BESCHLUSS (EU, Euratom) 2018/559 DER KOMMISSION

vom 6. April 2018

zur Festlegung von Durchführungsbestimmungen zu Artikel 6 des Beschlusses (EU, Euratom) 2017/46 über die Sicherheit von Kommunikations- und Informationssystemen in der Europäischen Kommission

DIE EUROPÄISCHE KOMMISSION —

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

gestützt auf den Vertrag zur Gründung der Europäischen Atomgemeinschaft,

gestützt auf den Beschluss (EU, Euratom) 2017/46 der Kommission vom 10. Januar 2017 über die Sicherheit von Kommunikations- und Informationssystemen in der Europäischen Kommission ([1]), insbesondere Artikel 6,

in Erwägung nachstehender Gründe:

(1) Mit der Annahme des Beschlusses (EU, Euratom) 2017/46 ist es nötig, dass die Kommission die Durchführungsbestimmungen zu dem aufgehobenen Beschluss C(2006) 3602 der Kommission über die Sicherheit der von der Kommission verwendeten Kommunikations- und Informationssysteme überprüft, auf den neuesten Stand bringt und konsolidiert.

(2) Das für Sicherheitsfragen zuständige Kommissionsmitglied wurde in voller Übereinstimmung mit der internen Geschäftsordnung ermächtigt, entsprechend Artikel 13 des Beschlusses (EU, Euratom) 2017/46 Durchführungsbestimmungen festzulegen ([2]).

(3) Die Durchführungsbestimmungen zu dem Beschluss C(2006) 3602 sollten daher aufgehoben werden —

HAT FOLGENDEN BESCHLUSS ERLASSEN:

KAPITEL 1

ALLGEMEINE BESTIMMUNGEN

Artikel 1

Gegenstand und Geltungsbereich

(1) Der Gegenstand und der Geltungsbereich dieses Beschlusses sind in Artikel 1 des Beschlusses (EU, Euratom) 2017/46 festgelegt.

(2) Die Bestimmungen des vorliegenden Beschlusses gelten für alle Kommunikations- und Informationssysteme (KIS). Die in diesem Beschluss definierten Zuständigkeiten gelten allerdings nicht für KIS, mit denen EU-Verschlusssachen verwaltet werden. Die jeweiligen Zuständigkeiten für diese Systeme werden gemäß Beschluss (EU, Euratom) 2015/444 der Kommission ([3]) von dem Systemeigner und der Sicherheitsstelle der Kommission festgelegt.

(3) Kapitel 2 dieses Beschlusses enthält einen Überblick über die praktische Umsetzung der Organisation und der Zuständigkeiten in Verbindung mit der IT-Sicherheit. Kapitel 3 dieses Beschlusses enthält einen Überblick über die Prozesse nach Artikel 6 des Beschlusses (EU, Euratom) 2017/46.

Artikel 2

Begriffsbestimmungen

Für diesen Beschluss gelten die Begriffsbestimmungen des Artikels 2 des Beschlusses (EU, Euratom) 2017/46. Zusätzlich gelten für die Zwecke des vorliegenden Beschlusses auch die folgenden Begriffsbestimmungen:

1. „Krypto-Zulassungsstelle“ bezeichnet eine Funktion der Sicherheitsstelle der Kommission, die dem Generaldirektor für Humanressourcen und Sicherheit untersteht.

([1]) ABl. L 6 vom 11.1.2017, S. 40.
([2]) Beschluss C(2017) 7428 der Kommission vom 8. November 2017 über eine Ermächtigung zum Erlass von Durchführungsbestimmungen, Normen und Leitlinien in Bezug auf die Sicherheit von Kommunikations- und Informationssystemen in der Europäischen Kommission.
([3]) Beschluss (EU, Euratom) 2015/444 der Kommission vom 13. März 2015 über die Sicherheitsvorschriften für den Schutz von EU-Verschlusssachen (ABl. L 72 vom 17.3.2015, S. 53).

