen übertragen.

(3) Die Krypto-Verteilungsstelle gewährleistet die Übermittlung des gesamten kryptografischen Materials über sichere Kanäle, die Schutz vor Manipulationen bieten und einen Nachweis etwaiger Manipulationen liefern; dabei gelten die Sicherheitsvorschriften für den Geheimhaltungsgrad der EU-VS, die durch dieses Material geschützt werden.

(4) Die Krypto-Verteilungsstelle berät den LSO und gegebenenfalls den LISO jeder Kommissionsdienststelle, die an der Erstellung, Verbreitung oder Verwendung des kryptografischen Materials beteiligt ist.

(5) Die Krypto-Verteilungsstelle stellt sicher, dass geeignete sicherheitsbezogene Betriebsverfahren für den Verteilungsprozess festgelegt werden.

KAPITEL 3

Kommissionsdienststellen

Artikel 8

Dienststellenleiter

(1) Jeder Dienststellenleiter ernennt

a) einen LSO sowie gegebenenfalls einen oder mehrere Stellvertreter für die Dienststelle oder das Kabinett;

b) einen RCO und gegebenenfalls einen oder mehrere Stellvertreter für jede Dienststelle, die eine EU-VS-Registratur unterhält;

c) einen Systemeigner für jedes Kommunikations- und Informationssystem, in dem EU-VS bearbeitet werden.

(2) Der Dienststellenleiter ersucht den Direktor der Direktion Sicherheit der Generaldirektion Humanressourcen und Sicherheit vor der Ernennung von LSO, stellvertretenden LSO, RCO und stellvertretenden RCO um Genehmigung.

(3) Der Dienststellenleiter ermittelt im Benehmen mit dem LSO alle Dienstposten, für die eine Ermächtigung zum Zugang zu EU-VS erforderlich ist. Die Bewerber für diese Dienstposten werden im Zuge des Einstellungsverfahrens darüber unterrichtet, dass eine solche Ermächtigung erforderlich ist.

(4) Der Leiter einer Dienststelle, die im Besitz von EU-VS ist, ist für die Aktivierung der Notfallpläne für die Auslagerung und Vernichtung von EU-VS zuständig. Die Pläne sehen eine Alternative für Situationen vor, in denen der Dienststellenleiter nicht kontaktiert werden kann.

Artikel 9

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

(1) Im Zuge eines Projekts zur Implementierung eines Kommunikations- und Informationssystems, in dem EU-VS bearbeitet werden, kontaktiert der Systemeigner die Sicherheitsakkreditierungsstelle so früh wie möglich, um die einschlägigen Sicherheitsstandards und -anforderungen festzulegen und das Verfahren der Sicherheitsakkreditierung einzuleiten.

(2) Der Systemeigner stellt sicher, dass die Sicherheitsmaßnahmen den Anforderungen der Sicherheitsakkreditierungsstelle entsprechen und dass EU-VS erst nach erfolgter Akkreditierung im Kommunikations- und Informationssystem bearbeitet werden.

(3) Der Systemeigner kontaktiert die Krypto-Zulassungsstelle zwecks Genehmigung der Verwendung von Verschlüsselungstechnologien. Systemeigner dürfen in Produktionssystemen ohne vorherige Genehmigung keine Verschlüsselungstechnologien einsetzen.

(4) Der Systemeigner konsultiert den LISO der Dienststelle in Fragen der Sicherheit von Kommunikations- und Informationssystemen.

(5) Der Systemeigner überprüft mindestens einmal jährlich die auf ein System angewandten Sicherheitsmaßnahmen, einschließlich des zugehörigen Sicherheitsplans.

(6) Kommt es in einem Kommunikations- und Informationssystem zu einem Sicherheitsvorfall, bei dem dieses System offenbar keinen angemessenen Schutz mehr für EU-VS bieten kann, so unterrichtet der Systemeigner den LSO und setzt sich unverzüglich mit der Sicherheitsakkreditierungsstelle in Verbindung, um Ratschläge zum weiteren Vorgehen einzuholen. In diesem Fall kann die Akkreditierung ausgesetzt und das System so lange außer Betrieb genommen werden, bis geeignete Abhilfemaßnahmen ergriffen wurden.

