Rat der
Europäischen Union

Brüssel, den 28. März 2022
(OR. en)

7670/22

Interinstitutionelles Dossier:
2022/0084(COD)

CSC 128
CSCI 45
CYBER 100
INST 99
INF 40
CODEC 385
IA 34

VORSCHLAG

Absender:	Frau Martine DEPREZ, Direktorin, im Auftrag der Generalsekretärin der Europäischen Kommission
Eingangsdatum:	22. März 2022
Empfänger:	Herr Jeppe TRANHOLM-MIKKELSEN, Generalsekretär des Rates der Europäischen Union
Nr. Komm.dok.:	COM(2022) 119 final
Betr.:	Vorschlag für eine VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES über die Informationssicherheit in den Organen, Einrichtungen und sonstigen Stellen der Union

Die Delegationen erhalten in der Anlage das Dokument COM(2022) 119 final.

Anl.: COM(2022) 119 final

EUROPÄISCHE
KOMMISSION

Brüssel, den 22.3.2022
COM(2022) 119 final

2022/0084 (COD)

Vorschlag für eine

VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES

über die Informationssicherheit in den Organen, Einrichtungen und sonstigen Stellen der Union

{SWD(2022) 65 final} - {SWD(2022) 66 final}

BEGRÜNDUNG

1. KONTEXT DES VORSCHLAGS

• Gründe und Ziele des Vorschlags

Dieser Vorschlag ist Teil der EU-Strategie für eine Sicherheitsunion[1], die die Kommission am 24. Juli 2020 angenommen hat und in der sie sich verpflichtet, den Mehrwert der Europäischen Union für die nationalen Bemühungen im Bereich der Sicherheit einzubringen. Teil dieser Verpflichtung ist die Initiative zur Straffung des internen Rechtsrahmens für die Informationssicherheit in allen Organen und Einrichtungen der Union.

Ein zentrales Element der vom Europäischen Rat im Juni 2019 angenommenen Strategischen Agenda für 2019–2024 ist der Schutz unserer Gesellschaft vor den sich ständig wandelnden Bedrohungen, die sich gegen die Informationen richten, mit denen die Organe und Einrichtungen umgehen. In seinen Schlussfolgerungen[2] ersucht der Europäische Rat insbesondere „die EU-Institutionen, zusammen mit den Mitgliedstaaten Maßnahmen auszuarbeiten, um die Resilienz zu stärken und die Sicherheitskultur der EU hinsichtlich Cyberbedrohungen und hybrider Bedrohungen von außerhalb der EU zu verbessern und die Kommunikations- und Informationsnetze der EU sowie ihre Entscheidungsprozesse besser vor böswilligen Aktivitäten aller Art zu schützen."

In diesem Sinne kam der Rat (Allgemeine Angelegenheiten) im Dezember 2019[3] zu dem Schluss, dass die Organe und Einrichtungen der EU mit Unterstützung der Mitgliedstaaten ein umfassendes Paket von Maßnahmen zur Gewährleistung ihrer Sicherheit entwickeln und umsetzen sollten. Dies spiegelt eine seit langem bestehende Forderung des Sicherheitsausschusses des Rates wider, einen gemeinsamen Kern von Sicherheitsvorschriften für den Rat, die Kommission und den Europäischen Auswärtigen Dienst[4] zu erarbeiten.

Gegenwärtig haben die Organe und Einrichtungen der Union entweder ihre eigenen Vorschriften für die Informationssicherheit, die auf ihrer Geschäftsordnung oder ihrem Gründungsakt beruhen, oder sie haben überhaupt keine Vorschriften für die Informationssicherheit. Dies ist vor allem bei einigen kleinen Einrichtungen der Fall, die über keine formelle Informationssicherheitsstrategie verfügen.

Aufgrund der ständig wachsenden Menge an vertraulichen, nicht als Verschlusssache eingestuften und als EU-Verschlusssachen eingestuften Informationen (im Folgenden „EU-VS"), die die Organe und Einrichtungen der Union untereinander austauschen müssen, und angesichts der dramatischen Entwicklung der Bedrohungslage ist die europäische Verwaltung in allen ihren Tätigkeitsbereichen Angriffen ausgesetzt. Die von den Organen und Einrichtungen der Union bearbeiteten Informationen sind ein sehr attraktives Ziel für die Angreifer und müssen angemessen geschützt werden. Hierzu sind umgehend Maßnahmen zu ergreifen, um den Schutz dieser Informationen zu verbessern.

Aus diesem Grund und um den Schutz der von der europäischen Verwaltung bearbeiteten Informationen zu verbessern, sollen mit dieser Initiative die verschiedenen Rechtsrahmen der Organe und Einrichtungen der Union in diesem Bereich mit folgenden Maßnahmen gestrafft werden:

---

1 Mitteilung über die EU-Strategie für eine Sicherheitsunion, COM(2020) 605, 24. Juli 2020 (Strategische Priorität „Ein zukunftsfähiges Sicherheitsumfeld").

2 EUCO 9/19.

3 14972/19.

4 WK 10563/2018 INIT Abschnitt 9.

- Festlegung harmonisierter und umfassender Kategorien von Informationen sowie gemeinsamer Vorschriften für den Umgang mit Informationen für alle Organe und Einrichtungen der Union
- Einrichtung eines effizienten Systems der Zusammenarbeit im Bereich der Informationssicherheit zwischen den Organen und Einrichtungen der Union, das eine kohärente Kultur der Informationssicherheit in der gesamten europäischen Verwaltung fördern kann
- Modernisierung der Strategien zur Informationssicherheit auf allen Ebenen der Klassifizierung/Kategorisierung für alle Organe und Einrichtungen der Union unter Berücksichtigung des digitalen Wandels und der Entwicklung der Telearbeit als strukturelle Praxis
- **Kohärenz mit den bestehenden Vorschriften in diesem Bereich**

Diese Initiative steht im Einklang mit einer Vielzahl von EU-Maßnahmen im Bereich der Sicherheit und Informationssicherheit.

Bereits 2016 erließen das Europäische Parlament und der Rat eine Richtlinie[5] über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union. Diese Richtlinie war die erste unionsweite Legislativmaßnahme, mit der die Zusammenarbeit zwischen den Mitgliedstaaten im Bereich der Cybersicherheit verstärkt werden sollte. Die Kommission hat zwar im Dezember 2020 einen Vorschlag zur Überarbeitung dieses Instruments angenommen, mit dem Aufsichtsmaßnahmen für die nationalen Behörden eingeführt werden, die Verwaltung der Union fällt jedoch weiterhin nicht in den Anwendungsbereich dieses Instruments.

In diesem Sinne und zur Ergänzung der Bemühungen der Mitgliedstaaten im Bereich der Sicherheit ist es von größter Bedeutung, dass die Organe und Einrichtungen der Union ein hohes Schutzniveau für ihre Informationen und die damit verbundenen Informations- und Kommunikationssysteme erreichen, um die Informationssicherheit zu gewährleisten.

Im Juli 2020 nahm die Kommission die Strategie für eine Sicherheitsunion[6] an, mit der sich die EU umfassend verpflichtet, die Anstrengungen der Mitgliedstaaten in allen Bereichen der Sicherheit zu ergänzen. Diese Strategie läuft von 2020 bis 2025 und umfasst vier strategische Prioritäten: ein zukunftsfähiges Sicherheitsumfeld, der Umgang mit sich wandelnden Bedrohungen, der Schutz der Europäerinnen und Europäer vor Terrorismus und organisierter Kriminalität und eine starke europäische Sicherheitsgemeinschaft. Im Mittelpunkt verschiedener Themen, die im Rahmen dieser Prioritäten angegangen werden, stehen die Informationssicherheit, die Cybersicherheit, die Zusammenarbeit und der Informationsaustausch sowie kritische Infrastrukturen.

Im Einklang mit der Strategie für eine Sicherheitsunion schlägt die Europäische Kommission die Schaffung von Mindestvorschriften für die Informationssicherheit in allen Organen und Einrichtungen der Union vor, das verbindliche und hohe gemeinsame Standards für den sicheren Austausch von Informationen vorsieht. Mit dieser Initiative setzen sich die Organe und Einrichtungen dafür ein, dass innerhalb der europäischen Verwaltung das gleiche Maß an Ehrgeiz im Bereich der Sicherheit herrscht, wie es von den Mitgliedstaaten gefordert wird.

---

5 Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union (ABl. L 194 vom 19.7.2016, S. 1).

6 C(2020) 605.

Am 16. Dezember 2020 stellten die Kommission und die Hohe Vertreterin für Außen- und Sicherheitspolitik eine neue Cybersicherheitsstrategie der EU[7] vor. Darin werden Prioritäten und Handlungsbereiche festgelegt, um Europas Resilienz, Autonomie, Führungsrolle und operative Kapazitäten angesichts der wachsenden und komplexen Bedrohungen für seine Netz- und Informationssystem aufzubauen und einen globalen und offenen Cyberraum und die diesbezüglichen internationalen Partnerschaften zu fördern. Ebenso wichtig ist es, dass die Organe und Einrichtungen der Union zur Verwirklichung dieser Prioritäten beitragen, indem sie gleichwertige Anforderungen im Bereich der Informations- und Cybersicherheit festlegen.

Mit diesem Vorschlag und dem Vorschlag für eine Verordnung über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in den Organen, Einrichtungen und sonstigen Stellen der Union soll der Regelungsrahmen der Strategie für eine Sicherheitsunion durch spezielle Anforderungen an die europäische Verwaltung vervollständigt werden. Angesichts der Verflechtungen zwischen Informationssicherheit und Cybersicherheit sollte bei diesen beiden Vorschlägen ein kohärenter Ansatz für den Schutz von nicht als Verschlusssache eingestuften Informationen gewährleistet werden.

- **Kohärenz mit der Politik der Union in anderen Bereichen**

Diese Initiative trägt auch der Politik der Union in anderen Bereichen Rechnung, die für die Informationssicherheit von Bedeutung sind.

Im Bereich des Datenschutzes gilt für die Verwaltung der Europäischen Union und der Europäischen Atomgemeinschaft (im Folgenden „Euratom“) die Verordnung (EU) 2018/1725[8] zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen und sonstigen Stellen der Union und zum freien Datenverkehr. In diesem Zusammenhang ist auch zu erwähnen, dass die EU-Gesetzgeber für einige Organe und Einrichtungen der Union spezielle Vorschriften zum Schutz personenbezogener Daten erlassen haben.

Im Bereich der Transparenz stützt sich dieser Vorschlag auf die Grundsätze der Verordnung (EG) Nr. 1049/2001[9] über den Zugang der Öffentlichkeit zu Dokumenten des Europäischen Parlaments, des Rates und der Kommission sowie auf andere einschlägige Vorschriften.

2. RECHTSGRUNDLAGE, SUBSIDIARITÄT UND VERHÄLTNISMÄßIGKEIT

- **Rechtsgrundlage**

In Anbetracht des Ziels und des Inhalts dieses Vorschlags ist die geeignetste Rechtsgrundlage Artikel 298 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV) und Artikel 106a des Vertrags zur Gründung der Europäischen Atomgemeinschaft.

Artikel 298 AEUV wurde durch den Vertrag von Lissabon eingeführt und ermöglicht es dem Gesetzgeber, Bestimmungen zur Schaffung einer effizienten und unabhängigen Verwaltung

---

[7] Die Cybersicherheitsstrategie der EU für die digitale Dekade | Gestaltung der digitalen Zukunft Europas (europa.eu) einschließlich einer Gemeinsamen Mitteilung mit der Hohen Vertreterin der Union für Außen- und Sicherheitspolitik (JOIN(2020) 18) und einer überarbeiteten Richtlinie über Netz- und Informationssicherheit (NIS) (COM(2020) 823).

[8] Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates vom 23. Oktober 2018 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen und sonstigen Stellen der Union, zum freien Datenverkehr und zur Aufhebung der Verordnung (EG) Nr. 45/2001 und des Beschlusses Nr. 1247/2002/EG (ABl. L 295 vom 21.11.2018, S. 39).

[9] Verordnung (EG) Nr. 1049/2001 des Europäischen Parlaments und des Rates vom 30. Mai 2001 über den Zugang der Öffentlichkeit zu Dokumenten des Europäischen Parlaments, des Rates und der Kommission (ABl. L 145 vom 31.5.2001, S. 43).

zu erlassen, die die Organe, Einrichtungen und sonstigen Stellen bei der Ausübung ihrer Aufgaben unterstützt.

Eine effiziente und unabhängige Verwaltung ist auf die Sicherheit ihrer Informationen angewiesen. Damit die Organe und Einrichtungen der Union ihre Aufgaben ausüben können, benötigen sie eine sichere Umgebung für die Informationen, die sie täglich bearbeiten und speichern. Die Bereitstellung einer gemeinsamen Grundlage von Standards, die für alle verbindlich sind, würde zudem ein hohes Sicherheitsniveau gewährleisten, das Risiko von Schwachstellen bei der Unterstützung der Interoperabilität zwischen den Organen und Einrichtungen verringern und Synergien nutzen, wodurch die Resilienz der Verwaltung gegenüber den sich wandelnden Bedrohungen verbessert würde.

Mit dem übergeordneten Ziel, ein hohes gemeinsames Sicherheitsniveau für EU-VS und nicht als Verschlusssache eingestufte Informationen, die von den Organen und Einrichtungen der Union bearbeitet und gespeichert werden, zu erreichen, ermöglicht dieser Vorschlag der europäischen Verwaltung einen besseren Schutz vor äußeren Eingriffen und Spionagetätigkeiten.

Artikel 298 AEUV ermöglicht es der Union, gemeinsame Vorschriften für die gesamte europäische Verwaltung festzulegen, um sicherzustellen, dass alle Organe und Einrichtungen der Union EU-VS und nicht als Verschlusssache eingestufte Informationen in gleicher Weise behandeln. Insofern werden in dieser Verordnung Vorschriften für die Verwaltung festgelegt, wobei mittelbar nur den Personen Verpflichtungen auferlegt werden können, die Aufgaben im Namen dieser Verwaltung oder auf vertraglicher Grundlage erfüllen (dies gilt nicht für die Kommissionsmitglieder, die im Rat handelnden Vertreter der Mitgliedstaaten, die Mitglieder des Europäischen Parlaments, die Richter der Gerichte der Union oder die Mitglieder des Europäischen Rechnungshofs).

Gemäß Artikel 298 AEUV beschließen das Europäische Parlament und der Rat gemäß dem ordentlichen Gesetzgebungsverfahren durch eine Verordnung.

Für diesen Vorschlag ist eine zusätzliche Rechtsgrundlage erforderlich, da er auch Informationen im Zusammenhang mit einigen Tätigkeiten der Europäischen Atomgemeinschaft abdeckt. Bei diesen Informationen handelt es sich nicht um Euratom-Verschlusssachen, doch werden sie von den Organen und Einrichtungen der Union nach der allgemeinen Regelung für EU-VS behandelt.

Diese zusätzliche Rechtsgrundlage ist Artikel 106a des Vertrags zur Gründung der Europäischen Atomgemeinschaft, durch den Artikel 298 AEUV auch auf die oben genannten Euratom-Tätigkeiten anwendbar wird.

- **Subsidiarität (bei nicht ausschließlicher Zuständigkeit)**

Nach dem in Artikel 5 Absatz 3 des Vertrags über die Europäische Union verankerten Subsidiaritätsprinzip wird die EU nur tätig, sofern und soweit die angestrebten Ziele auf Ebene der Mitgliedstaaten nicht ausreichend erreicht werden können und daher wegen ihres Umfangs oder ihrer Wirkungen besser auf EU-Ebene zu verwirklichen sind.

Da nur die Union Vorschriften für EU-VS und nicht als Verschlusssache eingestufte vertrauliche Informationen erlassen kann, die von den Organen und Einrichtungen der Union bearbeitet und gespeichert werden, findet das Subsidiaritätsprinzip keine Anwendung.

- **Verhältnismäßigkeit**

Die Schaffung einer gemeinsamen Grundlage für die Informationssicherheit aller Organe und Einrichtungen der Union ist notwendig, um eine unabhängige und effiziente Verwaltung zu gewährleisten.

Im Einklang mit dem in Artikel 5 Absatz 4 EUV verankerten Grundsatz der Verhältnismäßigkeit sind die Bestimmungen der Verordnung nicht übermäßig präskriptiv und lassen Raum für verschiedene Ebenen spezifischer Maßnahmen, die dem Sicherheitsniveau der einzelnen Organe und Einrichtungen der Union entsprechen.

Außerdem hat die Lösung nur begrenzte Auswirkungen auf die Grundrechte des Einzelnen. Insofern geht der Vorschlag nicht über das Maß hinaus, das notwendig ist, um das Problem der fehlenden gemeinsamen Vorschriften für die Informationssicherheit für alle Organe und Einrichtungen der Union zu lösen.

- **Wahl des Instruments**

Eine Verordnung auf der Grundlage von Artikel 298 AEUV wird als das geeignete Rechtsinstrument angesehen.

Die Wahl einer Verordnung als Rechtsinstrument ist dadurch gerechtfertigt, dass Elemente überwiegen, die eine einheitliche Anwendung ohne Umsetzungsspielraum der Organe und Einrichtungen der Union erfordern und durch die ein minimaler horizontaler Rahmen geschaffen wird.

3. ERGEBNISSE DER EX-POST-BEWERTUNG, DER KONSULTATION DER INTERESSENTRÄGER UND DER FOLGENABSCHÄTZUNG

- **Ex-post-Bewertung/Eignungsprüfungen bestehender Rechtsvorschriften**

Entfällt.

- **Konsultation der Interessenträger**

Die Kommission hat eine umfassende Konsultation der wichtigsten Interessenträger zu verschiedenen Aspekten der Vorschriften für die Informationssicherheit der Organe und Einrichtungen der Union durchgeführt. Übergeordnetes Ziel der Konsultation war es, relevante Beiträge für die Ausarbeitung einer Gesetzesinitiative zu gemeinsamen Vorschriften für die Informationssicherheit für alle Organe und Einrichtungen der Union zu sammeln. Mit den Konsultationen sollten Beiträge zu folgenden Themen gesammelt werden:

- Probleme im Zusammenhang mit dem bestehenden Rahmen für die Informationssicherheit in den Organen und Einrichtungen der Union, die nach Ansicht der Interessenträger in der Initiative berücksichtigt werden sollten
- Relevanz, Wirksamkeit, Effizienz und Mehrwert der Initiative
- erwartete Auswirkungen der Initiative und mögliche weitere Folgen für die Interessenträger

Bei der Ausarbeitung dieses Legislativvorschlags hat die Kommission die folgenden Kategorien von Interessenträgern konsultiert:

1. Organe, Einrichtungen, Ämter und Agenturen der Europäischen Union
2. Nationale Sicherheitsbehörden in den Mitgliedstaaten
3. Sachverständige der Gemeinsamen Forschungsstelle der Kommission

In Anbetracht der Besonderheit dieser Initiative, die ausschließlich für die Organe und Einrichtungen der Union gilt und nur geringe Auswirkungen auf die europäischen Bürger und Bürgerinnen sowie Unternehmen hat, haben die Kommissionsdienststellen beschlossen, der Sammlung von Standpunkten der relevanten Interessenträger Vorrang einzuräumen. Daher wurde speziell für diese Gesetzesinitiative **keine öffentliche Konsultation durchgeführt**.

Während des Konsultationsprozesses haben die Kommissionsdienststellen verschiedene **Konsultationsmethoden und -formen** angewandt:

1. Gelegenheit für alle interessierten Parteien, über die Plattform „Ihre Meinung zählt“ der Kommission Rückmeldung zur Folgenabschätzung in der Anfangsphase zu geben
2. ein gezielter Fragebogen an die Sachverständigen für Informationssicherheit in den Organen und Einrichtungen der Union über eine Online-Umfrage der EU
3. ein gezielter Fragebogen an die nationalen Sicherheitsbehörden der Mitgliedstaaten über eine Online-Umfrage der EU
4. ein Antrag auf eine maßgeschneiderte Risikobewertung der wichtigsten Komponenten der Informationssicherheit
5. zahlreiche Sitzungen und Gespräche mit Vertretern von Organen, Einrichtungen, Ämtern und Agenturen sowie mit den nationalen Sicherheitsbehörden der Mitgliedstaaten

Als wichtigste Ergebnisse der Konsultation hebt die Kommission die folgenden Punkte hervor:

- Die Uneinheitlichkeit der einschlägigen Rechtsrahmen der Organe und Einrichtungen der EU führt zu erheblicher Doppelarbeit bei der Erstellung und Aufrechterhaltung interner Vorschriften sowie zu nicht miteinander kompatiblen Verfahren im Umgang mit Informationen. Die Verschiedenartigkeit dieser Vorschriften erhöht für die Mitgliedstaaten das Risiko von Missverständnissen, Fehlinterpretationen und Nichteinhaltung.
- Durch die Festlegung einer gemeinsamen Grundlage für die Informationssicherheit aller Organe und Einrichtungen der Union würde zwar ein System mit standardisierten Sicherheitsvorschriften und bewährten Verfahren geschaffen, doch sind die Vielfalt und das unterschiedliche Tätigkeitsumfeld der einzelnen Organe und Einrichtungen der Union zu berücksichtigen, und es sollten lokale Lösungen zugelassen werden.
- Diese Initiative sollte die Autonomie und den unterschiedlichen Entwicklungsstand der Informationssicherheit der einzelnen Organe und Einrichtungen der Union respektieren, die für ihre Organisation der Informationssicherheit voll verantwortlich bleiben.

- **Einholung und Nutzung von Expertenwissen**

Die Kommission nutzte zur Durchführung der Konsultation der Interessenträger ihre eigenen Ressourcen. Die Direktion Sicherheit der GD HR hat die damit verbundenen Arbeiten an den Umfragen, Videokonferenzen und anderen Workshops durchgeführt. Diese Aufgabe umfasste sowohl die Auswahl der Teilnehmer als auch die Organisation der Veranstaltungen und die Auswertung der eingegangenen Beiträge.

Die Gemeinsame Forschungsstelle (GFS) führte eine Risikobewertung der wichtigsten Komponenten der Informationssicherheit durch, die als Grundlage für die Folgenabschätzung diente.

- **Folgenabschätzung**

Diese Initiative richtet sich ausschließlich an die Organe und Einrichtungen der Union und hat nur begrenzte Auswirkungen auf die Mitgliedstaaten und Einzelpersonen. Daher war es nicht

notwendig, eine umfassende Folgenabschätzung durchzuführen, da keine klar erkennbaren oder erheblichen Auswirkungen auf Bürger und Bürgerinnen oder Unternehmen festgestellt wurden. Ein umfassender Fahrplan wurde auf der Europa-Website veröffentlicht und es wurde Feedback von den relevanten Interessenträgern eingeholt.

- **Effizienz der Rechtsetzung und Vereinfachung**

Entfällt.

- **Grundrechte**

Die EU setzt alles daran, hohe Standards für den Schutz der Grundrechte zu gewährleisten. Diese Initiative gewährleistet die vollständige Einhaltung der Grundrechte, wie sie in der Charta der Grundrechte der Europäischen Union[10] verankert sind:

- Recht auf eine gute Verwaltung[11]

Die Organe und Einrichtungen der Union tragen zur Verwirklichung des Grundsatzes der guten Verwaltungspraxis bei, indem sie die Sicherheit der Informationen erhöhen, mit denen sie bei der Behandlung der Angelegenheiten der europäischen Bürger und Bürgerinnen umgehen.

- Schutz personenbezogener Daten[12]

Die gesamte Verarbeitung personenbezogener Daten im Rahmen dieses Vorschlags fände in vertrauenswürdiger Umgebung unter uneingeschränkter Einhaltung der Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates statt.

- Recht auf Zugang zu Dokumenten[13]

Der Zugang der Öffentlichkeit zu EU-VS und nicht als Verschlusssache eingestuften vertraulichen Dokumenten wird weiterhin vollständig durch die Verordnung (EG) Nr. 1049/2001 des Europäischen Parlaments und des Rates geregelt.

- Recht auf den Schutz geistigen Eigentums [14]

Bei der Bearbeitung und Verwahrung von nicht als Verschlusssache eingestuften Informationen und EU-VS schützen die Organe und Einrichtungen der Union das geistige Eigentum gemäß der Richtlinie 2001/29/EG des Europäischen Parlaments und des Rates.[15]

- Freiheit der Meinungsäußerung und Informationsfreiheit[16]

Zwar hat jeder die Freiheit, Informationen und Ideen zu erhalten und auszutauschen, ohne dass eine Behörde eingreift, doch hindert dies die Union nicht daran, die Bedingungen für den Zugang zu bestimmten Arten von Informationen sowie deren Bearbeitung und Verwahrung auf der Grundlage ihrer Vertraulichkeitsstufe festzulegen.

Für die Ausübung dieser Freiheiten können Bedingungen und Beschränkungen gelten, die gesetzlich vorgesehen und in einer demokratischen Gesellschaft notwendig sind, um die Weitergabe von vertraulichen Informationen zu verhindern und die Sicherheit der EU zu gewährleisten.

---

10 Charta der Grundrechte der Europäischen Union (ABl. C 326 vom 26.10.2012, S. 391).

11 Artikel 41 der Charta der Grundrechte der Europäischen Union.

12 Artikel 8 der Charta der Grundrechte der Europäischen Union.

13 Artikel 42 der Charta der Grundrechte der Europäischen Union.

14 Artikel 17 der Charta der Grundrechte der Europäischen Union.

15 Richtlinie 2001/29/EG des Europäischen Parlaments und des Rates vom 22. Mai 2001 zur Harmonisierung bestimmter Aspekte des Urheberrechts und der verwandten Schutzrechte in der Informationsgesellschaft (ABl. L 167 vom 22.6.2001, S. 10).