2. „Externe Netzwerkverbindung“ bezeichnet eine elektronische Kommunikationsverbindung zwischen dem internen Netzwerk der Kommission und einem beliebigen anderen Netzwerk, einschließlich Internet. Netzwerke Dritter, die im Rahmen eines Vertrags als Teil des internen Netzwerks der Kommission bereitgestellt werden, sind hiervon ausgenommen.
3. „Schlüsselhinterlegung“ bezeichnet ein Verfahren zur Speicherung der Kopien kryptografischer Schlüssel bei einer oder mehreren verschiedenen Parteien, wobei für die Trennung von Aufgabenbereichen gesorgt wird, um im Falle des Verlusts der Arbeitskopie deren Wiederherstellung zu ermöglichen. Die Schlüssel können in zwei oder mehrere Teile aufgeteilt werden, wobei jeder Teil bei einer anderen Partei hinterlegt wird, um sicherzustellen, dass nicht eine Partei über den vollständigen Schlüssel verfügt.
4. „RASCI“ ist eine Abkürzung für die Zuweisung von Zuständigkeiten auf der Grundlage folgender Attribute:
   a) „zuständig“ (responsible, R) bedeutet, verpflichtet zu sein, zu handeln und Entscheidungen zu treffen, um verlangte Ergebnisse zu erzielen;
   b) „verantwortlich“ (accountable, A) bedeutet, rechenschaftspflichtig für Handlungen, Entscheidungen und Leistungen zu sein;
   c) „unterstützend“ (supports, S) bedeutet, verpflichtet zu sein, mit der zuständigen Person zusammenzuarbeiten, um eine Aufgabe zu erfüllen;
   d) „beratend“ (consulted, C) bedeutet, für Ratschläge oder eine Meinung herangezogen zu werden;
   e) „informiert“ (informed, I) bedeutet, auf dem neuesten Stand relevanter Informationen zu sein.

KAPITEL 2

ORGANISATION UND ZUSTÄNDIGKEITEN

Artikel 3

Rollen und Zuständigkeiten

Die Rollen und Zuständigkeiten in Verbindung mit den Artikeln 4 bis 8 des vorliegenden Beschlusses werden in Einklang mit dem RASCI-Modell im Anhang definiert.

Artikel 4

Abstimmung mit dem Informationssicherheitskonzept der Kommission

(1) Die Generaldirektion Humanressourcen und Sicherheit überprüft das IT-Sicherheitskonzept der Kommission und die damit verbundenen Normen und Leitlinien, um deren Übereinstimmung mit den allgemeinen Sicherheitskonzepten der Kommission, insbesondere Beschluss (EU, Euratom) 2015/443 der Kommission [1] und Beschluss (EU, Euratom) 2015/444, sicherzustellen.

(2) Auf Antrag anderer Kommissionsdienststellen kann die Generaldirektion Humanressourcen und Sicherheit ihre IT-Sicherheitskonzepte oder andere IT-Sicherheitsdokumente prüfen, um deren Übereinstimmung mit dem Informationssicherheitskonzept der Kommission sicherzustellen. Der Leiter der betreffenden Kommissionsdienststelle sorgt dafür, dass jegliche Abweichung davon korrigiert wird.

(3) Als zuständige Stelle für Informationssicherheit arbeitet die Generaldirektion Humanressourcen und Sicherheit mit der Generaldirektion Informatik zusammen, um dafür zu sorgen, dass die IT-Sicherheitsprozesse der Sicherheitseinstufung und den Sicherheitsgrundsätzen nach Beschluss (EU, Euratom) 2015/443, insbesondere Artikel 3 und 9, vollständig Rechnung tragen.

KAPITEL 3

IT-SICHERHEITSPROZESSE

Artikel 5

Verschlüsselungstechnologien

(1) Die Verwendung von Verschlüsselungstechnologien zum Schutz von EU-Verschlusssachen (EU-VS) erfolgt im Einklang mit Beschluss (EU, Euratom) 2015/444.