(7) Der Systemeigner unterstützt die Sicherheitsakkreditierungsstelle jederzeit uneingeschränkt bei ihren Aufgaben im Zusammenhang mit der Akkreditierung des Kommunikations- und Informationssystems.

Artikel 10

Für den Betrieb zuständige Stelle für Informationssicherung (Information Assurance Operational Authority)

Die für den Betrieb des jeweiligen Informations- und Kommunikationssystems zuständige Stelle für Informationssicherung hat folgende Aufgaben:

a) Erstellung der Sicherheitsdokumentation im Einklang mit den Sicherheitskonzepten und -leitlinien, insbesondere Ausarbeitung des Sicherheitsplans, der mit dem System zusammenhängenden sicherheitsbezogenen Betriebsverfahren und der kryptografischen Dokumentation im Rahmen des Akkreditierungsverfahrens für das Kommunikations- und Informationssystem;

b) Mitwirkung bei der 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;

c) Mitwirkung bei der Auswahl der TEMPEST-Sicherheitsmaßnahmen und -vorrichtungen, sofern dies im Sicherheitsplan verlangt wird, und — in Zusammenarbeit mit der TEMPEST-Stelle — Gewährleistung, dass sie sicher installiert und gewartet werden;

d) Überwachung der Implementierung und Anwendung der sicherheitsbezogenen Betriebsverfahren für den Betrieb des Systems;

e) Management und Handhabung von kryptografischen Produkten in Zusammenarbeit mit der Krypto-Verteilungsstelle zur Gewährleistung der ordnungsgemäßen Aufbewahrung von kryptografischem Material und der Kontrolle unterliegendem Material sowie erforderlichenfalls Gewährleistung der Generierung kryptografischer Variablen;

f) Durchführung von Sicherheitsanalysen, -überprüfungen und -tests, insbesondere im Hinblick auf die Erstellung der von der Sicherheitsakkreditierungsstelle verlangten einschlägigen Risikoberichte;

g) Durchführung von für das Kommunikations- und Informationssystem spezifischen Schulungen in Bezug auf Informationssicherung;

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

KAPITEL 4

Lokaler Sicherheitsbeauftragter

Artikel 11

Ernennung des lokalen Sicherheitsbeauftragten (Local Security Officer — LSO)

(1) Der LSO sowie stellvertretende LSO sind Beamte oder Bedienstete auf Zeit.

(2) Alle LSO sowie stellvertretenden LSO müssen im Besitz einer gültigen Sicherheitsermächtigung für den Zugang zu EU-VS bis zum Geheimhaltungsgrad „SECRET UE/EU SECRET“ und erforderlichenfalls bis zum Geheimhaltungsgrad „TRES SECRET UE/EU TOP SECRET“ sein. Der LSO und der stellvertretende LSO müssen die Sicherheitsermächtigung vor ihrer Ernennung erlangen.

(3) Die Vertretungen der Kommission können die Sicherheitsstelle der Kommission ersuchen, eine Ausnahme von den Anforderungen der Absätze 1 und 2 zu gewähren.

Artikel 12

Sicherheitsbezogene Betriebsverfahren für besonders geschützte Bereiche

(1) Der LSO der betreffenden Kommissionsdienststelle erstellt für jeden besonders geschützten Bereich seines Zuständigkeitsbereichs sicherheitsbezogene Betriebsverfahren.

(2) Der LSO stellt sicher, dass die sicherheitsbezogenen Betriebsverfahren folgende Anforderungen enthalten:

a) Nur Bediensteten, die über eine gültige Sicherheitsermächtigung verfügen und nachweislich Zugang zu Dokumenten des Geheimhaltungsrads „CONFIDENTIEL UE/EU CONFIDENTIAL“ oder höher haben müssen, wird während der Bürozeiten unbegleiteter Zugang zu einem besonders geschützten Bereich gewährt;

b) der unbegleitete Zugang zu einem besonders geschützten Bereich außerhalb der Bürozeiten wird nur dem LSO der Dienststelle, dem (den) RCO des besonders geschützten Bereichs, ihren Stellvertretern und ermächtigten Bediensteten der Direktion Sicherheit der Generaldirektion Humanressourcen und Sicherheit gewährt;

