E-Government-Recht für die Bundesverwaltung

herausgegeben von

Prof. Dr. Lorenz Franck

Hochschule des Bundes für öffentliche Verwaltung, Brühl

Textausgaben Informationsrecht | Band II

2025

Vorwort

Die vielzitierte sog. Speyerer Definition des E-Government umfaßt „die Abwicklung geschäftlicher Prozesse im Zusammenhang mit Regieren und Verwalten (Government) mit Hilfe von Informations- und Kommunikationstechniken über elektronische Medien."

Und dann eine *gedruckte* Gesetzessammlung zum E-Government – Ist das ein Stück Realsatire?

Zunächst ist festzuhalten, daß es inzwischen einen stattlichen Bestand an einschlägigen Rechtsnormen gibt, die eine solche Textsammlung rechtfertigen. Zugleich soll den Studierenden die Möglichkeit eröffnet werden, den Gesetzestext als zulässiges Hilfsmittel in schriftlichen und mündlichen Prüfungen zu verwenden. Dies ist (leider) nach dem derzeitigen Stand der Verwaltungsdigitalisierung in den meisten Fällen noch immer lediglich papiergebunden möglich. Elektronische Prüfungsformen unter Zuhilfenahme elektronischer Hilfsmittel sind noch nicht flächendeckend etabliert. Das E-Government-Recht wird also zunächst in Papierform in die Aus- und Fortbildung hineingetragen.

Die erste Schwierigkeit bei der Zusammenstellung einer Gesetzessammlung stellt naturgemäß die Auswahl der Texte dar. Das E-Goverment-Recht als vielschichtige Querschnittsmaterie fußt dabei auf mehreren thematischen Säulen. Im hiesigen Band sind zunächst die einschlägigen Vorschriften

zur **Digitalen Verwaltung**, also dem zum E-Government im engeren Sinne,

zu elektronischen **Identitäten** und

zum Bereich **Open Data** zusammengefaßt.

Die großen Themenfelder Datenschutz und Cybersicherheit, auf die das E-Government-Recht regelmäßig verweist und welche für eine rechtskonforme Verwaltungsdigitalisierung schlechthin unverzichtbar sind, stellen demgegenüber eigenständige Vorschriftensammlungen dar.

Brühl im Mai 2025

Lorenz Franck

Inhaltsverzeichnis

Digitale Verwaltung

Identitäten

Open Data

Gesetz zur Förderung der elektronischen Verwaltung (E-Government-Gesetz - EGovG)

Inhaltsübersicht

§ 1 Geltungsbereich

(1) Dieses Gesetz gilt für die öffentlich-rechtliche Verwaltungstätigkeit der Behörden des Bundes einschließlich der bundesunmittelbaren Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts.

(2) Dieses Gesetz mit Ausnahme der §§ 2a, 9a bis 9c gilt auch für die öffentlich-rechtliche Verwaltungstätigkeit der Behörden der Länder, der Gemeinden und Gemeindeverbände und der sonstigen der Aufsicht des Landes unterstehenden juristischen Personen des öffentlichen Rechts, wenn sie Bundesrecht ausführen.

(3) Für die Tätigkeit der Gerichtsverwaltungen und der Behörden der Justizverwaltung einschließlich der ihrer Aufsicht unterliegenden Körperschaften des öffentlichen Rechts gilt dieses Gesetz nur, soweit die Tätigkeit der Nachprüfung durch die Gerichte der Verwaltungsgerichtsbarkeit oder der Nachprüfung durch die in verwaltungsrechtlichen Anwalts-, Patentanwalts- und Notarsachen zuständigen Gerichte unterliegt.

(4) Dieses Gesetz gilt, soweit nicht Rechtsvorschriften des Bundes inhaltsgleiche oder entgegenstehende Bestimmungen enthalten.

(5) Dieses Gesetz gilt nicht für

1. die Strafverfolgung, die Verfolgung und Ahndung von Ordnungswidrigkeiten, die Rechtshilfe für das Ausland in Straf- und Zivilsachen, die Steuer- und Zollfahndung (§ 208 der Abgabenordnung) und für Maßnahmen des Richterdienstrechts,
2. Verfahren vor dem Deutschen Patent- und Markenamt und den bei diesem errichteten Schiedsstellen,
3. die Verwaltungstätigkeit nach dem Zweiten Buch Sozialgesetzbuch

§ 2 Elektronischer Zugang zur Verwaltung

(1) Jede Behörde ist verpflichtet, auch einen Zugang für die Übermittlung elektronischer Dokumente, auch soweit sie mit einer qualifizierten elektronischen Signatur oder einem qualifizierten elektronischen Siegel versehen sind, zu eröffnen.

(2) Jede Behörde des Bundes ist verpflichtet, in Verwaltungsverfahren, in denen sie die Identität einer Person auf Grund einer Rechtsvorschrift festzustellen hat oder aus anderen Gründen eine Identifizierung für notwendig erachtet, einen elektronischen Identitätsnachweis nach § 18 des Personalausweisgesetzes, nach § 12 des eID-Karte-Gesetzes oder nach § 78 Absatz 5 des Aufenthaltsgesetzes anzubieten. Mit der Anbindung an das Bürgerkonto nach § 3 Absatz 1 des Onlinezugangsgesetzes wird diese Verpflichtung erfüllt.

§ 2a Siegeldienst; Verordnungsermächtigung

(1) Das Bundesministerium des Innern und für Heimat wird ermächtigt, durch Rechtsverordnung, die nicht der Zustimmung des Bundesrates bedarf, eine öffentliche Stelle des Bundes zu bestimmen, die den Behörden des Bundes zur Unterstützung ihrer elektronischen Verwaltungstätigkeit einen zentralen Siegeldienst bereitstellt. Auf der Grundlage einer Verwaltungsvereinbarung mit dem Bundesministerium des Innern und für Heimat können Länder diesen Siegeldienst zur Unterstützung der elektronischen Verwaltungstätigkeit ihrer Behörden mitnutzen.

(2) Der zentrale Siegeldienst erfüllt mindestens die folgenden Basisfunktionen:

1. Erstellung qualifizierter elektronischer Siegel,
2. Validierung qualifizierter elektronischer Siegel und Signaturen sowie
3. Erstellung digitaler Siegel zum optisch verifizierbaren kryptographischen Schutz von Verwaltungsdokumenten.

§ 3 Information zu Behörden und über ihre Verfahren in öffentlich zugänglichen Netzen

(1) Jede Behörde stellt über öffentlich zugängliche Netze in allgemein verständlicher Sprache Informationen über ihre Aufgaben, ihre Anschrift, ihre Geschäftszeiten sowie postalische, telefonische und elektronische Erreichbarkeiten zur Verfügung.

(2) Jede Behörde soll über öffentlich zugängliche Netze in allgemein verständlicher Sprache über ihre nach außen wirkende öffentlich-rechtliche Tätigkeit, damit verbundene Gebühren, beizubringende Unterlagen und die zuständige Ansprechstelle und ihre Erreichbarkeit informieren sowie erforderliche Formulare bereitstellen.

(3) Die obersten Bundesbehörden stellen mit Unterstützung einer Bundesredaktion insbesondere zu neuen und zu ändernden leistungsbegründenden Rechtsvorschriften des Bundes nach dem vom IT-Planungsrat beschlossenen Standard allgemeine Leistungsinformationen zur Verfügung. Unter Leistungsinformationen fallen Leistungszuschnitte und -beschreibungen sowie Prozess- und Datenfeldinformationen.

(4) Für Gemeinden und Gemeindeverbände gelten die Absätze 1 und 2 nur dann, wenn dies nach Landesrecht angeordnet ist.

§ 4 Elektronische Bezahlmöglichkeiten

(1) Fallen im Rahmen eines elektronisch durchgeführten Verwaltungsverfahrens Gebühren oder sonstige Forderungen an, muss die Behörde die Einzahlung dieser Gebühren oder die Begleichung dieser sonstigen Forderungen durch Teilnahme an verschiedenen im elektronischen Geschäftsverkehr üblichen, möglichst barrierefreien und hinreichend sicheren Zahlungsverfahren ermöglichen.

(2) Erfolgt die Einzahlung von Gebühren oder die Begleichung sonstiger Forderungen durch ein elektronisches Zahlungsabwicklungsverfahren des Bundes, sollen Rechnungen oder Quittungen elektronisch angezeigt werden. Dies gilt auch, wenn die sonstige Forderung außerhalb eines Verwaltungsverfahrens erhoben wird.