16 Artikel 11 der Charta der Grundrechte der Europäischen Union.

4. AUSWIRKUNGEN AUF DEN HAUSHALT

Dieser Vorschlag erfordert die Zuweisung eines Beamten der Funktionsgruppe AD und eines Beamten der Funktionsgruppe AST für das ständige Sekretariat der Koordinierungsgruppe, das von der Kommission in der Direktion Sicherheit der Generaldirektion Humanressourcen und Sicherheit eingerichtet wird.

Für die Organe und Einrichtungen werden Kosteneinsparungen bei den gemeinsamen Aufgaben und der Zusammenarbeit sowie bei der Vermeidung potenzieller wirtschaftlicher Schäden infolge von Sicherheitsvorfällen aufgrund von Verbesserungen der Informationssicherheit erwartet. Zum anderen können die für die Durchführung der neuen Rechtsvorschriften erforderlichen finanziellen Aufwendungen im Rahmen der bestehenden Programme zur Verbesserung der Informationssicherheit in den einzelnen Organen und Einrichtungen der Union gedeckt werden.

5. WEITERE ANGABEN

- **Durchführungspläne sowie Monitoring-, Bewertungs- und Berichterstattungsmodalitäten**

Die Kommission ist gemäß dem Vorschlag verpflichtet, dem Europäischen Parlament und dem Rat alle drei Jahre über die Durchführung dieser Verordnung, einschließlich der Funktionsweise der mit dieser Verordnung geschaffenen Governance, Bericht zu erstatten.

Darüber hinaus wird die Kommission alle fünf Jahre diese Verordnung evaluieren, um ihre tatsächliche Leistung zu bewerten und auf dieser Grundlage zu ermitteln, ob eine Änderung der Rechtsvorschriften erforderlich ist.

- **Ausführliche Erläuterung einzelner Bestimmungen des Vorschlags**

Im Mittelpunkt dieses Vorschlags stehen die Anforderungen an den Umgang mit und die Speicherung von nicht als Verschlusssache eingestuften Informationen und EU-VS, die den Hauptgegenstand der Initiative bilden und deren besserer Schutz das eigentliche Ziel der Initiative ist.

Gegenstand und Anwendungsbereich (Artikel 1 und Artikel 2)

Diese Verordnung soll ein Mindestmaß an Vorschriften für die Informationssicherheit schaffen, die für alle Organe und Einrichtungen der Union gelten.

Sie gilt für alle Informationen, die von den Organen und Einrichtungen der Union bearbeitet und gespeichert werden, einschließlich der Informationen im Zusammenhang mit den Tätigkeiten der Europäischen Atomgemeinschaft, mit Ausnahme von Euratom-Verschlusssachen. Sowohl die nicht als Verschlusssache eingestuften Informationen als auch die EU-VS fallen unter diese Verordnung.

Begriffsbestimmungen und allgemeine Grundsätze (Artikel 3 bis 5)

Die Begriffsbestimmungen in Artikel 3 stützen sich auf die geltenden Vorschriften zur Informationssicherheit, die von den Organen und Einrichtungen der Union gesondert erlassen wurden.

Neben den allgemeinen Grundsätzen des Unionsrechts – Transparenz, Verhältnismäßigkeit, Effizienz und Rechenschaftspflicht – enthält diese Verordnung die wichtigsten verbindlichen Leitlinien, wie z. B. ein von allen Organen und Einrichtungen der Union gesondert durchgeführtes Verfahren für das Risikomanagement im Bereich der Informationssicherheit und die Bewertung ihrer Informationen im Hinblick auf eine angemessene Kategorisierung.

Governance und Organisation der Sicherheit (Artikel 6 bis 8)

Alle Organe und Einrichtungen der Union arbeiten in einer interinstitutionellen Koordinierungsgruppe für Informationssicherheit zusammen, die im Konsens und im gemeinsamen Interesse der Organe und Einrichtungen der Union handelt.

In der Koordinierungsgruppe kommen die Sicherheitsbehörden aller Organe und Einrichtungen zusammen und erstellen Leitfäden für die Durchführung dieser Verordnung. Sie steht in regelmäßigem Kontakt mit den nationalen Sicherheitsbehörden der Mitgliedstaaten, die in einem Ausschuss für Informationssicherheit zusammenkommen.

Zur Straffung der Verfahren und aus anderen praktischen Gesichtspunkten im Zusammenhang mit der Informationssicherheit werden fünf Untergruppen eingesetzt, in denen Sachverständige aus verschiedenen Organen und Einrichtungen vertreten sind.

Jedes Organ und jede Einrichtung der Union ist verpflichtet, eine Sicherheitsbehörde zu benennen, die für die Festlegung interner Maßnahmen zur Informationssicherheit und für deren Umsetzung verantwortlich ist. Die Sicherheitsbehörde legt spezifische Funktionen fest, wie z. B. die Stelle für Informationssicherung, die für den Betrieb zuständige Stelle für Informationssicherung, die Sicherheitsakkreditierungsstelle, die TEMPEST-Stelle, die Krypto-Zulassungsstelle und die Krypto-Verteilungsstelle, die aus Effizienz- oder Ressourcengründen an ein anderes Organ oder eine andere Einrichtung delegiert werden können.

Informationssicherung und Kommunikations- und Informationssysteme (Artikel 9 bis 11)

Mit der Verordnung wird eine Untergruppe für Informationssicherung eingesetzt, deren Ziel es ist, die Kohärenz zwischen den Vorschriften für die Informationssicherheit und den Cybersicherheitsgrundregeln, wie in der Verordnung über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in den Organen, Einrichtungen und sonstigen Stellen der Union festgelegt, zu verbessern.

Die Organe und Einrichtungen der Union sind verpflichtet, die in diesen Artikeln genannten Grundsätze einzuhalten und gesonderte interne Vorschriften für spezifische Sicherheitsmaßnahmen zu erlassen, die an ihr eigenes Sicherheitsumfeld angepasst sind.

Nicht als Verschlusssache eingestufte Informationen (Artikel 12 bis 17 und Anhang I)

In der Verordnung sind drei Kategorien von nicht als Verschlusssache eingestuften Informationen vorgesehen: Für die Öffentlichkeit bestimmte Informationen, normale Informationen und nicht als Verschlusssache eingestufte vertrauliche Informationen. Alle diese Kategorien werden definiert, außerdem werden Kennzeichnungsvorschriften und Vorschriften für den Umgang mit diesen Informationen festgelegt, um diese zu schützen.

Für die Koordinierung der Arbeiten zur Gleichwertigkeit der von einigen Organen und Einrichtungen der Union festgelegten Kategorien mit den in der Verordnung vorgesehenen gemeinsamen Kategorien wird im Rahmen des Vorschlags eine Untergruppe für nicht als Verschlusssache eingestufte Informationen eingesetzt.

EU-VS (Artikel 18 bis 58 und Anhänge II bis VI)

Dieses Kapitel ist der umfangreichste Teil des Vorschlags und gliedert sich in sieben Abschnitte: Allgemeine Bestimmungen, Personeller Geheimschutz, Materieller Geheimschutz, Behandlung von EU-VS, Schutz in Kommunikations- und Informationssystemen, Geheimschutz in der Wirtschaft und Weitergabe von EU-VS und Austausch von Verschlusssachen.

Im Abschnitt „Allgemeine Bestimmungen“ sind vier Stufen von EU-VS vorgesehen: „TRES SECRET UE/EU TOP SECRET“, „SECRET UE/EU SECRET“, „CONFIDENTIEL UE/EU CONFIDENTIAL“, „RESTREINT UE/EU RESTRICTED“ – sowie eine Verpflichtung der Organe und Einrichtungen der Union, die erforderlichen Sicherheitsmaßnahmen in Übereinstimmung mit den Ergebnissen eines Verfahrens zum Risikomanagement der Informationssicherheit zu ergreifen.

Im Mittelpunkt der übrigen Abschnitte stehen die Standards für den Schutz von EU-VS, die sich auf den jeweiligen Bereich beziehen. Die Einzelheiten dieses Schutzes von EU-VS sind in den Anhängen II bis V festgelegt. Anhang VI enthält eine Entsprechungstabelle für die Kennzeichnung des Geheimhaltungsgrades der Mitgliedstaaten und der Europäischen Atomgemeinschaft.

Um die einschlägigen Verfahren in diesem Bereich zu straffen und Doppelarbeit zu vermeiden, werden mit der Verordnung Untergruppen für Informationssicherung, für nicht als Verschlusssache eingestufte Informationen, für den materiellen Geheimschutz, für die Akkreditierung von Kommunikations- und Informationssystemen, in denen EU-VS verarbeitet und gespeichert werden, sowie für die Weitergabe von EU-VS und den Austausch von Verschlusssachen eingesetzt.

Schlussbestimmungen (Artikel 59 bis 62)

Mit den Schlussbestimmungen wird der Übergang von den derzeitigen Vorschriften und Verfahren zu dem durch diese Verordnung geschaffenen neuen Rechtsrahmen gewährleistet. Sie betreffen die derzeit in den Organen und Einrichtungen der Union geltenden internen Vorschriften für die Informationssicherheit, die Anerkennung von Bewertungsbesuchen, die vor Beginn der Anwendung der Verordnung durchgeführt wurden, die Behandlung zuvor geschlossener Verwaltungsvereinbarungen und die Beibehaltung der für Finanzhilfevereinbarungen geltenden spezifischen Sicherheitsrahmen.

Die Anwendung dieser Verordnung beginnt zwei Jahre nach ihrem Inkrafttreten.

2022/0084 (COD)

Vorschlag für eine

VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES

über die Informationssicherheit in den Organen, Einrichtungen und sonstigen Stellen der Union

DAS EUROPÄISCHE PARLAMENT UND DER RAT DER EUROPÄISCHEN UNION —

gestützt auf den Vertrag über die Arbeitsweise der Europäischen Union, insbesondere auf Artikel 298,

gestützt auf den Vertrag zur Gründung der Europäischen Atomgemeinschaft, insbesondere auf Artikel 106a,

auf Vorschlag der Europäischen Kommission,

nach Zuleitung des Entwurfs des Gesetzgebungsakts an die nationalen Parlamente,

gemäß dem ordentlichen Gesetzgebungsverfahren,

in Erwägung nachstehender Gründe:

(1) Gegenwärtig haben die Organe und Einrichtungen der Union entweder ihre eigenen Vorschriften für die Informationssicherheit, die auf ihrer Geschäftsordnung oder ihrem Gründungsakt beruhen, oder sie haben überhaupt keine derartigen Vorschriften. In diesem Zusammenhang verwenden die einzelnen Organe und Einrichtungen der Union erhebliche Anstrengungen auf die Annahme unterschiedlicher Konzepte, was dazu führt, dass der Informationsaustausch nicht immer zuverlässig ist. Das Fehlen eines gemeinsamen Konzepts behindert den Einsatz gemeinsamer Instrumente, die auf einem vereinbarten Regelwerk je nach den Sicherheitsanforderungen der zu schützenden Informationen aufbauen.

(2) Zwar wurden Fortschritte auf dem Weg zu kohärenteren Vorschriften für den Schutz von EU-Verschlusssachen („EU-VS“) und nicht als Verschlusssache eingestuften Informationen erzielt, doch ist die Interoperabilität der einschlägigen Systeme nach wie vor begrenzt, was eine nahtlose Übermittlung von Informationen zwischen den verschiedenen Organen und Einrichtungen der Union verhindert. Somit sollten weitere Anstrengungen unternommen werden, um einen interinstitutionellen Ansatz für die Weitergabe von EU-VS und nicht als Verschlusssache eingestuften vertraulichen Informationen zu ermöglichen, der gemeinsame Kategorien von Informationen und gemeinsame Grundregeln für den Umgang mit diesen Informationen vorsieht. Des Weiteren sollte eine gemeinsame Grundlage für die Vereinfachung der Verfahren für den Austausch von EU-VS und nicht als Verschlusssache eingestuften vertraulichen Informationen zwischen den Organen und Einrichtungen der Union und mit den Mitgliedstaaten angestrebt werden.

(3) Daher sollten einschlägige Vorschriften zur Gewährleistung eines einheitlichen Niveaus der Informationssicherheit in allen Organen und Einrichtungen der Union festgelegt werden. Diese sollten einen umfassenden und kohärenten allgemeinen Rahmen für den Schutz von EU-VS und nicht als Verschlusssache eingestuften

Informationen bilden und die Gleichwertigkeit der Grundprinzipien und Mindeststandards gewährleisten.

(4) Die jüngste Pandemie hat zu einer erheblichen Veränderung der Arbeitsweisen geführt, bei der Fernkommunikationsmittel zur Regel geworden sind. So wurden viele Verfahren, die zumindest teilweise noch papiergestützt waren, rasch angepasst, um die elektronische Verarbeitung und den elektronischen Austausch von Informationen zu ermöglichen. Diese Entwicklungen erfordern Änderungen im Umgang mit und im Schutz von Informationen. Die vorliegende Verordnung trägt den neuen Arbeitsweisen Rechnung.

(5) Durch die Schaffung eines gemeinsamen Mindestschutzniveaus für EU-VS und nicht als Verschlusssache eingestufte Informationen trägt diese Verordnung dazu bei, dass die Organe und Einrichtungen der Union bei der Ausübung ihrer Aufgaben von einer effizienten und unabhängigen Verwaltung unterstützt werden. Gleichzeitig bleibt es jedem Organ und jeder Einrichtung der Union überlassen zu entscheiden, wie sie die in dieser Verordnung festgelegten Regeln entsprechend ihren eigenen Sicherheitsbedürfnissen umsetzen. Diese Verordnung darf die Organe und Einrichtungen keinesfalls bei der Ausführung der ihnen durch die Rechtsvorschriften der Union übertragenen Aufgaben behindern und ihre institutionelle Autonomie nicht einschränken.

(6) Diese Verordnung lässt die folgenden Verordnungen unberührt: Verordnung (Euratom) Nr. 3/1958[17], Verordnung Nr. 31 (EWG), Nr. 11 (EAG) über das Statut der Beamten und über die Beschäftigungsbedingungen für die sonstigen Bediensteten der Europäischen Wirtschaftsgemeinschaft und der Europäischen Atomgemeinschaft[18], Verordnung (EG) Nr. 1049/2001 des Europäischen Parlaments und des Rates[19], Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates[20], Verordnung (EWG, EURATOM) Nr. 354/83 des Rates[21], Verordnung (EU, Euratom) 2018/1046 des Europäischen Parlaments und des Rates[22], Verordnung (EU) 2021/697 des Europäischen Parlaments und des Rates[23], Verordnung (EU) [...] des Europäischen

---

17 Verordnung (Euratom) Nr. 3 vom 31. Juli 1958 zur Anwendung des Artikels 24 des Vertrags zur Gründung der Europäischen Atomgemeinschaft (ABl. 17 vom 6.10.1958, S. 406).

18 ABl. 45 vom 14.6.1962, S. 1385.

19 Verordnung (EG) Nr. 1049/2001 des Europäischen Parlaments und des Rates vom 30. Mai 2001 über den Zugang der Öffentlichkeit zu Dokumenten des Europäischen Parlaments, des Rates und der Kommission (ABl. L 145 vom 31.5.2001, S. 43).

20 Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates vom 23. Oktober 2018 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen und sonstigen Stellen der Union, zum freien Datenverkehr und zur Aufhebung der Verordnung (EG) Nr. 45/2001 und des Beschlusses Nr. 1247/2002/EG (ABl. L 295 vom 21.11.2018, S. 39).

21 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 (ABl. L 43 vom 15.2.1983, S. 1).

22 Verordnung (EU, Euratom) 2018/1046 des Europäischen Parlaments und des Rates vom 18. Juli 2018 über die Haushaltsordnung für den Gesamthaushaltsplan der Union, zur Änderung der Verordnungen (EU) Nr. 1296/2013, (EU) Nr. 1301/2013, (EU) Nr. 1303/2013, (EU) Nr. 1304/2013, (EU) Nr. 1309/2013, (EU) Nr. 1316/2013, (EU) Nr. 223/2014, (EU) Nr. 283/2014 und des Beschlusses Nr. 541/2014/EU sowie zur Aufhebung der Verordnung (EU, Euratom) Nr. 966/2012 (ABl. L 193 vom 30.7.2018, S. 1).

23 Verordnung (EU) 2021/697 des Europäischen Parlaments und des Rates vom 29. April 2021 zur Einrichtung des Europäischen Verteidigungsfonds und zur Aufhebung der Verordnung (EU) 2018/1092 (ABl. L 170 vom 12.5.2021, S. 149).

Parlaments und des Rates[24] über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in den Organen, Einrichtungen und sonstigen Stellen der Union (noch anzunehmen).

(7) Zur Gewährleistung des besonderen Charakters der Tätigkeiten der Europäischen Atomgemeinschaft, die in der Verordnung Nr. 3/1958 des Rates der Europäischen Atomgemeinschaft[25] geregelt sind, sollte diese Verordnung nicht für Euratom-Verschlusssachen gelten. Alle Informationen im Zusammenhang mit anderen Euratom-Tätigkeiten, die nicht unter die Verordnung 3/1958 fallen, sollten jedoch in den Anwendungsbereich der vorliegenden Verordnung fallen.

(8) Im Hinblick auf die Schaffung einer formellen Struktur für die Zusammenarbeit zwischen den Organen und Einrichtungen der Union im Bereich der Informationssicherheit ist es erforderlich, eine interinstitutionelle Koordinierungsgruppe (im Folgenden „Koordinierungsgruppe“) einzusetzen, in der die Sicherheitsbehörden aller Organe und Einrichtungen der Union vertreten sind. Ohne über Entscheidungsbefugnisse zu verfügen, sollte die Koordinierungsgruppe die Kohärenz der Maßnahmen im Bereich der Informationssicherheit verbessern und zur Harmonisierung der Verfahren und Instrumente der Informationssicherheit in den Organen und Einrichtungen der Union beitragen.

(9) Die Arbeit der Koordinierungsgruppe benötigt die Unterstützung von Experten aus verschiedenen Bereichen der Informationssicherheit: Kategorisierung und Kennzeichnung, Kommunikations- und Informationssysteme, Akkreditierung, materieller Geheimschutz, Weitergabe von EU-VS und Austausch von Verschlusssachen. Um Doppelarbeit in den Organen und Einrichtungen der Union zu vermeiden, sollten thematische Untergruppen eingerichtet werden. Außerdem sollte die Koordinierungsgruppe bei Bedarf weitere Untergruppen mit spezifischen Aufgaben einsetzen können.

(10) Mit dem Ziel, die Informationssicherheit in der Union zu verbessern, sollte die Koordinierungsgruppe eng mit den nationalen Sicherheitsbehörden der Mitgliedstaaten zusammenarbeiten. Zu diesem Zweck sollte ein Ausschuss für Informationssicherheit der Mitgliedstaaten eingesetzt werden, der die Koordinierungsgruppe berät.

(11) Obwohl die gemeinsamen Einrichtungen, die alle Organe und Einrichtungen der Union vertreten, nach dem Grundsatz der Zusammenarbeit geschaffen wurden, sollte jedes Organ und jede Einrichtung die volle Verantwortung für die Sicherheit der Informationen innerhalb ihrer Organisation behalten. Jedes Organ und jede Einrichtung der Union sollte über eine Sicherheitsbehörde und erforderlichenfalls über weitere Behörden verfügen, die für bestimmte Aufgaben im Zusammenhang mit der Informationssicherheit zuständig sind.

(12) Der Grundsatz des Informationssicherheits-Risikomanagements sollte im Mittelpunkt der von jedem Organ und jeder Einrichtung der Union in diesem Bereich zu entwickelnden Politik stehen. Zwar müssen die in dieser Verordnung festgelegten Mindestanforderungen erfüllt werden, doch sollte jedes Organ und jede Einrichtung der Union entsprechend den Ergebnissen einer internen Risikobewertung spezifische

---

[24] Verordnung [...] des Europäischen Parlaments und des Rates über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in den Organen, Einrichtungen und sonstigen Stellen der Union (noch anzunehmen).

[25] EAG Rat: Verordnung Nr. 3 zur Anwendung des Artikels 24 des Vertrages zur Gründung der Europäischen Atomgemeinschaft (ABl. 17 vom 6.10.1958, S. 406).

Sicherheitsmaßnahmen zum Schutz der Informationen ergreifen. Ebenso sollten die technischen Mittel zum Schutz der Informationen an die spezifische Situation der einzelnen Organe und Einrichtungen angepasst werden.

(13) Angesichts der Vielfalt der Kategorien von nicht als Verschlusssache eingestuften Informationen, die die Organe und Einrichtungen der Union auf der Grundlage ihrer eigenen Sicherheitsinformationsvorschriften entwickelt haben, und um Verzögerungen bei der Durchführung dieser Verordnung zu vermeiden, sollten die Organe und Einrichtungen der Union in der Lage sein, ihr eigenes Kennzeichnungssystem für interne Zwecke oder für den Austausch von Informationen mit ihren jeweiligen Ansprechpartnern in anderen Organen und Einrichtungen oder in den Mitgliedstaaten beizubehalten.

(14) Im Zuge der Anpassung an die modernen Telearbeitsverfahren sollten die Netze, die für die Verbindung zu den Fernzugangsdiensten des Organs oder der Einrichtung der Union genutzt werden, durch angemessene Sicherheitsmaßnahmen geschützt sein.

(15) Da die Organe und Einrichtungen der Union häufig auf Auftragnehmer und Outsourcing zurückgreifen, ist es wichtig, gemeinsame Bestimmungen für die Mitarbeiter von Auftragnehmern festzulegen, die Aufgaben im Bereich der Informationssicherheit wahrnehmen.

(16) Die materiellrechtlichen Vorschriften für den Zugang zu EU-VS in den internen Vorschriften der verschiedenen Organe und Einrichtungen der Union sind derzeit angeglichen, es bestehen jedoch erhebliche Unterschiede in Bezug auf die Bezeichnungen und die erforderlichen Verfahren. Dies stellt eine Belastung für die nationalen Sicherheitsbehörden der Mitgliedstaaten dar, die sich auf unterschiedliche Anforderungen einstellen müssen. Daher ist es notwendig, ein gemeinsames Glossar und gemeinsame Verfahren im Bereich der Personalsicherheit zu entwickeln, um so die Zusammenarbeit mit den nationalen Sicherheitsbehörden der Mitgliedstaaten zu vereinfachen und das Risiko einer Gefährdung von EU-VS zu begrenzen.

(17) Angesichts der ungleichen Ressourcenausstattung der Organe und Einrichtungen der Union und zur Straffung ihrer einschlägigen Verfahren und Praktiken können die Aufgaben der Sicherheitsermächtigung der Kommission übertragen werden, um die langjährige Praxis im Bereich der Sicherheitsermächtigung fortzusetzen und zur Zentralisierung der den einzelnen Sicherheitsbehörden übertragenen Aufgaben beizutragen.

(18) Der Schutz von EU-VS wird auch durch technische und organisatorische Maßnahmen gewährleistet, die für die Räumlichkeiten, Gebäude, Räume, Büros oder Einrichtungen der Organe und Einrichtungen der Union gelten, in denen EU-VS erörtert, bearbeitet oder verwahrt werden. In dieser Verordnung ist die Einführung eines Informationssicherheitsmanagements im Bereich des materiellen Geheimschutzes vorgesehen, der es den Organen und Einrichtungen der Union ermöglicht, die für ihre Standorte geeigneten Sicherheitsmaßnahmen auszuwählen.

(19) Alle Organe und Einrichtungen der Union, die EU-VS bearbeiten und verwahren, sollten an ihren Standorten materiell geschützte Bereiche einrichten, um das gleiche Schutzniveau für die entsprechenden Geheimhaltungsgrade von EU-VS, die dort bearbeitet und verwahrt werden, zu gewährleisten. Diese Bereiche sollten als Verwaltungsbereiche und Sicherheitsbereiche ausgewiesen werden und gemeinsame Mindeststandards für den Schutz von EU-VS beinhalten.

(20) Die Herausgeberkontrolle ist ein wichtiger Grundsatz bei der Behandlung von EU-VS, diese muss daher klar festgelegt und entwickelt werden. In dieser Hinsicht überträgt die Erstellung von EU-VS dem Herausgeber eine Verantwortung, die den gesamten Lebenszyklus des betreffenden EU-VS-Dokuments umfassen sollte.

(21) Die Organe und Einrichtungen der Union haben ihre Kommunikations- und Informationssysteme traditionell eigenständig entwickelt und dabei nicht ausreichend auf die Interoperabilität zwischen allen Organen und Einrichtungen der Union geachtet. Daher müssen Mindestsicherheitsanforderungen für die Kommunikations- und Informationssysteme (CIS) festgelegt werden, in denen sowohl EU-VS als auch nicht als Verschlusssache eingestufte Informationen verarbeitet und gespeichert werden, um so einen nahtlosen Informationsaustausch mit den betroffenen Akteuren zu gewährleisten.

(22) Mit dem Ziel, einen einheitlichen Standard für die Akkreditierung von Kommunikations- und Informationssystemen, in denen EU-VS verarbeitet und gespeichert werden, zu erreichen, sollten die Organe und Einrichtungen der Union in einer zu diesem Zweck eingerichteten Gruppe zusammenarbeiten. Es wird empfohlen, dass alle Organe und Einrichtungen der Union diesen Standard verwenden, um zu einem allgemeinen Schutzniveau für EU-VS beizutragen. Was die organisatorische Autonomie anbelangt, so liegt die Entscheidung jedoch bei der zuständigen Behörde des jeweiligen Organs oder der jeweiligen Einrichtung.