(2) Über die Verwendung von Verschlüsselungstechnologien zum Schutz von Nicht-EU-VS-Daten entscheidet der Systemeigner des jeweiligen KIS, und zwar unter Berücksichtigung der Risiken, die durch die Verschlüsselung reduziert werden sollen, sowie der Risiken, die durch die Verschlüsselung entstehen.

(3) Jegliche Verwendung einer Verschlüsselungstechnologie muss vorab von der Krypto-Zulassungsstelle genehmigt werden, es sei denn, die Verschlüsselung dient allein dem Schutz der Vertraulichkeit von Nicht-EU-VS-Daten bei deren Übertragung und es werden Standard-Netzwerkprotokolle verwendet.

[1] Beschluss (EU, Euratom) 2015/443 der Kommission vom 13. März 2015 über Sicherheit in der Kommission (ABl. L 72 vom 17.3.2015, S. 41).

(4) Mit Ausnahme des in Absatz 3 dieses Artikels genannten Falls stellen die Kommissionsdienststellen sicher, dass von sämtlichen Entschlüsselungsschlüsseln Sicherheitskopien angefertigt und im Rahmen der Schlüsselhinterlegung gespeichert werden, damit gespeicherte Daten entschlüsselt werden können, falls der Entschlüsselungsschlüssel nicht verfügbar ist. Die Entschlüsselung verschlüsselter Daten mithilfe einer Sicherheitskopie eines Entschlüsselungsschlüssels darf nur dann erfolgen, wenn dies im Einklang mit der von der Krypto-Zulassungsstelle festgelegten Norm genehmigt worden ist.

(5) Die Anträge auf Genehmigung für die Verwendung von Verschlüsselungstechnologien werden offiziell dokumentiert und enthalten Einzelheiten über das KIS und die Daten, die geschützt werden sollen, sowie über die zu verwendenden Technologien und die damit verbundenen sicherheitsbezogenen Betriebsverfahren. Diese Genehmigungsanträge sind vom Systemeigner zu unterzeichnen.

(6) Genehmigungsanträge für die Verwendung von Verschlüsselungstechnologien werden entsprechend den öffentlichen Normen und Vorgaben von der Krypto-Zulassungsstelle geprüft.

Artikel 6

IT-Sicherheitsüberprüfungen

(1) Die Generaldirektion Humanressourcen und Sicherheit führt IT-Sicherheitsüberprüfungen durch, um zu prüfen, ob die IT-Sicherheitsmaßnahmen den IT-Sicherheitskonzepten der Kommission entsprechen und ob die Integrität dieser Kontrollmaßnahmen gegeben ist.

(2) Die IT-Sicherheitsüberprüfungen können von der Generaldirektion Humanressourcen und Sicherheit durchgeführt werden:

a) auf eigene Initiative;

b) auf Antrag des Lenkungsausschusses für Informationssicherheit (ISSB);

c) auf Antrag eines Systemeigners;

d) nach einem Sicherheitsvorfall; oder

e) nach Identifizierung eines hohen Risikos für ein bestimmtes System.

(3) Bevor sie ihre Informationen in einem KIS speichern, können die Dateneigner eine IT-Sicherheitsüberprüfung beantragen.

(4) Die Ergebnisse einer Überprüfung werden in einem offiziellen Bericht an den Systemeigner dokumentiert, der Feststellungen und Empfehlungen enthält, wie die Übereinstimmung des KIS mit dem IT-Sicherheitskonzept verbessert werden kann; der LISO erhält eine Kopie dieses Berichts. Wichtige Angelegenheiten und Empfehlungen werden dem ISSB von der Generaldirektion Humanressourcen und Sicherheit gemeldet.

(5) Die Umsetzung der Empfehlungen wird von der Generaldirektion Humanressourcen und Sicherheit überwacht.

(6) Gegebenenfalls werden im Rahmen der IT-Sicherheitsüberprüfungen auch die dem Systemeigner von internen und externen Dienstleistern bereitgestellten Dienstleistungen, Räumlichkeiten und Betriebsmittel überprüft.