§ 4a Elektronischer Rechnungsempfang; Verordnungsermächtigung

(1) Elektronische Rechnungen, die nach Erfüllung von öffentlichen Aufträgen und Aufträgen sowie zu Konzessionen von Stellen im Sinne von § 159 Absatz 1 Nummer 1 bis 4 des Gesetzes gegen Wettbewerbsbeschränkungen ausgestellt wurden, sind nach Maßgabe einer Rechtsverordnung nach Absatz 3 zu empfangen und zu verarbeiten. Diese Verpflichtung gilt unabhängig von dem Geltungsbereich gemäß § 1 Absatz 1 bis 3 und unabhängig davon, ob der Wert des vergebenen öffentlichen Auftrags, des vergebenen Auftrags oder der Vertragswert der vergebenen Konzession den gemäß § 106 des Gesetzes gegen Wettbewerbsbeschränkungen jeweils maßgeblichen Schwellenwert erreicht oder überschreitet. Vertragliche Regelungen, die die elektronische Rechnungsstellung vorschreiben, bleiben unberührt.

(2) Eine Rechnung ist elektronisch, wenn

1. sie in einem strukturierten elektronischen Format ausgestellt, übermittelt und empfangen wird und
2. das Format die automatische und elektronische Verarbeitung der Rechnung ermöglicht.

(3) Die Bundesregierung wird ermächtigt, durch Rechtsverordnung ohne Zustimmung des Bundesrates besondere Vorschriften zur Ausgestaltung des elektronischen Rechnungsverkehrs zu erlassen. Diese Vorschriften können sich beziehen auf

1. die Art und Weise der Verarbeitung der elektronischen Rechnung, insbesondere auf die elektronische Verarbeitung,
2. die Anforderungen an die elektronische Rechnungsstellung, und zwar insbesondere auf die von den elektronischen Rechnungen zu erfüllenden Voraussetzungen, den Schutz personenbezogener Daten, das zu verwendende Rechnungsdatenmodell sowie auf die Verbindlichkeit der elektronischen Form,
3. die Befugnis von öffentlichen Auftraggebern, Sektorenauftraggebern und Konzessionsgebern, in Ausschreibungsbedingungen die Erteilung elektronischer Rechnungen vorzusehen sowie
4. Ausnahmen für verteidigungs- und sicherheitsspezifische Aufträge und Angelegenheiten des Auswärtigen Dienstes.

(4) Als Rechnung oder gleichwertige Zahlungsaufstellung im Sinne von § 286 Absatz 3 des Bürgerlichen Gesetzbuchs gelten Rechnungen, die von der Verpflichtung zur elektronischen Einreichung nach Absatz 1 sowie nach Vorschriften auf Grundlage von Absatz 3 erfasst sind, nur dann, wenn sie elektronisch im Sinne dieses Gesetzes und der Rechtsverordnung nach Absatz 3 gestellt werden. In diesem Fall ist § 1 Absatz 4 nicht anzuwenden.

(5) Das Beschaffungsamt des Bundesministeriums des Innern und für Heimat ist zuständig für die fachliche Betreuung und zentrale Steuerung des elektronischen Rechnungsverkehrs in der gesamten Bundesverwaltung. Das Beschaffungsamt des Bundesministeriums des Innern und für Heimat hat hierbei in Zusammenarbeit mit den beteiligten Stellen insbesondere die Aufgabe, den elektronischen Rechnungsverkehr in der Bundesverwaltung kontinuierlich weiterzuentwickeln und die Interessen der Bundesrepublik Deutschland in Angelegenheiten des elektronischen Rechnungsverkehrs in diesem Bereich in nationalen, europäischen und internationalen Gremien zu vertreten.

§ 5 Nachweisabruf; Nachweiserbringung

(1) Wird ein antragsgebundenes Verwaltungsverfahren elektronisch durchgeführt, erfolgt die Nachweiserbringung auf elektronischem Wege nach Wahl des Antragstellers,

1. indem die nachweisanfordernde Stelle den jeweiligen Nachweis automatisiert bei der nachweisliefernden Stelle abruft, sofern der jeweils erforderliche Nachweis des Antragstellers elektronisch vorliegt und automatisiert abgerufen werden kann, oder
2. indem der Antragsteller den jeweiligen Nachweis elektronisch einreicht.

Die §§ 24 bis 27 des Verwaltungsverfahrensgesetzes bleiben unberührt. Die Verantwortung für die Zulässigkeit der Nachweiserhebung und des Nachweisabrufs nach Satz 1 Nummer 1 in Verbindung mit den Absätzen 3 bis 5 trägt die nachweisanfordernde Stelle.

(2) Nachweise im Sinne dieses Gesetzes sind Unterlagen und Daten jeder Art unabhängig vom verwendeten Medium, die zur Ermittlung des Sachverhalts geeignet sind. Nachweisanfordernde Stelle kann die für die Entscheidung über den Antrag zuständige Behörde oder auch eine andere öffentliche Stelle sein, die dafür zuständig ist, Nachweise einzuholen und an die für die Entscheidung über den Antrag zuständige Behörde weiterzuleiten. Nachweisliefernde Stelle ist diejenige öffentliche Stelle, die dafür zuständig ist, den Nachweis auszustellen.

(3) Hat sich der Antragsteller für den automatisierten Nachweisabruf entschieden, darf die nachweisanfordernde Stelle den Nachweis des Antragstellers bei der nachweisliefernden Stelle abrufen und die nachweisliefernde Stelle darf den Nachweis an die nachweisanfordernde Stelle übermitteln, wenn

1. dies zur Erfüllung der Aufgabe der nachweisanfordernden Stelle erforderlich ist und
2. die nachweisanfordernde Stelle den Nachweis auch aufgrund anderer Rechtsvorschriften beim Antragsteller erheben dürfte.

Die in Absatz 2 Satz 2 genannte andere öffentliche Stelle darf den Nachweis an die für die Entscheidung über den Antrag zuständige Stelle übermitteln. Die Datenübermittlungen zwischen öffentlichen Stellen nach diesem Absatz sind durch die jeweiligen Stellen in einer Weise zu protokollieren, die eine Kontrolle der Zulässigkeit von Datenabrufen technisch unterstützt. Die Pflicht nach Satz 3 gilt ab dem Tag, der dem Tag folgt, an dem das Bundesministerium des Innern und für Heimat im Bundesanzeiger bekannt gibt, dass die technischen und rechtlichen Voraussetzungen für eine Anzeige der Datenübermittlungen nach diesem Absatz im Datenschutzcockpit nach § 10 des Onlinezugangsgesetzes vorliegen. § 9 Absatz 2 und 3 des Identifikationsnummerngesetzes gilt ab diesem Zeitpunkt entsprechend.

(4) Soll der Nachweis aus einem Register, welches in der Anlage zum Identifikationsnummerngesetz vom 28. März 2021 (BGBl. I S. 591), das durch Artikel 15 des Gesetzes vom 28. Juni 2021 (BGBl. I S. 2250) geändert worden ist, aufgeführt ist, abgerufen werden, darf die nachweisanfordernde Stelle die Identifikationsnummer nach § 1 des Identifikationsnummerngesetzes zur Zuordnung der Datensätze zum Antragsteller und zum Abruf des Nachweises an die nachweisliefernde Stelle übermitteln. Das Nachweisabrufersuchen darf zusätzlich weitere Daten im Sinne von § 4 Absatz 2 und 3 des Identifikationsnummerngesetzes, in der Regel das Geburtsdatum, zur Validierung der Zuordnung enthalten. Zu diesem Zweck darf die nachweisliefernde Stelle diese Daten verarbeiten.

(5) Bevor die für die Entscheidung über den Antrag zuständige Behörde den abgerufenen Nachweis verwenden darf, um die antragsgebundene Verwaltungsleistung zu erbringen, hat der Antragsteller im Fall des Absatzes 1 Satz 1 Nummer 1, wenn der Nachweis ohne zeitlichen Verzug automatisiert abgerufen werden kann, die Möglichkeit, den Nachweis vorab einzusehen. Der Antragsteller kann in diesem Fall entscheiden, ob der Nachweis für das Antragsverfahren verwendet werden soll.

§ 5a Grenzüberschreitende Nachweisabrufe

(1) Die zuständige Behörde darf bei einer Behörde eines anderen Mitgliedstaats der Europäischen Union einen Nachweis nach Artikel 14 Absatz 2 der Verordnung (EU) 2018/1724 des Europäischen Parlaments und des Rates vom 2. Oktober 2018 über die Einrichtung eines einheitlichen digitalen Zugangstors zu Informationen, Verfahren, Hilfs- und Problemlö-

sungsdiensten und zur Änderung der Verordnung (EU) Nr. 1024/2012 (ABl. L 295 vom 21.11.2018, S. 1), die durch die Verordnung (EU) 2022/868 (ABl. L 152 vom 3.6.2022, S.1) geändert worden ist, automatisiert abrufen, wenn dies zur Erfüllung ihrer Aufgaben für eines der Verfahren nach Artikel 14 Absatz 1 der Verordnung (EU) 2018/1724 erforderlich ist.

(2) Die automatisierte Übermittlung eines Nachweises nach Artikel 14 Absatz 2 der Verordnung (EU) 2018/1724 an eine Behörde eines anderen Mitgliedstaats der Europäischen Union ist zulässig, wenn diese Behörde zuständig ist und die Übermittlung zur Erfüllung ihrer Aufgaben für eines der Verfahren nach Artikel 14 Absatz 1 der Verordnung (EU) 2018/1724 erforderlich ist.