(23) Alle Organe und Einrichtungen der Union sollten bei der Vergabe und Durchführung von als Verschlusssache eingestuften Aufträgen oder Finanzhilfevereinbarungen dieselben Verfahren befolgen und dieselben Maßnahmen anwenden. Daher ist es notwendig, sowohl die obligatorischen als auch die fakultativen Elemente als Verschlusssache eingestuften Aufträgen und Finanzhilfevereinbarungen klar festzulegen. Die Maßnahmen zum Schutz von EU-VS im Zusammenhang mit als Verschlusssache eingestuften Aufträgen und Finanzhilfevereinbarungen sollten jedoch den Vorschriften Rechnung tragen, die von den Organen und Einrichtungen der Union zusammen mit den Mitgliedstaaten in diesem Bereich bereits gesondert entwickelt wurden.

(24) Die enge Zusammenarbeit zwischen den Organen und Einrichtungen der Union sowie die zahlreichen Synergien, die sich zwischen ihnen entwickelt haben, erfordern den Austausch einer großen Menge an Informationen. Im Interesse der Sicherheit von Verschlusssachen sollte die Vertrauenswürdigkeit eines Organs oder einer Einrichtung der Union bewertet werden, bevor sie EU-VS einer bestimmten Geheimhaltungsstufe bearbeiten und speichern.

(25) Außerdem sollte die Weitergabe von EU-VS zwischen den Organen und Einrichtungen der Union und der Austausch von Verschlusssachen mit internationalen Organisationen und Drittstaaten ebenfalls durch geeignete Sicherheitsmaßnahmen zum Schutz dieser Informationen geregelt werden. Wenn Vereinbarungen über die Sicherheit von Informationen geplant sind, sollten die Bestimmungen von Artikel 218 AEUV Anwendung finden.

(26) Die Abkommen über die Sicherheit von Informationen sollen den rechtlichen Gesamtrahmen für den Austausch von Verschlusssachen der Union mit Drittstaaten und internationalen Organisationen gewährleisten; außerdem muss die Möglichkeit vorgesehen werden, dass die Organe und Einrichtungen der Union Verwaltungsvereinbarungen mit einem bestimmten Partner in einem Drittstaat oder

einer internationalen Organisation zum Zwecke des Austauschs von EU-VS schließen können.

(27) Mit dieser Verordnung wird ein gemeinsamer Rahmen für alle Organe und Einrichtungen der Union geschaffen. Um den Organen und Einrichtungen der Union bei der Anpassung ihrer internen Sicherheitsvorschriften an die Bestimmungen dieser Verordnung keinen übermäßigen Verwaltungsaufwand aufzuerlegen, sollte diese Verordnung zwei Jahre nach ihrem Inkrafttreten anwendbar werden.

(28) Im Einklang mit den Nummern 22 und 23 der Interinstitutionellen Vereinbarung vom 13. April 2016 über bessere Rechtsetzung[26] sollte die Kommission diese Verordnung bewerten, um ihre tatsächlichen Auswirkungen und die Notwendigkeit weiterer Maßnahmen zu beurteilen. Die Kommission sollte dem Europäischen Parlament und dem Rat spätestens drei Jahre nach dem Beginn der Anwendung einen Bericht über die Durchführung dieser Verordnung vorlegen.

(29) Der Europäische Datenschutzbeauftragte wurde gemäß Artikel 42 der Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates[27] angehört und hat am ... eine Stellungnahme abgegeben.

HABEN FOLGENDE VERORDNUNG ERLASSEN:

Kapitel 1
Allgemeine Bestimmungen

Artikel 1

Gegenstand

(1) Mit dieser Verordnung werden Vorschriften für die Informationssicherheit in allen Organen und Einrichtungen der Union festgelegt.

Artikel 2

Anwendungsbereich

(1) Diese Verordnung gilt für alle Informationen, die von den Organen und Einrichtungen der Union bearbeitet und verwahrt werden, einschließlich Informationen im Zusammenhang mit Tätigkeiten der Europäischen Atomgemeinschaft, mit Ausnahme von Euratom-Verschlusssachen.

(2) Sie gilt für Informationen der folgenden Vertraulichkeitsstufen:

a) nicht als Verschlusssache eingestufte Informationen der drei Stufen: für die Öffentlichkeit bestimmte Information, normale Information, nicht als Verschlusssache eingestufte vertrauliche Information;

b) EU-Verschlusssachen der vier Geheimhaltungsstufen: RESTREINT UE/EU RESTRICTED,

---

[26] Interinstitutionelle Vereinbarung zwischen dem Europäischen Parlament, dem Rat der Europäischen Union und der Europäischen Kommission über bessere Rechtsetzung (ABl. L 123 vom 12.5.2016, S. 1).

[27] Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates vom 23. Oktober 2018 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen und sonstigen Stellen der Union, zum freien Datenverkehr und zur Aufhebung der Verordnung (EG) Nr. 45/2001 und des Beschlusses Nr. 1247/2002/EG (ABl. L 295 vom 21.11.2018).

CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET, TRES SECRET UE/EU TOP SECRET.

(3) Die Einstufungen spiegeln den Schaden wider, der für die legitimen privaten und öffentlichen Interessen, einschließlich der Interessen der Union, der Organe und Einrichtungen der Union, der Mitgliedstaaten oder anderer Interessenträger, durch eine unbefugte Offenlegung entstehen kann, und sollen sicherstellen, dass geeignete Schutzmaßnahmen ergriffen werden können.

Artikel 3

Begriffsbestimmungen

Für die Zwecke dieser Verordnung bezeichnet der Ausdruck

a) „Information“ jegliche Daten in mündlicher, visueller, elektronischer, magnetischer oder materieller Form oder in Form von Material, Ausrüstung oder Technologie, einschließlich Vervielfältigungen, Übersetzungen und im Stadium der Entwicklung befindlichen Materials;

b) „Informationssicherheit“ die Gewährleistung der Authentizität, Verfügbarkeit, Vertraulichkeit, Integrität und Beweisbarkeit von Informationen;

c) „Bearbeitung“ alle möglichen Handlungen, denen Informationen während ihres gesamten Lebenszyklus unterliegen können; diese umfassen ihre Erstellung, Sammlung und Registrierung, die Zuweisung einer Vertraulichkeitsstufe, ihre Verarbeitung, Anzeige, Abfrage, Beförderung, Übermittlung, Herabstufung, die Aufhebung ihres Geheimhaltungsgrads, ihre Archivierung und Vernichtung;

d) „Verwahrung“ die Aufbewahrung beziehungsweise Speicherung von Informationen auf einem beliebigen Medium, sodass ihre Verfügbarkeit für eine künftige Nutzung gewährleistet ist;

e) „Organe und Einrichtungen der Union“ die Organe, Einrichtungen und sonstigen Stellen der Union, die durch den Vertrag über die Europäische Union, den Vertrag über die Arbeitsweise der Europäischen Union, den Vertrag zur Gründung der Europäischen Atomgemeinschaft oder einen Rechtsakt oder auf deren Grundlage geschaffen wurden;

f) „Euratom-Verschlusssache“ Informationen im Sinne der Verordnung Nr. 3/1958 des Rates der Europäischen Atomgemeinschaft;

g) „Sicherheitsbehörde“ die Sicherheitsfunktion, die gemäß der Geschäftsordnung oder dem Gründungsakt jedes Organs und jeder Einrichtung der Union benannt wird;

h) „Informationssicherheitsrisiko-Managementprozess“ den gesamten Prozess der Ermittlung, Kontrolle und Minimierung möglicher Zwischenfälle, die die Sicherheit einer Organisation oder der von ihr benutzten Systeme beeinträchtigen könnten; darunter fallen sämtliche risikobezogenen Tätigkeiten, einschließlich der Risikobewertung, -behandlung, -akzeptanz und -kommunikation;

i) „Wert“ alles, was für die Organe oder Einrichtungen der Union, ihre Tätigkeiten und deren Kontinuität von Nutzen ist, einschließlich der

Informationsressourcen, auf die sie sich bei der Wahrnehmung ihrer Aufgaben stützen;

j) „sicherheitsbezogene Betriebsverfahren“ in Anhang III aufgeführte dokumentierte Verfahren für den Betrieb eines Sicherheitsbereichs, eines Kommunikations- und Informationssystems oder anderer sicherheitsrelevanter Werte oder Dienste, die deren Wirksamkeit gewährleisten;

k) „Kommunikations- und Informationssystem“ oder „CIS“ (Communication and Information System) ein System, das die Bearbeitung und Speicherung von Informationen in elektronischer Form ermöglicht, mitsamt sämtlicher für seinen Betrieb benötigten Werte;

l) „Informationssicherung“ die Gewissheit, dass Kommunikations- und Informationssysteme die in ihnen bearbeiteten und gespeicherten Informationen schützen, dass sie jederzeit ordnungsgemäß funktionieren, von rechtmäßigen Nutzern kontrolliert werden und ein angemessenes Niveau der Authentizität, Verfügbarkeit, Vertraulichkeit, Integrität und Beweisbarkeit sicherstellen;

m) „Akkreditierung“ die von der Sicherheitsakkreditierungsstelle erteilte förmliche Zulassung eines Kommunikations- und Informationssystems für die Verarbeitung oder eines Sicherheitsbereichs für die Verwahrung von EU-VS eines bestimmten Geheimhaltungsgrads;

n) „Akkreditierungsverfahren“ die im Hinblick auf eine Akkreditierung erforderlichen Schritte und Aufgaben;

o) „TEMPEST-Sicherheitsvorkehrungen“ Maßnahmen, die die Kommunikations- und Informationssysteme, in denen als „CONFIDENTIEL UE/EU CONFIDENTIAL“ und höher eingestufte Verschlusssachen bearbeitet und gespeichert werden, so schützen, dass von den betreffenden Informationen nicht über unbeabsichtigte elektromagnetische Abstrahlung unbefugt Kenntnis genommen werden kann;

p) „CERT-EU“ das Cybersicherheitszentrum für die Organe und Einrichtungen der Union im Sinne der Verordnung (EU) [...] des Europäischen Parlaments und des Rates über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in den Organen, Einrichtungen und sonstigen Stellen der Union;

q) „Informationssicherheitsvorfall“ jeglichen Vorfall, der die Authentizität, Verfügbarkeit, Vertraulichkeit, Integrität oder Beweisbarkeit von Informationen bei ihrer Verwahrung, Übertragung oder Bearbeitung gefährden kann;

r) „Kenntnis nur, wenn nötig“ das Erfordernis, dass eine Person zu einer bestimmten Information, die von einem Organ oder einer Einrichtung der Union bearbeitet oder verwahrt wird, Zugang haben muss, um die Aufgaben des betreffenden Organs oder der betreffenden Einrichtung der Union zu erfüllen;

s) „Zero-Trust“ ein Sicherheitsmodell, eine Reihe von Systemdesign-Grundsätzen und eine koordinierte Cybersicherheits- und Systemmanagement-Strategie, die sich mit innerhalb und außerhalb traditioneller Netzgrenzen bestehenden Bedrohungen auseinandersetzen;

t) „Kennzeichnung“ ein Hinweis, der auf Informationen angebracht wird, um sicherzustellen, dass geeignete Sicherheitsmaßnahmen angewandt werden;

u) „Sicherheitskennzeichnung“ eine Kennzeichnung, die den Grad der Vertraulichkeit der Information angibt;

v) „Verteilungskennzeichnung“ eine Kennzeichnung, die angibt, an welche internen Adressaten sich eine aus dem Organ oder der Einrichtung der Union stammende Information richtet;

w) „Weitergabekennzeichnung“ eine Kennzeichnung, die angibt, an welche externen Adressaten eine aus dem Organ oder der Einrichtung der Union stammende Information verteilt werden darf;

x) „Systemeigner“ die Person, die für die Beschaffung, die Entwicklung, die Integration, die Änderung, den Betrieb, die Wartung und die Ausbuchung eines Kommunikations- und Informationssystems insgesamt verantwortlich ist;

y) „Informationssicherheitsbedrohung“ ein Ereignis oder einen Faktor, das beziehungsweise der nach vernünftigem Ermessen die Informationssicherheit beeinträchtigen kann, falls keine Gegenmaßnahmen ergriffen werden;

z) „Schwachstelle“ eine Anfälligkeit, Empfindlichkeit oder Fehlfunktion eines Werts, eines Systems, eines Prozesses oder einer Kontrolle, die durch eine oder mehrere Bedrohungen ausgenutzt werden kann;

aa) „Risiko“ die Möglichkeit, dass bei einer bestimmten Bedrohung die internen und externen Schwachstellen eines Organs oder einer Einrichtung der Union oder eines von ihnen verwendeten Systems ausgenutzt und dadurch die legitimen öffentlichen und privaten Interessen geschädigt werden, gemessen als die Kombination der Wahrscheinlichkeit des Eintretens von Bedrohungen und ihrer Auswirkungen;

ab) „Restrisiko“ das nach dem Ergreifen von Sicherheitsmaßnahmen verbleibende Risiko;

ac) „Risikobewertung“ die Ermittlung von Bedrohungen und Schwachstellen und die Durchführung diesbezüglicher Risikoanalysen, d. h. die Analyse der Eintrittswahrscheinlichkeit und der Auswirkungen;

ad) „Risikobehandlung“ die Minderung, Beseitigung, Verringerung (durch eine geeignete Kombination von technischen, materiellen, organisatorischen oder verfahrensbezogenen Maßnahmen) sowie die Übertragung oder Überwachung des Risikos;

ae) „europäisches Cybersicherheitszertifikat“ ein Zertifikat im Sinne von Artikel 2 Nummer 11 der Verordnung (EU) Nr. 2019/881[28];

af) „Besitzer“ eine ordnungsgemäß ermächtigte Person, die nachweislich Kenntnis von einer zu schützenden Information haben muss, in deren Besitz ist und dementsprechend für deren Schutz verantwortlich zeichnet;

ag) „Material“ Dokumente, Datenträger, Geräte oder Ausrüstungsgegenstände, die bereits hergestellt oder noch in der Herstellung befindlich sind;

[28] Verordnung (EU) 2019/881 des Europäischen Parlaments und des Rates vom 17. April 2019 über die ENISA (Agentur der Europäischen Union für Cybersicherheit) und über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik und zur Aufhebung der Verordnung (EU) Nr. 526/2013 (Rechtsakt zur Cybersicherheit) (ABl. L 151 vom 7.6.2019, S. 15).

ah) „EU-Verschlusssache“ oder „EU-VS“ alle mit einem EU-Geheimhaltungsgrad gekennzeichneten Informationen oder Materialien, deren unbefugte Offenlegung den Interessen der Union oder eines oder mehrerer ihrer Mitgliedstaaten in unterschiedlichem Maße Schaden zufügen könnte;

ai) „Ermächtigung zum Zugang zu EU-VS“ ein Beschluss einer Sicherheitsbehörde, der bescheinigt, dass einem Beamten, sonstigen Bediensteten oder abgeordneten nationalen Sachverständigen eines Organs oder einer Einrichtung der Union für einen bestimmten Zeitraum Zugang zu EU-VS bis zu einem bestimmten Geheimhaltungsgrad gewährt werden kann;

aj) „nationale Sicherheitsbehörde“ oder „NSA“ (National Security Authority) die staatliche Behörde eines Mitgliedstaats, bei der die Endverantwortung für den Schutz von Verschlusssachen in dem betreffenden Mitgliedstaat liegt;

ak) „benannte Sicherheitsbehörde“ oder „DSA“ (Designated Security Authority) eine Behörde eines Mitgliedstaats (NSA oder jede andere zuständige Behörde), die für die Leitung und Unterstützung der Durchführung des Geheimschutzes in der Wirtschaft oder von Sicherheitsermächtigungsverfahren oder beides zuständig ist;

al) „Sicherheitsüberprüfung“ Überprüfung, die von der zuständigen Behörde eines Mitgliedstaats nach den innerstaatlichen Rechtsvorschriften und Regelungen durchgeführt wird, um Gewissheit darüber zu erlangen, dass über die betreffende Person keine nachteiligen Erkenntnisse vorliegen, die dem Zugang zu Verschlusssachen bis zu einem bestimmten Geheimhaltungsgrad („CONFIDENTIEL UE/EU CONFIDENTIAL“ oder höher) entgegenstehen;

am) „materieller Geheimschutz“ die Anwendung von technischen, materiellen und organisatorischen Maßnahmen auf Räumlichkeiten, Gebäude, Räume, Büros oder Anlagen eines Organs oder einer Einrichtung der Union, die vor unbefugtem Zugang zu Informationen, welche dort bearbeitet, verwahrt oder erörtert werden, zu schützen sind;

an) „Standorte“ die Räumlichkeiten, Gebäude, Räume, Büros oder Anlagen eines Organs oder einer Einrichtung der Union;

ao) „tief gestaffelte Verteidigung“ mehrstufige Sicherheitsmechanismen, bei denen mehrere unabhängige Ebenen von Sicherheitskontrollen eingesetzt werden, um sicherzustellen, dass bei Ausfall einer Komponente eine andere funktioniert;

ap) „kryptografisches Material“ oder „Kryptomaterial“ kryptografische Algorithmen, kryptografische Hardware- und Softwaremodule und Produkte, die Implementierungsdetails enthalten, sowie die dazugehörige Dokumentation und das Verschlüsselungsmaterial;

aq) „kryptografisches Produkt“ ein Produkt, dessen erste und wichtigste Funktion es ist, durch einen oder mehrere kryptografische Mechanismen Sicherheitsdienste (Authentizität, Verfügbarkeit, Vertraulichkeit, Integrität und Beweisbarkeit) bereitzustellen;

ar) „Herausgeber“ das Organ oder die Einrichtung der Europäischen Union, der Mitgliedstaat, der Drittstaat oder die internationale Organisation, unter dessen/deren Verantwortung Verschlusssachen erstellt und/oder in die Strukturen der Union eingebracht wurden;

as) „Dokument“ als Schrift-, Bild- oder Tonaufzeichnung verfügbarer Inhalt, unabhängig von der Form des Datenträgers (auf Papier oder in elektronischer, magnetischer oder sonstiger Form);

at) „Registrierung zu Sicherheitszwecken“ die Durchführung von Verfahren, bei denen jede Phase des Lebenszyklus des Materials und auch dessen Weitergabe und Vernichtung, aufgezeichnet wird;

au) „Aufhebung des Geheimhaltungsgrads“ die Löschung jeder Geheimhaltungskennzeichnung;

av) „Herabstufung“ die Einstufung in einen niedrigeren Geheimhaltungsgrad;

aw) „als Verschlusssache eingestufter Vertrag“ einen Rahmenvertrag oder Vertrag im Sinne der Verordnung (EU, Euratom) 2018/1046 des Europäischen Parlaments und des Rates zwischen einem Organ oder einer Einrichtung der Union und einem Auftragnehmer über die Lieferung beweglicher oder unbeweglicher Werte, die Durchführung von Arbeiten oder die Erbringung von Dienstleistungen, dessen Ausführung die Bearbeitung, einschließlich der Erstellung, oder Verwahrung von EU-VS erfordert oder vorsieht;

ax) „als Verschlusssache eingestufte Finanzhilfevereinbarung“ eine Vereinbarung, mit der ein Organ oder eine Einrichtung der Union eine Finanzhilfe im Sinne von Titel VIII der Verordnung (EU, Euratom) 2018/1046 gewährt und deren Erfüllung die Bearbeitung, einschließlich der Erstellung, oder die Verwahrung von EU-VS erfordert oder vorsieht;

ay) „als Verschlusssache eingestufter Unterauftrag“ einen Vertrag zwischen einem Auftragnehmer oder Begünstigten eines Organs oder einer Einrichtung der Union und einem Unterauftragnehmer über die Lieferung beweglicher oder unbeweglicher Werte, die Durchführung von Arbeiten oder die Erbringung von Dienstleistungen, dessen Ausführung die Bearbeitung, einschließlich der Erstellung, oder Verwahrung von EU-VS erforderlich macht oder umfasst;

az) „Programm- oder Projekt-Sicherheitsanweisung“ oder „PSI“ (Programme or Project Security Instruction) eine Liste von Sicherheitsverfahren, die für ein spezifisches Programm oder Projekt verwendet werden, um die Sicherheitsverfahren zu vereinheitlichen;

ba) „Geheimschutzklausel“ oder „SAL“ (Security Aspects Letter) besondere vom öffentlichen Auftraggeber oder von der Vergabebehörde festgelegte Vertragsbedingungen, die fester Bestandteil jedes bzw. jeder als Verschlusssache eingestuften und mit dem Zugang zu oder der Erstellung von EU-VS verbundenen Vertrags bzw. Finanzhilfevereinbarung sind und in denen die Sicherheitsanforderungen und die zu schützenden Teile des Vertrags oder der Finanzhilfevereinbarung festgelegt sind;

bb) „VS-Einstufungsliste“ oder „SCG“ (Security Classification Guide) ein Dokument, in dem die Komponenten eines als Verschlusssache eingestuften Programms, Projekts oder Vertrags beziehungsweise einer als Verschlusssache eingestuften Finanzhilfevereinbarung beschrieben und die anzuwendenden Geheimhaltungsgrade angegeben sind.

Artikel 4

Allgemeine Grundsätze

(1) Jedes Organ und jede Einrichtung der Union ist für die Umsetzung der Bestimmungen dieser Verordnung im eigenen Hause unter Berücksichtigung des eigenen Informationssicherheitsrisiko-Managementprozesses verantwortlich.

(2) Jede Nichteinhaltung dieser Verordnung, insbesondere die unbefugte Offenlegung von Informationen der in Artikel 2 Absatz 2 genannten Vertraulichkeitsstufen mit Ausnahme von für die Öffentlichkeit bestimmten Informationen, wird untersucht und kann dazu führen, dass Mitarbeiter im Einklang mit den Verträgen oder den einschlägigen Personalvorschriften zur Verantwortung gezogen werden.

(3) Die Organe und Einrichtungen der Union bewerten alle von ihnen bearbeiteten und verwahrten Informationen, um sie entsprechend den Vertraulichkeitsstufen gemäß Artikel 2 Absatz 2 einzustufen.

(4) In Bezug auf alle Informationen, die sie bearbeiten und verwahren, berücksichtigen die Organe und Einrichtungen der Union bei der Festlegung der Sicherheitsanforderungen die folgenden Aspekte:

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

b) Verfügbarkeit: die Informationen sind auf Anfrage einer befugten Stelle zugänglich und nutzbar;

c) Vertraulichkeit: Informationen werden gegenüber unbefugten Personen, Stellen oder Prozessen nicht offengelegt;

d) Integrität: die Informationen sind vollständig und ihre Vollständigkeit bleibt gewährleistet;

e) Beweisbarkeit: es kann nachgewiesen werden, dass ein Vorgang oder ein Ereignis stattgefunden hat, sodass dieser Vorgang oder dieses Ereignis zu einem späteren Zeitpunkt nicht abgestritten werden kann.

(5) Für jedes Kommunikations- und Informationssystem in ihrem Zuständigkeitsbereich legen die Organe und Einrichtungen der Union fest, welche Vertraulichkeitsstufe darin höchstens bearbeitet und gespeichert werden darf, führen eine Bewertung des Informationssicherheitsrisikos durch und überwachen regelmäßig die Sicherheitsanforderungen und die ordnungsgemäße Umsetzung der festgelegten Schutzmaßnahmen.

(6) Alle Organe und Einrichtungen der Union bieten in Bezug auf die Bearbeitung und Verwahrung von nicht als Verschlusssache eingestuften Informationen und von EU-VS Schulungs- und Sensibilisierungsmaßnahmen an.

EU-VS bearbeitende und verwahrende Organe und Einrichtungen der Union organisieren mindestens alle fünf Jahre obligatorische Schulungen für alle Personen, die über eine Ermächtigung zum Zugang zu EU-VS verfügen. Für die mit Aufgaben im Bereich der Informationssicherheit betrauten Funktionen sehen die betreffenden Organe und Einrichtungen spezielle Schulungen vor.

Die Organe und Einrichtungen der Union können ihre Schulungs- und Sensibilisierungsmaßnahmen mit anderen Organen und Einrichtungen der Union abstimmen.

Artikel 5

Informationssicherheitsrisiko-Managementprozess

(1) Jedes Organ und jede Einrichtung der Union richtet einen Informationssicherheitsrisiko-Managementprozess ein, um die bearbeiteten und verwahrten Informationen zu schützen.

(2) Der Informationssicherheitsrisiko-Managementprozess umfasst die folgenden Schritte:

a) Ermittlung von Bedrohungen und Schwachstellen;

b) Risikobewertung;

c) Risikobehandlung;

d) Risikoakzeptanz;

e) Risikokommunikation.

(3) Der Informationssicherheitsrisiko-Managementprozess berücksichtigt alle für das betreffende Organ oder die betreffende Einrichtung der Union relevanten Faktoren, insbesondere:

a) die Vertraulichkeitsstufe der Informationen und die damit verbundenen rechtlichen Verpflichtungen;

b) die Form und Menge der Informationen sowie die Anlagen oder Kommunikations- und Informationssysteme, in denen die Informationen bearbeitet und verwahrt werden;

c) die Personen, die von den Standorten aus oder über Fernverbindungen auf die Informationen zugreifen;

d) die Umgebung und die Struktur der Gebäude oder Bereiche, in denen die Informationen verwahrt werden;

e) die Bedrohungen, denen die Union, die Organe und Einrichtungen der Union oder die Mitgliedstaaten im Hinblick auf Cyberangriffe, nachrichtendienstliche Tätigkeiten, Sabotage, Terrorismus, subversive und sonstige kriminelle Handlungen ausgesetzt sind;

f) die Betriebskontinuität und die Wiederherstellung nach einem Notfall;

g) gegebenenfalls die Ergebnisse von Inspektionen, Prüfungen oder Bewertungsbesuchen.