c) Aufzeichnungs- und Kommunikationsgeräte wie Mobiltelefone, Computer, Kameras oder andere intelligente Geräte sind in besonders geschützten Bereichen ohne vorherige Genehmigung durch die Sicherheitsstelle der Kommission nicht gestattet; jede Ausnahme ist vorab bei der Sicherheitsstelle der Kommission zu beantragen; der LSO fungiert als Kontaktstelle;

d) das gesamte interne oder externe Personal, das Zugang zu einem besonders geschützten Bereich benötigt, aber die unter Buchstabe a genannten Kriterien nicht erfüllt, wird von einem dazu ermächtigten Bediensteten jederzeit begleitet und überwacht; jeder derartige Zugang zu einem besonders geschützten Bereich ist in einem Logbuch am Eingang des besonders geschützten Bereichs zu erfassen;

e) der LSO stellt sicher, dass die Einbruchmeldeanlagen zur Überwachung eines besonders geschützten Bereichs jederzeit scharf geschaltet sind und ordnungsgemäß funktionieren, und verwaltet alle damit zusammenhängenden Passwörter, Schlüssel, PINs oder andere Zugangs- und Authentifizierungsmechanismen;

f) Alarme in einem besonders geschützten Bereich werden der Direktion Sicherheit der Generaldirektion Humanressourcen und Sicherheit gemeldet, die unverzüglich den LSO benachrichtigt;

g) der LSO der Dienststelle, in der sich der besonders geschützte Bereich befindet, führt Aufzeichnungen über jede Intervention nach einem Alarm oder Sicherheitsvorfall;

h) es müssen Verfahren für den Alarmfall oder andere Notfallsituationen innerhalb des besonders geschützten Bereichs vorhanden sein, einschließlich Verfahren für die Evakuierung des Personals und der Gewährleistung einer raschen Reaktion eines Notfallteams unter der Aufsicht der Sicherheitsstelle der Kommission und gegebenenfalls externer Notfalldienste;

i) der LSO meldet der Sicherheitsstelle der Kommission unverzüglich jede Sicherheitsverletzung innerhalb eines besonders geschützten Bereichs oder im Zusammenhang mit einem solchen Bereich, um eine angemessene Reaktion festzulegen;

j) einzelne Büros, Räume und Panzerschränke innerhalb eines besonders geschützten Bereichs sind stets abzuschließen, wenn sie unbeaufsichtigt bleiben;

k) das Personal darf sich in den Gängen oder anderen gemeinsam genutzten Räumlichkeiten des besonders geschützten Bereichs nicht über Verschlusssachen unterhalten, wenn sich unbefugte Personen in der Nähe befinden.

Artikel 13

Sicherheitsschlüssel und Kombinationen

(1) Der LSO trägt die Gesamtverantwortung für die ordnungsgemäße Handhabung und Verwahrung von Schlüsseln und Kombinationen, die in besonders geschützten Bereichen oder für den Zugang dazu verwendet werden. Schlüssel und Kombinationen sind in einem Sicherheitskasten zu verwahren und mindestens auf Ebene desselben Geheimhaltungsgrades schützen wie das Material, zu dem sie den Zugang ermöglichen.

(2) Der LSO führt ein Verzeichnis der Sicherheitskästen und Tresorräume sowie eine aktuelle Liste aller Bediensteten, die unbegleitet Zugang dazu haben.

(3) Der LSO führt ein Register der Schlüssel für Sicherheitskästen und Tresorräume, einschließlich der Bediensteten, denen sie zugewiesen sind. Für jeden ausgegebenen Schlüssel wird eine Bestätigung aufbewahrt, einschließlich der Identifikationsnummer des Schlüssels, des Empfängers, des Datums und der Uhrzeit.

(4) Schlüssel und Kombinationen werden nur Bediensteten ausgehändigt, die Kenntnis von Verschlusssachen haben müssen und denen die entsprechende Ermächtigung für den Zugang zu EU-VS erteilt wurde. Der LSO muss jeden Schlüssel zurückverlangen, wenn diese Bedingungen nicht mehr erfüllt sind.