(3) Bei der Verarbeitung personenbezogener Daten nach den Absätzen 1 und 2 können intermediäre Plattformen zum Einsatz kommen.

§ 6 Ende-zu-Ende-Digitalisierung; Verordnungsermächtigung

(1) Der Bund hat für seine wesentlichen elektronischen Verwaltungsleistungen spätestens zum Ablauf des fünften auf die Verkündung des Gesetzes vom 19. Juli 2024 (BGBl. 2024 I Nr. 245) folgenden Kalenderjahres eine vollständige elektronische Abwicklung sicherzustellen.

(2) Die Umsetzung und die Auswirkungen des Absatzes 1 werden durch das Bundesministerium des Innern und für Heimat nach Ablauf des fünften auf die Verkündung des Gesetzes vom 19. Juli 2024 (BGBl. 2024 I Nr. 245) folgenden Kalenderjahres evaluiert. Der Evaluierungsbericht ist dem Bundestag vorzulegen.

(3) Das Bundesministerium des Innern und für Heimat wird ermächtigt, im Einvernehmen mit dem für das jeweilige Bundesgesetz zuständigen Bundesministerium nach Anhörung der kommunalen Spitzenverbände durch Rechtsverordnung mit Zustimmung des Bundesrates für elektronische Verwaltungsleistungen, die der Ausführung von Bundesgesetzen durch die Länder dienen, zu bestimmen, dass diese Verwaltungsleistungen vollständig elektronisch abzuwickeln sind. Die Länder können von den in der Rechtsverordnung getroffenen Regelungen durch Landesrecht abweichen.

§ 6a Elektronische Aktenführung

Die Behörden des Bundes sollen ihre Akten elektronisch führen. Satz 1 gilt nicht für solche Behörden, bei denen das Führen elektronischer Akten bei langfristiger Betrachtung unwirtschaftlich ist. Wird eine Akte elektronisch geführt, ist durch geeignete technisch-organisatorische Maßnahmen nach dem Stand der Technik sicherzustellen, dass die Grundsätze ordnungsgemäßer Aktenführung eingehalten werden.

§ 7 Übertragen und Vernichten des Papieroriginals

(1) Die Behörden des Bundes sollen, soweit sie Akten elektronisch führen, an Stelle von Papierdokumenten deren elektronische Wiedergabe in der elektronischen Akte aufbewahren. Bei der Übertragung in elektronische Dokumente ist nach dem Stand der Technik sicherzustellen, dass die elektronischen Dokumente mit den Papierdokumenten bildlich und inhaltlich übereinstimmen, wenn sie lesbar gemacht werden. Von der Übertragung der Papierdokumente in elektronische Dokumente kann abgesehen werden, wenn die Übertragung unverhältnismäßigen technischen Aufwand erfordert.

(2) Papierdokumente nach Absatz 1 sollen nach der Übertragung in elektronische Dokumente vernichtet oder zurückgegeben werden, sobald eine weitere Aufbewahrung nicht mehr aus rechtlichen Gründen oder zur Qualitätssicherung des Übertragungsvorgangs erforderlich ist.

§ 8 Akteneinsicht

Soweit ein Recht auf Akteneinsicht besteht, können die Behörden des Bundes, die Akten elektronisch führen, Akteneinsicht dadurch gewähren, dass sie

1. einen Aktenausdruck zur Verfügung stellen,
2. die elektronischen Dokumente auf einem Bildschirm wiedergeben,
3. elektronische Dokumente übermitteln oder
4. den elektronischen Zugriff auf den Inhalt der Akten gestatten.

§ 9 Optimierung von Verwaltungsabläufen und Information zum Verfahrensstand

(1) Behörden des Bundes sollen Verwaltungsabläufe, die erstmals zu wesentlichen Teilen elektronisch unterstützt werden, vor Einführung der informationstechnischen Systeme unter Nutzung gängiger Methoden dokumentieren, analysieren und optimieren. Dabei sollen sie im Interesse der Verfahrensbeteiligten die Abläufe so gestalten, dass Informationen zum Verfahrensstand und zum weiteren Verfahren sowie die Kontaktinformationen der zum Zeitpunkt der Anfrage zuständigen Ansprechstelle auf elektronischem Wege abgerufen werden können.

(2) Von den Maßnahmen nach Absatz 1 kann abgesehen werden, soweit diese einen nicht vertretbaren wirtschaftlichen Mehraufwand bedeuten würden oder sonstige zwingende Gründe entgegenstehen. Von den Maßnahmen nach Absatz 1 Satz 2 kann zudem abgesehen werden, wenn diese dem Zweck des Verfahrens entgegenstehen oder eine gesetzliche Schutznorm verletzen. Die Gründe nach den Sätzen 1 und 2 sind zu dokumentieren.

(3) Die Absätze 1 und 2 gelten entsprechend bei allen wesentlichen Änderungen der Verwaltungsabläufe oder der eingesetzten informationstechnischen Systeme.

§ 9a Verwaltungsportal des Bundes; Verordnungsermächtigung

(1) Das Verwaltungsportal des Bundes nach § 1a Absatz 1 des Onlinezugangsgesetzes wird durch die dafür zuständige öffentliche Stelle zur fachunabhängigen und fachübergreifenden Unterstützung der elektronischen Verwaltungstätigkeit der Behörden des Bundes zur Verfügung gestellt.

(2) Das Bundesministerium des Innern und für Heimat wird ermächtigt, durch Rechtsverordnung, die nicht der Zustimmung des Bundesrates bedarf, die für das Verwaltungsportal des Bundes zuständige öffentliche Stelle zu bestimmen. Die Zuständigkeit der jeweils fachlich zuständigen Behörde für ihre Verwaltungsleistungen bleibt davon unberührt.

(3) Das Verwaltungsportal des Bundes stellt zur Unterstützung der Abwicklung von elektronischen Verwaltungsleistungen Basisfunktionen bereit, um folgende Zwecke zu erfüllen:

1. Ermöglichung einer elektronischen Suche nach Verwaltungsleistungen des Bundes und der Länder im Portalverbund,

2. Ermöglichung des elektronischen Identitätsnachweises über ein Nutzerkonto nach § 2 Absatz 5 des Onlinezugangsgesetzes,
3. Bereitstellung von Online-Formularen für die Unterstützung bei der Abwicklung von elektronischen Verwaltungsleistungen, die in der Zuständigkeit des Bundes liegen und von Behörden des Bundes ausgeführt werden, einschließlich der Erbringung erforderlicher Nachweise,
4. Bereitstellung eines sicheren Übermittlungswegs, über den Nutzer auch strukturierte Daten und elektronische Informationen, einschließlich erforderlicher Nachweise, zur Abwicklung elektronischer Verwaltungsleistungen, die in der Zuständigkeit des Bundes liegen und von Behörden des Bundes ausgeführt werden, übermitteln können,
5. Ermöglichung eines sicheren elektronischen Übermittlungswegs für die Behörden des Bundes, die an das Verwaltungsportal des Bundes angeschlossen sind, mit dem sie
   a) Online-Formulare empfangen und herunterladen können,
   b) Bescheide, elektronische Dokumente, Informationen und Nachrichten hochladen und elektronisch an das Nutzerkonto des Nutzers übermitteln können und
   c) elektronische Dokumente, Informationen und Nachrichten aus dem Nutzerkonto des Nutzers empfangen können und
6. Ermöglichung der Teilnahme an verschiedenen im elektronischen Geschäftsverkehr üblichen, möglichst barrierefreien und hinreichend sicheren Zahlungsverfahren für die Behörden des Bundes.

§ 9b Verarbeitung personenbezogener Daten im Verwaltungsportal des Bundes

(1) Die für die Zwecke nach § 9a Absatz 3 erforderlichen personenbezogenen Daten dürfen im Verwaltungsportal des Bundes verarbeitet werden. Dies gilt auch für die Verarbeitung besonderer Kategorien personenbezogener Daten im Sinne des Artikels 9 Absatz 1 der 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 (ABl. L 119 vom 4.5.2016, S. 1; L 314 vom 22.11.2016, S. 72; L 127 vom 23.5.2018, S. 2), soweit diese für eine Verwaltungsleistung, die über das Verwaltungsportal des Bundes elektronisch abgewickelt wird, erforderlich sind. § 22 Absatz 2 des Bundesdatenschutzgesetzes gilt entsprechend.

(2) Die erforderlichen Stamm- und Verfahrensdaten, die im Verwaltungsportal des Bundes über ein Online-Formular einer Behörde erhoben werden, dürfen auf Veranlassung des Nutzers darüber hinaus gespeichert werden (zwischengespeicherte Verfahrensdaten), um dem Nutzer zu ermöglichen, das Online-Formular zu einem späteren Zeitpunkt zu vervollständigen, zu korrigieren oder zu löschen und auch nach Übermittlung an die zuständige Behörde einzusehen, zu ergänzen oder die zwischengespeicherten Verfahrensdaten erneut zu verwenden. § 22 Absatz 2 des Bundesdatenschutzgesetzes gilt im Rahmen der Zwischenspeicherung besonderer Kategorien personenbezogener Daten im Sinne des Artikels 9 Absatz 1 der Verordnung (EU) 2016/679 entsprechend.