Kapitel 2
Steuerung und Organisation der Sicherheit

Artikel 6

Interinstitutionelle Koordinierungsgruppe für Informationssicherheit

(1) Es wird eine interinstitutionelle Koordinierungsgruppe für Informationssicherheit (im Folgenden „Koordinierungsgruppe“) eingesetzt.

Der Gruppe gehören alle Sicherheitsbehörden der Organe und Einrichtungen der Union an, und sie hat das Mandat, die gemeinsame Strategie für den Bereich der Informationssicherheit festzulegen.

(2) Die Koordinierungsgruppe wird einvernehmlich und im gemeinsamen Interesse aller Organe und Einrichtungen der Union

a) eine Geschäftsordnung verabschieden und jährlich gemeinsame Ziele und Prioritäten festlegen;

b) Beschlüsse über die Einsetzung thematischer Untergruppen und deren Mandate erlassen;

c) Leitlinien für die Anwendung dieser Verordnung erstellen und sich dabei gegebenenfalls mit dem in Artikel 9 der Verordnung (EU) [...] über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in den Organen, Einrichtungen und sonstigen Stellen der Union genannten interinstitutionellen Cybersicherheitsbeirat abstimmen;

d) für den Austausch von bewährten Verfahren und Wissen über für die Informationssicherheit relevante gemeinsame Themen und zur Unterstützung bei Informationssicherheitsvorfällen spezielle Plattformen einrichten;

e) sicherstellen, dass die Sicherheitsmaßnahmen zum Schutz von EU-VS erforderlichenfalls mit den zuständigen nationalen Sicherheitsbehörden abgestimmt werden.

(3) Die Koordinierungsgruppe benennt aus dem Kreis ihrer Mitglieder einen Vorsitzenden und zwei stellvertretende Vorsitzende für einen Zeitraum von drei Jahren.

(4) Die Koordinierungsgruppe tritt mindestens einmal jährlich auf Initiative ihres Vorsitzenden oder auf Antrag eines Organs oder einer Einrichtung der Union zusammen.

(5) Die Koordinierungsgruppe erhält administrative Unterstützung durch ein von der Kommission gestelltes ständiges Sekretariat.

(6) Jedes Organ und jede Einrichtung der Union ist in der Koordinierungsgruppe und gegebenenfalls in den thematischen Untergruppen angemessen vertreten.

(7) Die Organe und Einrichtungen der Union unterrichten die Koordinierungsgruppe über jede wichtige Entwicklung der in ihrer Organisation angewandten Informationssicherheitsstrategie.

(8) Bei der Wahrnehmung der in Absatz 2 Buchstabe e genannten Aufgaben wird die Koordinierungsgruppe von einem Ausschuss für Informationssicherheit unterstützt. Diesem Ausschuss gehört je ein Vertreter jeder nationalen Sicherheitsbehörde an, wobei das in Absatz 5 genannte Sekretariat der Koordinierungsgruppe den Vorsitz führt. Der Ausschuss für Informationssicherheit hat beratende Funktion.

Artikel 7

Thematische Untergruppen

(1) Die Koordinierungsgruppe setzt die folgenden ständigen thematischen Untergruppen ein, um die Anwendung dieser Verordnung zu erleichtern:

a) eine Untergruppe für Informationssicherung;

b) eine Untergruppe für nicht als Verschlusssache eingestufte Informationen;

c) eine Untergruppe für materiellen Geheimschutz;

d) eine Untergruppe für die Akkreditierung von Kommunikations- und Informationssystemen, in denen EU-VS bearbeitet und gespeichert werden;

e) eine Untergruppe für die Weitergabe von EU-VS und den Austausch von Verschlusssachen.

(2) Erforderlichenfalls kann die Koordinierungsgruppe für bestimmte Aufgaben befristete Ad-hoc-Untergruppen einsetzen.

(3) Sofern in ihren Mandaten nichts anderes bestimmt ist, steht die Mitgliedschaft in den Untergruppen Vertretern der betreffenden Organe oder Einrichtungen der Union offen. Die Mitglieder der Untergruppen sind Experten ihres jeweiligen Fachgebiets.

(4) Das in Artikel 6 Absatz 5 genannte Sekretariat der Koordinierungsgruppe unterstützt die Arbeit aller Untergruppen und stellt die Kommunikation zwischen ihren Mitgliedern sicher.

Artikel 8

Organisation der Sicherheit

(1) Jedes Organ und jede Einrichtung der Union benennt eine Sicherheitsbehörde, die die in dieser Verordnung sowie gegebenenfalls in internen Sicherheitsvorschriften festgelegten Zuständigkeiten wahrnimmt. Bei der Wahrnehmung ihrer Aufgaben wird jede Sicherheitsbehörde von der für Informationssicherheit zuständigen Dienststelle oder Person unterstützt.

(2) Erforderlichenfalls erlassen die Sicherheitsbehörden der Organe und Einrichtungen der Union im Einklang mit ihrem jeweiligen durch die Rechtvorschriften der Union übertragenen Auftrag und auf der Grundlage ihrer institutionellen Autonomie für den Schutz der Informationen interne Durchführungsbestimmungen.

(3) Jede Sicherheitsbehörde kann gegebenenfalls auch folgende Aufgaben wahrnehmen:

a) Ausarbeitung der Sicherheitskonzepte und -leitlinien für Informationssicherung sowie Überwachung ihrer Wirksamkeit und Angemessenheit (Informationssicherungsstelle);

b) Ausarbeitung der Sicherheitsdokumentation, insbesondere der sicherheitsbezogenen Betriebsverfahren und des Kryptokonzepts im Rahmen des Akkreditierungsverfahrens für Kommunikations- und Informationssysteme, (für den Betrieb zuständige Informationssicherungsstelle);

c) Akkreditierung von Sicherheitsbereichen und Kommunikations- und Informationssystemen für die Bearbeitung und Verwahrung von EU-VS (Sicherheitsakkreditierungsstelle);

d) Genehmigung der Maßnahmen zum Schutz von EU-VS vor Kenntnisnahme durch unbeabsichtigte elektronische Abstrahlung (TEMPEST-Stelle);

e) Genehmigung von Anträgen der Systemeigner zur Verwendung von Verschlüsselungstechnologien (Krypto-Zulassungsstelle);

f) Verteilung des kryptografischen Materials zum Schutz von EU-VS (Kodiergeräte, Kryptografieschlüssel, Zertifikate und zugehörige Authentisierer) an die betreffenden Nutzer (Krypto-Verteilungsstelle).

(4) Die Zuständigkeiten für eine oder mehrere der in Absatz 3 genannten Aufgaben können einem anderen Organ oder einer anderen Einrichtung der Union übertragen

werden, sofern die Auslagerung dieser Sicherheitsdienste erhebliche Effizienzvorteile oder Ressourcen- oder Zeiteinsparungen ermöglicht.

Kapitel 3
Informationssicherung und Kommunikations- und Informationssysteme (CIS)

Artikel 9

Grundsätze der Informationssicherung

(1) Die Bewertung der Informationssicherheitsanforderungen in Bezug auf alle Kommunikations- und Informationssysteme, einschließlich interner, ausgelagerter und hybrider Systeme, wird jeweils von Beginn an bei der Einrichtung oder bei der Auftragsvergabe berücksichtigt.

(2) Jedes Kommunikations- und Informationssystem, in dem EU-VS bearbeitet und gespeichert werden, muss gemäß Kapitel 5 Abschnitt 5 akkreditiert sein. Jedes Kommunikations- und Informationssystem, in dem nicht als Verschlusssache eingestufte vertrauliche Informationen bearbeitet und gespeichert werden, muss die in Kapitel 4 festgelegten Mindestanforderungen erfüllen.

Artikel 10

Untergruppe für Informationssicherung

(1) Die Untergruppe für Informationssicherung gemäß Artikel 7 Absatz 1 Buchstabe a hat folgende Aufgaben und Zuständigkeiten:

a) Bereitstellung von Leitlinien und bewährten Vorgehensweisen für die Kennzeichnung, Bearbeitung und Speicherung von Informationen in Kommunikations- und Informationssystemen in enger Abstimmung mit dem in Artikel 9 der Verordnung (EU) [...] über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in den Organen, Einrichtungen und sonstigen Stellen der Union genannten interinstitutionellen Cybersicherheitsbeirat;

b) Festlegung eines Metadatenschemas für Kennzeichnungen und alle erforderlichen technischen Informationen, um den Organen und Einrichtungen der Union bei der Zusammenschaltung ihrer Kommunikations- und Informationssysteme einen interoperablen und nahtlosen Informationsaustausch zu ermöglichen;

c) Förderung der Kohärenz zwischen den Organen und Einrichtungen der Union in Bezug auf die Informationssicherheitsvorschriften und die Cybersicherheitsgrundregeln gemäß Artikel 5 der Verordnung (EU) [...] über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in den Organen, Einrichtungen und sonstigen Stellen der Union.

Artikel 11

Anforderungen an Kommunikations- und Informationssysteme

(1) Die Organe und Einrichtungen der Union informieren die Nutzer über die Vertraulichkeitsstufen der Informationen, die in Kommunikations- und

Informationssystemen bearbeitet und gespeichert werden können. Werden in einem Kommunikations- und Informationssystem Informationen mehrerer Vertraulichkeitsstufen bearbeitet und gespeichert, so sind Metadaten und visuelle Kennzeichnungen zu verwenden, um sicherzustellen, dass die verschiedenen Stufen unterscheidbar sind.

(2) Die Organe und Einrichtungen der Union ermitteln die Nutzer des Kommunikations- und Informationssystems, denen Zugang zu Informationen anderer Vertraulichkeitsstufen als „für die Öffentlichkeit bestimmte Information“ gewährt werden soll. Die Authentifizierung der Nutzer erfolgt auf einem der Vertraulichkeitsstufe angemessenen Sicherheitsniveau. Gegebenenfalls wird ein sicheres gemeinsames Identifizierungssystem verwendet.

(3) Für alle Kommunikations- und Informationssysteme werden geeignete Sicherheitsprotokolle geführt, um im Falle von Sicherheitsverletzungen oder unbefugter Weitergabe von Informationen rasche Ermittlungen zu ermöglichen. Diese Protokolle werden für einen in der Folgenabschätzung oder in den einschlägigen Sicherheitskonzepten festgelegten Zeitraum als Beweismittel aufbewahrt.

Werden in einem Kommunikations- und Informationssystem EU-VS bearbeitet und gespeichert, so werden für die jeweiligen Informationen Protokolle über die „Kenntnis nur, wenn nötig“-Ermächtigungen und den Zugang zu Informationen so lange geführt, bis der Geheimhaltungsgrad der Information aufgehoben wird. Die Sicherheitsprotokolle müssen für die Sicherheitsbehörde zugänglich sein und von ihr durchsucht werden können.

(4) Die Organe und Einrichtungen der Union erlassen interne Vorschriften für die Sicherheit von Kommunikations- und Informationssystemen, in denen die Sicherheitsmaßnahmen zur Gewährleistung der jeweiligen Sicherheitsanforderungen der zu bearbeitenden und zu speichernden Informationen festgelegt werden, wobei sie auch die Rechtsvorschriften der Länder berücksichtigen, an die die Informationen übermittelt werden und in denen sie verwahrt oder bearbeitet werden. Diese Maßnahmen umfassen gegebenenfalls Folgendes:

a) Einschränkungen in Bezug auf geografische Standorte;

b) die Berücksichtigung potenzieller Interessenkonflikte, Boykotte oder Sanktionen in Bezug auf Auftragnehmer;

c) vertragliche Bestimmungen zur Gewährleistung der Informationssicherheit;

d) die Verschlüsselung von ruhenden Informationen sowie von Informationen während der Übertragung;

e) für das Personal der Auftragnehmer geltende Zugangsbeschränkungen bezüglich Informationen der Organe und Einrichtungen der Union;

f) den Schutz personenbezogener Daten im Einklang mit den geltenden Datenschutzvorschriften.

(5) Die Organe und Einrichtungen der Union verwalten ihre Kommunikations- und Informationssysteme nach den folgenden Grundsätzen:

a) Jedes Kommunikations- und Informationssystem verfügt über einen Systemeigner oder eine für den Betrieb zuständige Informationssicherungsstelle, die für seine Sicherheit zuständig sind.

b) Es wird ein Informationssicherheitsrisiko-Managementprozess angewendet, der die Aspekte der Informationssicherheit abdeckt.

c) Die Sicherheitsanforderungen und sicherheitsbezogenen Betriebsverfahren werden förmlich festgelegt, umgesetzt, überprüft und überarbeitet.

d) Informationssicherheitsvorfälle werden gemäß der Verordnung (EU) Nr. [XXX] über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in den Organen, Einrichtungen und sonstigen Stellen der Union förmlich aufgezeichnet und weiterverfolgt.

Kapitel 4
Nicht als Verschlusssache eingestufte Informationen

Artikel 12

Für die Öffentlichkeit bestimmte Informationen

(1) Für die Öffentlichkeit oder die amtliche Veröffentlichung bestimmte oder bereits offengelegte Informationen, die innerhalb oder außerhalb der Organe und Einrichtungen der Union ohne Einschränkungen weitergegeben werden können, werden als für die Öffentlichkeit bestimmte Informationen eingestuft und entsprechend bearbeitet und verwahrt.

(2) Die Organe und Einrichtungen der Union können Informationen nach Absatz 1 mit der Kennzeichnung „PUBLIC USE“ versehen.

(3) Alle Organe und Einrichtungen der Union gewährleisten die Integrität und Verfügbarkeit von für die Öffentlichkeit bestimmten Informationen durch geeignete, den Sicherheitsanforderungen entsprechende Maßnahmen.

Artikel 13

Normale Informationen

(1) Informationen, die die Organe und Einrichtungen der Union im Rahmen ihrer Aufgaben verwenden und bei denen es sich weder um nicht als Verschlusssache eingestufte vertrauliche Informationen noch um für die Öffentlichkeit bestimmte Informationen handelt, werden als normale Informationen eingestuft, bearbeitet und verwahrt. Diese Kategorie umfasst alle Informationen für den normalen Geschäftsbetrieb, die in dem betreffenden Organ oder der betreffenden Einrichtung der Union verarbeitet werden.

(2) Normale Informationen können visuell oder über Metadaten gekennzeichnet werden, wenn dies zur Gewährleistung ihres Schutzes erforderlich ist, insbesondere wenn sie außerhalb der Organe und Einrichtungen der Union weitergegeben werden. In diesem Fall ist die Kennzeichnung „EU NORMAL“ oder „*[Name oder Akronym des Organs oder der Einrichtung der Union]* NORMAL“ zu verwenden.

(3) Die Organe und Einrichtungen der Union legen für normale Informationen Standardschutzmaßnahmen fest und berücksichtigen dabei die Leitlinien der Untergruppe für nicht als Verschlusssache eingestufte Informationen sowie die etwaigen spezifischen Risiken im Zusammenhang mit ihren Aufgaben und Tätigkeiten.

(4) Normale Informationen werden außerhalb der Organe und Einrichtungen der Union nur mit natürlichen oder juristischen Personen ausgetauscht, die Kenntnis davon haben
müssen.

Artikel 14

Nicht als Verschlusssache eingestufte vertrauliche Informationen

(1) Die Organe und Einrichtungen der Union stufen alle Informationen, die nicht als Verschlusssache eingestuft sind, jedoch aufgrund rechtlicher Verpflichtungen oder aufgrund des Schadens, der den berechtigten privaten oder öffentlichen Interessen (einschließlich der Interessen der Organe und Einrichtungen der Union, der Mitgliedstaaten oder Einzelpersonen) durch ihre unbefugte Offenlegung entstehen kann, zu schützen sind, als nicht als Verschlusssache eingestufte vertrauliche Information ein und bearbeiten und verwahren sie als solche.

(2) Jedes Organ und jede Einrichtung der Union versieht die nicht als Verschlusssache eingestuften vertraulichen Informationen mit einer sichtbaren Sicherheitskennzeichnung und legt gemäß Anhang I entsprechende Bearbeitungsanweisungen fest.

(3) Die Organe und Einrichtungen der Union schützen die nicht als Verschlusssache eingestuften vertraulichen Informationen, indem sie in Bezug auf deren Bearbeitung und Verwahrung geeignete Maßnahmen anwenden. Diese Informationen dürfen innerhalb der Organe und Einrichtungen der Union nur Personen zugänglich gemacht werden, die zur Erfüllung der ihnen übertragenen Aufgaben von diesen Informationen Kenntnis haben müssen.

(4) Nicht als Verschlusssache eingestufte vertrauliche Informationen werden außerhalb der Organe und Einrichtungen der Union unter Berücksichtigung der mit diesen Informationen verbundenen Bearbeitungsanweisungen nur mit natürlichen oder juristischen Personen ausgetauscht, die Kenntnis davon haben müssen. Alle Beteiligten sind über die entsprechenden Bearbeitungsanweisungen zu informieren.

Artikel 15

Schutz der nicht als Verschlusssache eingestuften Informationen und Interoperabilität

(1) Die Organe und Einrichtungen der Union legen Verfahren für die Meldung und die Bewältigung von Vorfällen oder mutmaßlichen Vorfällen fest, die zu einer Gefährdung der Sicherheit von nicht als Verschlusssache eingestuften Informationen führen könnten.

(2) Erforderlichenfalls verwenden die Organe und Einrichtungen der Union die in den Artikeln 12, 13 und 14 vorgesehenen Kennzeichnungen. In Ausnahmefällen können intern und in Bezug auf ihre jeweiligen Partner in anderen Organen und Einrichtungen der Union oder in den Mitgliedstaaten andere gleichwertige Kennzeichnungen verwendet werden, sofern alle Parteien dem zustimmen. Jede solche Ausnahme wird der Untergruppe für nicht als Verschlusssache eingestufte Informationen gemäß Artikel 7 Absatz 1 Buchstabe b mitgeteilt.

(3) Es werden vertragliche Vorkehrungen getroffen, um den Schutz normaler und nicht als Verschlusssache eingestufter vertraulicher Informationen, die von ausgelagerten

Diensten verarbeitet werden, zu gewährleisten. Diese Schutzvorkehrungen sind so zu gestalten, dass sie ein Schutzniveau gewährleisten, das dem in dieser Verordnung vorgesehenen mindestens gleichwertig ist, und schließen Vertraulichkeits- und Geheimhaltungsverpflichtungen ein, die von allen relevanten und an der Bereitstellung der ausgelagerten Systeme beteiligten Dienstleistern zu unterzeichnen sind.

Artikel 16

Untergruppe für nicht als Verschlusssache eingestufte Informationen

(1) Die Untergruppe für nicht als Verschlusssache eingestufte Informationen gemäß Artikel 7 Absatz 1 Buchstabe b hat folgende Aufgaben und Zuständigkeiten:

a) Straffung der Verfahren für die Bearbeitung und Verwahrung der nicht als Verschlusssache eingestuften Informationen und Ausarbeitung der einschlägigen Leitlinien;

b) Koordinierung mit der Untergruppe für Informationssicherung gemäß Artikel 7 Absatz 1 Buchstabe a in allen Angelegenheiten bezüglich Systemen, in denen nicht als Verschlusssache eingestufte Informationen bearbeitet und gespeichert werden;

c) Ausarbeitung von Bearbeitungsanweisungen für nicht als Verschlusssache eingestufte Informationen verschiedener Vertraulichkeitsstufen;

d) Unterstützung der Organe und Einrichtungen der Union bei der Festlegung der Gleichwertigkeit zwischen ihren jeweiligen Kategorien von nicht als Verschlusssache eingestuften Informationen und den in den Artikeln 12, 13 und 14 vorgesehenen Kategorien;

e) Unterstützung und Beratung zur Erleichterung des Austauschs von nicht als Verschlusssache eingestuften Informationen zwischen den Organen und Einrichtungen der Union.

Artikel 17

Bearbeitung und Speicherung von nicht als Verschlusssache eingestuften vertraulichen Informationen in Kommunikations- und Informationssystemen

(1) Die Organe und Einrichtungen der Union stellen sicher, dass die Kommunikations- und Informationssysteme in Bezug auf die Bearbeitung und Speicherung von nicht als Verschlusssache eingestuften vertraulichen Informationen die folgenden Mindestanforderungen erfüllen:

a) Für den Zugriff auf nicht als Verschlusssache eingestufte vertrauliche Informationen wird eine starke Authentisierung eingesetzt, und nicht als Verschlusssache eingestufte vertrauliche Informationen werden bei der Übermittlung und Speicherung verschlüsselt.

b) Die für die Speicherung verwendeten Kryptografieschlüssel fallen unter die Verantwortung der für den Betrieb des betreffenden Kommunikations- und Informationssystems zuständigen Organe oder Einrichtungen der Union.

c) Nicht als Verschlusssache eingestufte vertrauliche Informationen werden in der Union verwahrt und verarbeitet.

d) In alle Auslagerungsverträge werden Vertragsbestimmungen über die Sicherheit von Personal, Werten und Informationen aufgenommen.

e) Es werden interoperable Metadaten verwendet, um den Vertraulichkeitsgrad elektronischer Dokumente festzuhalten und die Automatisierung von Sicherheitsmaßnahmen zu erleichtern.

f) Um nicht als Verschlusssache eingestufte vertrauliche Informationen zu schützen, treffen die Organe und Einrichtungen der Union Maßnahmen zur Verhinderung und Erkennung von unbefugter Weitergabe von Daten.

g) Soweit vorhanden wird Sicherheitsausrüstung mit europäischem Cybersicherheitszertifikat verwendet.

h) Um den Zugang von Dienstleistern und Auftragnehmern zu nicht als Verschlusssache eingestuften vertraulichen Informationen auf ein Mindestmaß zu beschränken, werden Sicherheitsmaßnahmen angewandt, die auf den Grundsätzen „Kenntnis nur, wenn nötig“ und „Zero-Trust“ beruhen.

(2) Ausnahmen von den Mindestanforderungen nach Absatz 1 bedürfen der Genehmigung durch die betreffende Verwaltungsebene des jeweiligen Organs oder der jeweiligen Einrichtung der Union auf der Grundlage einer Risikobewertung, die die rechtlichen und technischen Risiken in Bezug auf die Sicherheit der nicht als Verschlusssache eingestuften vertraulichen Informationen abdeckt.

(3) Die Informationssicherungsstelle des betreffenden Organs oder der betreffenden Einrichtung der Union kann die Einhaltung der in Absatz 1 genannten Grundsätze während des Lebenszyklus eines Kommunikations- und Informationssystems jederzeit überprüfen.

Kapitel 5
EU-Verschlusssachen

ABSCHNITT 1
ALLGEMEINE BESTIMMUNGEN

Artikel 18

Geheimhaltungsgrade und Kennzeichnungen

(1) EU-Verschlusssachen werden in einen der folgenden Geheimhaltungsgrade eingestuft und entsprechend gekennzeichnet:

a) TRES SECRET UE/EU TOP SECRET: Informationen und Materialien, deren unbefugte Offenlegung den wesentlichen Interessen der Union oder eines oder mehrerer Mitgliedstaaten äußerst schweren Schaden zufügen könnte;

b) SECRET UE/EU SECRET: Informationen und Materialien, deren unbefugte Offenlegung den wesentlichen Interessen der Union oder eines oder mehrerer Mitgliedstaaten schweren Schaden zufügen könnte;

c) CONFIDENTIEL UE/EU CONFIDENTIAL: Informationen und Materialien, deren unbefugte Offenlegung den wesentlichen Interessen der Union oder eines oder mehrerer Mitgliedstaaten Schaden zufügen könnte;

d) RESTREINT UE/EU RESTRICTED: Informationen und Materialien, deren unbefugte Offenlegung für die Interessen der Union oder eines oder mehrerer Mitgliedstaaten nachteilig sein könnte.

(2) Die Koordinierungsgruppe nimmt Leitlinien für die Erstellung und Einstufung von EU-VS an.

Artikel 19

Befugnis zur Bearbeitung und Verwahrung von EU-Verschlusssachen

(1) Die Organe und Einrichtungen der Union sind befugt, EU-VS zu bearbeiten und zu verwahren, sofern alle folgenden Bedingungen erfüllt sind:

a) sie legen im Einklang mit dieser Verordnung Vorschriften und Verfahren fest, die den Schutz der Information gemäß ihrem Geheimhaltungsgrad gewährleisten; und

b) sie wurden einem Bewertungsbesuch nach Artikel 53 unterzogen, und ihre Fähigkeit, EU-VS im Einklang mit dieser Verordnung und gegebenenfalls anderen einschlägigen Vorschriften und Verfahren zu schützen, wurde bestätigt.

(2) In Bezug auf die Mitglieder der Untergruppe für die Weitergabe von EU-VS und den Austausch von Verschlusssachen gemäß Artikel 7 Absatz 1 Buchstabe e gelten die in Absatz 1 des vorliegenden Artikels genannten Bedingungen grundsätzlich als erfüllt.

Artikel 20

Schutz von EU-Verschlusssachen

(1) Der Besitzer jedweder EU-VS ist dafür verantwortlich, diese zu schützen.

(2) Überträgt ein Mitgliedstaat Verschlusssachen, die mit einem nationalen Geheimhaltungsgrad gekennzeichnet sind, in die Strukturen oder Netze eines Organs oder einer Einrichtung der Union, so schützt dieses Organ oder diese Einrichtung diese Verschlusssachen gemäß der im Abkommen zwischen den im Rat vereinigten Mitgliedstaaten der Union über den Schutz der im Interesse der Europäischen Union ausgetauschten Verschlusssachen[29] festgelegten jeweiligen Kennzeichnung. Die Entsprechungstabelle findet sich in Anhang VI dieser Verordnung.