Artikel 7

Zugriff aus externen Netzwerken

(1) Die Generaldirektion Humanressourcen und Sicherheit legt die Regeln dazu in einer Norm über die Zugangsberechtigung zwischen den KIS der Kommission und externen Netzwerken fest.

(2) Bei den Regeln wird zwischen unterschiedlichen Arten externer Netzwerkverbindungen unterschieden, und es werden geeignete Sicherheitsregeln für die einzelnen Verbindungsarten festgelegt, in denen unter anderem geregelt wird, ob die Verbindung gemäß Absatz 4 dieses Artikels vorab durch die entsprechende Stelle genehmigt werden muss.

(3) Soweit erforderlich, wird die Zugangsberechtigung auf der Grundlage eines offiziellen Antrags- und Genehmigungsverfahrens erteilt. Die Genehmigung ist für einen bestimmten Zeitraum gültig und ist vor Aktivierung der Verbindung einzuholen.

(4) Die Gesamtzuständigkeit für die Genehmigung von Anträgen obliegt der Generaldirektion Humanressourcen und Sicherheit, wobei sie die Zuständigkeit für die Genehmigung bestimmter Verbindungsarten nach Artikel 17 Absatz 3 des Beschlusses (EU, Euratom) 2015/443 und entsprechend den Bedingungen gemäß Ziffer 8 nach eigenem Ermessen übertragen darf.

(5) Die genehmigende Stelle darf zusätzliche Sicherheitsanforderungen als Voraussetzung für die Genehmigung auferlegen, um die KIS und die Netzwerke der Kommission vor dem Risiko eines unbefugten Zugriffs oder anderer Sicherheitsverletzungen zu schützen.

(6) Die Netzwerkdienste für die Kommission werden standardmäßig von der Generaldirektion Informatik bereitgestellt. Alle anderen Kommissionsdienststellen, die ein Netzwerk betreiben, das nicht von der Generaldirektion Informatik bereitgestellt wird, müssen zunächst die Genehmigung des ISSB einholen. Die Kommissionsdienststelle dokumentiert den wirtschaftlichen Grund für den Antrag und weist nach, dass ausreichende Netzwerkkontrollmaßnahmen bestehen, um die Anforderungen für die Kontrolle eingehender und ausgehender Informationsflüsse zu erfüllen.

(7) Der Systemeigner eines KIS legt die Sicherheitsanforderungen für den externen Zugriff auf dieses KIS fest und stellt mit Unterstützung des LISO sicher, dass geeignete Maßnahmen zur Gewährleistung der Systemsicherheit ergriffen werden.

(8) Die Sicherheitsmaßnahmen für externe Netzwerkverbindungen basieren auf dem Grundsatz, dass nur nötige Informationen („Need to know") bereitgestellt und so wenig Rechte wie möglich („Least Privilege") gewährt werden, damit die betreffenden Personen nur die Informationen und Zugriffsrechte erhalten, die sie für die Ausübung ihrer amtlichen Tätigkeiten für die Kommission benötigen.

(9) Um potenzielle Sicherheitsverletzungen zu erkennen, werden alle externen Netzwerkverbindungen gefiltert und überwacht.

(10) Wird eine Verbindung zum Zweck der Auslagerung eines KIS eingerichtet, wird die Genehmigung unter der Voraussetzung erteilt, dass das in Artikel 8 beschriebene Verfahren erfolgreich abgeschlossen wird.

Artikel 8

Auslagerung von KIS

(1) Für die Zwecke dieses Beschlusses wird ein KIS als ausgelagert betrachtet, wenn es auf der Grundlage eines Vertrags mit einem Drittanbieter bereitgestellt wird, laut dem das KIS außerhalb der Räumlichkeiten der Kommission untergebracht ist. Dazu gehören die Auslagerung einzelner oder mehrerer KIS oder sonstiger IT-Dienste, Datenzentren außerhalb der Räumlichkeiten der Kommission sowie die Verarbeitung von Datensätzen der Kommission durch externe Dienstleister.

