BESCHLUSS (EU) 2021/2243 DER KOMMISSION

vom 15. Dezember 2021

zur Festlegung interner Vorschriften über die Unterrichtung betroffener Personen und die Beschränkung bestimmter Rechte dieser Personen im Zusammenhang mit der Verarbeitung personenbezogener Daten für die Zwecke der Sicherheit der Informations- und Kommunikationssysteme der Kommission

DIE EUROPÄISCHE KOMMISSION —

gestützt auf den Vertrag über die Arbeitsweise der Europäischen Union, insbesondere auf Artikel 249 Absatz 1,

in Erwägung nachstehender Gründe:

(1) Bei der Wahrnehmung ihrer Aufgaben ist die Kommission verpflichtet, die in Artikel 8 Absatz 1 der Charta der Grundrechte der Europäischen Union und in Artikel 16 Absatz 1 des Vertrags über die Arbeitsweise der Europäischen Union verankerten Rechte natürlicher Personen bei der Verarbeitung personenbezogener Daten zu achten. Außerdem muss sie die in der Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates ([1]) vorgesehenen Rechte wahren. Gleichzeitig muss die Kommission mit IT-Sicherheitsvorfällen gemäß den in Artikel 15 des Beschlusses (EU, Euratom) 2017/46 ([2]) festgelegten Vorschriften umgehen.

(2) Zur Gewährleistung der IT-Sicherheit, d. h. der Wahrung der Vertraulichkeit, Integrität und Verfügbarkeit der Kommunikations- und Informationssysteme und der von ihnen verarbeiteten Datensätze in Bezug auf Personen, Vermögenswerte und Informationen, hat die Kommission, insbesondere über ihre Generaldirektion Informatik, Maßnahmen ergriffen, wie sie im Beschluss (EU, Euratom) 2017/46 und im Beschluss C(2017) 8841 final ([3]) vorgesehen sind. Zu diesen Maßnahmen gehören die Beobachtung der IT-Sicherheitsrisiken und der getroffenen IT-Sicherheitsmaßnahmen, die Aufforderung an Systemeigner, spezifische IT-Sicherheitsmaßnahmen zu ergreifen, um IT-Sicherheitsrisiken für die Kommunikations- und Informationssysteme der Kommission zu mindern, und die Bewältigung von IT-Sicherheitsvorfällen.

(3) Die Generaldirektion Informatik stellt IT-Sicherheitsvorkehrungen und -dienste für die Kommission bereit und muss mehrere Kategorien personenbezogener Daten verarbeiten, um

— Meldungen und Warnungen im Zusammenhang mit IT-Sicherheitsereignissen und -vorfällen zu übermitteln,

— auf IT-Sicherheitsereignisse und -vorfälle zu reagieren und diese einzudämmen,

— Werkzeuge und Vorkehrungen bereitzustellen, und zwar mithilfe von Sicherheitsprüfungen, Sicherheitsbewertungen und Schwachstellenmanagement,

— das Bewusstsein der Kommissionsbediensteten im Bereich der Cybersicherheit zu schärfen,

— das Auftreten von IT-Sicherheitsereignissen und -vorfällen zu überwachen, aufzudecken und zu verhindern,

— privilegierte Benutzerkonten zu überprüfen.

(4) IT-Sicherheitsvorfälle, die eine Gefahr für die Sicherheit der Informations- und Kommunikationssysteme der Kommission darstellen könnten, können bei allen von der Kommission durchgeführten Verarbeitungsvorgängen auftreten. Sie können alle Kategorien personenbezogener Daten betreffen, die von der Kommission verarbeitet werden.

([1]) 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).

([2]) 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).

([3]) Beschluss C(2017) 8841 der Kommission vom 13. Dezember 2017 mit Durchführungsbestimmungen zu den Artikeln 3, 5, 7, 8, 9, 10, 11, 12, 14 und 15 des Beschlusses (EU, Euratom) 2017/46 der Kommission über die Sicherheit von Kommunikations- und Informationssystemen in der Europäischen Kommission.