(3) Durch technische und organisatorische Maßnahmen ist sicherzustellen, dass die jeweils zuständige Behörde nicht auf die zwischengespeicherten Verfahrensdaten zugreifen kann. Vor der Übermittlung des Online-Formulars an die zuständige Behörde zwischengespeicherte Verfahrensdaten sind nach Ablauf von 30 Tagen nach der letzten Bearbeitung durch den Nutzer zu löschen. Nach der Übermittlung des Online-Formulars an die zuständige Behörde zwischengespeicherte Verfahrensdaten sind zu löschen, wenn diese für die Zwecke nach Absatz 2 nicht mehr erforderlich sind oder der Nutzer diese erkennbar nicht mehr weiterverwenden möchte. Der Nutzer ist vorab über eine automatische Löschung der Verfahrensdaten zu informieren.

(4) Der Zugriff auf die zwischengespeicherten Verfahrensdaten wird für die Nutzer im Verwaltungsportal des Bundes portalübergreifend ermöglicht. Die für den Zweck der Ermöglichung des portalübergreifenden Zugriffs erforderlichen Stamm- und Verfahrensdaten dürfen im Verwaltungsportal des Bundes verarbeitet werden.

§ 9c Datenschutzrechtliche Verantwortlichkeit

(1) Für die Verarbeitung personenbezogener Daten im Verwaltungsportal des Bundes nach § 9a Absatz 3 Nummer 3 bis 6 und nach § 9b Absatz 2 und 3 ist die jeweils zuständige Behörde des Bundes datenschutzrechtlich verantwortlich; die für das Verwaltungsportal des Bundes zuständige öffentliche Stelle wird insofern tätig als Auftragsverarbeiter nach Artikel 4 Nummer 8 der 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 (ABl. L 119 vom 4.5.2016, S. 1; L 314 vom 22.11.2016, S. 72; L 127 vom 23.5.2018, S. 2).

(2) Im Übrigen führt die für das Verwaltungsportal des Bundes zuständige öffentliche Stelle die Verarbeitung personenbezogener Daten in ausschließlich eigener datenschutzrechtlicher Verantwortlichkeit aus.

§ 10 Umsetzung von Standardisierungsbeschlüssen des IT-Planungsrates

Fasst der Planungsrat für die IT-Zusammenarbeit der öffentlichen Verwaltung zwischen Bund und Ländern (IT-Planungsrat) einen Beschluss über fachunabhängige und fachübergreifende IT-Interoperabilitäts- oder IT-Sicherheitsstandards gemäß § 1 Absatz 1 Satz 1 Nummer 2 und § 3 des Vertrages über die Errichtung des IT-Planungsrats und über die Grundlagen der Zusammenarbeit beim Einsatz der Informationstechnologie in den Verwaltungen von Bund und Ländern – Vertrag zur Ausführung von Artikel 91c GG (BGBl. 2010 I S. 662, 663), so beschließt der Rat der IT-Beauftragten der Bundesregierung (IT-Rat) die Umsetzung dieses Beschlusses innerhalb der Bundesverwaltung. § 12 des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik gilt entsprechend.

§ 11 Gemeinsame Verfahren

(1) Gemeinsame Verfahren sind automatisierte Verfahren, die mehreren Verantwortlichen im Sinne des Artikels 26 der 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; L 314 vom 22.11.2016, S. 72; L 127 vom 23.5.2018, S. 2) in der jeweils geltenden Fassung die Verarbeitung personenbezogener Daten in oder aus einem Datenbestand ermöglichen.

(2) Die Beteiligung öffentlicher Stellen des Bundes nach § 2 Absatz 1 des Bundesdatenschutzgesetzes an gemeinsamen Verfahren ist nur zulässig, wenn dies unter Berücksichtigung der schutzwürdigen Interessen der betroffenen Personen und der Aufgaben der beteiligten Stellen angemessen ist. Die Vorschriften über die Zulässigkeit der Verarbeitung der Daten im Einzelfall bleiben unberührt.

(3) Vor der Einrichtung oder wesentlichen Änderung eines gemeinsamen Verfahrens schließen die Verantwortlichen eine Vereinbarung nach Maßgabe des Artikels 26 Absatz 1 und 2 der Verordnung (EU) 2016/679. In dieser Vereinbarung können auch Verantwortliche bestimmt werden, die andere Stellen mit der Verarbeitung personenbezogener Daten für das gemeinsame Verfahren gemäß Artikel 28 der Verordnung (EU) 2016/679 beauftragen dürfen.

(4) Soweit für die beteiligten Stellen ungeachtet der Verordnung (EU) 2016/679 unterschiedliche bundes- oder landesrechtliche Datenschutzvorschriften gelten, ist vor der Einrichtung eines gemeinsamen Verfahrens zu regeln, welche dieser Datenschutzvorschriften angewendet werden. Weiterhin ist zu bestimmen, welche Kontrollstellen die Einhaltung der Datenschutzvorschriften prüfen.

§ 12 Anforderungen an das Bereitstellen von Daten, Verordnungsermächtigung

(1) Stellen Behörden über öffentlich zugängliche Netze Daten zur Verfügung, an denen ein Nutzungsinteresse, insbesondere ein Weiterverwendungsinteresse im Sinne des Datennutzungsgesetzes, zu erwarten ist, so sind grundsätzlich maschinenlesbare Formate zu verwenden. Ein Format ist maschinenlesbar, wenn die enthaltenen Daten durch Software automatisiert ausgelesen und verarbeitet werden können. Die Daten sollen mit Metadaten versehen werden.

(2) Die Bundesregierung wird ermächtigt, durch Rechtsverordnung mit Zustimmung des Bundesrates Bestimmungen für die Nutzung der Daten gemäß Absatz 1 festzulegen. Die Nutzungsbestimmungen sollen die kommerzielle und nichtkommerzielle Nutzung abdecken. Sie sollen insbesondere den Umfang der Nutzung, Nutzungsbedingungen, Gewährleistungs- und Haftungsausschlüsse regeln. Es können keine Regelungen zu Geldleistungen getroffen werden.

(3) Regelungen in anderen Rechtsvorschriften über technische Formate, in denen Daten verfügbar zu machen sind, gehen vor, soweit sie Maschinenlesbarkeit gewährleisten.

(4) Absatz 1 gilt für Daten, die vor dem 31. Juli 2013 erstellt wurden, nur, wenn sie in maschinenlesbaren Formaten vorliegen.

(5) Absatz 1 gilt nicht, soweit Rechte Dritter, insbesondere der Länder, entgegenstehen.

§ 12a Offene Daten des Bundes, Verordnungsermächtigung

(1) Die Behörden des Bundes mit Ausnahme der Selbstverwaltungskörperschaften stellen unbearbeitete maschinenlesbare Daten, die sie zur Erfüllung ihrer öffentlich-rechtlichen Aufgaben erhoben haben oder durch Dritte in ihrem Auftrag haben erheben lassen, zum Datenabruf über öffentlich zugängliche Netze bereit. Ein Anspruch auf Bereitstellung dieser Daten wird hierdurch nicht begründet. Satz 1 gilt nicht für natürliche Personen und juristische Personen des Privatrechts, denen hoheitliche Aufgaben zur selbständigen Wahrnehmung übertragen wurden.

(2) Absatz 1 Satz 1 gilt nur für Daten, die

1. der Behörde elektronisch gespeichert und in Sammlungen strukturiert vorliegen, insbesondere in Tabellen oder Listen,
2. ausschließlich Tatsachen enthalten, die außerhalb der Behörde liegende Verhältnisse betreffen,
3. nicht das Ergebnis einer Bearbeitung anderer Daten durch eine Behörde des Bundes sind,
4. nach der Erhebung keine Bearbeitung erfahren haben, ausgenommen eine Bearbeitung,
   a) die der Fehlerbereinigung dient oder
   b) die aus rechtlichen oder aus tatsächlichen Gründen erfolgt ist und ohne die eine Veröffentlichung der Daten nicht möglich wäre, und
5. bei Personenbezug derart umgewandelt wurden, dass
   a) sie sich nicht mehr auf eine identifizierte oder identifizierbare natürliche Person beziehen oder
   b) die betroffene Person nicht oder nicht mehr identifiziert werden kann.

(3) Abweichend von Absatz 1 Satz 1 müssen die Daten nicht bereitgestellt werden, wenn

1. an den Daten
   a) kein oder nur ein eingeschränktes Zugangsrecht insbesondere gemäß den §§ 3, 4 und 6 des Informationsfreiheitsgesetzes besteht oder
   b) ein Zugangsrecht erst nach der Beteiligung Dritter bestünde,
2. die Daten ohne Auftrag der Behörde von Dritten erstellt und ihr ohne rechtliche Verpflichtung übermittelt werden,
3. es sich um Daten handelt, die zu Forschungszwecken erhoben wurden und bereits über öffentlich zugängliche Netze entgeltfrei bereitgestellt werden; die Möglichkeit der freiwilligen Bereitstellung dazugehöriger Metadaten über das nationale Metadatenportal GovData bleibt davon unberührt, oder
4. die Daten unter das Bankgeheimnis fallen.

