Dieser Text dient lediglich zu Informationszwecken und hat keine Rechtswirkung. Die EU-Organe übernehmen keine Haftung für seinen Inhalt. Verbindliche Fassungen der betreffenden Rechtsakte einschließlich ihrer Präambeln sind nur die im Amtsblatt der Europäischen Union veröffentlichten und auf EUR-Lex verfügbaren Texte. Diese amtlichen Texte sind über die Links in diesem Dokument unmittelbar zugänglich

►**B**

BESCHLUSS (EU, Euratom) 2017/46 DER KOMMISSION

vom 10. Januar 2017

über die Sicherheit von Kommunikations- und Informationssystemen in der Europäischen Kommission

(ABl. L 6 vom 11.1.2017, S. 40)

Berichtigt durch:

►**C1** Berichtigung, ABl. L 261 vom 11.10.2017, S. 31 (2017/46)

▼B

BESCHLUSS (EU, Euratom) 2017/46 DER KOMMISSION

vom 10. Januar 2017

über die Sicherheit von Kommunikations- und Informationssystemen in der Europäischen Kommission

KAPITEL 1

ALLGEMEINE BESTIMMUNGEN

Artikel 1

Gegenstand und Geltungsbereich

(1) Dieser Beschluss gilt für alle Kommunikations- und Informationssysteme (KIS), die Eigentum der Kommission sind bzw. von ihr oder in ihrem Namen beschafft, verwaltet oder betrieben werden, sowie für alle Arten der Nutzung dieser KIS durch die Kommission.

(2) In diesem Beschluss werden die Grundsätze und Ziele, die Organisation und die Zuständigkeiten in Bezug auf die Sicherheit dieser KIS festgelegt, insbesondere für die Kommissionsdienststellen, die KIS als Eigentum besitzen oder KIS beschaffen, verwalten oder betreiben, einschließlich der von einem internen IT-Dienstleister bereitgestellten KIS. Wird ein KIS auf der Grundlage einer bilateralen Vereinbarung oder eines Vertrags mit der Kommission von externer Seite bereitgestellt, verwaltet oder betrieben oder ist es auf dieser Grundlage deren Eigentum, müssen die Bestimmungen der Vereinbarung oder des Vertrags mit diesem Beschluss vereinbar sein.

(3) Dieser Beschluss gilt für alle Kommissionsdienststellen und Exekutivagenturen. Wird ein KIS der Kommission von anderen Einrichtungen oder Organen auf der Grundlage einer bilateralen Vereinbarung mit der Kommission genutzt, müssen die Bestimmungen der Vereinbarung mit diesem Beschluss vereinbar sein.

(4) Ungeachtet besonderer Anweisungen für bestimmte Gruppen von Mitarbeitern gilt dieser Beschluss für die Mitglieder der Kommission, für die unter das Statut der Beamten der Europäischen Union („Statut“) und die Beschäftigungsbedingungen für die sonstigen Bediensteten der Union („BBSB“) ([1]) fallenden Kommissionsbediensteten, für die zur Kommission abgeordneten nationalen Sachverständigen („ANS“) ([2]), für externe Dienstleister und deren Mitarbeiter, Praktikanten und sonstige Personen, die Zugang zu den von diesem Beschluss erfassten KIS haben.

([1]) Festgelegt durch die Verordnung (EWG, Euratom, EGKS) Nr. 259/68 des Rates vom 29. Februar 1968 zur Festlegung des Statuts der Beamten der Europäischen Gemeinschaften und der Beschäftigungsbedingungen für die sonstigen Bediensteten dieser Gemeinschaften sowie zur Einführung von Sondermaßnahmen, die vorübergehend auf die Beamten der Kommission anwendbar sind (Beschäftigungsbedingungen für die sonstigen Bediensteten) (ABl. L 56 vom 4.3.1968, S. 1).

([2]) Beschluss der Kommission vom 12. November 2008 über die Regelung für zur Kommission abgeordnete oder sich zu Zwecken der beruflichen Weiterbildung bei der Kommission aufhaltende nationale Sachverständige (K(2008) 6866 endg.).

▼B

(5) Dieser Beschluss findet auf das Europäische Amt für Betrugsbekämpfung (OLAF) Anwendung, soweit dies mit dem Unionsrecht und mit dem Beschluss 1999/352/EG, EGKS, Euratom der Kommission ([1]) vereinbar ist. Insbesondere dürfen im vorliegenden Beschluss vorgesehene Maßnahmen, darunter Überprüfungen, Untersuchungen und ähnliche Maßnahmen, nicht auf das KIS des Amtes angewandt werden, wenn dies mit der Unabhängigkeit der Untersuchungstätigkeit des Amtes oder der Vertraulichkeit der von ihm in Ausübung dieser Tätigkeit erlangten Informationen unvereinbar wäre.

Artikel 2

Begriffsbestimmungen

Für die Zwecke dieses Beschlusses gelten die folgenden Begriffsbestimmungen:

1. „Verantwortlich“ bedeutet rechenschaftspflichtig für Handlungen, Entscheidungen und Leistungen;

2. „CERT-EU“ ist das IT-Notfallteam für die Organe, Einrichtungen und sonstigen Stellen der EU. Es hat die Aufgabe, die Organe und Einrichtungen der EU beim Selbstschutz vor beabsichtigten und böswilligen Angriffen, welche die Integrität ihrer IT-Anlagen beeinträchtigen und den Interessen der EU schaden würden, zu unterstützen. Die Tätigkeitsbereiche des CERT-EU umfassen die Prävention, Erkennung, Reaktion und Wiederherstellung;

3. „Kommissionsdienststelle“ ist eine Generaldirektion oder Dienststelle der Kommission oder ein Kabinett eines Mitglieds der Kommission;

4. „Sicherheitsstelle der Kommission“ bezieht sich auf die im Beschluss (EU, Euratom) 2015/444 festgelegte Funktion;