(5) Unter bestimmten Umständen kann es erforderlich sein, die Rechte der betroffenen Personen gemäß der Verordnung (EU) 2018/1725 mit der Notwendigkeit in Einklang zu bringen, dass die Kommission ihre Aufgaben im Zusammenhang mit der Gewährleistung der IT-Sicherheit von Personen, Vermögenswerten und Informationen in der Kommission gemäß dem Beschluss (EU, Euratom) 2017/46 und unter uneingeschränkter Achtung der Grundrechte und Grundfreiheiten anderer betroffener Personen wirksam wahrnehmen kann. Zu diesem Zweck wird die Kommission mit Artikel 25 Absatz 1 der Verordnung (EU) 2018/1725 dazu ermächtigt, die Anwendung der Artikel 14 bis 17, 19, 20 und 35 der Verordnung und des in Artikel 4 Absatz 1 Buchstabe a der Verordnung genannten Transparenzgrundsatzes — soweit dessen Bestimmungen den in den Artikeln 14 bis 17, 19 und 20 der Verordnung vorgesehenen Rechten und Pflichten entsprechen — zu beschränken.

(6) Dieser Beschluss sollte für alle Verarbeitungsvorgänge gelten, die die Kommission als Datenverantwortliche in Wahrnehmung ihrer Aufgaben durchführt, um die Sicherheit von Personen, Vermögenswerten und Informationen in der Kommission gemäß dem Beschluss (EU, Euratom) 2017/46 zu gewährleisten. Deshalb sollte er für betroffene Personen aus den Kategorien personenbezogener Daten gehören, die von all diesen Verarbeitungsvorgängen erfasst werden, d. h. Personen, die mit Informations- und Kommunikationssystemen der Kommission interagieren.

(7) Personenbezogene Daten werden in einem gesicherten elektronischen Umfeld gespeichert, um einen unrechtmäßigen Zugriff auf Daten durch Personen außerhalb der Kommission zu verhindern. Für verschiedene Verarbeitungsvorgänge gelten je nach Art der betreffenden personenbezogenen Daten unterschiedliche Aufbewahrungsfristen. Die Aktenaufbewahrung in der Kommission wird durch die Gemeinsame Aufbewahrungsliste der Kommission (SEC(2019) 900) geregelt, einem Rechtsdokument in Form eines Aufbewahrungszeitplans, in dem die Aufbewahrungsfristen für verschiedene Arten von Kommissionsakten festgelegt sind, um die Aufbewahrung der Daten auf das erforderliche Maß zu beschränken.

(8) Die Kommission muss möglicherweise die Anwendung der Rechte betroffener Personen einschränken, um ihre innere Sicherheit gemäß Artikel 25 Absatz 1 Buchstabe d der Verordnung (EU) 2018/1725 zu gewährleisten (d. h. zur Wahrung der Vertraulichkeit, Integrität und Verfügbarkeit ihrer Kommunikations- und Informationssysteme und der von ihnen verarbeiteten Datensätze, ihrer Vermögenswerte und Informationen). Die Kommission muss dies insbesondere tun, um

— Meldungen und Warnungen im Zusammenhang mit IT-Sicherheitsereignissen und -vorfällen zu übermitteln,

— auf IT-Sicherheitsereignisse und -vorfälle zu reagieren und diese einzudämmen, Werkzeuge und Vorkehrungen bereitzustellen, und zwar mithilfe von Sicherheitsprüfungen, Sicherheitsbewertungen und Schwachstellenmanagement,

— das Bewusstsein der Kommissionsbediensteten im Bereich der Cybersicherheit zu schärfen,

— das Auftreten von IT-Sicherheitsereignissen und -vorfällen zu überwachen, aufzudecken und zu verhindern,

— privilegierte Benutzerkonten zu überprüfen.

(9) Zur Bewältigung von IT-Sicherheitsvorfällen gemäß Artikel 15 des Beschlusses (EU, Euratom) 2017/46 kann die Generaldirektion Informatik mit dem Reaktionsteam für Cyberangriffe (*Cyber Attack Response Team*) der Generaldirektion Humanressourcen und Sicherheit Informationen austauschen.

(10) Zur Einhaltung der Artikel 14, 15 und 16 der Verordnung (EU) 2018/1725 sollte die Kommission alle natürlichen Personen über die Tätigkeiten informieren, bei denen deren personenbezogenen Daten verarbeitet werden und bei denen in deren Rechte eingegriffen wird. Sie sollte dies auf transparente und kohärente Weise tun, indem sie einen Datenschutzhinweis auf der Website der Kommission veröffentlicht. Erforderlichenfalls sollte die Kommission zusätzliche Schutzvorkehrungen treffen, um alle betroffenen Personen einzeln in angemessener Form zu unterrichten.