(3a) Abweichend von Absatz 1 Satz 1 müssen Datensätze, die personenbezogene Daten enthalten, nicht bereitgestellt werden.

(4) Die Bereitstellung der Daten nach Absatz 1 Satz 1 erfolgt unverzüglich nach der Erhebung, sofern der Zweck der Erhebung dadurch nicht beeinträchtigt wird, andernfalls unverzüglich nach Wegfall der Beeinträchtigung. Ist aus technischen oder sonstigen gewichtigen Gründen eine unverzügliche Bereitstellung nicht möglich, sind die Daten unverzüglich nach Wegfall dieser Gründe bereitzustellen. Sofern sich aus spezialgesetzlichen Regelungen nichts anderes ergibt, sind abweichend von Satz 1 Daten, die zu Forschungszwecken erhoben wurden, erst bereitzustellen, wenn das der Datenerhebung zugrunde liegende Forschungsvorhaben abgeschlossen und der Forschungszweck erfüllt ist. Der für die freiwillige Teilnahme an einer Forschungsmaßnahme festgelegte Zweck gilt unbeschadet hiervon fort.

(5) Die Daten nach Absatz 1 Satz 1 sind mit Metadaten zu versehen. Diese Metadaten werden im nationalen Metadatenportal GovData eingestellt.

(6) Der Abruf von Daten nach Absatz 1 Satz 1 muss entgeltfrei und zur uneingeschränkten Weiterverwendung der Daten durch jedermann ermöglicht werden. Der Abruf von Daten nach Absatz 1 Satz 1 soll jederzeit, ohne verpflichtende Registrierung und ohne Begründung möglich sein.

(7) Die Behörden des Bundes sollen die Anforderungen an die Bereitstellung von Daten im Sinne des Absatzes 1 Satz 1 bereits frühzeitig berücksichtigen bei:

1. der Optimierung von Verwaltungsabläufen gemäß § 9,
2. dem Abschluss von vertraglichen Regelungen zur Erhebung oder Verarbeitung der Daten sowie
3. bei der Beschaffung von informationstechnischen Systemen für die Speicherung und Verarbeitung der Daten.

(8) Die Behörden des Bundes sind nicht verpflichtet, die bereitzustellenden Daten auf Richtigkeit, Vollständigkeit, Plausibilität oder in sonstiger Weise zu prüfen.

(9) Jede nach Absatz 1 verpflichtete Stelle mit Ausnahme der in § 3 Nummer 8 des Informationsfreiheitsgesetzes genannten Stellen sowie von Hauptzollämtern oder vergleichbaren örtlichen Bundesbehörden benennt einen Open-Data-Koordinator oder eine Open-Data-Koordinatorin. Der Koordinator oder die Koordinatorin wirkt in der Funktion als zentraler Ansprechpartner oder zentrale Ansprechpartnerin der jeweiligen Behörde auf die Identifizierung, Bereitstellung und Weiterverwendung der offenen Daten seiner oder ihrer Behörde hin. Die Möglichkeit der freiwilligen Benennung entsprechender Open-Data-Koordinatoren oder Open-Data-Koordinatorinnen in den übrigen Behörden der Bundesverwaltung bleibt davon unberührt.

(10) Die Bundesregierung richtet eine zentrale Stelle ein, die die Behörden der Bundesverwaltung zu Fragen der Bereitstellung von Daten als offene Daten berät und Ansprechpartner für entsprechende Stellen der Länder ist.

(11) Die Bundesregierung berichtet dem Bundestag alle zwei Jahre über die Fortschritte bei der Bereitstellung von Daten durch die Behörden der Bundesverwaltung als offene Daten. Mit Blick auf die beabsichtigte Erweiterung des Anwendungsbereichs nach Absatz 1 Satz 1 bis zum Jahr 2025 evaluiert sie dabei auch die mögliche Ausweitung der Bereitstellungspflicht auf Selbstverwaltungskörperschaften und natürliche Personen und juristische Personen des Privatrechts, denen hoheitliche Aufgaben zur selbständigen Wahrnehmung übertragen wurden, sowie die Einführung eines Anspruchs auf die Bereitstellung von Daten im Sinne des Absatzes 1 Satz 2.

(12) Das Bundesministerium des Innern, für Bau und Heimat wird ermächtigt, im Einvernehmen mit den übrigen Bundesministerien und den Beauftragten der Bundesregierung durch Rechtsverordnung ohne Zustimmung des Bundesrates Bestimmungen zum Bereitstellungsprozess der Daten nach Absatz 1 Satz 1 zu erlassen.

§ 13 Elektronische Formulare

Ist durch Rechtsvorschrift die Verwendung eines bestimmten Formulars vorgeschrieben, das ein Unterschriftsfeld vorsieht, wird allein dadurch nicht die Anordnung der Schriftform be-

wirkt. Bei einer für die elektronische Versendung an die Behörde bestimmten Fassung des Formulars entfällt das Unterschriftsfeld.

§ 14 Georeferenzierung

(1) Wird ein elektronisches Register, welches Angaben mit Bezug zu inländischen Grundstücken enthält, neu aufgebaut oder überarbeitet, hat die Behörde in das Register eine bundesweit einheitlich festgelegte direkte Georeferenzierung (Koordinate) zu dem jeweiligen Flurstück, dem Gebäude oder zu einem in einer Rechtsvorschrift definierten Gebiet aufzunehmen, auf welches sich die Angaben beziehen.

(2) Register im Sinne dieses Gesetzes sind solche, für die Daten auf Grund von Rechtsvorschriften des Bundes erhoben oder gespeichert werden; dies können öffentliche und nichtöffentliche Register sein.

§ 15 Amtliche Mitteilungs- und Verkündungsblätter

(1) Eine durch Rechtsvorschrift des Bundes bestimmte Pflicht zur Publikation in einem amtlichen Mitteilungs- oder Verkündungsblatt des Bundes, eines Landes oder einer Gemeinde kann unbeschadet des Artikels 82 Absatz 1 des Grundgesetzes zusätzlich oder ausschließlich durch eine elektronische Ausgabe erfüllt werden, wenn diese über öffentlich zugängliche Netze angeboten wird.

(2) Jede Person muss einen angemessenen Zugang zu der Publikation haben, insbesondere durch die Möglichkeit, Ausdrucke zu bestellen oder in öffentlichen Einrichtungen auf die Publikation zuzugreifen. Es muss die Möglichkeit bestehen, die Publikation zu abonnieren oder elektronisch einen Hinweis auf neue Publikationen zu erhalten. Gibt es nur eine elektronische Ausgabe, ist dies in öffentlich zugänglichen Netzen auf geeignete Weise bekannt zu machen. Es ist sicherzustellen, dass die publizierten Inhalte allgemein und dauerhaft zugänglich sind und eine Veränderung des Inhalts ausgeschlossen ist. Bei gleichzeitiger Publikation in elektronischer und papiergebundener Form hat die herausgebende Stelle eine Regelung zu treffen, welche Form als die authentische anzusehen ist.

§ 16 Nutzerfreundlichkeit und Barrierefreiheit

Die Behörden des Bundes gestalten die elektronische Kommunikation und die elektronischen Dokumente nutzerfreundlich und barrierefrei. Für die barrierefreie Gestaltung gilt die Barrierefreie-Informationstechnik-Verordnung entsprechend.

§ 16a Open Source

Die Behörden des Bundes sollen offene Standards nutzen und bei neu anzuschaffender Software Open-Source-Software vorrangig vor solcher Software beschaffen, deren Quellcode nicht öffentlich zugänglich ist oder deren Lizenz die Verwendung, Weitergabe und Veränderung einschränkt.

§ 17 Änderung verwaltungsrechtlicher Rechtsverordnungen des Bundes

Soweit Anordnungen der Schriftform in Rechtsverordnungen des Bundes nach dem Bericht der Bundesregierung zu Artikel 30 Absatz 2 Nummer 1 des Gesetzes zur Förderung der elektronischen Verwaltung sowie zur Änderung weiterer Vorschriften vom 25. Juli 2013 (BGBl. I S. 2749) verzichtbar sind (Bundestagsdrucksache 18/9177, S. 29 bis 47), sind diese aufzuhe-

ben oder mit dem Ziel einer möglichst einfachen elektronischen Verfahrensabwicklung zu ergänzen.

§ 18 Anwendungsregelung

Für subzentrale öffentliche Auftraggeber sowie für Sektorenauftraggeber und für Konzessionsgeber ist § 4a erst ab dem 27. November 2019 anzuwenden. Subzentrale öffentliche Auftraggeber sind alle öffentlichen Auftraggeber, die keine obersten Bundesbehörden sind. Verfassungsorgane des Bundes sind für die Zwecke dieses Gesetzes den obersten Bundesbehörden gleichgestellt.