5. „Kommunikations- und Informationssystem (KIS)“ ist ein System, mit dem Informationen elektronisch verarbeitet werden können; dazu gehören alle für den Betrieb erforderlichen Anlagen sowie Infrastrukturen, Organisation, Personal und Informationsressourcen. Diese Begriffsbestimmung erfasst Geschäftsanwendungen, gemeinsam genutzte IT-Dienste, an Dritte ausgelagerte Systeme und Endnutzergeräte;

6. „Managementkontrollgremium“ (*Corporate Management Board*, CMB) führt die oberste Aufsicht über das Gesamtmanagement betrieblicher und verwaltungstechnischer Fragen in der Kommission;

7. „Dateneigner“ ist die Person, die für den Schutz und die Verwendung eines bestimmten Datensatzes, der von einem KIS verarbeitet wird, zuständig ist;

8. „Datensatz“ ist ein Informationsbestand, der einem bestimmten Geschäftsprozess oder einer bestimmten Tätigkeit der Kommission dient;

9. „Notverfahren“ ist eine vorbestimmte Reihe von Methoden und Zuständigkeiten für die Reaktion auf Notsituationen zur Verhinderung großer Auswirkungen auf die Kommission;

([1]) Beschluss 1999/352/EG, EGKS, Euratom der Kommission vom 28. April 1999 zur Errichtung des Europäischen Amtes für Betrugsbekämpfung (OLAF) (ABl. L 136 vom 31.5.1999, S. 20).

▼B

10. „Informationssicherheitskonzept“ ist eine Reihe von Informationssicherheitszielen, die festgelegt, umgesetzt und kontrolliert werden (müssen). Es umfasst u. a. die Beschlüsse (EU, Euratom) 2015/444 und (EU, Euratom) 2015/443;

11. „Lenkungsausschuss für Informationssicherheit“ (ISSB) ist das Leitungsgremium, welches das Managementkontrollgremium bei der Wahrnehmung seiner Aufgaben in Bezug auf die IT-Sicherheit unterstützt;

12. „interner IT-Dienstleister“ ist eine Kommissionsdienststelle, die gemeinsam genutzte IT-Dienste bereitstellt;

13. „IT-Sicherheit“ oder „KIS-Sicherheit“ ist die Wahrung der Vertraulichkeit, Integrität und Verfügbarkeit von Kommunikations- und Informationssystemen und der von ihnen verarbeiteten Datensätze;

14. „IT-Sicherheitsleitlinien“ sind empfohlene, aber freiwillige Maßnahmen, die helfen, IT-Sicherheitsnormen zu unterstützen, oder bei Fehlen anwendbarer Normen als Bezugspunkt dienen;

15. „IT-Sicherheitsvorfall“ ist ein Vorkommnis, das die Vertraulichkeit, Integrität oder Verfügbarkeit eines KIS beeinträchtigen könnte;

16. „IT-Sicherheitsmaßnahme“ ist eine technische oder organisatorische Maßnahme zur Minderung von IT-Sicherheitsrisiken;

17. „IT-Sicherheitsbedarf“ ist eine genaue und eindeutige Festlegung des Vertraulichkeits-, Integritäts- und Verfügbarkeitsgrads einer Information oder eines Informations- oder IT-Systems, um das erforderliche Schutzniveau zu bestimmen;

18. „IT-Sicherheitsziel“ ist eine Absichtserklärung zur Abwehr bestimmter Bedrohungen und/oder zur Einhaltung bestimmter organisatorischer Sicherheitsanforderungen oder -annahmen;

19. „IT-Sicherheitsplan“ ist die Dokumentation der IT-Sicherheitsmaßnahmen, die erforderlich sind, um den IT-Sicherheitsbedarf eines KIS zu decken;

20. „IT-Sicherheitskonzept“ ist eine Reihe von IT-Sicherheitszielen, die festgelegt, umgesetzt und kontrolliert werden (müssen). Es umfasst diesen Beschluss und seine Durchführungsbestimmungen;

21. „IT-Sicherheitsanforderung“ ist ein in einem vorher festgelegten Prozess formulierter IT-Sicherheitsbedarf;

22. „IT-Sicherheitsrisiko“ ist eine Folge, die sich durch die Ausnutzung einer Schwachstelle aus einer IT-Sicherheitsbedrohung auf ein KIS ergeben kann. Ein IT-Sicherheitsrisiko ist durch zwei Faktoren gekennzeichnet: 1) Ungewissheit, d. h. die Wahrscheinlichkeit, dass eine IT-Sicherheitsbedrohung ein unerwünschtes Vorkommnis verursacht, und 2) die Auswirkung, d. h. die möglichen Konsequenzen eines solchen unerwünschten Vorkommnisses auf ein KIS;

▼B

23. „IT-Sicherheitsnormen“ sind bestimmte verbindliche IT-Sicherheitsmaßnahmen, die helfen, das IT-Sicherheitskonzept durchzusetzen und zu unterstützen;

24. „IT-Sicherheitsstrategie“ ist eine Reihe von Projekten und Tätigkeiten, die dazu beitragen sollen, die Ziele der Kommission zu erfüllen, und die festgelegt, umgesetzt und kontrolliert werden müssen;

25. „IT-Sicherheitsbedrohung“ ist ein Faktor, der potenziell zu einem unerwünschten Vorkommnis führen kann, durch das ein Schaden an einem KIS entsteht. Solche Bedrohungen können unbeabsichtigt oder beabsichtigt sein und unterscheiden sich nach Bedrohungselementen, potenziellen Zielen und Angriffsmethoden;

26. „Lokaler IT-Sicherheitsbeauftragter (LISO)“ ist die in einer Kommissionsdienststelle für die Zusammenarbeit in IT-Sicherheitsfragen zuständige Person;

27. die Begriffe „personenbezogene Daten“, „Verarbeitung personenbezogener Daten“, „für die Verarbeitung Verantwortlicher“ und „Datei mit personenbezogenen Daten“ haben dieselbe Bedeutung wie in der Verordnung (EG) Nr. 45/2001, insbesondere in deren Artikel 2;