(11) Bei der Einhaltung der Artikel 14, 15 und 16 der Verordnung (EU) 2018/1725 könnten Hinweise auf gemäß Artikel 15 des Beschlusses (EU, Euratom) 2017/46 bestehende IT-Sicherheitsmaßnahmen, Schwachstellen oder Vorfälle offengelegt werden. Eine Offenlegung solcher IT-Sicherheitsmaßnahmen, Schwachstellen und Vorfälle würde das Risiko erhöhen, dass dann die dargelegte IT-Sicherheitsmaßnahme umgangen oder die dargelegte Schwachstelle missbraucht würde sowie dass eine laufende Analyse von IT-Sicherheitsvorfällen beeinträchtigt werden könnte, weil Artefakte versehentlich oder vorsätzlich von einem Nutzer oder böswilligen Akteur manipuliert werden könnten. Die Fähigkeit der Kommission, ihre IT-Sicherheit zu gewährleisten und insbesondere IT-Sicherheitsvorfälle künftig wirksam zu bewältigen, könnte dadurch ernsthaft beeinträchtigt werden.

(12) Nach Artikel 25 Absatz 1 Buchstabe h der Verordnung (EU) 2018/1725 ist die Kommission auch befugt, die Anwendung der Rechte betroffener Personen zu beschränken, um die Rechte und Freiheiten anderer Personen im Zusammenhang mit IT-Sicherheitsvorfällen, die IT-Sicherheitsvorkehrungen beeinträchtigen könnten, zu schützen.

(13) Die Kommission muss möglicherweise auch die Unterrichtung betroffener Personen und die Anwendung anderer Rechte betroffener Personen im Zusammenhang mit personenbezogenen Daten, die sie von Drittländern oder internationalen Organisationen erhalten hat, beschränken, um ihrer Pflicht zur Zusammenarbeit mit diesen Ländern oder Organisationen nachzukommen. Dies ist Teil der Pflicht der Kommission, ein wichtiges Ziel des allgemeinen öffentlichen Interesses der Union gemäß Artikel 25 Absatz 1 Buchstabe c der Verordnung (EU) 2018/1725 zu wahren. Unter bestimmten Umständen können die Interessen oder Grundrechte der betroffenen Person jedoch Vorrang vor dem Interesse an einer internationalen Zusammenarbeit haben.

(14) Die Kommission hat daher die in Artikel 25 Absatz 1 Buchstaben c, d und h der Verordnung (EU) 2018/1725 genannten Gründe als Gründe für Beschränkungen festgelegt, die für die Datenverarbeitung durch die Generaldirektion Informatik im Zusammenhang mit deren IT-Sicherheitsvorkehrungen und -diensten erforderlich sein können.

(15) Jede auf der Grundlage dieses Beschlusses vorgenommene Beschränkung sollte notwendig und verhältnismäßig sein und die Risiken für die Rechte und Freiheiten der betroffenen Personen berücksichtigen.

(16) Die Kommission sollte alle Beschränkungen transparent anwenden und im entsprechenden Verzeichnis erfassen.

(17) Nach Artikel 25 Absatz 8 der Verordnung (EU) 2018/1725 können die für die Datenverarbeitung Verantwortlichen die Unterrichtung über die Gründe für die Anwendung einer Beschränkung auf die betroffene Person zurückstellen, unterlassen oder ablehnen, wenn diese Unterrichtung die Wirkung der Beschränkung in irgendeiner Weise beeinträchtigen würde. Dies gilt insbesondere für Beschränkungen der in den Artikeln 16 und 35 der Verordnung (EU) 2018/1725 vorgesehenen Pflichten. Die Kommission sollte die vorgenommenen Beschränkungen regelmäßig überprüfen, um sicherzustellen, dass die Rechte der betroffenen Person auf Unterrichtung nach den Artikeln 16 und 35 der Verordnung (EU) 2018/1725 nur so lange beschränkt werden, wie dies erforderlich ist, um der Kommission die Gewährleistung ihrer IT-Sicherheit und insbesondere die Bewältigung von IT-Sicherheitsvorfällen zu ermöglichen.