§ 19 Übergangsvorschriften

(1) § 12a gilt für Daten, die nach dem 13. Juli 2017 erhoben werden. Für Daten, die vor dem 13. Juli 2017 erhoben wurden, gilt § 12a nur, soweit diese Daten nach dem 13. Juli 2017 zur Erfüllung öffentlich-rechtlicher Aufgaben der Behörden nach § 12a Absatz 1 Satz 1 verwendet werden.

(2) Die Behörden der mittelbaren Bundesverwaltung stellen die Daten nach § 12a spätestens zwölf Monate nach dem 23. Juli 2021 erstmals bereit. Erfordert die Bereitstellung der Daten erhebliche technische Anpassungen und ist sie deshalb innerhalb des in Satz 1 genannten Zeitraums nur mit unverhältnismäßig hohem Aufwand möglich, verlängert sich der Zeitraum für die erstmalige Bereitstellung der Daten auf bis zu zwei Jahre, um die technischen Anpassungen durchzuführen. Im Fall des Satzes 2 müssen bei der erstmaligen Bereitstellung nur die aktuellen Daten bereitgestellt werden.

(3) Abweichend von den Absätzen 1 und 2 und unbeschadet der Regelung in § 12a Absatz 4 Satz 3 stellen Behörden des Bundes Daten, die zu Forschungszwecken erhoben wurden, spätestens 36 Monate nach dem 23. Juli 2021 erstmals bereit.

(4) Abweichend von Absatz 1 gilt die Pflicht nach § 12a Absatz 9 Satz 1 für Behörden der unmittelbaren Bundesverwaltung mit weniger als 30 Beschäftigten sowie für Behörden der mittelbaren Bundesverwaltung spätestens 36 Monate nach dem 23. Juli 2021, für Behörden der unmittelbaren Bundesverwaltung mit weniger als 50 Beschäftigten spätestens 24 Monate nach dem 23. Juli 2021.

Gesetz zur Verbesserung des Onlinezugangs zu Verwaltungsleistungen (Onlinezugangsgesetz - OZG)

Inhaltsübersicht

§ 1 Anwendungsbereich

(1) Dieses Gesetz gilt für Verwaltungsleistungen der öffentlichen Stellen

1. des Bundes einschließlich der bundesunmittelbaren Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts,
2. der Länder, einschließlich der Gemeinden, Gemeindeverbände und der sonstigen der Aufsicht des Landes unterstehenden juristischen Personen des öffentlichen Rechts.

(2) Für die Tätigkeit der Gerichtsverwaltungen und der Behörden der Justizverwaltung einschließlich der ihrer Aufsicht unterliegenden Körperschaften des öffentlichen Rechts gilt dieses Gesetz nur, soweit die Tätigkeit der Nachprüfung durch die Gerichte der Verwaltungsgerichtsbarkeit oder der Nachprüfung durch die in verwaltungsrechtlichen Anwalts-, Patentanwalts- und Notarsachen zuständigen Gerichte unterliegt.

§ 1a Portalverbund für digitale Verwaltungsleistungen

(1) Bund und Länder sind verpflichtet, ihre Verwaltungsleistungen auch elektronisch über Verwaltungsportale anzubieten. Davon abweichend sollen Verwaltungsleistungen, die der Ausführung von Bundesgesetzen dienen und ausschließlich Nutzer im Sinne des § 2 Absatz 4 Nummer 2 betreffen, spätestens mit Ablauf des fünften auf die Verkündung des Gesetzes vom 19. Juli 2024 (BGBl. 2024 I Nr. 245) folgenden Kalenderjahres ausschließlich elektronisch angeboten werden. Von dem ausschließlich elektronischen Angebot einer Verwaltungsleistung nach Satz 2 kann bei berechtigtem Interesse des Nutzers abgewichen werden. Erfolgt ein ausschließlich elektronisches Angebot bereits vor Ablauf des Zeitraums nach Satz 2, so ist darüber an geeigneter Stelle mit angemessenem Vorlauf elektronisch zu informieren.

(2) Nach Ablauf des vierten auf die Verkündung des Gesetzes vom 19. Juli 2024 (BGBl. 2024 I Nr. 245) folgenden Kalenderjahres haben Nutzer einen Anspruch auf einen elektronischen Zugang zu den Verwaltungsleistungen des Bundes. Schadensersatzansprüche und Entschädigungsansprüche sind ausgeschlossen.

(3) Bund und Länder sind verpflichtet, ihre Verwaltungsportale miteinander zu einem Portalverbund zu verknüpfen, sodass Nutzer über alle Verwaltungsportale von Bund und Ländern einen medienbruch- und barrierefreien Zugang zu elektronischen Verwaltungsleistungen dieser Verwaltungsträger erhalten. Die Länder sind verpflichtet, die technischen und organisatorischen Voraussetzungen für die Anbindung der Gemeinden und Gemeindeverbände sowie der sonstigen der Aufsicht des Landes unterstehenden juristischen Personen des öffentlichen Rechts an den Portalverbund sicherzustellen.

(4) Der Bund stellt im Verwaltungsportal des Bundes für die Suche nach elektronischen Verwaltungsleistungen im Portalverbund einen Suchdienst bereit. Auf Grundlage einer Verwaltungsvereinbarung mit dem Bundesministerium des Innern und für Heimat können Länder diesen Suchdienst auch für ihre Verwaltungsportale mitnutzen.

§ 2 Begriffsbestimmungen

(1) Der „Portalverbund“ ist eine technische Verknüpfung der Verwaltungsportale von Bund und Ländern, über den der Zugang zu Verwaltungsleistungen auf unterschiedlichen Portalen angeboten wird.

(2) Ein „Verwaltungsportal“ bezeichnet ein bereits gebündeltes elektronisches Verwaltungsangebot mit entsprechenden Angeboten einzelner Behörden.

(3) „Elektronische Verwaltungsleistungen“ im Sinne dieses Gesetzes sind die elektronische Abwicklung von Verwaltungsverfahren und die dazu erforderliche elektronische Information des Nutzers und Kommunikation mit dem Nutzer über allgemein zugängliche Netze.

(4) „Nutzer“ im Sinne dieses Gesetzes sind

1. natürliche Personen,
2. Unternehmen im Sinne des § 3 Absatz 1 des Unternehmensbasisdatenregistergesetzes und
3. Behörden.

(5) Ein „Nutzerkonto“ ist eine zentrale IT-Komponente zur einmaligen oder dauerhaften Identifizierung und Authentifizierung der Nutzer zu Zwecken der Inanspruchnahme von

Verwaltungsleistungen der öffentlichen Verwaltung sowie zur vorgangsbezogenen sicheren Kommunikation über ein Postfach im Sinne des Absatzes 7. Ein Nutzerkonto wird als Bürger- oder Organisationskonto bereitgestellt. Das „Bürgerkonto" ist ein Nutzerkonto, das natürlichen Personen zur Verfügung steht. Das „Organisationskonto" ist ein Nutzerkonto, das Unternehmen im Sinne des § 3 Absatz 1 des Unternehmensbasisdatenregistergesetzes sowie Behörden zur Verfügung steht.

(6) „IT-Komponenten" im Sinne dieses Gesetzes sind IT-Anwendungen, Basisdienste, digitale Werkzeuge und die elektronische Realisierung von Standards, Schnittstellen und Sicherheitsvorgaben, die für die Anbindung an den Portalverbund, für den Betrieb des Portalverbundes und für die Abwicklung der Verwaltungsleistungen im Portalverbund erforderlich sind.

(7) Ein „Postfach" ist eine IT-Komponente, über die Nutzer medienbruchfrei, barrierefrei und sicher mit den an den Portalverbund angeschlossenen öffentlichen Stellen vorgangsbezogen kommunizieren können sowie elektronische Dokumente und Informationen senden und empfangen können. Das Postfach ist Bestandteil eines Nutzerkontos.

(8) Ein „Onlinedienst" ist eine IT-Komponente, die ein eigenständiges elektronisches Angebot an die Nutzer darstellt, welches die Abwicklung einer oder mehrerer elektronischer Verwaltungsleistungen von Bund oder Ländern ermöglicht. Der Onlinedienst dient dem elektronischen Ausfüllen der Online-Formulare für Verwaltungsleistungen von Bund oder Ländern, der Offenlegung dieser Daten an die zuständige Fachbehörde sowie der Übermittlung elektronischer Dokumente und Informationen zu Verwaltungsvorgängen an die Nutzer, gegebenenfalls unter Einbindung von Nutzerkonten einschließlich deren Funktion zur Übermittlung von Daten aus einem Nutzerkonto an eine für die Verwaltungsleistung zuständige Behörde. Der Onlinedienst kann auch verfahrensunabhängig und länderübergreifend, insbesondere in der Verantwortung einer Landesbehörde zur Nutzung durch weitere Länder, bereitgestellt werden.