(2) Bei der Auslagerung eines KIS sind bezüglich der Sensibilität oder Einstufung der verarbeiteten Informationen folgende Dinge zu berücksichtigen:

a) KIS, die EU-VS verarbeiten, müssen gemäß Beschluss (EU, Euratom) 2015/444 akkreditiert werden, wobei vorab die Sicherheitsakkreditierungsstelle der Kommission (SAA) zu konsultieren ist. Die Auslagerung von Systemen, die EU-VS verarbeiten, ist verboten.

b) Der Systemeigner eines KIS, das Nicht-EU-VS verarbeitet, hat unter Berücksichtigung der Risiken einer Auslagerung angemessene Maßnahmen zu ergreifen, um die Sicherheitsanforderungen gemäß den einschlägigen rechtlichen Verpflichtungen bzw. entsprechend der Sensibilität der Informationen zu erfüllen. Die Generaldirektion Humanressourcen und Sicherheit darf dabei zusätzliche Anforderungen auferlegen.

c) Ausgelagerte Entwicklungsprojekte müssen die Sensibilität des entwickelten Codes und aller bei der Entwicklung verwendeten Testdaten berücksichtigen.

(3) Zusätzlich zu den Grundsätzen nach Artikel 3 des Beschlusses (EU, Euratom) 2017/46 gelten für ausgelagerte KIS folgende Grundsätze:

a) Auslagerungsvereinbarungen werden so gestaltet, dass die Abhängigkeit von einzelnen Anbietern vermieden wird.

b) Durch Vereinbarungen über die Sicherheit bei der Auslagerung wird die Möglichkeit verringert, dass Mitarbeiter Dritter auf die Informationen der Kommission zugreifen oder diese verändern.

c) Mitarbeiter Dritter, die Zugriff auf ein ausgelagertes KIS haben, müssen eine Vertraulichkeitsvereinbarung vorweisen.

d) Die Auslagerung eines KIS ist im Bestandsverzeichnis der KIS zu erfassen.

(4) Unter Mitwirkung des Dateneigners ist der Systemeigner verpflichtet,

a) die Risiken der Auslagerung zu prüfen und zu dokumentieren;

b) entsprechende Sicherheitsanforderungen festzulegen;

c) die Systemeigner aller verbundenen KIS zu konsultieren, um sicherzustellen, dass deren Sicherheitsanforderungen abgedeckt sind;

d) dafür zu sorgen, dass der Auslagerungsvertrag angemessene Sicherheitsanforderungen und Rechte enthält;

e) sämtliche anderen Anforderungen zu erfüllen, die in dem ausführlichen Verfahren nach Absatz 8 dieses Artikels beschrieben sind.

Diese Maßnahmen sind jeweils vor der Unterzeichnung eines Vertrags oder einer sonstigen Vereinbarung über die Auslagerung einer oder mehrerer KIS zu treffen.

(5) Um die festgelegten Sicherheitsanforderungen zu erfüllen, müssen die Systemeigner die Risiken in Zusammenhang mit der Auslagerung während der gesamten Lebensdauer des KIS steuern.

(6) Die Systemeigner sorgen dafür, dass Drittanbieter dazu verpflichtet werden, die Kommission umgehend über jegliche IT-Sicherheitsvorfälle in Zusammenhang mit einem ausgelagerten KIS der Kommission zu informieren.

(7) Der Systemeigner hat sicherzustellen, dass das KIS, der Auslagerungsvertrag und die Sicherheitsvorkehrungen den Vorschriften der Kommission über die Informationssicherheit und die IT-Sicherheit entsprechen.

(8) Die Generaldirektion Humanressourcen und Sicherheit legt im Einklang mit dem nachstehenden Artikel 10 eine ausführliche Norm über die in den Ziffern 1 bis 7 dargelegten Zuständigkeiten und Maßnahmen fest.