28. „Informationsverarbeitung“ sind alle Funktionen eines KIS in Bezug auf Datensätze, beispielsweise das Erstellen, Ändern, Anzeigen, Speichern, Übertragen und Archivieren von Informationen. Die Verarbeitung von Informationen kann von einem KIS als Funktionsangebot für die Nutzer oder als IT-Dienste für andere KIS durchgeführt werden;

29. „Berufsgeheimnis“ ist der Schutz von Geschäftsdaten und -informationen, die ihrem Wesen nach unter das Berufsgeheimnis fallen, insbesondere von Informationen über Unternehmen, ihre Geschäftsbeziehungen und ihre Kostenelemente gemäß Artikel 339 AEUV;

30. „zuständig“ bedeutet verpflichtet zu sein, zu handeln und Entscheidungen zu treffen, um verlangte Ergebnisse zu erzielen;

31. „Sicherheit in der Kommission“ ist die Sicherheit von Personen, Vermögenswerten und Informationen in der Kommission, insbesondere die physische Unversehrtheit von Personen und Vermögenswerten, die Integrität, Vertraulichkeit und Verfügbarkeit von Informationen und Kommunikations- und Informationssystemen sowie die ungehinderte Arbeitsfähigkeit der Kommission;

32. „gemeinsam genutzter IT-Dienst“ ist ein Dienst, den ein KIS für andere KIS für die Informationsverarbeitung bereitstellt;

33. „Systemeigner“ ist die Person, die insgesamt für Beschaffung, Entwicklung, Integration, Änderung, Betrieb, Wartung und Ablösung eines KIS zuständig ist;

34. „Nutzer“ ist jede Person, die von einem KIS bereitgestellte Funktionen innerhalb oder außerhalb der Kommission benutzt.

Artikel 3

Grundsätze für die IT-Sicherheit in der Kommission

(1) Die IT-Sicherheit in der Kommission beruht auf den Grundsätzen der Legalität, Transparenz, Verhältnismäßigkeit und Verantwortlichkeit.

▼B

(2) Fragen der IT-Sicherheit werden bei der Entwicklung und Umsetzung der Kommunikations- und Informationssysteme der Kommission von Anfang an berücksichtigt. Dazu werden die Generaldirektion Informatik und die Generaldirektion für Humanressourcen und Sicherheit in ihren jeweiligen Zuständigkeitsbereichen eingebunden.

(3) Eine wirksame IT-Sicherheit muss Folgendes in angemessenem Umfang sicherstellen:

a) Authentizität: Es ist sichergestellt, dass die Informationen echt sind und aus gutgläubigen Quellen stammen;

b) Verfügbarkeit: Die Informationen sind auf Anfrage einer befugten Stelle verfügbar und nutzbar;

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

d) Integrität: Die Genauigkeit und die Vollständigkeit der Informationen und Vermögenswerte sind gewährleistet;

e) Beweisbarkeit: Es kann nachgewiesen werden, dass ein Vorgang oder ein Ereignis stattgefunden hat, sodass dieser Vorgang oder dieses Ereignis nicht nachträglich abgestritten werden kann;

f) Schutz personenbezogener Daten: Es bestehen angemessene Schutzvorkehrungen für personenbezogene Daten im vollen Einklang mit der Verordnung (EG) Nr. 45/2001;

g) Berufsgeheimnis: der Schutz von Informationen, die ihrem Wesen nach unter das Berufsgeheimnis fallen, insbesondere von Informationen über Unternehmen, ihre Geschäftsbeziehungen und ihre Kostenelemente gemäß Artikel 339 AEUV.

(4) Die IT-Sicherheit beruht auf einem Risikomanagementprozess. Dieser Prozess dient der Bestimmung der Höhe der IT-Sicherheitsrisiken und der Festlegung von Sicherheitsmaßnahmen zur Verringerung dieser Risiken auf eine angemessene Höhe zu verhältnismäßigen Kosten.

(5) Alle KIS müssen ermittelt, einem Systemeigner zugewiesen und in einem Bestandverzeichnis erfasst werden.

(6) Die Sicherheitsanforderungen an alle KIS richten sich nach ihrem eigenen Sicherheitsbedarf und nach dem Sicherheitsbedarf der von ihnen verarbeiteten Informationen. KIS, die Dienste für andere KIS bereitstellen, können dafür ausgelegt sein, bestimmte Sicherheitsbedarfsniveaus zu unterstützen.

(7) IT-Sicherheitspläne und IT-Sicherheitsmaßnahmen müssen in einem angemessenen Verhältnis zum Sicherheitsbedarf des KIS stehen.

▼C1

(8) Die Prozesse in Bezug auf die in den Absätzen 1 bis 7 genannten Grundsätze und Tätigkeiten werden gemäß Artikel 13 in Durchführungsbestimmungen im Einzelnen festgelegt.

▼B

KAPITEL 2

ORGANISATION UND ZUSTÄNDIGKEITEN

Artikel 4

Managementkontrollgremium

Das Managementkontrollgremium hat die allgemeine Zuständigkeit für die Leitung der gesamten IT-Sicherheit in der Kommission.

Artikel 5

Lenkungsausschuss für Informationssicherheit (ISSB)

(1) Den Vorsitz des ISSB führt der stellvertretende Generalsekretär, der für die Leitung der IT-Sicherheit in der Kommission zuständig ist. Seine Mitglieder repräsentieren Geschäfts-, Technik- und Sicherheitsinteressen der gesamten Kommissionsdienststellen und umfassen Vertreter der Generaldirektion Informatik, der Generaldirektion für Humanressourcen und Sicherheit, der Generaldirektion Haushalt und in zweijährlichem Turnus wechselnde Vertreter vier weiterer beteiligter Kommissionsdienststellen, für deren Betrieb die IT-Sicherheit von großer Bedeutung ist. Die Mitglieder gehören der höheren Führungsebene an.