(9) Behörde im Sinne dieses Gesetzes ist jede Stelle, die Aufgaben der öffentlichen Verwaltung wahrnimmt.

§ 3 Nutzerkonten, Identifizierung und Authentifizierung; Verordnungsermächtigung

(1) Die Identifizierung und Authentifizierung der Nutzer im Sinne des § 2 Absatz 4 Nummer 1 für die Inanspruchnahme elektronischer Verwaltungsleistungen im Portalverbund erfolgt, soweit nicht durch Bundesgesetz etwas anderes bestimmt ist, über ein zentrales Bürgerkonto, das der Bund bereitstellt. Die Verwendung des Bürgerkontos ist für die Nutzer freiwillig. Das Bundesministerium des Innern und für Heimat wird ermächtigt, durch Rechtsverordnung, die nicht der Zustimmung des Bundesrates bedarf, zu bestimmen, welche öffentliche Stelle des Bundes das Bürgerkonto bereitstellt.

(2) Das Bundesministerium des Innern und für Heimat wird ermächtigt, durch Rechtsverordnung mit Zustimmung des Bundesrates zu bestimmen, welche staatlichen Stellen ein einheitliches Organisationskonto im Portalverbund bereitstellen.

(3) Für öffentliche Stellen, die Verwaltungsleistungen im Portalverbund anbieten, ist die Verwendung des Organisationskontos verpflichtend.

(4) Der Nachweis der Identität des Nutzers erfolgt

1. im Bürgerkonto

a) für elektronische Verwaltungsleistungen, für die höchstens das Vertrauensniveau „substantiell“ erforderlich ist, durch ein sicheres Verfahren nach § 87a Absatz 6 der Abgabenordnung oder durch ein anderes elektronisches Identifizierungsmittel, welches nach Artikel 6 der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG (ABl. L 257 vom 28.8.2014, S. 73) mindestens mit dem Sicherheitsniveau „substantiell“ im Sinne des Artikels 8 Absatz 2 Buchstabe b der Verordnung (EU) Nr. 910/2014 anerkannt worden ist,

b) für elektronische Verwaltungsleistungen, für die das Vertrauensniveau „hoch“ erforderlich ist, durch einen elektronischen Identitätsnachweis nach § 18 des Personalausweisgesetzes, nach § 12 des eID-Karte-Gesetzes oder nach § 78 Absatz 5 des Aufenthaltsgesetzes oder durch ein anderes elektronisches Identifizierungsmittel, welches nach Artikel 6 der Verordnung (EU) Nr. 910/2014 mit dem Sicherheitsniveau „hoch“ im Sinne des Artikels 8 Absatz 2 Buchstabe c der Verordnung (EU) 910/2014 anerkannt worden ist, und

2. im einheitlichen Organisationskonto durch ein sicheres Verfahren nach § 87a Absatz 6 der Abgabenordnung oder durch ein anderes elektronisches Identifizierungsmittel, welches nach Artikel 6 der Verordnung (EU) Nr. 910/2014 mindestens mit dem Sicherheitsniveau „substantiell“ im Sinne des Artikels 8 Absatz 2 Buchstabe b der Verordnung (EU) Nr. 910/2014 anerkannt worden ist.

(5) Über den Nachweis der Identität nach Absatz 4 hinausgehende Anforderungen an die Identifizierung einer Person, die zur Durchführung eines Verwaltungsverfahrens erforderlich sind, bleiben unberührt.

§ 3a Beratungsangebot im Portalverbund

(1) Bund und Länder stellen für Nutzer im Portalverbund eine allgemeine fachunabhängige, barrierearme Beratung für die Abwicklung ihrer über Verwaltungsportale angebotenen, elektronischen Verwaltungsleistungen bereit und bestimmen dafür öffentliche Stellen. Diese öffentlichen Stellen unterstützen Nutzer bei der Abwicklung von Verwaltungsleistungen im Portalverbund.

(2) Die beteiligten Stellen dürfen die von der betroffenen Person übermittelten, zur Aufgabenerfüllung nach Absatz 1 erforderlichen personenbezogenen Daten verarbeiten. Soweit hierzu die Verarbeitung besonderer Kategorien personenbezogener Daten im Sinne des Artikels 9 Absatz 1 der 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 (ABl. L 119 vom 4.5.2016, S. 1; L 314 vom 22.11.2016, S. 72; L 127 vom 23.5.2018, S. 2; L 74 vom 4.3.2021, S. 35) erforderlich ist, dürfen die beteiligten Stellen sie auf Veranlassung des Nutzers verarbeiten. § 22 Absatz 2 des Bundesdatenschutzgesetzes gilt entsprechend.

§ 4 Elektronische Abwicklung von Verwaltungsverfahren; Verordnungsermächtigung

(1) Für die elektronische Abwicklung von Verwaltungsverfahren, die der Durchführung unmittelbar geltender Rechtsakte der Europäischen Union, für die dem Bund die Gesetzgebungskompetenz zusteht, oder der Ausführung von Bundesgesetzen dienen, wird die Bun-

desregierung ermächtigt, im Benehmen mit dem IT-Planungsrat durch Rechtsverordnung ohne Zustimmung des Bundesrates die Verwendung bestimmter IT-Komponenten nach § 2 Absatz 6 verbindlich vorzugeben. In der Rechtsverordnung kann auch die Verwendung von IT-Komponenten geregelt werden, die das jeweils zuständige Bundesministerium bereitstellt. Die Länder können von den in der Rechtsverordnung getroffenen Regelungen durch Landesrecht abweichen, soweit sie für den Betrieb im Portalverbund geeignete IT-Komponenten bereitstellen.

(2) Die Länder sind verpflichtet, die technischen und organisatorischen Voraussetzungen für den Einsatz der nach Absatz 1 vorgegebenen Verfahren sicherzustellen.

(3) Bei der Bereitstellung der IT-Komponenten im Sinne des Absatzes 1 sollen offene Standards und offene Schnittstellen verwendet werden und soll Open-Source-Software vorrangig vor solcher Software eingesetzt werden, deren Quellcode nicht öffentlich zugänglich ist oder deren Lizenz die Verwendung, Weitergabe und Veränderung einschränkt.

§ 5 IT-Sicherheit; Verordnungsermächtigung

Für die im Portalverbund und für die zur Anbindung an den Portalverbund genutzten IT-Komponenten werden die zur Gewährleistung der IT-Sicherheit erforderlichen Standards durch Rechtsverordnung des Bundesministeriums des Innern und für Heimat ohne Zustimmung des Bundesrates festgelegt. Die Einhaltung der Standards der IT-Sicherheit ist für alle Stellen verbindlich, die entsprechende IT-Komponenten nutzen. Von den in der Rechtsverordnung getroffenen Regelungen kann durch Landesrecht nicht abgewichen werden. § 4 Absatz 2 gilt entsprechend.

§ 6 Standards; Verordnungsermächtigungen

(1) Für die informationstechnischen Systeme, die für den übergreifenden informationstechnischen Zugang zu den Verwaltungsleistungen von Bund und Ländern genutzt werden, legt das Bundesministerium des Innern und für Heimat im Einvernehmen mit dem IT-Planungsrat bis zum Ablauf des zweiten auf die Verkündung des Gesetzes vom 19. Juli 2024 (BGBl. 2024 I Nr. 245) folgenden Kalenderjahres durch Rechtsverordnung ohne Zustimmung des Bundesrates die erforderlichen

1. Architekturvorgaben,
2. Qualitätsanforderungen und
3. Interoperabilitätsstandards einschließlich der Prozessmodelle, Datenformate, Transportprotokolle, Schnittstellenbeschreibungen zur Anbindung von Onlineverfahren und Fachverfahren sowie die für die Anbindung von Basisdiensten erforderlichen Schnittstellen

fest.

(2) Für die Abwicklung von Verwaltungsverfahren, die der Durchführung unmittelbar geltender Rechtsakte der Europäischen Union, für die dem Bund die Gesetzgebungskompetenz zusteht, oder der Ausführung von Bundesgesetzen dienen, legt das für den jeweiligen Rechtsakt oder das jeweilige Bundesgesetz zuständige Bundesministerium im Einvernehmen mit dem Bundesministerium des Innern und für Heimat und dem IT-Planungsrat durch Rechtsverordnung ohne Zustimmung des Bundesrates die Vorgaben im Sinne des Absatzes 1 fest.

(3) Die Einhaltung der durch die Rechtsverordnung nach den Absätzen 1 und 2 festgelegten Vorgaben ist für alle Stellen verbindlich, deren Verwaltungsleistungen über den Portalverbund angeboten werden. Von den durch die Rechtsverordnung nach den Absätzen 1 und 2 getroffenen Regelungen kann durch Landesrecht nicht abgewichen werden. § 4 Absatz 2 gilt entsprechend.