(5) Der LSO bewahrt Ersatzschlüssel sowie eine schriftliche Aufzeichnung der einzelnen Kombinationen in einzelnen versiegelten, undurchsichtigen, unterzeichneten und datierten Umschlägen auf, die von dem für die Schlüssel verantwortlichen Bediensteten zur Verfügung zu stellen sind. Diese Umschläge werden in einem Sicherheitskasten verwahrt, der für das Material mit dem höchsten Geheimhaltungsgrad, das im entsprechenden Behälter oder Tresorraum verwahrt wird, zugelassen ist.

(6) Wird bei einer Kombinationsänderung oder einem Schlüsselwechsel im Rahmen der Rotation festgestellt, dass ein Umschlag Spuren einer Manipulation oder Beschädigung aufweist, so behandelt der LSO dies als Sicherheitsvorfall und informiert die Sicherheitsstelle der Kommission unverzüglich hierüber.

(7) Änderungen der Kombinationseinstellungen von Sicherheitskästen in besonders geschützten Bereichen sind unter Aufsicht des LSO vorzunehmen. Kombinationen werden mindestens alle zwölf Monate und immer dann zurückgesetzt, wenn

a) ein neuer Kasten in Empfang genommen oder ein neues Schloss installiert wird (insbesondere sind die Standardkombinationen unverzüglich zu ändern);

b) eine Kompromittierung vermutet wird oder erfolgt ist;

c) eine Person, die eine Kombination besitzt, keinen Zugang mehr benötigt.

(8) Der LSO führt Aufzeichnungen über das jeweilige Datum der Kombinationsänderungen gemäß Absatz 7.

Artikel 14

Notfallpläne für die Evakuierung und Vernichtung von EU-VS

(1) Der LSO unterstützt den Dienststellenleiter bei der Erstellung von Notfallplänen für die Evakuierung und Vernichtung von EU-VS; die Grundlage hierfür bieten die Leitlinien der HR.DS.

(2) Der LSO stellt sicher, dass die gesamte für die Durchführung der in Absatz 1 genannten Pläne erforderliche Ausrüstung leicht zugänglich und stets betriebsbereit ist.

(3) Der LSO überprüft zusammen mit den in den Plänen nach Absatz 1 genannten Beamten mindestens alle zwölf Monate den Stand der Pläne und ergreift die zu ihrer Aktualisierung erforderlichen Maßnahmen.

Artikel 15

Sicherheitsermächtigungen

(1) Der LSO führt Aufzeichnungen über alle Dienstposten innerhalb der Dienststelle, für die eine Sicherheitsermächtigung der Kommission erforderlich ist, sowie über das Personal, das diese Dienstposten innehat. Im Zuge des Einstellungsverfahrens ist in der Stellenausschreibung anzugeben, dass eine Sicherheitsermächtigung erforderlich ist; ferner ist der Bewerber beim Bewerbungsgespräch darauf hinzuweisen.

(2) Der LSO überwacht alle Anträge auf Erteilung von Sicherheitsermächtigungen für den Zugang zu EU-VS. Der LSO ist der Ansprechpartner innerhalb der Dienststelle und setzt sich bezüglich der Sicherheitsermächtigungen mit der Sicherheitsstelle der Kommission in Verbindung.

(3) Der LSO leitet den Antrag auf Einleitung des Sicherheitsermächtigungsverfahren für den betreffenden Bediensteten ein und stellt sicher, dass dieser den Fragebogen für die nationale Sicherheitsüberprüfung zügig an die Sicherheitsstelle der Kommission zurücksendet.

(4) Der LSO stellt sicher, dass die sicherheitsüberprüften Bediensteten der Dienststelle die vorgeschriebene EU-VS-Unterweisung absolvieren, um ihre Sicherheitsermächtigung zu erhalten.

(5) Der LSO steht mit der Personalabteilung der Dienststelle hinsichtlich aller Änderungen in Bezug auf Dienstposten, für die eine Sicherheitsermächtigung erforderlich ist, in regelmäßigem Kontakt, und unterrichtet die Sicherheitsstelle der Kommission unverzüglich über diese Änderungen.

(6) Der LSO unterrichtet die Sicherheitsstelle der Kommission, wenn ein neuer Mitarbeiter mit gültiger Sicherheitsüberprüfung einen Dienstposten antritt, für den eine Sicherheitsermächtigung erforderlich ist.