(2) Der ISSB unterstützt das Managementkontrollgremium bei der Wahrnehmung seiner Aufgaben in Bezug auf die IT-Sicherheit. Der ISSB hat die operative Zuständigkeit für die Leitung der gesamten IT-Sicherheit in der Kommission.

(3) Der ISSB empfiehlt der Kommission das IT-Sicherheitskonzept der Kommission zur Annahme.

(4) Alle zwei Jahre nimmt der ISSB eine Überprüfung der Leitungsangelegenheiten und der IT-Sicherheitsfragen einschließlich ernster IT-Sicherheitsvorfälle vor und erstattet dem Managementkontrollgremium hierüber Bericht.

(5) Der ISSB überwacht und überprüft die Gesamtdurchführung dieses Beschlusses und erstattet dem Managementkontrollgremium hierüber Bericht.

(6) Auf Vorschlag der Generaldirektion Informatik überprüft, billigt und überwacht der ISSB die Umsetzung der fortlaufenden IT-Sicherheitsstrategie. Der ISSB erstattet dem Managementkontrollgremium hierüber Bericht.

(7) Der ISSB überwacht, bewertet und kontrolliert die Risikolage der Kommission in Bezug auf die Informationsverarbeitung und kann erforderlichenfalls förmliche Anforderungen für Verbesserungen festlegen.

▼C1

(8) Die Prozesse in Bezug auf die in den Absätzen 1 bis 7 genannten Zuständigkeiten und Tätigkeiten werden gemäß Artikel 13 in Durchführungsbestimmungen im Einzelnen festgelegt.

▼B

Artikel 6

Generaldirektion Humanressourcen und Sicherheit

In Bezug auf die IT-Sicherheit hat die Generaldirektion Humanressourcen und Sicherheit folgende Zuständigkeiten:

▼B

1. Sie gewährleistet die Abstimmung zwischen dem IT-Sicherheitskonzept und dem Informationssicherheitskonzept der Kommission;

2. sie stellt einen Rahmen für die Genehmigung der Anwendung von Verschlüsselungstechnik bei der Speicherung und Übermittlung von Informationen durch KIS auf;

3. sie informiert die Generaldirektion Informatik über konkrete Bedrohungen, die sich beträchtlich auf die Sicherheit von KIS und der von ihnen verarbeiteten Datensätze auswirken könnten;

4. sie führt IT-Sicherheitsüberprüfungen durch, um die Einhaltung des Sicherheitskonzepts durch die KIS der Kommission zu beurteilen, und erstattet dem ISSB über die Ergebnisse Bericht.

5. sie stellt einen Rahmen für die Genehmigung des Zugangs von externen Netzen zu den KIS der Kommission und für die dafür geltenden angemessenen Sicherheitsvorschriften auf und arbeitet in enger Zusammenarbeit mit der Generaldirektion Informatik die entsprechenden IT-Sicherheitsnormen und -leitlinien aus;

6. sie schlägt Grundsätze und Vorschriften für die Auslagerung von KIS an Dritte vor, damit eine angemessene Kontrolle der Informationssicherheit gewahrt bleibt;

▼C1

7. sie arbeitet in enger Zusammenarbeit mit der Generaldirektion Informatik entsprechende IT-Sicherheitsnormen und -leitlinien in Bezug auf die Nummern 1 bis 6 aus;

8. die Prozesse in Bezug auf die unter den Nummern 1 bis 7 genannten Zuständigkeiten und Tätigkeiten werden gemäß Artikel 13 in Durchführungsbestimmungen im Einzelnen festgelegt.

▼B

Artikel 7

Generaldirektion Informatik

In Bezug auf die allgemeine IT-Sicherheit der Kommission hat die Generaldirektion Informatik folgende Zuständigkeiten:

1. Außer in den in Artikel 6 genannten Fällen arbeitet sie IT-Sicherheitsnormen und -leitlinien in enger Zusammenarbeit mit der Generaldirektion Humanressourcen und Sicherheit aus, um die Übereinstimmung zwischen dem IT-Sicherheitskonzept und dem Informationssicherheitskonzept der Kommission zu gewährleisten, und schlägt sie dem ISSB vor;

2. sie bewertet die Methoden, Prozesse und Ergebnisse des IT-Sicherheitsrisikomanagements aller Kommissionsdienststellen und erstattet dem ISSB hierüber regelmäßig Bericht;

3. sie schlägt eine fortlaufende IT-Sicherheitsstrategie vor, die sie dem ISSB zur Überarbeitung und Annahme sowie zur weiteren Billigung durch das Managementkontrollgremium vorlegt; außerdem schlägt sie ein Programm mit der Projektplanung und den Tätigkeiten zur Umsetzung der IT-Sicherheitsstrategie vor;

4. sie überwacht die Durchführung der IT-Sicherheitsstrategie der Kommission und erstattet dem ISSB hierüber regelmäßig Bericht;

5. sie überwacht die IT-Sicherheitsrisiken und die in den KIS umgesetzten IT-Sicherheitsmaßnahmen und erstattet dem ISSB hierüber regelmäßig Bericht;

▼B

6. sie erstattet dem ISSB regelmäßig Bericht über die Gesamtdurchführung und die Einhaltung dieses Beschlusses;

7. sie fordert die Systemeigner — nach Konsultation der Generaldirektion Humanressourcen und Sicherheit — auf, bestimmte IT-Sicherheitsmaßnahmen zu ergreifen, um IT-Sicherheitsrisiken in Bezug auf die KIS der Kommission zu mindern;

8. sie sorgt dafür, dass den Systemeignern und Dateneignern ein angemessener Katalog der Generaldirektion Informatik für IT-Sicherheitsdienste zur Verfügung steht, damit sie ihre Zuständigkeiten für die IT-Sicherheit wahrnehmen sowie das IT-Sicherheitskonzept und die IT-Sicherheitsnormen einhalten können;