(3) Eine Gesamtheit von EU-VS kann ein Schutzniveau erfordern, das einem höheren Geheimhaltungsgrad als dem ihrer einzelnen Bestandteile entspricht.

Artikel 21

Sicherheitsrisiko-Managementprozess für EU-Verschlusssachen

(1) Die zum Schutz von EU-VS während ihres gesamten Lebenszyklus vorgesehenen Sicherheitsmaßnahmen werden auf der Grundlage der Ergebnisse einer von dem jeweiligen Organ oder der jeweiligen Einrichtung der Union durchgeführten Risikobewertung von der Sicherheitsbehörde des Organs oder der Einrichtung der Union genehmigt.

[29] ABl. C 202 vom .8.7.2011, S. 13.

(2) Die von den einzelnen Organen und Einrichtungen der Union getroffenen Sicherheitsmaßnahmen müssen dem Geheimhaltungsgrad der bearbeiteten und verwahrten Informationen, ihrer Form und ihrer Menge, dem geografischen Standort und den Schutzmerkmalen der Anlagen, in denen sie bearbeitet und verwahrt werden sowie der Einschätzung hinsichtlich der örtlichen Bedrohung durch böswillige oder kriminelle Handlungen angemessen sein.

(3) Sämtliche Organe und Einrichtungen der Union erstellen

a) Notfallpläne, um die Sicherheit von EU-VS in Notfällen zu gewährleisten;

b) Betriebskontinuitätspläne mit Präventions- und Wiederherstellungsmaßnahmen, um die Auswirkungen größerer Störungen oder Sicherheitsvorfälle auf die Bearbeitung und Verwahrung von EU-VS so gering wie möglich zu halten.

Artikel 22

Verletzungen der Sicherheit und Kenntnisnahme von EU-VS durch Unbefugte

(1) Jede Handlung oder Unterlassung eines Organs oder einer Einrichtung der Union oder einer Person, die einen Verstoß gegen diese Verordnung darstellt, gilt als Verletzung der Sicherheit.

(2) EU-VS gelten als der Kenntnisnahme durch Unbefugte ausgesetzt, wenn sie infolge einer Verletzung der Sicherheit ganz oder teilweise an eine oder mehrere Personen weitergegeben wurden, die nicht zum Zugang zu diesen Informationen ermächtigt sind.

(3) Jede Kenntnisnahme oder vermutete Kenntnisnahme von EU-VS durch Unbefugte ist unverzüglich der Sicherheitsbehörde des betreffenden Organs oder der betreffenden Einrichtung der Union zu melden, die eine Sicherheitsuntersuchung durchführt und mindestens

a) den Herausgeber verständigt;

b) sicherstellt, dass der Fall zur Aufklärung des Sachverhalts von Personal untersucht wird, das von der Sicherheitsverletzung nicht unmittelbar betroffen ist;

c) den potenziellen Schaden für die Interessen der Union oder der Mitgliedstaaten einschätzt;

d) dafür sorgt, dass sich ein solcher Vorfall nicht wiederholt;

e) die zuständigen Behörden über die tatsächliche oder potenzielle Kenntnisnahme durch Unbefugte und die getroffenen Maßnahmen unterrichtet.

ABSCHNITT 2
PERSONELLER GEHEIMSCHUTZ

Artikel 23

Grundsätze

(1) Die Sicherheitsbehörde eines Organs oder einer Einrichtung der Union kann Einzelpersonen Zugang zu EU-VS gewähren, wenn alle folgenden Bedingungen erfüllt sind:

a) die Personen erfüllen das „Kenntnis, nur wenn nötig“-Kriterium;

b) die Personen wurden über die Sicherheitsvorschriften und -verfahren für den Schutz von EU-VS sowie die entsprechenden Sicherheitsstandards und -leitlinien belehrt und haben ihre Verantwortlichkeiten hinsichtlich des Schutzes solcher Informationen schriftlich anerkannt;

c) für als „CONFIDENTIEL UE/EU CONFIDENTIAL“ oder höher eingestufte Verschlusssachen müssen die betreffenden Personen über eine Sicherheitsermächtigung verfügen und eine Ermächtigung für den entsprechenden Geheimhaltungsgrad erhalten haben.

(2) Die Organe und Einrichtungen der Union berücksichtigen die Loyalität, Vertrauenswürdigkeit und Zuverlässigkeit einer Person, die durch eine von den zuständigen Behörden des Mitgliedstaats, dessen Staatsangehörigkeit der Antragsteller besitzt, durchgeführte Sicherheitsüberprüfung festgestellt wurde.

(3) Die Organe und Einrichtungen der Union können Sicherheitsermächtigungen von Drittstaaten und internationalen Organisationen, mit denen die Union ein Geheimschutzabkommen geschlossen hat, anerkennen.

(4) Die Organe und Einrichtungen der Union können die Sicherheitsermächtigungsverfahren autonom verwalten oder für die Zwecke der Sicherheitsermächtigung eine Leistungsvereinbarung (Service Level Agreement, SLA) mit der Kommission anstreben.

Wird eine Leistungsvereinbarung geschlossen, ist die Sicherheitsbehörde der Kommission die Kontaktstelle zwischen den Sicherheitsbüros der betreffenden Organe und Einrichtungen der Union und den zuständigen nationalen Behörden der Mitgliedstaaten im Zusammenhang mit Fragen der Sicherheitsermächtigung.

(5) Die Sicherheitsbehörde jedes Organs und jeder Einrichtung der Union führt Aufzeichnungen über ihre Sicherheitsermächtigungen, Unterweisungen, schriftlichen Bestätigungen und Ermächtigungen zum Zugang zu EU-VS.

(6) Die Organe und Einrichtungen der Union, die mit der Kommission eine Leistungsvereinbarung schließen, stellen der Sicherheitsbehörde der Kommission einschlägige Aufzeichnungen mindestens über den Geheimhaltungsgrad der EU-VS, zu denen die betreffende Person Zugang erhalten kann, das Datum der Erteilung der Ermächtigung zum Zugang zu EU-VS und deren Gültigkeitsdauer zur Verfügung. Diese Aufzeichnungen sind anderen Organen und Einrichtungen der Union, die über eine Leistungsvereinbarung verfügen, in begründeten Fällen zugänglich.

Artikel 24

Ermächtigung zum Zugang zu EU-VS

(1) Jedes Organ und jede Einrichtung der Union bestimmt die internen Dienstposten, für die ein Zugang zu als „CONFIDENTIEL UE/EU CONFIDENTIAL“ oder höher eingestuften Verschlusssachen erforderlich ist, um dem Inhaber die Erfüllung seiner Verpflichtungen zu ermöglichen.

(2) Benötigt eine Person die Ermächtigung zum Zugang zu als „CONFIDENTIEL UE/EU CONFIDENTIAL“ oder höher eingestuften Verschlusssachen, so unterrichtet das betreffende Organ oder die betreffende Einrichtung die zuständige Sicherheitsbehörde, die die in Anhang II Nummer 1 vorgeschriebenen Formalitäten erledigt.

(3) Die Sicherheitsbehörde jedes Organs und jeder Einrichtung der Union ist für die Gewährung, Aussetzung, Entziehung und Verlängerung der Ermächtigungen zum Zugang zu EU-VS für ihr Personal verantwortlich.

(4) Unter außergewöhnlichen Umständen - wenn dies im dienstlichen Interesse hinreichend begründet ist und bis zum Abschluss einer umfassenden Sicherheitsüberprüfung - kann die Sicherheitsbehörde eines Organs oder einer Einrichtung der Union Personen unbeschadet der Bestimmungen über die Verlängerung der Ermächtigung zum Zugang zu EU-VS und nach Überprüfung durch die zuständige nationale Sicherheitsbehörde eine befristete Ermächtigung zum Zugang zu EU-VS für einen bestimmten Dienstposten erteilen.

(5) Die Organe und Einrichtungen der Union halten die in Anhang II festgelegten Verfahren für die Verwaltung der Ermächtigungen zum Zugang zu EU-VS ein.

Artikel 25

Anerkennung von Ermächtigungen zum Zugang zu EU-VS

(1) Eine Ermächtigung zum Zugang zu EU-VS bis zu dem angegebenen Geheimhaltungsgrad ist in jedem Organ und jeder Einrichtung der Union, dem/der die betreffende Person zugewiesen ist, gültig.

(2) Die Organe und Einrichtungen der Union erkennen die von anderen Organen oder Einrichtungen der Union erteilten Ermächtigungen zum Zugang zu EU-VS an.

(3) Nimmt der Inhaber einer Ermächtigung zum Zugang zu EU-VS eine Beschäftigung bei einem anderen Organ oder einer anderen Einrichtung der Union auf, so teilt dieses Organ bzw. diese Einrichtung der Union der betreffenden nationalen Sicherheitsbehörde über die zuständige Sicherheitsbehörde den Wechsel des Arbeitgebers mit.

Artikel 26

Unterrichtung zu EU-VS

(1) Die Sicherheitsbehörde eines Organs oder einer Einrichtung der Union unterrichtet alle Personen, die Zugang zu EU-VS benötigen, über jegliche Sicherheitsbedrohungen und über ihre Pflicht, verdächtige Handlungen zu melden. Die Unterrichtung findet vor der Gewährung des Zugangs zu EU-VS und danach mindestens alle fünf Jahre statt.

(2) Nach der in Absatz 1 genannten Unterrichtung bestätigen alle betreffenden Personen schriftlich, dass sie sich ihrer Pflichten in Bezug auf den Schutz von EU-VS und der Folgen einer Kenntnisnahme von EU-VS durch Unbefugte bewusst sind.

(3) Die Unterrichtung nach Absatz 1 enthält folgende Informationen:

a) Gegen jede Person, die für eine Verletzung der Sicherheitsvorschriften dieser Verordnung verantwortlich ist, können disziplinarische Maßnahmen gemäß den geltenden Vorschriften ergriffen werden.

b) Gegen jede Person, die für die Kenntnisnahme von EU-VS durch Unbefugte oder deren Verlust verantwortlich ist, können gemäß den geltenden Gesetzen und Vorschriften Disziplinarmaßnahmen ergriffen oder rechtliche Schritte unternommen werden.

(4) Benötigen Personen, denen Ermächtigungen zum Zugang zu EU-VS erteilt wurden, diesen Zugang nicht mehr, so stellen die Organe und Einrichtungen der Union sicher, dass sich diese Personen ihrer Verpflichtungen in Bezug auf den fortgesetzten Schutz von EU-VS bewusst sind und diese Verpflichtungen gegebenenfalls schriftlich bestätigen.

(5) Die Erstellung und Verwaltung der Unterrichtungen zu EU-VS können die Organe und Einrichtungen der Union gemeinsam organisieren, sofern deren spezifischen Anforderungen Rechnung getragen wird.

ABSCHNITT 3
MATERIELLER GEHEIMSCHUTZ

Artikel 27

Grundsätze

(1) Jedes Organ und jede Einrichtung der Union legt auf der Grundlage einer von seiner/ihrer Sicherheitsbehörde durchgeführten Risikobewertung die für seine/ihre Standorte geeigneten materiellen Geheimschutzmaßnahmen im Einklang mit Anhang III und dem Grundsatz der mehrstufigen Sicherheitsmechanismen (gestaffeltes Sicherheitskonzept) fest. Die Maßnahmen sollen Folgendes gewährleisten:

a) Verhinderung des Zugangs zu EU-VS oder des gewaltsamen Eindringens unbefugter Personen;

b) Abschreckung, Verhinderung und Aufdeckung unbefugter Handlungen und schnellstmögliche Reaktion auf Sicherheitsvorfälle;

c) Einteilung des Personals in Bezug auf seinen Zugang zu EU-VS nach dem Grundsatz „Kenntnis nur, wenn nötig“ und gegebenenfalls der Sicherheitsermächtigung.

(2) Die Organe und Einrichtungen der Union treffen materielle Geheimschutzmaßnahmen für alle Standorte, an denen EU-VS erörtert, aufbewahrt oder bearbeitet werden, einschließlich der Bereiche, in denen Kommunikations- und Informationssysteme gemäß Abschnitt 5 dieses Kapitels untergebracht sind.

(3) Für den materiellen Schutz von als „CONFIDENTIEL UE/EU CONFIDENTIAL“ oder höher eingestuften Verschlusssachen dürfen nur von der Sicherheitsbehörde eines Organs oder einer Einrichtung der Union genehmigte Sicherheitsausrüstungen verwendet werden.

(4) Die Organe und Einrichtungen der Union können nach Abschluss einer Vereinbarung Sicherheitsbereiche gemäß Anhang III für die Bearbeitung und Aufbewahrung von EU-VS gemeinsam nutzen.

Artikel 28

Untergruppe für materiellen Geheimschutz

(1) Die Untergruppe für materiellen Geheimschutz gemäß Artikel 7 Absatz 1 Buchstabe c hat folgende Aufgaben und Zuständigkeiten:

a) Ausarbeitung von Leitfäden zu Fragen des materiellen Geheimschutzes;

b) Festlegung der allgemeinen Sicherheitskriterien für den Erwerb von Ausrüstung wie Sicherheitsbehältern, Schreddermaschinen, Türschlössern, elektronischen Zugangskontrollsystemen, Einbruchmeldesystemen und Alarmsystemen zum materiellen Schutz von EU-VS;

c) Unterstützung der Organe und Einrichtungen der Union bei der Festlegung geeigneter Sicherheitsmaßnahmen für ihre Standorte;

d) Vorschläge für Ausgleichsmaßnahmen für den Schutz von EU-VS, wenn EU-VS außerhalb der materiell geschützten Bereiche eines Organs bzw. einer Einrichtung der Union bearbeitet werden.

Artikel 29

Materieller Schutz von EU-VS

(1) Um den materiellen Schutz von EU-VS zu gewährleisten, richten die Organe und Einrichtungen der Union die folgenden materiell geschützten Bereiche ein:

a) Verwaltungsbereiche gemäß Anhang III;

b) gegebenenfalls Sicherheitsbereiche der Klassen I und II und technische Sicherheitsbereiche gemäß Anhang III.

(2) Die Sicherheitsbehörde des betreffenden Organs und der betreffenden Einrichtung der Union führt eine interne Inspektion durch, um zu überprüfen, ob die in Anhang III festgelegten Bedingungen für die Einrichtung eines Verwaltungsbereichs oder Sicherheitsbereichs erfüllt sind. Geht aus dem Inspektionsbericht hervor, dass die Bedingungen erfüllt sind, kann die Sicherheitsbehörde für den Sicherheitsbereich zum Schutz von EU-VS bis zu dem angegebenen Geheimhaltungsgrad eine Akkreditierung für einen Zeitraum von höchstens fünf Jahren erteilen.

Die Sicherheitsbehörde des betreffenden Organs oder der betreffenden Einrichtung der Union ist dafür zuständig, die Sicherheitsbereiche vor Ablauf der Akkreditierung oder nach Durchführung von Änderungen im akkreditierten Bereich erneut zu akkreditieren.

(3) Jedes Organ und jede Einrichtung der EU legt für Büros, Räume, Tresorräume und Sicherheitsbehältnisse, die für als CONFIDENTIEL UE/EU CONFIDENTIAL oder höher eingestufte EU-VS verwendet werden, Verfahren für die Verwaltung der Schlüssel und Kombinationen fest.

(4) Die Sicherheitsbehörde kann Durchsuchungen an den Ein- und Ausgängen gestatten, um vom unbefugten Verbringen von Material in die Räumlichkeiten oder der unbefugten Mitnahme von EU-VS aus den Räumlichkeiten abzuschrecken und solche Handlungen aufzudecken.

(5) Die Organe und Einrichtungen der Union legen die Maßnahmen für den materiellen Schutz von EU-VS gemäß Anhang III fest.

ABSCHNITT 4
BEHANDLUNG VON EU-VERSCHLUSSSACHEN

Artikel 30

Grundsätze

(1) Die EU-VS werden im Einklang mit den für die Akten des jeweiligen Organs und der jeweiligen Einrichtung der Union geltenden Grundsätzen und Vorschriften aufgezeichnet, abgelegt, aufbewahrt und schließlich vernichtet, ausgesondert oder an die einschlägigen Archive übermittelt.

(2) Organe und Einrichtungen der Union, die EU-VS herausgeben, legen bei deren Erstellung im Einklang mit Artikel 18 Absatz 1 den Geheimhaltungsgrad dieser Informationen fest.

(3) Die Organe und Einrichtungen der Union teilen den Empfängern jeden Geheimhaltungsgrad eindeutig mit, entweder mittels einer Einstufungskennzeichnung oder, wenn die Informationen mündlich übermittelt werden, durch eine entsprechende Ankündigung.

(4) Die für ein Originaldokument geltenden Sicherheitsmaßnahmen finden auch auf Entwürfe, Kopien und Übersetzungen dieses Dokuments Anwendung.

(5) Die Organe und Einrichtungen der Union legen die Maßnahmen für die Behandlung von EU-VS gemäß Anhang IV fest.

Artikel 31

Erstellung von EU-Verschlusssachen

(1) Die Organe und Einrichtungen der Union, unter deren Aufsicht EU-VS erstellt werden, stellen sicher, dass folgende Anforderungen erfüllt sind:

a) auf jeder Seite wird der Geheimhaltungsgrad eindeutig vermerkt;

b) jede Seite wird nummeriert;

c) das Dokument wird mit einem Aktenzeichen sowie gegebenenfalls mit einer Registrierungsnummer und mit einem Betreff versehen, der selbst keine EU-VS ist, sofern er nicht ebenfalls entsprechend gekennzeichnet ist;

d) das Dokument enthält das Datum seiner Erstellung;

e) alle Anhänge und Anlagen werden nach Möglichkeit auf der ersten Seite aufgeführt;

f) Dokumente des Geheimhaltungsgrads „SECRET UE/EU SECRET“ oder höher, die in mehreren Exemplaren verteilt werden sollen, erhalten auf jeder Seite eine eigene Exemplarnummer. Elektronische Kopien, die außerhalb des Verwahrsystems verteilt werden, müssen eine eindeutige Kennung auf der Grundlage einer elektronischen Signatur tragen.

Artikel 32

Herausgeberkontrolle

(1) Das Organ oder die Einrichtung der Union, unter dessen/deren Aufsicht ein EU-VS erstellt wird, hat die Kontrolle über dieses Dokument. Der Herausgeber bestimmt den Geheimhaltungsgrad des Dokuments und ist für die Festlegung des ursprünglichen Empfängerkreises verantwortlich. Ungeachtet der Verordnung Nr. 1049/2001 ist die schriftliche Zustimmung des Herausgebers einzuholen, bevor

a) der Geheimhaltungsgrad von Verschlusssachen aufgehoben bzw. eine Verschlusssache herabgestuft wird;

b) Verschlusssachen für andere als die vom Herausgeber festgelegten Zwecke verwendet werden;

c) Verschlusssachen an Stellen außerhalb des verwahrenden Organs oder der verwahrenden Einrichtung der Union weitergeleitet werden, einschließlich eines Drittstaats oder einer internationalen Organisation, eines anderen Organs oder einer anderen Einrichtung der Union, eines Mitgliedstaats, eines Auftragnehmers oder potenziellen Auftragnehmers, eines Begünstigten oder potenziellen Begünstigten;

d) Verschlusssachen des Geheimhaltungsgrads „TRES SECRET UE/EU TOP SECRET“ kopiert oder übersetzt werden.

(2) Kann der Herausgeber einer EU-VS nicht ermittelt werden, übt das sie verwahrende Organ oder die sie verwahrende Einrichtung der Union die Herausgeberkontrolle aus.

(3) Die Herausgeber von EU-VS führen Aufzeichnungen über alle als Verschlusssache eingestuften Quellen, die für die Erstellung von Verschlusssachen verwendet werden, einschließlich Angaben zu Quellen, die ursprünglich von Mitgliedstaaten, internationalen Organisationen oder Drittstaaten stammen. Falls erforderlich, werden zusammengefasste Verschlusssachen so gekennzeichnet, dass die Herausgeber des als Verschlusssache eingestuften Quellenmaterials weiterhin erkennbar sind.

Artikel 33

Einstufungskennzeichnungen

(1) Gegebenenfalls können EU-VS-Dokumente zusätzlich zu einer Kennzeichnung mit einem Geheimhaltungsgrad mit weiteren Kennzeichnungen versehen sein, z. B. mit einer Verteilungs- oder Weitergabekennzeichnung oder mit der Angabe des Herausgebers.

(2) Einzelne Teile einer EU-VS können unterschiedlichen Geheimhaltungsgraden unterliegen und sind entsprechend zu kennzeichnen. Der Geheimhaltungsgrad des Gesamtdokuments oder der Datei entspricht mindestens dem Geheimhaltungsgrad seines/ihres am höchsten eingestuften Teils.

(3) Dokumente, die Teile mit unterschiedlichen Geheimhaltungsgraden umfassen, sollten so untergliedert werden, dass Teile mit verschiedenen Geheimhaltungsgraden leicht zu erkennen sind und gegebenenfalls abgetrennt werden können.

Artikel 34

Registratursystem für EU-Verschlusssachen

(1) Alle Organe und Einrichtungen der Union, die als „CONFIDENTIEL UE/EU CONFIDENTIAL“ oder höher eingestufte Verschlusssachen bearbeiten und aufbewahren, richten eine oder mehrere

Registraturen für EU-VS ein, um sicherzustellen, dass diese Verschlusssachen, wenn sie bei einem Organ oder einer Einrichtung der Union eintreffen oder dieses Organ bzw. diese Einrichtung verlassen, für Sicherheitszwecke registriert werden.

(2) Alle Registraturen für EU-VS werden in Sicherheitsbereichen im Sinne des Anhangs III eingerichtet.

(3) Die Organe und Einrichtungen der Union benennen für die Verwaltung jeder EU-VS-Registratur einen Registraturkontrollbeauftragten (RCO). Der RCO verfügt über eine entsprechende Sicherheitsermächtigung und eine Ermächtigung gemäß Artikel 24. Die Organe und Einrichtungen der Union sorgen für eine angemessene Schulung ihres RCO.

Artikel 35

Herabstufung und Aufhebung des Geheimhaltungsgrades

(1) Informationen bleiben nur so lange als Verschlusssache eingestuft, wie sie Schutz benötigen. EU-VS, bei denen der ursprüngliche Geheimhaltungsgrad nicht mehr notwendig ist, werden auf einen niedrigeren Geheimhaltungsgrad herabgestuft. EU-VS, die nicht mehr als Verschlusssache zu betrachten sind, werden freigegeben.

(2) Der Herausgeber teilt, sofern möglich und insbesondere bei Verschlusssachen mit dem Geheimhaltungsgrad „RESTREINT UE/EU RESTRICTED“, zum Zeitpunkt der Erstellung einer EU-VS mit, ob deren Geheimhaltungsgrad zu einem bestimmten Zeitpunkt oder im Anschluss an ein bestimmtes Ereignis herabgestuft oder aufgehoben werden kann.

(3) Das eine EU-VS herausgebende Organ oder die eine EU-VS herausgebende Einrichtung der Union entscheidet darüber, ob die EU-VS herabgestuft oder freigegeben werden kann. Sie überprüfen die Informationen und die Risiken regelmäßig, mindestens aber alle fünf Jahre, daraufhin, ob der ursprüngliche Geheimhaltungsgrad noch angemessen ist.

(4) Organe und Einrichtungen der Union, die im Besitz von EU-VS, jedoch nicht deren Herausgeber sind, dürfen diese ohne vorherige schriftliche Zustimmung des Herausgebers weder herabstufen noch freigeben, noch dürfen sie die in Artikel 18 Absatz 1 genannten Kennzeichnungen verändern oder entfernen.

(5) Die Organe und Einrichtungen der Union können von ihnen erstellte EU-VS teilweise herabstufen oder freigeben. In diesem Fall ist der herabgestufte oder freigegebene Teil als Auszug vorzulegen.

(6) Die Organe und Einrichtungen der Union unterrichten die Empfängerorganisation der EU-VS über die Herabstufung oder Aufhebung des Geheimhaltungsgrads.

Artikel 36

Kennzeichnung von herabgestuften und freigegebenen Dokumenten

(1) Beschließen die Organe und Einrichtungen der Union, den Geheimhaltungsgrad eines EU-VS-Dokuments aufzuheben, so ist zu prüfen, ob es mit einer für nicht als Verschlusssache eingestufte vertrauliche Informationen vorgesehenen Verteilungskennzeichnung versehen werden soll.

(2) Die ursprüngliche Einstufungskennzeichnung oben und unten auf jeder Seite muss sichtbar durchgestrichen werden, indem bei elektronischen Formaten die Funktion

„Durchstreichen“ verwendet wird und bei Papierfassungen die Kennzeichnung von Hand durchgestrichen wird. Die ursprüngliche Einstufungskennzeichnung darf nicht entfernt werden.

(3) Auf der ersten Seite oder der Titelseite werden die Herabstufung oder Aufhebung des Geheimhaltungsgrads mit einem Stempel vermerkt und die Einzelheiten zu der hierfür zuständigen Stelle sowie das entsprechende Datum angegeben. Bei elektronischen EU-VS wird die Herabstufung oder Aufhebung des Geheimhaltungsgrads durch eine elektronische Signatur unter der Aufsicht des Herausgebers beurkundet.

Artikel 37

Vernichtung und Löschung von EU-Verschlusssachen

(1) Die Organe und Einrichtungen der Union überprüfen ihre EU-VS in Papierform und in Kommunikations- und Informationssystemen mindestens alle fünf Jahre, um festzustellen, ob sie vernichtet oder gelöscht werden sollen. Werden EU-VS vernichtet oder gelöscht, so werden alle Personen, die zuvor diese EU-VS erhalten haben, informiert.