(7) Der LSO stellt sicher, dass die Mitarbeiter der Dienststelle das Verfahren zur Erneuerung einer Sicherheitsüberprüfung innerhalb der vorgeschriebenen Frist abschließen. Jeder Bedienstete, der sich weigert, das Verfahren zu durchlaufen, wird auf einen Dienstposten versetzt, für den keine Sicherheitsermächtigung erforderlich ist.

Artikel 16

EU-VS-Registratur

(1) Unterhält eine Dienststelle eine EU-VS-Registratur, so überwacht der LSO die Tätigkeiten der RCO bezüglich der Bearbeitung von EU-VS und der Einhaltung der Sicherheitsvorschriften für den Schutz von EU-VS.

(2) Der LSO führt mindestens alle zwölf Monate sowie bei einem Wechsel des RCO oder stellvertretenden RCO folgende Überprüfungen durch:

a) Überprüfung einer Stichprobe von Dokumenten in der EU-VS-Registratur zur Bestätigung ihres Status und der Korrektheit des Verschlusssachenregisters;

b) Überprüfung einer Stichprobe von Empfangs- und Übermittlungsbestätigungen für die Übermittlung von EU-VS an die und aus der EU-VS-Registratur;

c) Überprüfung einer Stichprobe von Vernichtungsbescheinigungen.

(3) Der LSO überprüft mindestens einmal pro Monat stichprobenartig das Verschlusssachenregister sowie kürzlich eingegangene Verschlusssachen, um sicherzustellen, dass die Dokumente ordnungsgemäß registriert werden.

(4) Alle Überprüfungen werden im Verzeichnis des Verschlusssachenregisters protokolliert.

Artikel 17

Sonstige Sicherheitsaufgaben

Die sonstigen Sicherheitsaufgaben des LSO werden in einem Sicherheitsvermerk speziell zu den Aspekten physische Sicherheit von Personen, Räumlichkeiten und andere Vermögenswerte sowie Informationen dargelegt.

KAPITEL 5

Registraturkontrollbeauftragter

Artikel 18

Ernennung des Registraturkontrollbeauftragten (Registry Control Officer — RCO)

(1) Der RCO sowie stellvertretende RCO sind Beamte oder Bedienstete auf Zeit.

(2) Alle RCO sowie stellvertretenden RCO müssen im Besitz einer gültigen Sicherheitsermächtigung für den Zugang zu EU-VS bis zum Geheimhaltungsgrad „SECRET UE/EU SECRET“ und erforderlichenfalls bis zum Geheimhaltungsgrad „TRES SECRET UE/EU TOP SECRET“ sein. Der RCO und der stellvertretende RCO müssen die Sicherheitsermächtigung vor ihrer Ernennung erlangen.

(3) Die Vertretungen der Kommission können die Sicherheitsstelle der Kommission ersuchen, eine Ausnahme von den Anforderungen der Absätze 1 und 2 zu gewähren.

Artikel 19

Zuständigkeiten

(1) RCO registrieren Verschlusssachen des Geheimhaltungsgrades „CONFIDENTIEL UE/EU CONFIDENTIAL“ oder höher zu Sicherheitszwecken,

a) wenn sie in einer Dienststelle der Kommission eingehen oder diese verlassen oder

b) wenn sie in einem Kommunikations- und Informationssystem eingehen oder dieses verlassen.

(2) RCO registrieren alle Ereignisse im Lebenszyklus aller Verschlusssachen des Geheimhaltungsgrades „CONFIDENTIEL UE/EU CONFIDENTIAL“ oder höher. RCO stellen ferner sicher, dass über alle als „RESTREINT UE/EU RESTRICTED“ oder gleichwertig eingestuften Verschlusssachen, die mit Drittländern und internationalen Organisationen ausgetauscht werden, Aufzeichnungen geführt werden. Dies erfolgt in Abstimmung mit der vom Generalsekretariat verwalteten EU-VS-Registratur.

(3) Der RCO registriert Dokumente des Geheimhaltungsgrades „CONFIDENTIEL UE/EU CONFIDENTIAL“ oder höher im Verschlusssachenregister und sorgt dafür, dass sie sicher in der EU-VS-Registratur aufbewahrt werden.

(4) Der RCO unterstützt die Bediensteten der Kommission bei der Erstellung und Übermittlung von als „CONFIDENTIEL UE/EU CONFIDENTIAL“ oder höher eingestuften Verschlusssachen.