9. sie stellt den Systemeignern und Dateneignern eine angemessene Dokumentation zur Verfügung und konsultiert sie gegebenenfalls zu den auf deren IT-Dienste angewandten IT-Sicherheitsmaßnahmen, um die Einhaltung des IT-Sicherheitskonzepts zu erleichtern und die Systemeigner beim IT-Risikomanagement zu unterstützen;

10. sie veranstaltet regelmäßige Sitzungen des LISO-Netzes und unterstützt die LISO bei der Erfüllung ihrer Aufgaben;

11. sie legt den Schulungsbedarf fest und koordiniert die Schulungsprogramme zur IT-Sicherheit in Zusammenarbeit mit den Kommissionsdienststellen; sie übernimmt die Entwicklung, Umsetzung und Koordinierung von Sensibilisierungskampagnen zur IT-Sicherheit in enger Zusammenarbeit mit der Generaldirektion Humanressourcen und Sicherheit;

12. sie sorgt dafür, dass Systemeigner, Dateneigner und andere Beteiligte mit Zuständigkeit für die IT-Sicherheit in den Kommissionsdienststellen mit dem IT-Sicherheitskonzept vertraut gemacht werden;

13. sie informiert die Generaldirektion Humanressourcen und Sicherheit über konkrete IT-Sicherheitsbedrohungen und -vorfälle sowie Ausnahmen vom IT-Sicherheitskonzept der Kommission, die von den Systemeignern gemeldet werden und sich beträchtlich auf die Sicherheit in der Kommission auswirken könnten;

14. sie stellt der Kommission in ihrer Rolle als interner Dienstleister einen Katalog für gemeinsam genutzte IT-Dienste mit festgelegten Sicherheitsgraden bereit. Dies erfolgt durch die systematische Bewertung, das Management und die Überwachung von IT-Sicherheitsrisiken im Hinblick auf die Umsetzung von Sicherheitsmaßnahmen, mit denen der festgelegte Sicherheitsgrad erreicht wird;

▼C1

15. die Prozesse in Bezug auf die unter den Nummern 1 bis 14 genannten Zuständigkeiten und Tätigkeiten werden gemäß Artikel 13 in Durchführungsbestimmungen im Einzelnen festgelegt.

▼B

Artikel 8

Kommissionsdienststellen

In Bezug auf die IT-Sicherheit in ihren Dienststellen haben alle Leiter einer Kommissionsdienststelle folgende Pflichten:

1. Sie ernennen förmlich als Systemeigner für jedes KIS einen Beamten oder Bediensteten auf Zeit, der für die IT-Sicherheit dieses KIS zuständig ist; ferner ernennen sie förmlich für jeden in einem KIS verarbeiteten Datensatz einen Dateneigner, der derselben Verwaltungseinheit angehören sollte, die auch für die Verarbeitung der unter die Verordnung (EG) Nr. 45/2001 fallenden Datensätze zuständig ist;

2. sie benennen förmlich einen lokalen IT-Sicherheitsbeauftragten (LISO), der seine Zuständigkeiten unabhängig von Systemeignern und Dateneignern wahrnehmen kann. Ein LISO kann für eine oder mehrere Kommissionsdienststellen benannt werden;

3. sie sorgen dafür, dass angemessene IT-Sicherheitsrisikobewertungen durchgeführt und IT-Sicherheitspläne aufgestellt und umgesetzt werden;

4. sie sorgen dafür, dass der Generaldirektion Informatik regelmäßig eine Zusammenfassung der IT-Sicherheitsrisiken und -maßnahmen übermittelt wird;

5. sie sorgen mit Unterstützung der Generaldirektion Informatik dafür, dass angemessene Prozesse, Verfahren und Lösungen bestehen, um eine effiziente Erkennung, Meldung und Behebung von IT-Sicherheitsvorfällen in Bezug auf ihre KIS zu gewährleisten;

6. sie leiten bei IT-Sicherheitsnotfällen ein Notverfahren ein;

7. sie sind letztlich für die IT-Sicherheit einschließlich der Zuständigkeiten des Systemeigners und Dateneigners verantwortlich;

8. sie tragen die Risiken in Bezug auf ihre KIS und Datensätze;

9. sie lösen Streitigkeiten zwischen Dateneignern und Systemeignern und legen fortdauernde Streitigkeiten dem ISSB zur Beilegung vor;

10. sie sorgen dafür, dass IT-Sicherheitspläne und IT-Sicherheitsmaßnahmen umgesetzt werden und dass den Risiken angemessen begegnet wird;

▼C1

11. die Prozesse in Bezug auf die unter den Nummern 1 bis 10 genannten Zuständigkeiten und Tätigkeiten werden gemäß Artikel 13 in Durchführungsbestimmungen im Einzelnen festgelegt.

▼B

Artikel 9

Systemeigner

(1) Der Systemeigner ist zuständig für die IT-Sicherheit des KIS und untersteht dem Leiter der Kommissionsdienststelle.

▼B

(2) In Bezug auf die IT-Sicherheit hat der Systemeigner folgende Pflichten:

a) Er sorgt für die Einhaltung des IT-Sicherheitskonzepts durch das KIS;

b) er sorgt dafür, dass das KIS im betreffenden Bestandsverzeichnis exakt erfasst wird;

c) er bewertet die IT-Sicherheitsrisiken und bestimmt den IT-Sicherheitsbedarf für jedes KIS in Zusammenarbeit mit den Dateneignern und in Abstimmung mit der Generaldirektion Informatik;

d) er stellt einen Sicherheitsplan auf, der gegebenenfalls Einzelheiten über die bewerteten Risiken und über zusätzlich erforderliche Sicherheitsmaßnahmen enthält;

e) er setzt angemessene IT-Sicherheitsmaßnahmen um, die im Verhältnis zu den festgestellten IT-Sicherheitsrisiken stehen, und kommt den vom ISSB gebilligten Empfehlungen nach;