(18) Beschränkt die Kommission die Anwendung anderer als der in den Artikeln 16 und 35 der Verordnung (EU) 2018/1725 genannten Rechte betroffener Personen, sollte der für die Datenverarbeitung Verantwortliche im Einzelfall prüfen, ob die Bekanntgabe der Beschränkung deren Zweck beeinträchtigen würde.

(19) Der Datenschutzbeauftragte der Kommission sollte eine unabhängige Überprüfung der Anwendung von Beschränkungen vornehmen, um die Einhaltung dieses Beschlusses zu gewährleisten.

(20) Dieser Beschluss sollte am zwanzigsten Tag nach seiner Veröffentlichung im *Amtsblatt der Europäischen Union* in Kraft treten, damit die Kommission im Einklang mit Artikel 25 der Verordnung (EU) 2018/1725 die Anwendung bestimmter Rechte und Pflichten unmittelbar beschränken kann.

(21) Der Europäische Datenschutzbeauftragte hat am 16. September 2021 eine Stellungnahme abgegeben —

HAT FOLGENDEN BESCHLUSS ERLASSEN:

Artikel 1

Gegenstand und Anwendungsbereich

(1) In diesem Beschluss werden die Vorschriften festgelegt, nach denen die Kommission betroffene Personen über die Verarbeitung ihrer Daten nach den Artikeln 14, 15 und 16 der Verordnung (EU) 2018/1725 unterrichtet, wenn sie ihre Aufgaben gemäß dem Beschluss (EU, Euratom) 2017/46 wahrnimmt.

Ferner werden die Bedingungen festgelegt, unter denen die Kommission die Anwendung der Artikel 4, 14 bis 17, 19, 20 und 35 der Verordnung (EU) 2018/1725 nach deren Artikel 25 Absatz 1 Buchstaben c, d und h beschränken kann, wenn sie ihre Aufgaben gemäß dem Beschluss (EU, Euratom) 2017/46 wahrnimmt.

(2) Dieser Beschluss gilt für die Verarbeitung personenbezogener Daten durch die Kommission selbst oder in ihrem Namen für die Zwecke der Tätigkeiten, die zur Gewährleistung der Sicherheit von Personen, Vermögenswerten und Informationen in der Kommission gemäß dem Beschluss (EU, Euratom) 2017/46 oder im Zusammenhang mit diesen Tätigkeiten durchgeführt werden.

Artikel 2

Ausnahmen und Beschränkungen

(1) Die Kommission prüft bei der Erfüllung ihrer Pflichten in Bezug auf die Rechte der betroffenen Personen nach der Verordnung (EU) 2018/1725, ob eine der in der genannten Verordnung festgelegten Ausnahmen Anwendung findet.

(2) Vorbehaltlich der Artikel 3 bis 7 dieses Beschlusses, wenn die Ausübung der in den Artikeln 14 bis 17, 19, 20 und 35 der Verordnung (EU) 2018/1725 vorgesehenen Rechte und Pflichten in Bezug auf von der Kommission verarbeitete personenbezogene Daten den Zweck der IT-Sicherheitsvorkehrungen und -dienste beeinträchtigen würde, unter anderem weil Ermittlungsinstrumente, Schwachstellen und Methoden der Kommission offengelegt oder die Rechte und Freiheiten sowie die Sicherheit anderer betroffener Personen beeinträchtigt würden, insbesondere bei der Verarbeitung personenbezogener Daten, um

— Meldungen und Warnungen im Zusammenhang mit IT-Sicherheitsereignissen und -vorfällen zu übermitteln,

— auf IT-Sicherheitsereignisse und -vorfälle zu reagieren und diese einzudämmen,

— Werkzeuge und Vorkehrungen bereitzustellen, und zwar mithilfe von Sicherheitsprüfungen, Sicherheitsbewertungen und Schwachstellenmanagement,

— das Bewusstsein der Kommissionsbediensteten im Bereich der Cybersicherheit zu schärfen,

— das Auftreten von IT-Sicherheitsereignissen und -vorfällen zu überwachen, aufzudecken und zu verhindern,

— privilegierte Benutzerkonten zu überprüfen,

kann die Kommission die Anwendung folgender Bestimmungen beschränken:

a) Artikel 14 bis 17, 19, 20 und 35 der Verordnung (EU) 2018/1725,

b) des Transparenzgrundsatzes nach Artikel 4 Absatz 1 Buchstabe a der Verordnung (EU) 2018/1725, soweit dessen Bestimmungen den in den Artikeln 14 bis 17, 19 und 20 der Verordnung (EU) 2018/1725 festgelegten Rechten und Pflichten entsprechen.