(2) Die Organe und Einrichtungen der Union können nicht länger benötigte Duplikate von EU-VS vernichten, wobei für die Originale die einschlägigen Vorschriften für die Dokumentenverwaltung zu berücksichtigen sind.

(3) Die Organe und Einrichtungen der Union lassen Papierkopien von als „CONFIDENTIEL UE/EU CONFIDENTIAL“ oder höher eingestuften Verschlusssachen ausschließlich durch ihren Registraturkontrollbeauftragten (RCO) vernichten. Der RCO aktualisiert die Dienstbücher und sonstigen Registrierungsinformationen entsprechend und bewahrt wichtige Metadaten des vernichteten Dokuments auf.

Bei Dokumenten des Geheimhaltungsgrads „SECRET UE/EU SECRET“ oder höher erfolgt die Vernichtung durch den RCO im Beisein eines Zeugen, der mindestens über eine Sicherheitsermächtigung für den Geheimhaltungsgrad des zu vernichtenden Dokuments verfügt.

(4) Der RCO und gegebenenfalls der Zeuge unterschreiben eine Vernichtungsbescheinigung, die in der Registratur abgelegt wird. Die Bescheinigung ist im Falle von als „CONFIDENTIEL UE/EU CONFIDENTIAL“ und als „SECRET UE/EU SECRET“ eingestuften Verschlusssachen mindestens fünf Jahre und im Falle von als „TRES SECRET UE/EU TOP SECRET“ eingestuften Verschlusssachen mindestens zehn Jahre lang aufzubewahren.

Artikel 38

Evakuierung und Vernichtung von EU-Verschlusssachen im Notfall

(1) Jedes Organ und jede Einrichtung der Union erstellt auf der Grundlage der örtlichen Bedingungen Notfallevakuierungs- und Vernichtungspläne, um EU-VS zu schützen, bei denen ein erhebliches Risiko besteht, dass sie in unbefugte Hände gelangen.

Die praktischen Einzelheiten der Notfallevakuierungs- und Vernichtungspläne werden als „RESTREINT UE/EU RESTRICTED“ eingestuft.

(2) In Notfällen, in denen die unmittelbare Gefahr einer unbefugten Offenlegung von EU-VS besteht, evakuieren die Organe und Einrichtungen der Union die EU-VS.

Wenn eine Evakuierung nicht möglich ist, werden die EU-VS so vernichtet, dass eine vollständige oder teilweise Wiederherstellung ausgeschlossen ist.

(3) Der Herausgeber und die herausgebende Registratur sind von der als Notfallmaßnahme durchgeführten Evakuierung oder Vernichtung der registrierten EU-VS in Kenntnis zu setzen.

(4) Wurden Notfallpläne aktiviert, wird der Evakuierung oder Vernichtung der höheren Geheimhaltungsgrade von EU-VS, einschließlich der Verschlüsselungseinrichtungen, Vorrang eingeräumt.

Artikel 39

Archivierung

(1) Die Organe und Einrichtungen der Union entscheiden im Einklang mit ihren Grundsätzen für die Dokumentenverwaltung, ob und wann EU-VS zu archivieren sind, und legen die entsprechenden praktischen Maßnahmen dafür fest.

(2) EU-VS dürfen nicht an das Historische Archiv der Europäischen Union übermittelt werden.

ABSCHNITT 5
SCHUTZ VON EU-VERSCHLUSSSACHEN IN KOMMUNIKATIONS- UND INFORMATIONSSYSTEMEN

Artikel 40

Untergruppe für die Akkreditierung von Kommunikations- und Informationssystemen, in denen EU-VS bearbeitet und gespeichert werden

Die Untergruppe für die Akkreditierung von Kommunikations- und Informationssystemen, in denen EU-VS bearbeitet und gespeichert werden gemäß Artikel 7 Absatz 1 Buchstabe d hat folgende Aufgaben und Zuständigkeiten:

a) Unterstützung der Organe und Einrichtungen der Union bei ihren Akkreditierungsverfahren;

b) Empfehlung eines Standards für die Akkreditierung, der von allen Organen und Einrichtungen der Union einzuhalten ist;

c) Verbreitung und Austausch bewährter Verfahren und Leitlinien für die Akkreditierung von Kommunikations- und Informationssystemen.

Artikel 41

Kommunikations- und Informationssysteme

Die Organe und Einrichtungen der Union erfüllen in Bezug auf Kommunikations- und Informationssysteme, in denen EU-VS bearbeitet und gespeichert werden, die folgenden Anforderungen:

a) bevor ein für die Bearbeitung und Speicherung von EU-VS bestimmtes Kommunikations- und Informationssystem entwickelt, beschafft oder für die Inbetriebnahme hergerichtet wird, konsultiert der Systemeigner oder die für

den Betrieb zuständige Informationssicherungsstelle die Sicherheitsakkreditierungsstelle, um die Anforderungen für die Akkreditierung festzulegen;

b) für die Gestaltung eines Kommunikations- und Informationssystems, in dem EU-VS bearbeitet und gespeichert werden, sind zentrale Sicherheitsgrundsätze zu beachten, die ab Beginn des Projekts und als Teil des Informationssicherheitsrisiko-Managementprozesses gelten, darunter der Grundsatz „Kenntnis nur, wenn nötig“, Mindestfunktionalitäten, ein gestaffeltes Sicherheitskonzept, das Prinzip der minimalen Berechtigung, der Grundsatz der Aufgabentrennung und das Vier-Augen-Prinzip;

c) die für die Speicherung, die zentrale Verarbeitung und das Netzmanagement eingesetzten Komponenten eines Kommunikations- und Informationssystems, in dem EU-VS bearbeitet und gespeichert werden, werden in einem Sicherheitsbereich gemäß Anhang III installiert;

d) es werden TEMPEST-Sicherheitsvorkehrungen umgesetzt, die dem Ausnutzungsrisiko und dem Geheimhaltungsgrad der Information entsprechen;

e) jeder am Betrieb eines Kommunikations- und Informationssystems, in dem EU-VS bearbeitet und gespeichert werden, beteiligte Mitarbeiter unterrichtet die Sicherheitsbehörde sowie den zuständigen Systemeigner oder die für den Betrieb zuständige Informationssicherungsstelle über potenzielle Sicherheitsmängel, Vorfälle, Verletzungen der Sicherheit oder Systemschwächen, die sich auf den Schutz des Kommunikations- und Informationssystems oder der darin enthaltenen EU-VS auswirken können;

f) gegebenenfalls unterrichtet die Sicherheitsbehörde die Sicherheitsbehörden der anderen betroffenen Organe und Einrichtungen der Union über potenzielle Sicherheitsmängel oder Vorfälle, die sich auf ihre für die Bearbeitung und Speicherung von EU-VS eingesetzten Kommunikations- und Informationssysteme auswirken könnten.

Artikel 42

Kryptografische Produkte

(1) Zugelassene kryptografische Produkte werden für die elektronische Übermittlung und Speicherung von EU-VS verwendet. Die Liste der zugelassenen kryptografischen Produkte wird vom Rat auf der Grundlage von Beiträgen der nationalen Sicherheitsbehörden geführt.

(2) Enthält die in Absatz 1 genannte Liste kein für den vorgesehenen Zweck geeignetes Produkt, so ersucht die Krypto-Zulassungsstelle des betreffenden Organs oder der betreffenden Einrichtung der Union den Rat um eine vorläufige Zulassung. Nach Möglichkeit wird ein kryptografisches Produkt ausgewählt, das von der nationalen Sicherheitsbehörde eines Mitgliedstaats zugelassen wurde.

Der Rat trifft die erforderlichen Maßnahmen, um sicherzustellen, dass ein geeignetes Produkt in die Liste aufgenommen wird.

(3) Die Zulassung kryptografischer Produkte gilt für höchstens fünf Jahre und wird danach jährlich überprüft.

(4) Der Rat streicht jedes kryptografische Produkt, für das die nationale Zulassung entzogen wurde oder dessen Zulassung abgelaufen ist, aus der Liste der zugelassenen kryptografischen Produkte.

(5) Die Koordinierungsgruppe unterrichtet den Rat jährlich über alle kryptografischen Produkte, die sie auf der Grundlage einer in den Organen und Einrichtungen der Union durchgeführten Erhebung zur Bewertung durch eine Krypto-Zulassungsstelle eines Mitgliedstaats empfiehlt.

Artikel 43

Akkreditierung von Kommunikations- und Informationssystemen, in denen EU-Verschlusssachen bearbeitet und gespeichert werden

(1) Mit der Akkreditierung von Kommunikations- und Informationssystemen, in denen EU-VS bearbeitet und gespeichert werden, bestätigen die Organe und Einrichtungen der Union, dass alle angemessenen Sicherheitsmaßnahmen durchgeführt wurden und dass ein ausreichender Schutz der EU-VS und des Kommunikations- und Informationssystems gemäß dieser Verordnung erreicht wird.

(2) Der Eigner des Kommunikations- und Informationssystems oder die für den Betrieb zuständige Informationssicherungsstelle ist für die Erstellung der Akkreditierungsdateien und -unterlagen, einschließlich Handbüchern für verschiedene Arten von Nutzern, zuständig.

(3) Die Sicherheitsakkreditierungsstelle jedes Organs und jeder Einrichtung der Union ist für die Einrichtung eines Akkreditierungsverfahrens mit klaren Bedingungen, die einer Genehmigung bedürfen, für alle ihrer Aufsicht unterstehenden Kommunikations- und Informationssysteme zuständig.

(4) Sind an einem Kommunikations- und Informationssystem, in dem EU-VS bearbeitet und gespeichert werden, sowohl Organe und Einrichtungen der Union als auch nationale Sicherheitsbehörden beteiligt, so richten die betreffenden Organe und Einrichtungen der Union im Wege weiterer Durchführungsbestimmungen, die gemäß Artikel 7 Absatz 2 erlassen werden, ein gemeinsames Gremium für die Sicherheitsakkreditierung ein, das für die Akkreditierung des Systems zuständig ist. Dieses Gremium setzt sich aus Vertretern der Sicherheitsakkreditierungsstelle der beteiligten Parteien zusammen; den Vorsitz führt die Sicherheitsakkreditierungsstelle des Organs oder der Einrichtung der Union, das bzw. die Eigner/in des Kommunikations- und Informationssystems ist.

Artikel 44

Akkreditierungsverfahren eines Kommunikations- und Informationssystems, in dem EU-Verschlusssachen bearbeitet und gespeichert werden

(1) Alle Kommunikations- und Informationssysteme, in denen EU-VS bearbeitet und gespeichert werden, werden einem Akkreditierungsverfahren unterzogen, das auf den Grundsätzen der Informationssicherung beruht und dessen Detailtiefe dem erforderlichen Schutzniveau entspricht.

(2) Das Akkreditierungsverfahren mündet in eine Akkreditierungserklärung, in der festgelegt wird, bis zu welchem Geheimhaltungsgrad und unter welchen Voraussetzungen Verschlusssachen in dem Kommunikations- und Informationssystem bearbeitet und gespeichert werden dürfen. Die

Akkreditierungserklärung beruht auf der förmlichen Validierung der Risikobewertung und der für das betreffende Kommunikations- und Informationssystem ergriffenen Sicherheitsmaßnahmen und bietet Gewähr für folgende Elemente:

a) das Informationssicherheitsrisiko-Managementverfahren wurde ordnungsgemäß durchgeführt;

b) der Systemeigner oder Risikoeigner hat das Restrisiko wissentlich akzeptiert;

c) ein hinreichender Schutz des Kommunikations- und Informationssystems und der darin bearbeiteten und gespeicherten EU-VS ist in Übereinstimmung mit dieser Verordnung sichergestellt.

(3) Die Akkreditierungserklärung wird von der Sicherheitsakkreditierungsstelle eines Organs oder einer Einrichtung der Union förmlich validiert. Nach erfolgreicher Validierung erteilt die Sicherheitsakkreditierungsstelle eine Betriebsgenehmigung, in der festgelegt ist, bis zu welchem Geheimhaltungsgrad und unter welchen Voraussetzungen EU-VS in dem Kommunikations- und Informationssystem bearbeitet werden dürfen. Die Genehmigung wird für einen bestimmten Zeitraum erteilt. Wenn eine oder mehrere erforderliche Sicherheitsmaßnahmen nicht vorhanden sind, sich dies aber nicht wesentlich auf die Gesamtsicherheit auswirkt, kann eine vorläufige Betriebsgenehmigung erteilt werden, in der die Punkte zur Behebung der Mängel festgelegt werden.

(4) Die Sicherheitsakkreditierungsstelle des betreffenden Organs oder der betreffenden Einrichtung der Union kann jederzeit während des Lebenszyklus eines Kommunikations- und Informationssystems folgende Maßnahmen ergreifen:

a) Anwendung eines Akkreditierungsverfahrens;

b) Durchführung einer Prüfung oder Kontrolle des Kommunikations- und Informationssystems;

c) wenn die Betriebsbedingungen nicht mehr erfüllt sind, z. B. wenn bei einem Sicherheitsvorfall eine erhebliche Schwachstelle im Kommunikations- und Informationssystem festgestellt wurde, muss innerhalb eines genau festgelegten Zeitrahmens ein Plan zur Verbesserung der Sicherheit erstellt und wirksam umgesetzt werden, wobei die Betriebsgenehmigung des Kommunikations- und Informationssystems möglicherweise entzogen wird, bis die Voraussetzungen für den Betrieb erfüllt sind.

(5) Der Systemeigner oder die für den Betrieb zuständige Informationssicherungsstelle legt der Sicherheitsakkreditierungsstelle während der Gültigkeitsdauer einer Betriebsgenehmigung jährlich einen förmlichen Bericht vor, der eine Zusammenfassung aller wesentlichen Vorfälle, Änderungen und Risikofaktoren enthält.

Artikel 45

Notsituationen

(1) In Notfällen, z. B. während drohender oder tatsächlicher Krisen, Konflikte, Kriegssituationen oder unter außergewöhnlichen operativen Umständen, können die Organe und Einrichtungen der Union für die Übermittlung oder Aufbewahrung von

EU-VS nach Genehmigung durch ihre Krypto-Zulassungsstelle besondere Verfahren anwenden.

(2) Unter den in Absatz 1 beschriebenen Umständen können EU-VS mit Hilfe kryptografischer Produkte, die für einen niedrigeren Geheimhaltungsgrad zugelassen sind, oder mit Zustimmung der zuständigen Behörde unverschlüsselt übermittelt werden, wenn eine Verzögerung einen Schaden verursachen würde, der deutlich größer wäre als der Schaden, der durch eine Offenlegung des als Verschlusssache eingestuften Materials entstehen würde, und wenn folgende Bedingungen vorliegen:

a) Absender und Empfänger verfügen nicht über die erforderliche Verschlüsselungsausrüstung, und

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

(3) Verschlusssachen, die unter den in Absatz 2 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.

(4) Über die Übermittlung von EU-VS unter den in Absatz 1 genannten Umständen wird der zuständigen Sicherheitsbehörde ein Bericht vorgelegt.

ABSCHNITT 6
GEHEIMSCHUTZ IN DER WIRTSCHAFT

Artikel 46

Grundsätze

(1) Jedes Organ oder jede Einrichtung der Union stellt als Auftraggeber oder Vergabebehörde sicher, dass die in diesem Abschnitt festgelegten Mindeststandards für den Geheimschutz in der Wirtschaft und die in Anhang V festgelegten Bedingungen für den Schutz von EU-VS in als Verschlusssache eingestuften Aufträgen und Finanzhilfevereinbarungen in solchen Verträgen oder Finanzhilfevereinbarungen genannt werden oder enthalten sind und dass sie bei der Vergabe von solchen Aufträgen oder Finanzhilfevereinbarungen eingehalten werden.

(2) Der Geheimschutz in der Wirtschaft beinhaltet die Anwendung von Maßnahmen, mit denen der Schutz von EU-VS durch folgende Personen oder Einrichtungen gewährleistet wird:

a) im Falle von direkter Mittelverwaltung[30] im Rahmen von als Verschlusssache eingestuften Aufträgen:

i) durch Bewerber oder Bieter während des gesamten Ausschreibungs- und Vergabeverfahren;

ii) durch Auftragnehmer oder Unterauftragnehmer während der Laufzeit von als Verschlusssache eingestuften Aufträgen;

[30] Verordnung (EU, Euratom) 2018/1046 des Europäischen Parlaments und des Rates

b) im Falle von direkter Mittelverwaltung[31] im Rahmen von als Verschlusssache eingestuften Finanzhilfevereinbarungen:

i) durch Antragsteller während Verfahren zur Vergabe von Finanzhilfen;

ii) durch Finanzhilfeempfänger oder Unterauftragnehmer während der Laufzeit von als Verschlusssache eingestuften Finanzhilfevereinbarungen;

c) im Falle von indirekter Mittelverwaltung im Rahmen von Finanzpartnerschafts-Rahmenvereinbarungen und den damit verbundenen Beitragsvereinbarungen durch die betrauten Einrichtungen während des gesamten Lebenszyklus dieser Vereinbarungen.

(3) Als betrauende Stelle beschreibt das Organ oder die Einrichtung der Union die spezifischen Sicherheitsanforderungen für die betraute Einrichtung im Sicherheitskapitel der Rahmenvereinbarung und der entsprechenden Beitragsvereinbarungen. Diese Anforderungen beruhen auf den Sicherheitsgrundsätzen und -bestimmungen dieser Verordnung in Bezug auf als Verschlusssache eingestufte Aufträge und Finanzhilfevereinbarungen, die entsprechend gelten.

(4) Als Verschlusssache eingestufte Aufträge und Finanzhilfevereinbarungen beinhalten keine als „TRÈS SECRET UE/EU TOP SECRET“ eingestuften Informationen.

(5) Die Bestimmungen dieses Kapitels, die sich auf als Verschlusssache eingestufte Aufträge oder die betreffenden Auftragnehmer oder auf als Verschlusssache eingestufte Finanzhilfen oder die betreffenden Empfänger beziehen, gelten auch für als Verschlusssache eingestufte Unteraufträge oder die betreffenden Unterauftragnehmer im Sinne von als Verschlusssache eingestufte Aufträge oder Finanzhilfen.

(6) Die Organe und Einrichtungen der Union arbeiten als Auftraggeber oder Vergabebehörden eng mit den Sicherheitsbehörden oder anderen zuständigen Behörden des Landes zusammen, in dessen Hoheitsgebiet die Vertragspartei oder der Finanzhilfeempfänger registriert ist, sowie mit den Sicherheits- oder anderen zuständigen Behörden der internationalen Organisation, an die der Auftrag oder die Finanzhilfe vergeben wurde.

(7) Die Organe und Einrichtungen der Union kommunizieren als Auftraggeber oder Vergabebehörden mit den Sicherheitsbehörden oder anderen zuständigen Behörden über ihre Sicherheitsbehörden.

(8) Wenn ein als Verschlusssache eingestufter Auftrag oder eine als Verschlusssache eingestufte Finanzhilfevereinbarung unterzeichnet wurde, unterrichten die Organe und Einrichtungen der Union als Auftraggeber oder Vergabebehörden über ihre Sicherheitsbehörde die in Absatz 6 genannten Behörden.

Die Mitteilung enthält relevante Daten wie die Namen des Auftragnehmers oder der Finanzhilfeempfänger, die Laufzeit des als Verschlusssache eingestuften Auftrags oder der als Verschlusssache eingestuften Finanzhilfevereinbarung und den höchsten Geheimhaltungsgrad.

Die Organe und Einrichtungen der Union unterrichten als Auftraggeber oder Vergabebehörden die in Absatz 6 genannten Behörden auch über ihre

[31] Ebenda.

Sicherheitsbehörde, wenn ein als Verschlusssache eingestufter Auftrag oder eine als Verschlusssache eingestufte Finanzhilfevereinbarung frühzeitig beendet wird.

(9) Die Organe und Einrichtungen der Union können als Auftraggeber oder Vergabebehörden als Verschlusssache eingestufte Aufträge oder Teile von Finanzhilfen nur an Stellen vergeben, die in Drittstaaten registriert sind oder von internationalen Organisationen gegründet wurden, mit denen die Union ein Geheimschutzabkommen geschlossen hat. Enthalten die betreffenden EU-VS personenbezogene Daten, so erfolgt deren Übermittlung an einen Drittstaat oder eine internationale Organisation gemäß der Verordnung (EU) 2018/1725.

Artikel 47

Sicherheitsmerkmale von als Verschlusssache eingestuften Aufträgen oder Finanzhilfevereinbarungen

(1) Als Verschlusssache eingestufte Aufträge oder Finanzhilfevereinbarungen umfassen folgende die Sicherheit betreffenden Bestandteile:

a) eine VS-Einstufungsliste (Security Classification Guide);

b) eine Geheimschutzklausel (Security Aspects Letter).

(2) Als Verschlusssache eingestufte Aufträge oder Finanzhilfevereinbarungen können Programm- oder Projekt-Sicherheitsanweisungen enthalten.

Artikel 48

Verschlusssachen-Einstufungsliste (Security Classification Guide)

(1) Vor der Unterzeichnung eines als Verschlusssache eingestuften Auftrags oder einer als Verschlusssache eingestuften Finanzhilfevereinbarung legt das Organ oder die Einrichtung der Union als Auftraggeber oder Vergabebehörde den Geheimhaltungsgrad aller Informationen fest, die von Auftragnehmern oder Finanzhilfeempfängern oder ihren Unterauftragnehmern zu erstellen sind. Zu diesem Zweck erstellen sie die bei der Ausführung des als VS eingestuften Auftrags bzw. der als VS eingestuften Finanzhilfevereinbarung zu verwendende VS-Einstufungsliste (Security Classification Guide, SCG).

(2) Die VS-Einstufungsliste kann während der Laufzeit des Programms oder Projekts gemäß Artikel 50, des Auftrags oder der Finanzhilfevereinbarung verändert werden, und Teile der Informationen können neu eingestuft oder herabgestuft werden.

(3) Für die Bestimmung des Geheimhaltungsgrads der verschiedenen Bestandteile eines als Verschlusssache eingestuften Auftrags oder einer als Verschlusssache eingestuften Finanzhilfevereinbarung gelten die folgenden Grundsätze:

a) bei der Erstellung einer VS-Einstufungsliste trägt das betreffende Organ oder die betreffende Einrichtung der Union als Auftraggeber oder Vergabebehörde allen relevanten Sicherheitsaspekten Rechnung, unter anderem auch dem Geheimhaltungsgrad, den der Herausgeber den zur Nutzung im Rahmen des als Verschlusssache eingestuften Auftrags oder der als Verschlusssache eingestuften Finanzhilfevereinbarung bereitgestellten und freigegebenen Informationen zugewiesen hat;

b) der globale Geheimhaltungsgrad des als Verschlusssache eingestuften Auftrags oder der als Verschlusssache eingestuften Finanzhilfevereinbarung darf nicht niedriger sein als der höchste Grad jeder einzelnen Komponente;

c) gegebenenfalls setzen sich die betreffenden Organe oder Einrichtungen der Union als Auftraggeber oder Vergabebehörden über ihre Sicherheitsbehörde mit den Sicherheitsbehörden oder anderen zuständigen Behörden des betreffenden Landes in Verbindung, wenn sie Änderungen an der VS-Einstufungsliste vornehmen.

Artikel 49

Geheimschutzklausel (Security Aspects Letter)

(1) Die Organe und Einrichtungen der Union beschreiben als Auftraggeber oder Vergabebehörden die spezifischen Sicherheitsanforderungen für den als Verschlusssache eingestuften Auftrag oder die als Verschlusssache eingestufte Finanzhilfevereinbarung in einer Geheimschutzklausel (Security Aspects Letter, SAL). Diese Klausel enthält die VS-Einstufungsliste und ist fester Bestandteil eines als Verschlusssache eingestuften Auftrags, einer als Verschlusssache eingestuften Finanzhilfevereinbarung oder eines entsprechenden Unterauftrags.

(2) Die Geheimschutzklausel enthält Bestimmungen, mit denen der Auftragnehmer oder Finanzhilfeempfänger und deren Unterauftragnehmer verpflichtet werden, die Bestimmungen dieser Verordnung und etwaiger weiterer Durchführungsbestimmungen, die gemäß Artikel 8 Absatz 2 in Bezug auf den Geheimschutz in der Wirtschaft erlassen werden, einzuhalten. Aus der Geheimschutzklausel geht eindeutig hervor, dass die Nichteinhaltung dieser Bestimmungen einen ausreichenden Grund für die Beendigung des als Verschlusssache eingestuften Auftrags oder der als Verschlusssache eingestuften Finanzhilfevereinbarung darstellen kann.

Artikel 50

Programm- oder Projekt-Sicherheitsanweisung

(1) Die Organe und Einrichtungen der Union können als Auftraggeber oder Vergabebehörden in enger Zusammenarbeit mit ihren Sicherheitsbehörden eine Programm- oder Projekt-Sicherheitsanweisung ausarbeiten, insbesondere für Programme und Projekte, die durch ihren erheblichen Umfang, ihre Reichweite oder ihre Komplexität oder die Vielzahl oder Vielfalt der Auftragnehmer, Begünstigten und sonstiger Partner und Beteiligter gekennzeichnet sind.

(2) Die Organe und Einrichtungen der Union legen als Auftraggeber oder Vergabebehörden über ihre Sicherheitsbehörde dem zuständigen beratenden Sicherheitsgremium des jeweiligen Mitgliedstaats, das sich aus dessen nationalen Sicherheitsbehörden und/oder benannten Sicherheitsbehörden zusammensetzt, die spezifische Programm- oder Projekt-Sicherheitsanweisung zur Beratung vor.