f) er stellt etwaige Abhängigkeiten von anderen KIS oder gemeinsam genutzten IT-Diensten fest und setzt gegebenenfalls angemessene Sicherheitsmaßnahmen um, wobei er sich auf die Sicherheitsgrade stützt, die von diesen KIS oder gemeinsam genutzten IT-Diensten vorgeschlagen werden;

g) er übernimmt das Management und die Überwachung der IT-Sicherheitsrisiken;

h) er berichtet dem Leiter der Kommissionsdienststelle regelmäßig über die IT-Sicherheitsrisikoprofile ihrer KIS und der Generaldirektion Informatik über die betreffenden Risiken, Risikomanagementtätigkeiten und ergriffenen Sicherheitsmaßnahmen;

i) er konsultiert den LISO der betreffenden Kommissionsdienststelle(n) zu Aspekten der IT-Sicherheit;

j) er gibt den Nutzern Anweisungen für die Nutzung des KIS und der zugehörigen Daten sowie im Hinblick auf die Verantwortlichkeiten der Nutzer im Zusammenhang mit dem KIS;

k) er beantragt bei der Generaldirektion Humanressourcen und Sicherheit, die als kryptografische Stelle tätig ist, Genehmigungen für KIS, die Verschlüsselungstechnik einsetzen;

l) er konsultiert vorab die Sicherheitsstelle der Kommission bezüglich jedes Systems, das EU-Verschlusssachen verarbeitet;

m) er stellt sicher, dass Sicherheitskopien aller zur Entschlüsselung benötigten Schlüssel in einem Sperrkonto gespeichert werden. Die Entschlüsselung der verschlüsselten Daten darf nur erfolgen, wenn dies im Einklang mit dem von der Generaldirektion Humanressourcen und Sicherheit festgelegten Rahmen genehmigt worden ist;

n) er befolgt alle Anweisungen der jeweiligen für die Datenverarbeitung Verantwortlichen bezüglich des Schutzes personenbezogener Daten und der Anwendung der Datenschutzvorschriften auf die Sicherheit der Verarbeitung;

o) er meldet der Generaldirektion Informatik alle Ausnahmen vom IT-Sicherheitskonzept der Kommission mit den jeweiligen Begründungen;

▼B

p) er berichtet dem Leiter der Kommissionsdienststelle über unlösbare Streitigkeiten zwischen Dateneigner und Systemeigner und benachrichtigt die jeweils Betroffenen zeitnah von IT-Sicherheitsvorfällen, soweit dies je nach der Schwere des Vorfalls gemäß Artikel 15 geboten ist;

q) bei an Dritte ausgelagerten Systemen sorgt er dafür, dass angemessene IT-Sicherheitsbestimmungen in die Auslagerungsverträge aufgenommen werden und dass IT-Sicherheitsvorfälle, die in dem ausgelagerten KIS auftreten, gemäß Artikel 15 gemeldet werden;

r) bei KIS, die gemeinsam genutzte IT-Dienste bereitstellen, sorgt er dafür, dass ein festgelegter Sicherheitsgrad zur Verfügung steht und eindeutig dokumentiert ist und dass Sicherheitsmaßnahmen für das KIS umgesetzt werden, um den festgelegten Sicherheitsgrad zu erreichen.

(3) Systemeigner können einige oder alle ihre IT-Sicherheitsaufgaben förmlich delegieren, sie bleiben aber für die IT-Sicherheit ihres KIS zuständig.

▼C1

(4) Die Prozesse in Bezug auf die in den Absätzen 1 bis 3 genannten Zuständigkeiten und Tätigkeiten werden gemäß Artikel 13 in Durchführungsbestimmungen im Einzelnen festgelegt.

▼B

Artikel 10

Dateneigner

(1) Der Dateneigner ist gegenüber dem Leiter der Kommissionsdienststelle für die IT-Sicherheit eines bestimmten Datensatzes zuständig und für die Vertraulichkeit, Integrität und Verfügbarkeit des Datensatzes verantwortlich.

(2) In Bezug auf diesen Datensatz hat der Dateneigner folgende Pflichten:

a) Er sorgt dafür, dass alle Datensätze, für die er zuständig ist, gemäß den Beschlüssen (EU, Euratom) 2015/443 und (EU, Euratom) 2015/444 angemessen eingestuft werden;

b) er definiert den Sicherheitsbedarf der Informationen und teilt ihn dem Systemeigner mit;

c) er nimmt an der Risikobewertung des KIS teil;

d) er berichtet dem Leiter der Kommissionsdienststelle über unlösbare Streitigkeiten zwischen Dateneigner und Systemeigner;

e) er meldet IT-Sicherheitsvorfälle gemäß Artikel 15.

(3) Dateneigner können einige oder alle ihre IT-Sicherheitsaufgaben förmlich delegieren, sie behalten aber ihre in diesem Artikel festgelegten Zuständigkeiten.

▼C1

(4) Die Prozesse in Bezug auf die in den Absätzen 1 bis 3 genannten Zuständigkeiten und Tätigkeiten werden gemäß Artikel 13 in Durchführungsbestimmungen im Einzelnen festgelegt.

▼B

Artikel 11

Lokale IT-Sicherheitsbeauftragte (LISO)

▼C1

(1) In Bezug auf die IT-Sicherheit hat der lokale IT-Sicherheitsbeauftragte folgende Pflichten:

a) Er ermittelt proaktiv Systemeigner, Dateneigner und andere Beteiligte mit Zuständigkeit für die IT-Sicherheit in den Kommissionsdienststellen und informiert sie über das IT-Sicherheitskonzept;

b) er arbeitet in Fragen der IT-Sicherheit in den Kommissionsdienststellen als Teil des LISO-Netzes mit der Generaldirektion Informatik zusammen;

c) er nimmt an den regelmäßigen Sitzungen des LISO-Netzes teil;

d) er behält den Überblick über den Risikomanagementprozess für die Informationssicherheit und über die Ausarbeitung und Umsetzung von Sicherheitsplänen für Informationssysteme;

e) er berät die Systemeigner, Dateneigner und Leiter der Kommissionsdienststellen in Fragen der IT-Sicherheit;

f) er arbeitet mit der Generaldirektion Informatik bei der Verbreitung der bewährten IT-Sicherheitspraxis zusammen und schlägt konkrete Sensibilisierungs- und Schulungsprogramme vor;

g) er berichtet dem Leiter der Kommissionsdienststelle(n) über die IT-Sicherheit, deckt Mängel auf und schlägt Verbesserungen vor.