KAPITEL 4

SONSTIGES UND SCHLUSSBESTIMMUNG

Artikel 9

Transparenz

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

Artikel 10

Normen

(1) Die Bestimmungen dieses Beschlusses werden, soweit erforderlich, in Normen und/oder Leitlinien, die in Einklang mit dem Beschluss (EU, Euratom) 2017/46 und dem Beschluss C(2017)7428 zu erlassen sind, im Einzelnen festgelegt. Diese Durchführungsbestimmungen und der Beschluss (EU, Euratom) 2017/46 werden in IT-Sicherheitsnormen und -Leitlinien, die sich auf spezifische Sicherheitsbereiche beziehen, gemäß ISO 27001:2013 Anhang A näher beschrieben. Diese Normen und Leitlinien beruhen auf branchenüblichen bewährten Praktiken und werden entsprechend der IT-Umgebung der Kommission ausgewählt.

(2) Erforderlichenfalls werden Normen nach ISO 27001:2013 Anhang A in den folgenden Bereichen entwickelt:

1. Organisation der Informationssicherheit;
2. Personalsicherheit;
3. Verwaltung der Werte;
4. Zugangssteuerung;
5. Kryptographie;
6. physische und umgebungsbezogene Sicherheit;
7. Betriebssicherheit;
8. Kommunikationssicherheit;
9. Anschaffung, Entwicklung und Instandhalten von Systemen;
10. Lieferantenbeziehungen;
11. Handhabung von Informationssicherheitsvorfällen;
12. Informationssicherheitsaspekte beim Business Continuity Management;
13. Compliance.

(3) Die Annahme der in den Absätzen 1 und 2 dieses Artikels genannten Normen erfordert die vorherige Zustimmung des ISSB.

(4) Die Durchführungsbestimmungen zum Beschluss C(2006) 3602, die mit dem Geltungsbereich des vorliegenden Beschlusses zusammenhängen, werden hiermit aufgehoben.

(5) Die gemäß Beschluss C(2006) 3602 vom 16. August 2006 angenommenen Normen und Leitlinien bleiben, soweit sie den vorliegenden Durchführungsbestimmungen nicht widersprechen, in Kraft, bis sie durch Normen oder Leitlinien aufgehoben oder ersetzt werden, die nach Artikel 13 des Beschlusses (EU, Euratom) 2017/46 anzunehmen sind.

Artikel 11

Inkrafttreten

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

Brüssel, den 6. April 2018

Für die Kommission,
im Namen des Präsidenten,
Günther OETTINGER
Mitglied der Kommission

ANHANG

ROLLEN UND ZUSTÄNDIGKEITEN (RASCI)

Gemäß dem RASCI-Modell erfolgt die Zuweisung von Rollen an bestimmte Stellen unter Verwendung folgender Abkürzungen:

a) R — zuständig (responsible)

b) A — verantwortlich (accountable)

c) S — unterstützend (supporting)

d) C — beratend (consulted)

e) I — informiert (informed)

Prozess \ Rolle	ISSB	HR (DS)	Kommissionsdienststellen	Systemeigner	Dateneigner	LISO	DIGIT	Auftragnehmer
Abstimmung mit dem Informationssicherheitskonzept der Kommission		**R/A**	**S**				**S**	
Verschlüsselungstechnologien		**C**	**A**	**R**	**I**	**C**		
IT-Sicherheitsüberprüfungen	**I**	**A/R**		**S**	**I**	**I**	**S**	
Zugriff aus externen Netzwerken	**C** [1]	**C**	**A**	**R**	**I**	**S**	**S**	
Auslagerung von KIS		**S/C**	**A**	**R/C** [2]	**S**	**C**		**S**

[1] Alle Kommissionsdienststellen außer der Generaldirektion Informatik konsultieren in Zusammenhang mit dem Betrieb interner Netzwerke den ISSB.

[2] Die Zuständigkeit liegt beim Systemeigner eines ausgelagerten KIS, während dem Systemeigner jedes anderen KIS, das mit einem ausgelagerten KIS verbunden wird, die beratende Rolle zukommt.