Die Kommission kann dies im Einklang mit Artikel 25 Absatz 1 Buchstaben c, d und h der Verordnung (EU) 2018/1725 tun.

(3) Vorbehaltlich der Artikel 3 bis 7 kann die Kommission die in Absatz 2 dieses Artikels genannten Rechte und Pflichten einschränken,

a) wenn die Wahrnehmung dieser Rechte und Pflichten im Zusammenhang mit von anderen Organen, Einrichtungen und sonstigen Stellen der Union erhaltenen personenbezogenen Daten auf der Grundlage der in Artikel 25 der Verordnung (EU) 2018/1725 genannten Rechtsakte oder nach Kapitel IX der genannten Verordnung durch diese anderen Organe, Einrichtungen und sonstigen Stellen der Union gemäß der Verordnung (EU) 2016/794 des Europäischen Parlaments und des Rates ([4]) oder der Verordnung (EU) 2017/1939 des Rates ([5]) beschränkt werden könnte,

b) wenn die Wahrnehmung dieser Rechte und Pflichten im Zusammenhang mit von einer zuständigen Behörde eines Mitgliedstaats erhaltenen personenbezogenen Daten durch die zuständigen Behörden dieses Mitgliedstaats auf der Grundlage der in Artikel 23 der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates ([6]) genannten Rechtsakte oder im Rahmen nationaler Maßnahmen zur Umsetzung des Artikels 13 Absatz 3, des Artikels 15 Absatz 3 oder des Artikels 16 Absatz 3 der Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates ([7]) beschränkt werden könnte,

([4]) Verordnung (EU) 2016/794 des Europäischen Parlaments und des Rates vom 11. Mai 2016 über die Agentur der Europäischen Union für die Zusammenarbeit auf dem Gebiet der Strafverfolgung (Europol) und zur Ersetzung und Aufhebung der Beschlüsse 2009/371/JI, 2009/934/JI, 2009/935/JI, 2009/936/JI und 2009/968/JI des Rates (ABl. L 135 vom 24.5.2016, S. 53).

([5]) Verordnung (EU) 2017/1939 des Rates vom 12. Oktober 2017 zur Durchführung einer Verstärkten Zusammenarbeit zur Errichtung der Europäischen Staatsanwaltschaft (EUStA) (ABl. L 283 vom 31.10.2017, S. 1).

([6]) Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. L 119 vom 4.5.2016, S. 1).

([7]) Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates (ABl. L 119 vom 4.5.2016, S. 89).

c) wenn durch die Wahrnehmung dieser Rechte und Pflichten die Zusammenarbeit der Kommission mit Drittländern oder internationalen Organisationen in Bezug auf gemeinsame Sicherheitsbedrohungen beeinträchtigt würde.

Bevor die Kommission in den in Unterabsatz 1 Buchstaben a und b genannten Fällen Beschränkungen anwendet, konsultiert sie die betreffenden Organe, Einrichtungen und sonstigen Stellen der Union oder die zuständigen Behörden der Mitgliedstaaten zu den möglichen Gründen für die Anwendung von Beschränkungen und zur Notwendigkeit und Verhältnismäßigkeit der betreffenden Beschränkungen, es sei denn, dadurch würden die Tätigkeiten der Kommission beeinträchtigt, und es sei denn, der Kommission ist klar, dass die Anwendung einer Beschränkung in einem der unter diesen Buchstaben genannten Rechtsakte vorgesehen ist oder dass eine derartige Konsultation den Zweck ihrer Tätigkeiten gemäß dem Beschluss (EU, Euratom) 2017/46 beeinträchtigen würde.

Unterabsatz 1 Buchstabe c findet keine Anwendung, wenn die Interessen oder die Grundrechte und Grundfreiheiten der betroffenen Person Vorrang vor den Interessen der Kommission an einer Zusammenarbeit mit Drittländern oder internationalen Organisationen haben.