(5) Gehen als „CONFIDENTIEL UE/EU CONFIDENTIAL“ oder höher eingestufte Dokumente von anderen Dienststellen oder externen Parteien ein, so stellt der RCO sicher, dass die Empfangsbestätigung ordnungsgemäß an den Herausgeber zurückgesandt wird.

(6) Bevor einem Bediensteten der Zugang zu einer in der EU-VS-Registratur verwahrten Verschlusssache gewährt wird, vergewissert sich der RCO beim LSO, dass der Bedienstete im Besitz einer Sicherheitsermächtigung der Sicherheitsstelle der Kommission ist.

(7) Der RCO führt ein Verzeichnis aller Personen, die die EU-VS-Registratur betreten und verlassen und nicht zum unbegleiteten Zugang berechtigt sind, und begleitet diese Personen während der Dauer ihres dortigen Verweilens.

(8) Entnimmt ein Bediensteter ein Dokument zur Einsichtnahme aus der EU-VS-Registratur, so stellt der RCO sicher, dass der Betreffende die einschlägigen ausgleichenden Sicherheitsmaßnahmen kennt und das Dokument zurückbringt, sobald es nicht mehr benötigt wird. Der RCO erinnert das Personal daran, solche Dokumente so bald wie möglich zurückzubringen.

(9) Die EU-VS-Registratur stellt einen Kurierausweis aus, wenn Verschlusssachen außerhalb des Landes, in dem sich die Registratur befindet, in persönlichem Gewahrsam befördert werden.

(10) Detaillierte Anweisungen für RCO bezüglich der Registrierung von Verschlusssachen werden in einem Sicherheitsvermerk festgelegt.

Artikel 20

Herabstufung und Aufhebung des Geheimhaltungsgrades

Der RCO unterstützt die herausgebenden Dienststellen beim Verfahren der Überprüfung registrierter EU-VS, um festzustellen, ob der ursprüngliche Geheimhaltungsgrad eines Dokuments noch angemessen ist oder ob er herabgestuft oder aufgehoben werden kann.

Artikel 21

Vernichtung

(1) Der RCO ist dafür verantwortlich, dass Verschlusssachen des Geheimhaltungsgrades „CONFIDENTIEL UE/EU CONFIDENTIAL“ und höher mit geeigneten Mitteln, gegebenenfalls in Anwesenheit von sicherheitsüberprüften Zeugen, vernichtet werden.

(2) Der RCO protokolliert jegliche Vernichtung von Verschlusssachen des Geheimhaltungsgrades „CONFIDENTIEL UE/EU CONFIDENTIAL“ oder höher im Verschlusssachenregister und bewahrt die entsprechenden Vernichtungsbescheinigungen in der EU-VS-Registratur auf.

Artikel 22

Weitere Aufgaben

(1) Der RCO leistet dem LSO jede erforderliche Unterstützung, wenn dieser Aufsichtstätigkeiten in der EU-VS-Registratur ausübt.

(2) Der RCO meldet dem LSO alle mutmaßlichen oder tatsächlichen Sicherheitsvorfälle, die dieser wiederum der Sicherheitsstelle der Kommission meldet.

(3) Der RCO der EU-VS-Registratur einer Kommissionsdienststelle, die eine vertrauliche Sitzung auf Ebene des Geheimhaltungsgrades „CONFIDENTIEL UE/EU CONFIDENTIAL“ oder höher organisiert, bereitet die während der Sitzung zu behandelnden EU-VS vor und stimmt sich mit dem Organisator ab, um sicherzustellen, dass alle Dokumente und Bescheinigungen im Einklang mit den einschlägigen Vorschriften behandelt werden.

KAPITEL 6

Schlussbestimmungen

Artikel 23

Transparenz

Dieser Beschluss wird den Bediensteten der Kommission und allen Personen, für die er gilt, zu Kenntnis gebracht und im *Amtsblatt der Europäischen Union* veröffentlicht.

Artikel 24

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

Brüssel, den 7. April 2022

Für die Kommission,
im Namen der Präsidentin,
Gertrud INGESTAD
Generaldirektorin
Generaldirektion Humanressourcen und Sicherheit