Verfügt ein Organ oder eine Einrichtung der Union nicht über ein solches beratendes Gremium, so wird die Programm- oder Projekt-Sicherheitsanweisung dem in Artikel 6 Absatz 8 genannten Ausschuss für Informationssicherheit vorgelegt.

ABSCHNITT 7
WEITERGABE VON EU-VERSCHLUSSSACHEN UND AUSTAUSCH VON VERSCHLUSSSACHEN

Artikel 51

Grundsätze

(1) Alle Organe und Einrichtungen der Union können unter den in Artikel 54 festgelegten Bedingungen EU-VS an andere Organe oder Einrichtungen der Union weitergeben.

(2) Die Organe und Einrichtungen der Union können EU-VS an die Mitgliedstaaten und die Europäische Atomgemeinschaft weitergeben, sofern sie diese Informationen gemäß der im Abkommen zwischen den im Rat vereinigten Mitgliedstaaten der Union über den Schutz der im Interesse der Union ausgetauschten Verschlusssachen festgelegten und in der Entsprechungstabelle in Anhang VI der vorliegenden Verordnung angegebenen Geheimhaltungskennzeichnung schützen.

(3) Die Organe und Einrichtungen der Union tauschen Verschlusssachen nur mit Drittstaaten oder internationalen Organisationen aus, mit denen ein Geheimschutzabkommen oder eine Verwaltungsvereinbarung gemäß den Artikeln 55 und 56 geschlossen wurde.

Solche Geheimschutzabkommen und Verwaltungsvereinbarungen enthalten Bestimmungen, mit denen sichergestellt wird, dass EU-VS nach Entgegennahme durch die Drittstaaten oder internationalen Organisationen in einer ihrem Geheimhaltungsgrad entsprechenden Weise und nach Maßgabe von Mindeststandards geschützt werden, die zumindest den in dieser Verordnung festgelegten Mindeststandards entsprechen.

(4) Besteht kein Geheimschutzabkommen oder keine Verwaltungsvereinbarung, so kann ein Organ oder eine Einrichtung der Union unter außergewöhnlichen Umständen EU-VS gemäß Artikel 58 an ein anderes Organ oder eine andere Einrichtung der Union, einen Drittstaat oder eine internationale Organisation weitergeben.

(5) Die Organe und Einrichtungen der Union benennen diejenigen Registraturen, die als Hauptein- und -ausgangspunkte für mit anderen Organen oder Einrichtungen der Union ausgetauschte EU-VS oder für mit Drittstaaten und internationalen Organisationen ausgetauschte Verschlusssachen dienen.

Artikel 52

Untergruppe für die Weitergabe von EU-Verschlusssachen und den Austausch von Verschlusssachen

(1) Die Untergruppe für die Weitergabe von EU-VS und den Austausch von Verschlusssachen gemäß Artikel 7 Absatz 1 Buchstabe e hat folgende Aufgaben und Zuständigkeiten:

a) Organisation von Bewertungsbesuchen bei Organen und Einrichtungen der Union, in Drittstaaten und internationalen Organisationen und Annahme des jährlichen Besuchsprogramms;

b) Vorbereitung und Durchführung der Bewertungsbesuche;

c) Erstellung eines Berichts über die Ergebnisse der Besuche gemäß Buchstabe a,

außer in den in Artikel 56 Absatz 2 genannten Fällen.

(2) Die Untergruppe für die Weitergabe von EU-VS und den Austausch von Verschlusssachen setzt sich aus Vertretern der Kommission, des Rates und des Europäischen Auswärtigen Dienstes zusammen und arbeitet einvernehmlich.

Artikel 53

Bewertungsbesuche im Zusammenhang mit der Weitergabe von EU-Verschlusssachen

(1) Die Untergruppe für die Weitergabe von EU-VS und den Austausch von Verschlusssachen führt in enger Zusammenarbeit mit den Beamten des besuchten Organs oder der besuchten Einrichtung der Union Bewertungsbesuche durch. Sie kann die nationale Sicherheitsbehörde, in deren Hoheitsgebiet sich das Organ oder die Einrichtung der Union befindet, um Unterstützung ersuchen.

(2) Mit den Bewertungsbesuchen bei den betreffenden Organen und Einrichtungen der Union

a) soll überprüft werden, ob die in dieser Verordnung festgelegten Anforderungen an den Schutz von EU-VS eingehalten werden und ob die durchgeführten Maßnahmen somit wirksam sind;

b) soll der Bedeutung der Sicherheitsaspekte und eines wirksamen Risikomanagements in den besuchten Stellen Nachdruck verliehen werden;

c) sollen Abhilfemaßnahmen empfohlen werden, um bei Einbußen in Bezug auf die Verfügbarkeit, Vertraulichkeit oder Integrität von Verschlusssachen die spezifischen Auswirkungen begrenzen zu können, und

d) sollen die laufenden Programme der Sicherheitsbehörden zur Schulung und Sensibilisierung in Sicherheitsfragen unterstützt werden.

(3) Am Ende des Bewertungsbesuchs führt die Untergruppe für die Weitergabe von EU-VS und den Austausch von Verschlusssachen folgende Tätigkeiten durch:

a) Erstellung eines Berichts mit den wichtigsten Schlussfolgerungen der Bewertung;

b) Einholung einer Stellungnahme des in Artikel 6 Absatz 8 genannten Ausschusses für Informationssicherheit zu dem Bericht;

c) Übermittlung des Berichts an die Sicherheitsbehörde des besuchten Organs oder der besuchten Einrichtung der Union zur Weiterverfolgung.

(4) Werden in dem Bericht Korrekturmaßnahmen vorgeschlagen oder Empfehlungen ausgesprochen, so wird ein Folgebesuch organisiert, um zu überprüfen, ob entsprechende Maßnahmen ergriffen oder entsprechende Empfehlungen befolgt wurden.

Artikel 54

Weitergabe von EU-Verschlusssachen

(1) Ein Organ bzw. eine Einrichtung der Union kann unter folgenden Bedingungen EU-VS an ein anderes Organ bzw. eine andere Einrichtung der Union weitergeben:

a) die Weitergabe ist nachweislich erforderlich;

b) bei dem betreffenden Organ oder der betreffenden Einrichtung der Union wurde gemäß Artikel 53 ein Bewertungsbesuch durchgeführt, dessen Ergebnis bestätigt, dass dieses Organ oder diese Einrichtung der Union in der Lage ist, EU-VS des jeweiligen Geheimhaltungsgrads zu bearbeiten und aufzubewahren;

c) die Sicherheitsbehörde des betreffenden Organs oder der betreffenden Einrichtung der Union beschließt, dass Verschlusssachen bis zu einem bestimmten Geheimhaltungsgrad an andere zertifizierte Organe und Einrichtungen der Union weitergegeben werden dürfen.

(2) Das Sekretariat der Koordinierungsgruppe erstellt eine Liste der Geheimhaltungsgrade für EU-VS, die von den einzelnen Organen und Einrichtungen der Union, die die Bedingungen des Absatzes 1 Buchstaben b und c erfüllen, bearbeitet und aufbewahrt werden dürfen. Diese Liste wird von ihm regelmäßig aktualisiert.

Artikel 55

Geheimschutzabkommen

(1) Ist ein langfristiger Austausch von Verschlusssachen mit einem Drittstaat oder einer internationalen Organisation erforderlich, so bemüht sich das zuständige Organ bzw. die zuständige Einrichtung um die Aushandlung und den Abschluss eines Geheimschutzabkommens gemäß Artikel 218 des Vertrags über die Arbeitsweise der Europäischen Union.

(2) In einem Geheimschutzabkommen werden die Grundprinzipien und Mindeststandards für den Austausch von Verschlusssachen zwischen der Union und einem Drittstaat oder einer internationalen Organisation niedergelegt.

(3) In Geheimschutzabkommen werden die technischen Durchführungsbestimmungen geregelt, die zwischen den zuständigen Sicherheitsbehörden der betreffenden Organe und Einrichtungen der Union und der zuständigen Sicherheitsbehörde des betreffenden Drittstaats bzw. der betreffenden internationalen Organisation zu vereinbaren sind.

(4) Vor der Genehmigung der in Absatz 3 genannten technischen Durchführungsbestimmungen führt die Untergruppe für die Weitergabe von EU-VS und den Austausch von Verschlusssachen einen Bewertungsbesuch gemäß Artikel 57 durch.

Artikel 56

Verwaltungsvereinbarungen mit Drittstaaten und internationalen Organisationen

(1) Wenn in ihrer Geschäftsordnung oder in ihren Gründungsakten eine solche Möglichkeit vorgesehen ist, können die Organe und Einrichtungen der Union mit den entsprechenden zuständigen Stellen in einem Drittstaat oder einer internationalen Organisation nach Unterrichtung der Untergruppe für die Weitergabe von EU-VS und den Austausch von Verschlusssachen eine Verwaltungsvereinbarung schließen, sofern die folgenden Bedingungen erfüllt sind:

a) in dem betreffenden Organ oder der betreffenden Einrichtung der Union muss der Bedarf bestehen, Verschlusssachen, die in der Regel höchstens als RESTREINT UE/EU RESTRICTED eingestuft sind, langfristig mit der

entsprechenden Stelle in einem Drittstaat oder einer internationalen Organisation auszutauschen;

b) das betreffende Organ oder die betreffende Einrichtung der Union erfüllt die Bedingungen gemäß Artikel 54 Absatz 1;

c) in dem in Artikel 57 genannten Bewertungsbericht wird bescheinigt, dass die entsprechende Stelle in dem betreffenden Drittstaat oder der betreffenden internationalen Organisation in der Lage ist, EU-VS eines bestimmten Geheimhaltungsgrads zu bearbeiten und aufzubewahren.

(2) Vor Abschluss einer Verwaltungsvereinbarung wird ein Bewertungsbesuch im Einklang mit den Grundsätzen des Artikels 57 durchgeführt. Das Organ oder die Einrichtung der Union, das bzw. die die Verwaltungsvereinbarung anstrebt, kann die Untergruppe für die Weitergabe von EU-VS und den Austausch von Verschlusssachen ersuchen, den Bewertungsbesuch in ihrem Namen durchzuführen oder an dem Besuch teilzunehmen.

(3) Die Sicherheitsbehörde des Organs oder der Einrichtung der Union, das bzw. die die Verwaltungsvereinbarung anstrebt, entscheidet über etwaige besondere Bedingungen für den Austausch sowie über den höchstens zulässigen Geheimhaltungsgrad von EU-VS. Dieser Geheimhaltungsgrad darf nicht höher sein als der Geheimhaltungsgrad, der für den Austausch von EU-VS mit anderen Organen und Einrichtungen der Union gemäß Artikel 54 festgelegt ist, und sollte gegebenenfalls nicht höher sein als der Geheimhaltungsgrad, der in einem Geheimschutzabkommen mit demselben Drittstaat oder derselben internationalen Organisation vorgesehen ist.

Artikel 57

Bewertungsbesuche für den Austausch von Verschlusssachen mit Drittstaaten und internationalen Organisationen

(1) Ein Bewertungsbesuch in einem Drittstaat oder einer internationalen Organisation wird durchgeführt, um festzustellen, ob ein Organ oder eine Einrichtung der Union Verschlusssachen mit dem betreffenden Drittstaat oder der betreffenden internationalen Organisation austauschen darf.

(2) Das Ziel des Bewertungsbesuchs ist es, zu bewerten, ob die Sicherheitsvorschriften und -verfahren in dem betreffenden Drittstaat oder der betreffenden internationalen Organisation hinsichtlich des Schutzes von EU-VS eines bestimmten Geheimhaltungsgrads wirksam sind. Der Bewertungsbesuch wird in gegenseitigem Einvernehmen mit dem betreffenden Drittstaat oder der betreffenden internationalen Organisation durchgeführt.

(3) Mit dem Bewertungsbesuch wird mindestens Folgendes bewertet:

a) der Rechtsrahmen für den Schutz von Verschlusssachen und seine Angemessenheit für den Schutz von EU-VS eines bestimmten Geheimhaltungsgrads;

b) alle spezifischen Merkmale des Sicherheitskonzepts und die Art und Weise der Organisation der Sicherheit in dem betreffenden Drittstaat oder bei der betreffenden internationalen Organisation, soweit sich dies darauf auswirken kann, welchen Geheimhaltungsgrad die auszutauschenden Verschlusssachen haben dürfen;

c) die tatsächlich bestehenden Sicherheitsmaßnahmen und -verfahren, und

d) die Verfahren für die Sicherheitsermächtigung des Personals für den Geheimhaltungsgrad der EU-VS, die weitergegeben werden sollen.

(4) Der in Artikel 6 Absatz 8 genannte Ausschuss für Informationssicherheit erhält einen Bericht über die Ergebnisse solcher Besuche, bevor die EU-VS tatsächlich an den betreffenden Drittstaat oder die betreffende internationale Organisation weitergegeben werden. Gegebenenfalls wird der Bericht auch dem betreffenden Organ oder der betreffenden Einrichtung der Union übermittelt.

(5) Die Sicherheitsbehörde des betreffenden Organs oder der betreffenden Einrichtung der Union unterrichtet den Drittstaat oder die internationale Organisation über den Zeitpunkt, ab dem sie in der Lage ist, EU-VS auszutauschen, sowie über den höchsten Geheimhaltungsgrad, bis zu dem EU-VS in Papierform oder elektronisch ausgetauscht werden dürfen.

(6) Folgebesuche werden organisiert, wenn folgende Bedingungen erfüllt sind:

a) der Geheimhaltungsgrad der EU-VS, die ausgetauscht werden dürfen, muss angehoben werden;

b) dem betreffenden Organ oder der betreffenden Einrichtung der Union wurden grundlegende Änderungen der Sicherheitsvorkehrungen des Drittstaats oder der internationalen Organisation mitgeteilt, die sich auf die Art und Weise auswirken könnten, wie EU-VS geschützt werden;

c) es ist ein schwerwiegender Informationssicherheitsvorfall mit unbefugter Offenlegung von EU-VS aufgetreten.

Artikel 58

Ad-hoc-Weitergabe von EU-Verschlusssachen in Ausnahmefällen

(1) In Ermangelung eines Geheimschutzabkommens oder einer Verwaltungsvereinbarung und wenn ein Organ oder eine Einrichtung der Union feststellt, dass die Weitergabe von EU-VS an ein anderes Organ oder eine andere Einrichtung der Union oder an einen Drittstaat oder eine internationale Organisation ausnahmsweise erforderlich ist, oder

wenn ein Geheimschutzabkommen oder eine Verwaltungsvereinbarung geschlossen wurde und ein Organ oder eine Einrichtung der Union feststellt, dass ausnahmsweise EU-VS mit einem höheren Geheimhaltungsgrad als in dem Abkommen oder der Vereinbarung vorgesehen weitergegeben werden müssen, ergreifen die Organe oder Einrichtungen der Union, die die EU-VS bereitstellen, folgende Schritte:

a) sie vergewissern sich, soweit möglich, zusammen mit den Sicherheitsbehörden des Drittstaats, der internationalen Organisation oder des Organs bzw. der Einrichtung der Union, die die EU-VS empfangen sollen, dass dessen bzw. deren Sicherheitsvorschriften, -strukturen und -verfahren einen Schutz der weitergegebenen EU-VS gewährleisten, der zumindest den in dieser Verordnung festgelegten Standards entspricht;

b) sie holen auf der Grundlage der Überprüfung gemäß Buchstabe a eine Stellungnahme des in Artikel 6 Absatz 8 genannten Ausschusses für Informationssicherheit ein, es sei denn, die operativen Umstände erfordern eine

sofortige Ad-hoc-Freigabe; in diesem Fall wird der Ausschuss für Informationssicherheit anschließend unterrichtet.

(2) Alle gemäß diesem Artikel freigegebenen Dokumente müssen eine Weitergabekennzeichnung tragen, aus der hervorgeht, an welche Drittstaaten, internationalen Organisationen bzw. Organe oder Einrichtungen der Union sie weitergegeben wurden.

(3) Vor oder bei der tatsächlichen Weitergabe holt das Organ oder die Einrichtung der Union, das bzw. die die EU-VS bereitstellt, von der empfangenden Partei eine schriftliche Erklärung ein, in der diese sich verpflichtet, die erhaltenen EU-VS zu schützen. Gegebenenfalls ist zu verlangen, dass diese sich dazu verpflichten, die EU-VS gemäß den Grundprinzipien und Mindeststandards dieser Verordnung zu schützen.

Kapitel 6
Schlussbestimmungen

Artikel 59

Durchführung

(1) Die Koordinierungsgruppe legt für die Durchführung dieser Verordnung Leitlinien für die Informationssicherheit fest.

(2) Die Organe und Einrichtungen der Union können auf der Grundlage ihres spezifischen Bedarfs interne Vorschriften für die Durchführung dieser Verordnung gemäß Artikel 8 Absatz 2 erlassen.

Artikel 60

Übergangsbestimmungen

(1) Die von den einzelnen Organen oder Einrichtungen der Union vor dem [TT/MM/JJJJ - Datum des Geltungsbeginns] erlassenen internen Vorschriften für die Informationssicherheit werden spätestens [drei Jahre nach Inkrafttreten dieser Verordnung] überprüft.

(2) Alle Organe und Einrichtungen der Union, die infolge einer von der Kommission, dem Rat oder dem EAD vor dem [TT.MM.JJJJ - Datum des Geltungsbeginns] durchgeführten Bewertung als für die Bearbeitung und Aufbewahrung von EU-VS geeignet eingestuft wurden, gelten als Organe und Einrichtungen der Union, die die in Artikel 19 Absatz 1 genannten Bedingungen erfüllen.

(3) Alle Verwaltungsvereinbarungen, die die Organe und Einrichtungen der Union mit Drittstaaten und internationalen Organisationen vor dem [TT.MM.JJJJ - Datum des Geltungsbeginns] geschlossen haben, behalten ihre Gültigkeit.

(4) Haben die Mitgliedstaaten, in deren Hoheitsgebiet die Empfänger der Finanzhilfevereinbarung der Kommission angesiedelt sind, beschlossen, im Rahmen des Europäischen Programms zur industriellen Entwicklung im Verteidigungsbereich einen spezifischen Sicherheitsrahmen für den Schutz und die Bearbeitung nationaler Verschlusssachen im Zusammenhang mit der betreffenden Finanzhilfevereinbarung einzusetzen, so beachtet die Kommission bei der Anwendung der in dieser

Verordnung vorgesehenen Verfahren für den Geheimschutz in der Wirtschaft diesen Sicherheitsrahmen bis zum Ende des Lebenszyklus der Finanzhilfevereinbarung.

Artikel 61

Überwachung und Evaluierung

(1) Spätestens am [TT/MM/JJJJ - drei Jahre nach Geltungsbeginn] legt die Kommission dem Europäischen Parlament und dem Rat einen Bericht über die Durchführung dieser Verordnung vor.

(2) Frühestens [fünf Jahre nach Geltungsbeginn] und danach alle fünf Jahre führt die Kommission eine Bewertung dieser Verordnung durch und legt dem Europäischen Parlament und dem Rat einen Bericht über die wichtigsten Ergebnisse vor.

Artikel 62

Inkrafttreten und Geltungsbeginn

(1) Diese Verordnung tritt am zwanzigsten Tag nach ihrer Veröffentlichung im Amtsblatt der Europäischen Union in Kraft.

(2) Sie gilt ab dem [Datum - erster Tag des Monats, der auf den Zeitraum von zwei Jahren nach dem Tag des Inkrafttretens folgt].

Diese Verordnung ist in allen ihren Teilen verbindlich und gilt unmittelbar in jedem Mitgliedstaat.

Geschehen zu Brüssel am […]

Im Namen des Europäischen Parlaments	*Im Namen des Rates*
Die Präsidentin	*Der Präsident /// die Präsidentin*
[...]	*[...]*

FINANZBOGEN ZU RECHTSAKTEN

1. RAHMEN DES VORSCHLAGS/DER INITIATIVE

1.1. Bezeichnung des Vorschlags/der Initiative

1.2. Politikbereich(e)

1.3. Der Vorschlag/Die Initiative betrifft

1.4. Ziel(e)

1.4.1 Allgemeine(s) Ziel(e)

1.4.2 Einzelziel(e)

1.4.3 Erwartete Ergebnisse und Auswirkungen

1.4.4 Leistungsindikatoren

1.5. Begründung des Vorschlags/der Initiative

1.5.1 Kurz- oder langfristig zu deckender Bedarf, einschließlich einer detaillierten Zeitleiste für die Durchführung der Initiative

1.5.2 Mehrwert aufgrund des Tätigwerdens der Union (kann sich aus unterschiedlichen Faktoren ergeben, z. B. Vorteile durch Koordinierung, Rechtssicherheit, größerer Wirksamkeit oder Komplementarität). Für die Zwecke dieser Nummer bezeichnet der Ausdruck „Mehrwert aufgrund des Tätigwerdens der Union" den Wert, der sich aus dem Tätigwerden der Union ergibt und den Wert ergänzt, der andernfalls allein von den Mitgliedstaaten geschaffen worden wäre.

1.5.3 Aus früheren ähnlichen Maßnahmen gewonnene wesentliche Erkenntnisse

1.5.4 Vereinbarkeit mit dem Mehrjährigen Finanzrahmen sowie mögliche Synergieeffekte mit anderen geeigneten Instrumenten

1.5.5 Beurteilung der verschiedenen verfügbaren Finanzierungsoptionen, einschließlich der Möglichkeiten für eine Umschichtung

1.6. Laufzeit und finanzielle Auswirkungen des Vorschlags/der Initiative

1.7. Vorgeschlagene Methode(n) der Mittelverwaltung

2. VERWALTUNGSMAßNAHMEN

2.1. Überwachung und Berichterstattung

2.2. Verwaltungs- und Kontrollsystem(e)

2.2.1 Begründung der Methode(n) der Mittelverwaltung, des Durchführungsmechanismus/der Durchführungsmechanismen für die Finanzierung, der Zahlungsmodalitäten und der Kontrollstrategie, wie vorgeschlagen

2.2.2 Angaben zu den ermittelten Risiken und dem/den zu deren Eindämmung eingerichteten System(en) der internen Kontrolle

2.2.3 Schätzung und Begründung der Kosteneffizienz der Kontrollen (Verhältnis zwischen den Kontrollkosten und dem Wert der betreffenden verwalteten Mittel) sowie Bewertung des erwarteten Ausmaßes des Fehlerrisikos (bei Zahlung und beim Abschluss)

2.3. Prävention von Betrug und Unregelmäßigkeiten

3. GESCHÄTZTE FINANZIELLE AUSWIRKUNGEN DES VORSCHLAGS/DER INITIATIVE

3.1. Betroffene Rubrik(en) des Mehrjährigen Finanzrahmens und Ausgabenlinie(n) im Haushaltsplan

3.2. Geschätzte finanzielle Auswirkungen des Vorschlags

3.2.1 Übersicht über die geschätzten Auswirkungen auf die operativen Mittel

3.2.2 Geschätzte Ergebnisse, die mit operativen Mitteln finanziert werden

3.2.3 Übersicht über die geschätzten Auswirkungen auf die Verwaltungsmittel

3.2.4 Vereinbarkeit mit dem Mehrjährigen Finanzrahmen

3.2.5 Finanzierungsbeteiligung Dritter

3.3. Geschätzte Auswirkungen auf die Einnahmen

FINANZBOGEN ZU RECHTSAKTEN

1. RAHMEN DES VORSCHLAGS/DER INITIATIVE

1.1. Bezeichnung des Vorschlags/der Initiative

Vorschlag für eine VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES über die Informationssicherheit in den Organen, Einrichtungen und sonstigen Stellen der Union

1.2. Politikbereich(e)

Europäische öffentliche Verwaltung

Die Vorschriften für die Informationssicherheit der Organe und Einrichtungen der Union sollten zusammen einen umfassenden und kohärenten allgemeinen Rahmen für den Schutz von Informationen in der europäischen Verwaltung bilden und die Gleichwertigkeit der Grundprinzipien und Mindeststandards gewährleisten. Auch das Schutzniveau der Informationen sollte in allen Organen und Einrichtungen der Union gleich sein.

1.3. Der Vorschlag/Die Initiative betrifft

☑eine neue Maßnahme

☐ eine neue Maßnahme im Anschluss an ein Pilotprojekt/eine vorbereitende Maßnahme[32]

☐ die Verlängerung einer bestehenden Maßnahme

☐ die Zusammenführung mehrerer Maßnahmen oder die Neuausrichtung mindestens einer Maßnahme

1.4. Ziel(e)

1.4.1. Allgemeine(s) Ziel(e)

Das allgemeine Ziel der Initiative besteht darin, Vorschriften für die Informationssicherheit für alle Organe und Einrichtungen der Union zu schaffen, um einen verbesserten und kohärenten Schutz gegen die sich wandelnden Bedrohungen für ihre Informationen zu gewährleisten.

1.4.2. Einzelziel(e)

• Einzelziel Nr. 1: Festlegung harmonisierter und umfassender Kategorien von Informationen sowie gemeinsamer Vorschriften für den Umgang mit den von der europäischen Verwaltung bearbeiteten Informationen und Erleichterung des sicheren Informationsaustauschs zwischen den Organen und Einrichtungen der Union bei gleichzeitiger Minimierung der Auswirkungen auf die Mitgliedstaaten

• Einzelziel Nr. 2: Gewährleistung, dass alle Organe und Einrichtungen der Union etwaige Sicherheitslücken in ihren Verfahren ermitteln und die erforderlichen Maßnahmen ergreifen, um gleiche Bedingungen für die Informationssicherheit zu gewährleisten

• Einzelziel Nr. 3: Einrichtung eines effizienten Systems der Zusammenarbeit im Bereich der Informationssicherheit zwischen den Organen und Einrichtungen der

[32] Im Sinne des Artikels 58 Absatz 2 Buchstabe a oder b der Haushaltsordnung.