(4) Die Absätze 1, 2 und 3 gelten unbeschadet der Anwendung anderer Beschlüsse der Kommission zur Festlegung interner Vorschriften über die Unterrichtung betroffener Personen und über die Beschränkung bestimmter Rechte gemäß Artikel 25 der Verordnung (EU) 2018/1725.

(5) Jede Beschränkung der in Absatz 2 genannten Rechte und Pflichten muss notwendig und hinsichtlich der Risiken für die Rechte und Freiheiten der betroffenen Personen verhältnismäßig sein.

(6) Vor der Anwendung von Beschränkungen wird die Notwendigkeit und Verhältnismäßigkeit im Einzelfall geprüft, und Beschränkungen werden auf das zur Erreichung des beabsichtigten Zwecks unbedingt erforderliche Maß begrenzt.

Artikel 3

Unterrichtung der betroffenen Personen

(1) Die Kommission veröffentlicht für alle betroffenen Personen auf ihrer Website einen Datenschutzhinweis mit Informationen über ihre Tätigkeiten, für die sie zur Erfüllung ihrer Aufgaben gemäß dem Beschluss (EU, Euratom) 2017/46 personenbezogene Daten dieser Personen verarbeitet, und mit einer Beschreibung der betroffenen Kategorien personenbezogener Daten. Die Kommission stellt sicher, dass die betroffenen Personen einzeln in angemessener Form unterrichtet werden, sofern dies möglich ist, ohne die IT-Sicherheit zu beeinträchtigen.

(2) Wenn die Kommission die Unterrichtung betroffener Personen, deren personenbezogene Daten sie zur Erfüllung ihrer Aufgaben gemäß dem Beschluss (EU, Euratom) 2017/46 verarbeitet, ganz oder teilweise beschränkt, so erfasst und registriert sie die Gründe für die Beschränkung nach Artikel 6 dieses Beschlusses.

Artikel 4

Auskunftsrecht der betroffenen Person, Recht auf Löschung und Recht auf Einschränkung der Verarbeitung

(1) Wenn die Kommission das Recht der betroffenen Person auf Zugang zu personenbezogenen Daten oder ihr Recht auf Löschung oder ihr Recht auf Einschränkung der Verarbeitung nach den Artikeln 17, 19 und 20 der Verordnung (EU) 2018/1725 ganz oder teilweise beschränkt, so unterrichtet sie die betroffene Person in ihrer Antwort auf den Antrag auf Auskunft, Löschung oder Einschränkung der Datenverarbeitung

a) über die angewandte Beschränkung und die Hauptgründe hierfür,

b) darüber, wie eine Beschwerde beim Europäischen Datenschutzbeauftragten eingereicht oder ein Rechtsbehelf beim Gerichtshof der Europäischen Union eingelegt werden kann.

(2) Die Kommission kann die Unterrichtung über die Gründe für die Beschränkung nach Absatz 1 so lange zurückstellen, unterlassen oder ablehnen, wie die Unterrichtung den Zweck der angewandten Beschränkung beeinträchtigen würde.

(3) Die Kommission erfasst und registriert die Gründe für die Beschränkung nach Artikel 6.

(4) Wenn das Auskunftsrecht ganz oder teilweise beschränkt ist, kann sich die betroffene Person zur Ausübung ihres Auskunftsrechts nach Artikel 25 Absätze 6, 7 und 8 der Verordnung (EU) 2018/1725 an den Europäischen Datenschutzbeauftragten wenden.

Artikel 5

Benachrichtigung der betroffenen Personen von einer Verletzung des Schutzes ihrer personenbezogenen Daten

Wenn die Kommission die Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person nach Artikel 35 der Verordnung (EU) 2018/1725 beschränkt, so erfasst und registriert sie die Gründe für die Beschränkung nach Artikel 6 dieses Beschlusses. Die Kommission übermittelt dem Europäischen Datenschutzbeauftragten diesen Vorgang zum Zeitpunkt der Meldung der Verletzung des Schutzes personenbezogener Daten.