(2) Die Prozesse in Bezug auf die in Absatz 1 genannten Zuständigkeiten und Tätigkeiten werden gemäß Artikel 13 in Durchführungsbestimmungen im Einzelnen festgelegt.

▼B

Artikel 12

Nutzer

(1) In Bezug auf die IT-Sicherheit haben die Nutzer folgende Pflichten:

a) Sie beachten das IT-Sicherheitskonzept und die Anweisungen des Systemeigners bezüglich der Nutzung jedes KIS;

b) sie melden IT-Sicherheitsvorfälle gemäß Artikel 15.

(2) Eine Nutzung der KIS der Kommission unter Missachtung des IT-Sicherheitskonzepts oder der Anweisungen des Systemeigners kann zur Einleitung eines Disziplinarverfahrens führen.

▼C1

(3) Die Prozesse in Bezug auf die in den Absätzen 1 und 2 genannten Zuständigkeiten und Tätigkeiten werden gemäß Artikel 13 in Durchführungsbestimmungen im Einzelnen festgelegt.

▼B

KAPITEL 3

SICHERHEITSANFORDERUNGEN UND SICHERHEITSPFLICHTEN

Artikel 13

Anwendung des Beschlusses

(1) ►C1 Der Erlass der in Artikel 6 Nummer 2 genannten Durchführungsbestimmungen und der betreffenden Normen und Leitlinien kann nach Maßgabe eines gesonderten Ermächtigungsbeschlusses der Kommission zugunsten des für Sicherheitsfragen zuständigen Kommissionsmitglieds erfolgen. ◄

(2) ►C1 Der Erlass aller anderen Durchführungsbestimmungen zu diesem Beschluss und der betreffenden IT-Normen und -Leitlinien kann nach Maßgabe eines gesonderten Ermächtigungsbeschlusses der Kommission zugunsten des für Informatik zuständigen Kommissionsmitglieds erfolgen. ◄

(3) Für den Erlass der in den Absätzen 1 und 2 genannten Durchführungsbestimmungen, Normen und Leitlinien ist die vorherige Zustimmung des ISSB erforderlich.

Artikel 14

Pflicht zur Einhaltung der Bestimmungen

(1) Die Einhaltung der Bestimmungen des IT-Sicherheitskonzepts und der IT-Sicherheitsnormen ist verbindlich vorgeschrieben.

(2) Die Nichteinhaltung des IT-Sicherheitskonzepts und der IT-Sicherheitsnormen kann Disziplinarmaßnahmen gemäß den Verträgen, dem Statut und der BBSB, vertragliche Sanktionen und/oder Gerichtsverfahren nach den nationalen Gesetzen und Vorschriften nach sich ziehen.

(3) Alle Ausnahmen vom IT-Sicherheitskonzept müssen der Generaldirektion Informatik gemeldet werden.

(4) Falls der ISSB feststellt, dass bei einem KIS der Kommission ein dauerhaftes inakzeptables Risiko besteht, muss die Generaldirektion Informatik in Zusammenarbeit mit dem Systemeigner dem ISSB Risikominderungsmaßnahmen zur Annahme vorschlagen. Diese Maßnahmen können u. a. eine verstärkte Überwachung und Berichterstattung sowie Dienstbeschränkungen und die Abschaltung vorsehen.

(5) Falls erforderlich, ordnet das ISSB die Anwendung angenommener Risikominderungsmaßnahmen an. Ferner kann das ISSB dem Generaldirektor der Generaldirektion Humanressourcen und Sicherheit die Einleitung einer Verwaltungsuntersuchung empfehlen. Die Generaldirektion Informatik erstattet dem ISSB über alle Situationen Bericht, in denen Risikominderungsmaßnahmen angeordnet werden.

▼C1

(6) Die Prozesse in Bezug auf die in den Absätzen 1 bis 5 genannten Zuständigkeiten und Tätigkeiten werden gemäß Artikel 13 in Durchführungsbestimmungen im Einzelnen festgelegt.

▼B

Artikel 15

Umgang mit IT-Sicherheitsvorfällen

(1) Die Generaldirektion Informatik ist für die Bereitstellung der hauptsächlichen operativen Reaktionsfähigkeit auf IT-Sicherheitsvorfälle in der Europäischen Kommission zuständig.

(2) Die Generaldirektion Humanressourcen und Sicherheit wirkt als Beteiligte an der Reaktion auf IT-Sicherheitsvorfälle mit und hat dabei folgende Aufgaben:

a) Sie hat ein Zugriffsrecht auf zusammengefasste Informationen über alle Vorfälle und erhält auf Anfrage Zugang zu den vollständigen Aufzeichnungen;

b) sie wirkt in Krisenmanagementgruppen für IT-Sicherheitsvorfälle und in IT-Sicherheitsnotverfahren mit;

c) sie ist für die Beziehungen zu Strafverfolgungsbehörden und Nachrichtendiensten zuständig;

d) sie führt forensische Cybersicherheitsanalysen gemäß Artikel 11 des Beschlusses (EU, Euratom) 2015/443 durch;

e) sie entscheidet über die Notwendigkeit der Einleitung einer förmlichen Untersuchung;

f) sie unterrichtet die Generaldirektion Informatik über alle IT-Sicherheitsvorfälle, aus denen sich ein Risiko für andere KIS ergeben könnte.