Union, das eine kohärente Kultur der Informationssicherheit in der gesamten europäischen Verwaltung fördern kann

• Einzelziel Nr. 4: Modernisierung der Strategien zur Informationssicherheit auf allen Ebenen der Klassifizierung/Kategorisierung für alle Organe und Einrichtungen der Union unter Berücksichtigung des digitalen Wandels und der Entwicklung der Telearbeit als grundlegende Arbeitsweise

1.4.3. Erwartete Ergebnisse und Auswirkungen

Bitte geben Sie an, wie sich der Vorschlag/die Initiative auf die Begünstigten/Zielgruppe auswirken dürfte.

Der Vorschlag wird folgende Auswirkungen auf die Organe und Einrichtungen der Union haben:

– Überprüfung ihrer internen Vorschriften und Verfahren mit dem Ziel der Anpassung an die Verordnung

– Kategorisierung aller bearbeiteten Informationen nach dem in der Verordnung vorgesehenen Schema

– Sicherstellung, dass ihre Kommunikations- und Informationssysteme den Anforderungen der Verordnung entsprechen

– Teilnahme an der interinstitutionellen Koordinierungsgruppe für Informationssicherheit („Koordinierungsgruppe“)

Die Mitgliedstaaten werden von dieser Verordnung profitieren, da die Zusammenarbeit mit den Organen und Einrichtungen der Union in allen relevanten Bereichen (Personalsicherheit, industrielle Sicherheit oder Informationsaustausch) auf denselben Konzepten, Regeln und Verfahren beruhen würde.

1.4.4. Leistungsindikatoren

Bitte geben Sie an, anhand welcher Indikatoren sich die Fortschritte und Ergebnisse verfolgen lassen.

Für das Einzelziel Nr. 1 relevante Indikatoren

– Annahme geeigneter Leitlinien

– Umsetzung der neuen Kennzeichnungen

– Veröffentlichung aktualisierter Anweisungen für den Umgang mit allen Kategorien von Informationen

– Einführung gemeinsamer Systeme für den Umgang mit nicht als Verschlusssache eingestuften vertraulichen Informationen und EU-VS

Für das Einzelziel Nr. 2 relevante Indikatoren

– Anzahl der abgegebenen / umgesetzten Empfehlungen

– Anzahl der Informationslecks in den Organen und Einrichtungen

Für das Einzelziel Nr. 3 relevante Indikatoren

– Statistiken über die zentrale gegenüber der lokalen Beschaffung

– Kontrollprotokolle

– Anzahl der vom Sekretariat der Koordinierungsgruppe für Informationssicherheit bearbeiteten Anfragen

Für das Einzelziel Nr. 4 relevante Indikatoren

– Anzahl der geschulten Benutzer

– Grad der Sensibilisierung des Personals hinsichtlich der Vorschriften für die Informationssicherheit

– Prozentualer Anteil des Personals, das in der Lage ist, mit sicheren Telearbeitsgeräten zu arbeiten

1.5. Begründung des Vorschlags/der Initiative

1.5.1. Kurz- oder langfristig zu deckender Bedarf, einschließlich einer detaillierten Zeitleiste für die Durchführung der Initiative

Die Umsetzung dieser Initiative erfolgt schrittweise nach folgendem Konzept:

– 2022/2023: Erlass der Verordnung, Inkrafttreten

– 2024/2025: Überprüfung der internen Vorschriften zur Informationssicherheit durch alle Organe und Einrichtungen der Union mit dem Ziel, diese an die Verordnung anzupassen

– 2025: organisatorische Arbeiten für die Einrichtung der Koordinierungsgruppe und ihres Sekretariats sowie der technischen Untergruppen

– 2024/2025: Beginn der Anwendung der Verordnung

– 2025/2026: Annahme der Geschäftsordnung für die Koordinierungsgruppe und die technischen Untergruppen

– 2026–2028: Arbeit an Leitfäden für die Durchführung der Verordnung, Austausch bewährter Verfahren zwischen den Organen und Einrichtungen

– 2029/2030: Vorbereitung der ersten Evaluierung der Verordnung (alle fünf Jahre ab dem Anwendungsbeginn)

– 2030: erste Evaluierung der Verordnung

1.5.2. Mehrwert aufgrund des Tätigwerdens der Union (kann sich aus unterschiedlichen Faktoren ergeben, z. B. Vorteile durch Koordinierung, Rechtssicherheit, größerer Wirksamkeit oder Komplementarität). Für die Zwecke dieser Nummer bezeichnet der Ausdruck „Mehrwert aufgrund des Tätigwerdens der Union“ den Wert, der sich aus dem Tätigwerden der Union ergibt und den Wert ergänzt, der andernfalls allein von den Mitgliedstaaten geschaffen worden wäre.

Die Initiative trägt dazu bei, dass die Organe und Einrichtungen der Union bei der Ausübung ihrer Aufgaben durch eine offene, effiziente und unabhängige Verwaltung unterstützt werden. Zudem ergänzt sie die allgemeinen nationalen Bemühungen der Mitgliedstaaten im Bereich der Sicherheit der EU, indem sie die Organe und Einrichtungen vor externen Eingriffen und Spionagetätigkeiten schützt.

1.5.3. Aus früheren ähnlichen Maßnahmen gewonnene wesentliche Erkenntnisse

Nicht zutreffend

1.5.4. Vereinbarkeit mit dem Mehrjährigen Finanzrahmen sowie mögliche Synergieeffekte mit anderen geeigneten Instrumenten

Im Rahmen des Projekts müssen zwei VZÄ für das Sekretariat der Koordinierungsgruppe für Informationssicherheit umgewidmet/zugewiesen werden. Andere Projekte, wie z. B. die Entwicklung gemeinsamer Instrumente und die Zentralisierung einiger Tätigkeiten, sind teilweise bereits im Gange und werden durch Dienstleistungsvereinbarungen und Rahmenverträge abgedeckt.

1.5.5. Beurteilung der verschiedenen verfügbaren Finanzierungsoptionen, einschließlich der Möglichkeiten für eine Umschichtung

Siehe vorheriger Abschnitt.

1.6. Laufzeit und finanzielle Auswirkungen des Vorschlags/der Initiative

☐ **befristete Laufzeit**

– ☐ Laufzeit: [TT.MM.]JJJJ bis [TT.MM.]JJJJ

– ☐ Finanzielle Auswirkungen auf die Mittel für Verpflichtungen von JJJJ bis JJJJ und auf die Mittel für Zahlungen von JJJJ bis JJJJ

– ☑ **unbefristete Laufzeit**

1.7. Vorgeschlagene Methode(n) der Mittelverwaltung[33]

☑ **Direkte Mittelverwaltung** durch die Kommission und durch die einzelnen Organe und Einrichtungen der Union

– ☑ durch ihre Dienststellen, einschließlich ihres Personals in den Delegationen der Union

– ☐ durch Exekutivagenturen

☐ **Geteilte Mittelverwaltung** mit Mitgliedstaaten

☐ **Indirekte Mittelverwaltung** durch Übertragung von Haushaltsvollzugsaufgaben an:

– ☐ Drittstaaten oder die von ihnen benannten Einrichtungen

– ☐ internationale Einrichtungen und deren Agenturen (bitte angeben)

– ☐ die EIB und den Europäischen Investitionsfonds

– ☐ Einrichtungen im Sinne der Artikel 70 und 71 der Haushaltsordnung

– ☐ öffentlich-rechtliche Körperschaften

– ☐ privatrechtliche Einrichtungen, die im öffentlichen Auftrag tätig werden, sofern ihnen ausreichende finanzielle Garantien bereitgestellt werden

– ☐ privatrechtliche Einrichtungen eines Mitgliedstaats, die mit der Umsetzung einer öffentlich-privaten Partnerschaft betraut werden und denen ausreichende finanzielle Garantien bereitgestellt werden

– ☐ Personen, die mit der Durchführung bestimmter Maßnahmen im Bereich der GASP im Rahmen des Titels V EUV betraut und in dem maßgeblichen Basisrechtsakt benannt sind

– *Falls mehrere Methoden der Mittelverwaltung angegeben werden, ist dies unter „Bemerkungen" näher zu erläutern.*

Bemerkungen

[33] Erläuterungen zu den Methoden der Mittelverwaltung und Verweise auf die Haushaltsordnung enthält die Website BudgWeb: https://myintracomm.ec.europa.eu/budgweb/DE/man/budgmanag/Pages/budgmanag.aspx

2. VERWALTUNGSMAßNAHMEN

2.1. Überwachung und Berichterstattung

Bitte geben Sie an, wie oft und unter welchen Bedingungen diese Tätigkeiten erfolgen.

Alle fünf Jahre wird die Verordnung evaluiert, und die Kommission wird dem Rat und dem Europäischen Parlament über ihre Ergebnisse berichten.

2.2. Verwaltungs- und Kontrollsystem(e)

2.2.1. Begründung der Methode(n) der Mittelverwaltung, des Durchführungsmechanismus/der Durchführungsmechanismen für die Finanzierung, der Zahlungsmodalitäten und der Kontrollstrategie, wie vorgeschlagen

In der Verordnung werden Vorschriften zur Informationssicherheit festgelegt, die für alle Organe und Einrichtungen der Union gelten. Die Überwachung der ordnungsgemäßen Durchführung erfolgt durch eine Koordinierungsgruppe, an der alle Sicherheitsbehörden der Organe und Einrichtungen beteiligt sind. Die volle Verantwortung für die Sicherheit verbleibt bei den Sicherheitsbehörden der einzelnen Organe und Einrichtungen und unterliegt dem bestehenden internen Kontrollrahmen der einzelnen Organe und Einrichtungen.

2.2.2. Angaben zu den ermittelten Risiken und dem/den zu deren Eindämmung eingerichteten System(en) der internen Kontrolle

Mit der Verordnung wird eine gemeinsame Grundlage von Vorschriften für die Informationssicherheit geschaffen und die Transparenz der Sicherheitsmaßnahmen für den Informationsaustausch zwischen den Organen und Einrichtungen der Union gewährleistet; damit werden die mit der Informationssicherheit verbundenen Risiken allgemein verringert. Die Verordnung steht im Einklang mit den Normen der internen Kontrolle und beinhaltet einen risikobasierten Ansatz für die Politikgestaltung.

2.2.3. Schätzung und Begründung der Kosteneffizienz der Kontrollen (Verhältnis zwischen den Kontrollkosten und dem Wert der betreffenden verwalteten Mittel) sowie Bewertung des erwarteten Ausmaßes des Fehlerrisikos (bei Zahlung und beim Abschluss)

Die bestehenden Kontrollmechanismen für die Organe und Einrichtungen werden anwendbar sein. Die Einhaltung der Verordnung und die mit der Informationssicherheit verbundenen Risiken sollten im Rahmen der jährlichen Risikoberichterstattung der Organe und Einrichtungen gemeldet werden.

2.3. Prävention von Betrug und Unregelmäßigkeiten

Bitte geben Sie an, welche Präventions- und Schutzmaßnahmen, z. B. im Rahmen der Betrugsbekämpfungsstrategie, bereits bestehen oder angedacht sind.

Nicht zutreffend

3. GESCHÄTZTE FINANZIELLE AUSWIRKUNGEN DES VORSCHLAGS/DER INITIATIVE

3.1. Betroffene Rubrik(en) des Mehrjährigen Finanzrahmens und Ausgabenlinie(n) im Haushaltsplan

- Bestehende Haushaltslinien

In der Reihenfolge der Rubriken des Mehrjährigen Finanzrahmens und der Haushaltslinien.

Rubrik des Mehrjährigen Finanzrahmens	Haushaltslinie	Art der Ausgaben	Finanzierungsbeiträge			
	Nummer	GM/NGM [34]	von EFTA-Ländern[35]	von Kandidatenländern[36]	von Drittstaaten	nach Artikel 21 Absatz 2 Buchstabe b der Haushaltsordnung
RUBRIK 7	20 01 02 01	NGM	NEIN	NEIN	NEIN	NEIN

- Neu zu schaffende Haushaltslinien

In der Reihenfolge der Rubriken des Mehrjährigen Finanzrahmens und der Haushaltslinien.

Rubrik des Mehrjährigen Finanzrahmens	Haushaltslinie	Art der Ausgaben	Finanzierungsbeiträge			
	Nummer	GM/NGM	von EFTA-Ländern	von Kandidatenländern	von Drittstaaten	nach Artikel 21 Absatz 2 Buchstabe b der Haushaltsordnung
	Keine		JA/NEIN	JA/NEIN	JA/NEIN	JA/NEIN

34 GM = Getrennte Mittel/NGM = Nichtgetrennte Mittel.
35 EFTA: Europäische Freihandelsassoziation.
36 Kandidatenländer und gegebenenfalls potenzielle Kandidaten des Westbalkans.

3.2. Geschätzte finanzielle Auswirkungen des Vorschlags auf die Mittel

3.2.1. Übersicht über die geschätzten Auswirkungen auf die operativen Mittel

– ☑ Für den Vorschlag/die Initiative werden keine operativen Mittel benötigt.

– ☐ Für den Vorschlag/die Initiative werden die folgenden operativen Mittel benötigt:

in Mio. EUR (3 Dezimalstellen)

Rubrik des Mehrjährigen Finanzrahmens	Nummer	

GD: <…….>			Jahr **N**[37]	Jahr **N+1**	Jahr **N+2**	Jahr **N+3**	Bei länger andauernden Auswirkungen (siehe 1.6.) bitte weitere Spalten einfügen.			**INSGESAMT**
• Operative Mittel										
Haushaltslinie[38]	Verpflichtungen	(1a)								
	Zahlungen	(2a)								
Haushaltslinie	Verpflichtungen	(1b)								
	Zahlungen	(2b)								
Aus der Dotation bestimmter operativer Programme finanzierte Verwaltungsausgaben[39]										
Haushaltslinie		(3)								
Mittel INSGESAMT für GD <…….>	Verpflichtungen	=1a + 1 b + 3								
	Zahlungen	=2a + 2								

37 Das Jahr N ist das Jahr, in dem mit der Umsetzung des Vorschlags/der Initiative begonnen wird. Bitte ersetzen Sie „N“ durch das voraussichtlich erste Jahr der Umsetzung (z. B. 2021). Dasselbe gilt für die folgenden Jahre.

38 Gemäß dem offiziellen Eingliederungsplan.

39 Technische und/oder administrative Hilfe und Ausgaben zur Unterstützung der Durchführung von Programmen bzw. Maßnahmen der EU (vormalige BA-Linien), indirekte Forschung, direkte Forschung.

		b + 3								

• Operative Mittel INSGESAMT	Verpflichtungen	(4)								
	Zahlungen	(5)								
• Aus der Dotation bestimmter spezifischer Programme finanzierte Verwaltungsausgaben INSGESAMT		(6)								
Mittel INSGESAMT unter RUBRIK <….> des Mehrjährigen Finanzrahmens	Verpflichtungen	=4 + 6								
	Zahlungen	=5 + 6								

Wenn der Vorschlag/die Initiative mehrere operative Rubriken betrifft, ist der vorstehende Abschnitt zu wiederholen:

• Operative Mittel INSGESAMT (alle operativen Rubriken)	Verpflichtungen	(4)								
	Zahlungen	(5)								
Aus der Dotation bestimmter spezifischer Programme finanzierte Verwaltungsausgaben INSGESAMT (alle operativen Rubriken)		(6)								
Mittel INSGESAMT unter den RUBRIKEN 1 bis 6 des Mehrjährigen Finanzrahmens (Referenzbetrag)	Verpflichtungen	=4 + 6								
	Zahlungen	=5 + 6								

Rubrik des Mehrjährigen Finanzrahmens	7	Verwaltungsausgaben

Zum Ausfüllen dieses Teils ist die „Tabelle für Verwaltungsausgaben“ zu verwenden, die zuerst in den Anhang des Finanzbogens zu Rechtsakten (Anhang V der Internen Vorschriften), der für die dienststellenübergreifende Konsultation in DECIDE hochgeladen wird, aufgenommen wird.

in Mio. EUR (3 Dezimalstellen)

		Jahr **2023**	Jahr **2024**	Jahr **2025**	Jahr **2026**	Jahr **2027**	**INSGESAMT**
GD: HR							
• Personal		0,314	0,314	0,314	0,314	0,314	**1,570**
• Sonstige Verwaltungsausgaben							
GD INSGESAMT <…….>	Mittel	0,314	0,314	0,314	0,314	0,314	**1,570**

Mittel INSGESAMT unter RUBRIK 7 des Mehrjährigen Finanzrahmens	(Verpflichtungen insges. = Zahlungen insges.)	0,314	0,314	0,314	0,314	0,314	**1,570**

in Mio. EUR (3 Dezimalstellen)

		Jahr **2023**	Jahr **2024**	Jahr **2025**	Jahr **2026**	Jahr **2027**	**INSGESAMT**
Mittel INSGESAMT unter den RUBRIKEN 1 bis 7 des Mehrjährigen Finanzrahmens	Verpflichtungen	0,314	0,314	0,314	0,314	0,314	**1,570**
	Zahlungen	0,314	0,314	0,314	0,314	0,314	**1,570**

3.2.2. Geschätzte Ergebnisse, die mit operativen Mitteln finanziert werden

Mittel für Verpflichtungen, in Mio. EUR (3 Dezimalstellen)

Ziele und Ergebnisse ⇩			Jahr **N**		Jahr **N+1**		Jahr **N+2**		Jahr **N+3**		Bei länger andauernden Auswirkungen (siehe 1.6.) bitte weitere Spalten einfügen.						**INSGESAMT**	
	ERGEBNISSE																	
	Art[40]	Durch-schnitts-kosten	Anzahl	Kosten	Anzahl	Kosten	Anzahl	Kosten	Anzahl	Kosten	Anzahl	Kosten	Anzahl	Kosten	Anzahl	Kosten	Gesamt-zahl	Gesamt-kosten
EINZELZIEL Nr. 1[41]…																		
- Ergebnis																		
- Ergebnis																		
- Ergebnis																		
Zwischensumme für Einzelziel Nr. 1																		
EINZELZIEL Nr. 2 ...																		
- Ergebnis																		
Zwischensumme für Einzelziel Nr. 2																		
INSGESAMT																		

40 Ergebnisse sind Produkte, die geliefert, und Dienstleistungen, die erbracht werden (z. B. Zahl der Austauschstudenten, gebaute Straßenkilometer usw.).

41 Wie unter 1.4.2 („Einzelziel(e)…“) beschrieben.

3.2.3. Übersicht über die geschätzten Auswirkungen auf die Verwaltungsmittel

– ☐ Für den Vorschlag/die Initiative werden keine Verwaltungsmittel benötigt.

– ☑ Für den Vorschlag/die Initiative werden die folgenden Verwaltungsmittel benötigt:

in Mio. EUR (3 Dezimalstellen)

	Jahr **2023**	Jahr **2024**	Jahr **2025**	Jahr **2026**	Jahr **2027**	**INSGESAMT**
RUBRIK 7 des Mehrjährigen Finanzrahmens						
Personal	0,314	0,314	0,314	0,314	0,314	**1,570**
Sonstige Verwaltungsausgaben						
Zwischensumme RUBRIK 7 des Mehrjährigen Finanzrahmens	0,314	0,314	0,314	0,314	0,314	**1,570**

Außerhalb der RUBRIK 7[42] des Mehrjährigen Finanzrahmens						
Personal						
Sonstige Verwaltungsausgaben						
Zwischensumme außerhalb RUBRIK 7 des Mehrjährigen Finanzrahmens						

INSGESAMT	0,314	0,314	0,314	0,314	0,314	**1,570**

Der Mittelbedarf für Personal- und sonstige Verwaltungsausgaben wird durch Mittel der GD gedeckt, die bereits für die Verwaltung der Maßnahme zugeordnet sind oder innerhalb der GD umgeschichtet wurden. Hinzu kommen etwaige zusätzliche Mittel, die der für die Verwaltung der Maßnahme zuständigen GD nach Maßgabe der verfügbaren Mittel im Rahmen der jährlichen Mittelzuweisung zugeteilt werden.

42 Technische und/oder administrative Hilfe und Ausgaben zur Unterstützung der Durchführung von Programmen bzw. Maßnahmen der EU (vormalige BA-Linien), indirekte Forschung, direkte Forschung.

3.2.3.1. Geschätzter Personalbedarf

– ☐ Für den Vorschlag/die Initiative wird kein Personal benötigt.

– ☑ Für den Vorschlag/die Initiative wird folgendes Personal benötigt:

Schätzung in Vollzeitäquivalenten

		Jahr **2023**	Jahr **2024**	Jahr **2025**	Jahr **2026**	Jahr **2027**
20 01 02 01 (am Sitz und in den Vertretungen der Kommission)		2	2	2	2	2
20 01 02 03 (in den Delegationen)						
01 01 01 01 (indirekte Forschung)						
01 01 01 11 (direkte Forschung)						
Sonstige Haushaltslinien (bitte angeben)						
20 02 01 (VB, ANS und LAK der Globaldotation)						
20 02 03 (VB, ÖB, ANS, LAK und JFD in den Delegationen)						
XX 01 xx **yy zz** [43]	- am Sitz der Kommission					
	- in Delegationen					
01 01 01 02 (VB, ANS und LAK - indirekte Forschung)						
01 01 01 12 (VB, ANS und LAK - direkte Forschung)						
Sonstige Haushaltslinien (bitte angeben)						
INSGESAMT		**2**	**2**	**2**	**2**	**2**

XX steht für den jeweiligen Politikbereich bzw. Haushaltstitel.

Der Personalbedarf wird durch der Verwaltung der Maßnahme zugeordnetes Personal der GD oder GD-interne Personalumschichtung gedeckt. Hinzu kommen etwaige zusätzliche Mittel, die der für die Verwaltung der Maßnahme zuständigen GD nach Maßgabe der verfügbaren Mittel im Rahmen der jährlichen Mittelzuweisung zugeteilt werden.

Beschreibung der auszuführenden Aufgaben:

Beamte sowie Bedienstete auf Zeit	Sekretariat der Koordinierungsgruppe für Informationssicherheit: 1 AD-Beamter + 1 AST-Beamter
Externes Personal	

[43] Teilobergrenze für aus operativen Mitteln finanziertes externes Personal (vormalige BA-Linien).

3.2.4. Vereinbarkeit mit dem Mehrjährigen Finanzrahmen

Der Vorschlag/Die Initiative

– ☑ kann durch Umschichtungen innerhalb der entsprechenden Rubrik des Mehrjährigen Finanzrahmens (MFR) in voller Höhe finanziert werden.

Nach dem Vorschlag sollen dem ständigen Sekretariat der Interinstitutionellen Koordinierungsgruppe, das in HR.DS angesiedelt ist, zwei Bedienstete zugewiesen werden.

– ☐ erfordert die Inanspruchnahme des verbleibenden Spielraums unter der einschlägigen Rubrik des MFR und/oder den Einsatz der besonderen Instrumente im Sinne der MFR-Verordnung.

Bitte erläutern Sie den Bedarf unter Angabe der betreffenden Rubriken und Haushaltslinien, der entsprechenden Beträge und der vorgeschlagenen einzusetzenden Instrumente.

– ☐ erfordert eine Revision des MFR.

Bitte erläutern Sie den Bedarf unter Angabe der betreffenden Rubriken und Haushaltslinien sowie der entsprechenden Beträge.

3.2.5. Finanzierungsbeteiligung Dritter

Der Vorschlag/Die Initiative

– ☑ sieht keine Kofinanzierung durch Dritte vor.

– ☐ sieht folgende Kofinanzierung durch Dritte vor:

Mittel in Mio. EUR (3 Dezimalstellen)

	Jahr **N**[44]	Jahr **N+1**	Jahr **N+2**	Jahr **N+3**	Insgesamt
Kofinanzierende Einrichtung					
Kofinanzierung INSGESAMT					

Hinweis: Der Vorschlag wird die derzeitige Zusammenarbeit im Bereich der Informationssicherheit durch SLAs intensivieren.

[44] Das Jahr N ist das Jahr, in dem mit der Umsetzung des Vorschlags/der Initiative begonnen wird. Bitte ersetzen Sie „N“ durch das voraussichtlich erste Jahr der Umsetzung (z. B. 2021). Dasselbe gilt für die folgenden Jahre.

3.3. Geschätzte Auswirkungen auf die Einnahmen

– ☑ Der Vorschlag/Die Initiative wirkt sich nicht auf die Einnahmen aus.

– ☐ Der Vorschlag/Die Initiative wirkt sich auf die Einnahmen aus, und zwar:

☐ auf die Eigenmittel

☐ auf die übrigen Einnahmen

Bitte geben Sie an, ob die Einnahmen bestimmten Ausgabenlinien zugewiesen sind. ☐

in Mio. EUR (3 Dezimalstellen)

Einnahmen-linie:	Für das laufende Haushaltsjahr zur Verfügung stehende Mittel	Auswirkungen des Vorschlags/der Initiative[45]			
		Jahr **N**	Jahr **N+1**	Jahr **N+2**	Jahr **N+3**

Bitte geben Sie für die zweckgebundenen Einnahmen die betreffende(n) Ausgabenlinie(n) im Haushaltsplan an.

Sonstige Anmerkungen (bei der Ermittlung der Auswirkungen auf die Einnahmen verwendete Methode/Formel oder weitere Informationen).

[45] Bei den traditionellen Eigenmitteln (Zölle, Zuckerabgaben) sind die Beträge netto, d. h. abzüglich 20 % für Erhebungskosten, anzugeben.