Artikel 6

Erfassung und Registrierung von Beschränkungen

(1) Die Kommission erfasst die Gründe für nach diesem Beschluss angewandte Beschränkungen mit Angabe der Rechtsgründe für die Beschränkung und einer Bewertung der Notwendigkeit und Verhältnismäßigkeit der Beschränkung unter Berücksichtigung aller relevanten Elemente nach Artikel 25 Absatz 2 der Verordnung (EU) 2018/1725.

(2) Es ist zu erfassen, wie die Ausübung eines Rechts durch die betroffene Person den Zweck der gemäß dem Beschluss (EU, Euratom) 2017/46 in der Kommission getroffenen IT-Sicherheitsvorkehrungen und -dienste oder der nach Artikel 2 Absatz 2 oder 3 dieses Beschlusses angewandten Beschränkungen gefährden oder die Rechte und Freiheiten anderer betroffener Personen beeinträchtigen würde.

(3) Die Kommission registriert diese Aufzeichnungen und etwaige Unterlagen, aus denen die zugrunde liegenden tatsächlichen und rechtlichen Umstände hervorgehen. Diese werden dem Europäischen Datenschutzbeauftragten auf Anfrage zur Verfügung gestellt.

Artikel 7

Dauer der Beschränkungen

(1) Die in den Artikeln 3, 4 und 5 genannten Beschränkungen gelten, solange die Gründe vorliegen, die diese Beschränkungen rechtfertigen.

(2) Wenn die in den Artikeln 3, 4 und 5 genannten Gründe nicht mehr vorliegen, muss die Kommission

a) die Beschränkung aufheben,

b) die betroffene Person über die Hauptgründe für die Beschränkung unterrichten,

c) der betroffenen Person mitteilen, wie sie jederzeit eine Beschwerde beim Europäischen Datenschutzbeauftragten einreichen oder einen Rechtsbehelf beim Gerichtshof der Europäischen Union einlegen kann.

Artikel 8

Schutzvorkehrungen und Aufbewahrungsfristen

(1) Die Kommission überprüft die Anwendung der in den Artikeln 3, 4 und 5 genannten Beschränkungen sechs Monate nach ihrer Festlegung und bei Beendigung der IT-Sicherheitsvorkehrung. Danach prüft und überwacht die Kommission alljährlich, inwieweit es erforderlich ist, eine Beschränkung aufrechtzuerhalten.

Diese Überprüfung schließt eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der Beschränkung unter Berücksichtigung aller relevanten Elemente nach Artikel 25 Absatz 2 der Verordnung (EU) 2018/1725 ein.

(2) Um zu verhindern, dass personenbezogene Daten, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden, unbeabsichtigt oder unrechtmäßig vernichtet werden, verloren gehen oder verändert werden, diese Daten unbefugt offengelegt werden oder unbefugt darauf zugegriffen wird, hat die Kommission hat technische und organisatorische Maßnahmen ergriffen wie die Verwaltung von Zugangsrechten, Regeln für die Datensicherung und andere Maßnahmen im Einklang mit dem Beschluss (EU, Euratom) 2017/46.

(3) Die Kommission erfasst die nach der Gemeinsamen Aufbewahrungsliste der Kommission geltenden Aufbewahrungsfristen und gibt den betroffenen Personen die betreffenden Aufbewahrungsfristen für diese Verarbeitungstätigkeiten in ihrem Datenschutzhinweis bekannt.

Artikel 9

Überprüfung durch den Datenschutzbeauftragten der Kommission

(1) Der Datenschutzbeauftragte der Kommission wird unverzüglich unterrichtet, wenn die Rechte der betroffenen Personen nach diesem Beschluss beschränkt werden. Auf Anfrage erhält der Datenschutzbeauftragte Zugang zu den erfassten Angaben und sonstigen Unterlagen, aus denen die zugrunde liegenden tatsächlichen und rechtlichen Umstände hervorgehen.

(2) Der Datenschutzbeauftragte kann eine Überprüfung der Beschränkungen verlangen und wird über das Ergebnis der Überprüfung unterrichtet.

(3) Die Kommission dokumentiert die Einbeziehung des Datenschutzbeauftragten, wenn die Rechte der betroffenen Personen nach diesem Beschluss beschränkt werden.

Artikel 10

Inkrafttreten

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

Brüssel, den 15. Dezember 2021

Für die Kommission
Die Präsidentin
Ursula VON DER LEYEN