(3) Zwischen der Generaldirektion Informatik und der Generaldirektion Humanressourcen und Sicherheit findet eine regelmäßige Kommunikation zum Austausch von Informationen und zur Koordinierung des Umgangs mit Sicherheitsvorfällen, insbesondere IT-Sicherheitsvorfällen, die eine förmliche Untersuchung erforderlich machen, statt.

(4) Die Koordinierungsdienste, die das IT-Notfallteam für die Organe, Einrichtungen und sonstigen Stellen der EU (CERT-EU) bei Vorfällen erbringt, können in Anspruch genommen werden, um nötigenfalls das Verfahren zur Bewältigung von Vorfällen zu unterstützen und um den Wissensaustausch mit anderen Organen, Einrichtungen und sonstigen Stellen der EU, die möglicherweise betroffen sind, zu erleichtern.

(5) Systemeigner, die von einem IT-Sicherheitsvorfall betroffen sind, haben folgende Pflichten:

a) Sie benachrichtigen unverzüglich den Leiter ihrer Kommissionsdienststelle, die Generaldirektion Informatik, die Generaldirektion Humanressourcen und Sicherheit, den LISO und gegebenenfalls den Dateneigner von allen größeren IT-Sicherheitsvorfällen, insbesondere wenn dabei die Vertraulichkeit von Daten verletzt wurde;

b) sie arbeiten mit den einschlägigen Stellen der Kommission zusammen und befolgen deren Anweisungen in Bezug auf die Information über den Vorfall, die Reaktion und Abhilfemaßnahmen.

▼B

(6) Die Nutzer melden zeitnah alle tatsächlichen oder mutmaßlichen IT-Sicherheitsvorfälle beim zuständigen IT-Helpdesk.

(7) Die Dateneigner melden zeitnah alle tatsächlichen oder mutmaßlichen IT-Sicherheitsvorfälle beim zuständigen Noteinsatzteam für IT-Sicherheitsvorfälle.

(8) Die Generaldirektion Informatik ist mit Unterstützung der anderen mitwirkenden Beteiligten zuständig für den Umgang mit IT-Sicherheitsvorfällen, die im Zusammenhang mit nicht an Dritte ausgelagerten KIS der Kommission festgestellt werden.

(9) Die Generaldirektion Informatik informiert alle betroffenen Kommissionsdienststellen, den betreffenden LISO und gegebenenfalls das CERT-EU über IT-Sicherheitsvorfälle nach dem Grundsatz „Kenntnis nur, wenn nötig“.

(10) Die Generaldirektion Informatik erstattet dem ISSB regelmäßig Bericht über größere IT-Sicherheitsvorfälle, von denen die KIS der Kommission betroffen sind.

(11) Der jeweilige LISO erhält auf Anfrage Zugang zu den Aufzeichnungen über IT-Sicherheitsvorfälle in Bezug auf die KIS der betreffenden Kommissionsdienststelle.

(12) Bei einem größeren IT-Sicherheitsvorfall fungiert die Generaldirektion Informatik als Kontaktstelle für das Krisenmanagement und koordiniert die Arbeit der Krisenmanagementgruppen für IT-Sicherheitsvorfälle.

(13) Im Notfall kann der Generaldirektor der Generaldirektion Informatik die Einleitung eines IT-Sicherheitsnotverfahrens beschließen. Die Generaldirektion Informatik arbeitet Notverfahren aus, die dem ISSB zur Genehmigung vorgelegt werden müssen.

(14) Die Generaldirektion Informatik erstattet dem ISSB und den Leitern der betroffenen Kommissionsdienststellen über die Durchführung der Notverfahren Bericht.

▼C1

(15) Die Prozesse in Bezug auf die in den Absätzen 1 bis 14 genannten Zuständigkeiten und Tätigkeiten werden gemäß Artikel 13 in Durchführungsbestimmungen im Einzelnen festgelegt.

▼B

KAPITEL 4

SCHLUSSBESTIMMUNGEN

Artikel 16

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.

▼B

Artikel 17

Verhältnis zu anderen Rechtsakten

Die Bestimmungen dieses Beschlusses gelten unbeschadet des Beschlusses (EU, Euratom) 2015/443, des Beschlusses (EU, Euratom) 2015/444, der Verordnung (EG) Nr. 45/2001, der Verordnung (EG) Nr. 1049/2001 des Europäischen Parlaments und des Rates ([1]), des Beschlusses 2002/47/EG, EGKS, Euratom der Kommission ([2]), der Verordnung (EU, Euratom) Nr. 883/2013 des Europäischen Parlaments und des Rates ([3]) und des Beschlusses 1999/352/EG, EGKS, Euratom.

Artikel 18

Aufhebung und Übergangsbestimmungen

Der Beschluss C(2006) 3602 vom 16. August 2006 wird aufgehoben.

Die gemäß Artikel 10 des Beschlusses C(2006) 3602 angenommenen Durchführungsbestimmungen und IT-Sicherheitsnormen bleiben insoweit in Kraft, wie sie dem vorliegenden Beschluss nicht widersprechen, bis sie durch Durchführungsbestimmungen und Normen ersetzt werden, die gemäß Artikel 13 des vorliegenden Beschlusses angenommen werden. Bezugnahmen auf Artikel 10 des Beschlusses C(2006) 3602 gelten als Bezugnahmen auf Artikel 13 des vorliegenden Beschlusses.

Artikel 19

Inkrafttreten

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

([1]) 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).

([2]) Beschluss 2002/47/EG, EGKS, Euratom der Kommission vom 23. Januar 2002 zur Änderung ihrer Geschäftsordnung (ABl. L 21 vom 24.1.2002, S. 23).

([3]) Verordnung (EU, Euratom) Nr. 883/2013 des Europäischen Parlaments und des Rates vom 11. September 2013 über die Untersuchungen des Europäischen Amtes für Betrugsbekämpfung (OLAF) und zur Aufhebung der Verordnung (EG) Nr. 1073/1999 des Europäischen Parlaments und des Rates und der Verordnung (Euratom) Nr. 1074/1999 des Rates (ABl. L 248 vom 18.9.2013, S. 1).