(4) Das Bundesministerium des Innern und für Heimat oder die von ihm beauftragte Stelle veröffentlicht in strukturierter Form elektronisch an zentraler Stelle die im Anwendungsbereich des Onlinezugangsgesetzes von Bund und Ländern angewendeten Standards. Zu Schnittstellen von IT-Komponenten sollen Spezifikationen und Dokumentationen in der jeweils aktuellen Fassung veröffentlicht werden. Das Bundesministerium des Innern und für Heimat kann durch Rechtsverordnung mit Zustimmung des Bundesrates die Aufgabe nach Satz 1

1. mit dessen Einvernehmen einem Land oder
2. einer anderen öffentlich-rechtlich getragenen Einrichtung

übertragen.

§ 7 Nutzerfreundlichkeit und Barrierefreiheit

(1) Bund und Länder stellen durch geeignete Maßnahmen die Nutzerfreundlichkeit sowie eine einfache und intuitive Bedienbarkeit des übergreifenden Zugangs zu elektronischen Verwaltungsleistungen, einschließlich der für diesen Zugang relevanten IT-Komponenten, sicher. Nutzer sollen in die Entwicklung neuer elektronischer Angebote einbezogen werden.

(2) Der übergreifende Zugang zu elektronischen Verwaltungsleistungen, einschließlich der für diesen Zugang relevanten IT-Komponenten, ist nach Maßgabe der Barrierefreie-Informationstechnik-Verordnung so zu gestalten, dass sie barrierefrei nutzbar sind.

§ 8 Rechtsgrundlagen der Datenverarbeitung in Nutzerkonten und zu Identifizierungszwecken

(1) Zur Feststellung der Identität des Nutzers eines Bürgerkontos dürfen, soweit dies erforderlich ist, folgende Daten verarbeitet werden:

1. Daten nach § 18 Absatz 3 des Personalausweisgesetzes,
2. die eindeutige Kennung sowie die spezifischen Daten, die von notifizierten elektronischen Identifizierungsmitteln nach der Verordnung (EU) Nr. 910/2014 vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG (ABl. L 257 vom 28.8.2014, S. 73), die zuletzt durch die Richtlinie (EU) 2022/2555 (ABl. L 333 vom 27.12.2022, S. 80) geändert worden ist, übermittelt werden,
3. die eindeutige Kennung, die von sonstigen anerkannten elektronischen Identifizierungsmitteln übermittelt wird, und
4. die Postfachreferenz des Nutzerkontos.

Bei späterer Nutzung des Nutzerkontos mit dem elektronischen Identitätsnachweis nach § 18 des Personalausweisgesetzes, nach § 12 des eID-Karte-Gesetzes oder nach § 78 Absatz 5 des Aufenthaltsgesetzes sind grundsätzlich das dienste- und kartenspezifische Kennzeichen und

die Anschrift zu übermitteln, bei elektronischen Identifizierungsmitteln nach Satz 1 Nummer 2 und 3 nur die jeweilige eindeutige Kennung.

(2) Zur Feststellung der Identität des Nutzers eines Organisationskontos und zur Feststellung der Vertretungs- oder Handlungsbefugnis einer für die Organisation handelnden natürlichen oder juristischen Person dürfen, soweit dies erforderlich ist, folgende Daten verarbeitet werden:

1. Unternehmensbasisdaten nach § 3 des Unternehmensbasisdatenregistergesetzes,
2. Daten nach § 139b Absatz 4a und § 139c Absatz 6a der Abgabenordnung,
3. die eindeutige Kennung sowie spezifische Daten, die von notifizierten elektronischen Identifizierungsmitteln nach der Verordnung (EU) Nr. 910/2014 übermittelt werden,
4. die eindeutige Kennung, die von sonstigen anerkannten elektronischen Identifizierungsmitteln übermittelt wird,
5. die Postfachreferenzen des Nutzerkontos,
6. Daten zur Vertretungs- oder Handlungsbefugnis sowie Daten nach Absatz 1 der für eine Organisation handelnden natürlichen Personen und
7. Daten der Mitglieder des Vertretungsorgans oder der gesetzlichen Vertreter.

Ist ein Mitglied des Vertretungsorgans oder der gesetzliche Vertreter eine juristische Person, so können deren Daten nach diesem Absatz verwendet werden.

(3) Zur Feststellung der Identität eines Nutzers darf die Finanzbehörde, die im Auftrag der obersten Finanzbehörden des Bundes und der Länder das sichere Verfahren nach § 87a Absatz 6 der Abgabenordnung betreibt,

1. die in § 139b Absatz 4a und § 139c Absatz 6a der Abgabenordnung aufgeführten Daten des Bundeszentralamts für Steuern sowie entsprechende, für das Besteuerungsverfahren gespeicherte Daten der Finanzämter bei diesen Finanzbehörden im automatisierten Verfahren auf Veranlassung des Nutzers abrufen und
2. die abgerufenen Daten auf Veranlassung des Nutzers an dessen Nutzerkonto übermitteln.

(4) Daten im Sinne der Absätze 1 und 2 dürfen auf Veranlassung des Nutzers auch zwischen den Nutzerkonten im Portalverbund ausgetauscht werden.

(5) Zur Kommunikation mit dem Nutzer dürfen zusätzlich folgende Daten verarbeitet werden:

1. Anrede,
2. weitere Anschriften,
3. De-Mail-Adresse oder vergleichbare Adresse eines Zustelldienstes eines Mitgliedstaats der Europäischen Union oder eines anderen Vertragsstaats des Abkommens über den Europäischen Wirtschaftsraum nach der Verordnung (EU) Nr. 910/2014,
4. E-Mail-Adresse,
5. Telefon- oder Mobilfunknummer,

6. Telefaxnummer und
7. Kommunikationsinhaltsdaten.

(6) Auf Veranlassung des Nutzers dürfen elektronische Dokumente zu Verwaltungsvorgängen und Status- und Verfahrensinformationen an das Nutzerkonto übermittelt und für Zwecke des Nutzerkontos verarbeitet werden, soweit dies erforderlich ist.

(7) Auf Veranlassung des Nutzers ist eine dauerhafte Speicherung der Daten nach den Absätzen 1, 2, 5 und 6 zulässig. Im Falle der dauerhaften Speicherung muss der Nutzer jederzeit die Möglichkeit haben, das Nutzerkonto und alle gespeicherten Daten selbständig zu löschen. Das Bürgerkonto wird bei zweijähriger Inaktivität des Nutzers automatisch gelöscht. Der Nutzer wird zwei Monate vorher automatisch elektronisch über die anstehende Löschung benachrichtigt. Die elektronische Identifizierung kann jeweils mittels einer einmaligen Abfrage der Identitätsdaten erfolgen.

(8) Die für den jeweiligen Zweck erforderlichen Daten nach den Absätzen 1, 2, 5 und 6 sowie nach § 9 Absatz 1 dürfen auf Veranlassung des Nutzers an die für die Verwaltungsleistung zuständige Behörde, ein Verwaltungsportal oder einen Onlinedienst übermittelt werden und durch diese verarbeitet werden, soweit dies für die Zwecke der Unterstützung bei der Inanspruchnahme elektronischer Verwaltungsleistungen oder deren Abwicklung erforderlich ist. Die Verantwortung für die Zulässigkeit der Übermittlung trägt der Dritte, an den die Daten übermittelt werden. Soweit gesetzlich nichts anderes bestimmt ist, darf der Dritte die Daten nur für den Zweck verarbeiten, zu dessen Erfüllung sie ihm übermittelt werden.

(9) Soweit nach den Absätzen 5 bis 8 Daten verarbeitet werden dürfen, gilt dies auch für besondere Kategorien personenbezogener Daten nach Artikel 9 Absatz 1 der Verordnung (EU) 2016/679. § 22 Absatz 2 des Bundesdatenschutzgesetzes gilt entsprechend.

(10) Für die Verarbeitung personenbezogener Daten im Nutzerkonto nach den Absätzen 1 bis 9 ist die für das Nutzerkonto jeweils zuständige Stelle nach Artikel 4 Nummer 7 der 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; L 314 vom 22.11.2016, S. 72; L 127 vom 23.5.2018, S. 2; L 74 vom 4.3.2021, S. 35) ausschließlich verantwortlich. Teilen sich mehrere Stellen die Zuständigkeit für ein Nutzerkonto, sind diese nach Artikel 26 der Verordnung (EU) 2016/679 gemeinsam verantwortlich.

§ 8a Rechtsgrundlagen der Datenverarbeitung in einem länderübergreifenden Onlinedienst

(1) Die einen länderübergreifenden Onlinedienst betreibende Behörde darf die für die Zwecke der Unterstützung bei der Inanspruchnahme einer elektronischen Verwaltungsleistung, der Offenlegung der Daten aus dem Online-Formular an die jeweils zuständige Behörde sowie der Übermittlung von elektronischen Dokumenten zu Verwaltungsvorgängen an den Nutzer erforderlichen personenbezogenen Daten verarbeiten. Dies gilt auch für die Verarbeitung von besonderen Kategorien personenbezogener Daten im Sinne des Artikels 9 Absatz 1 der Verordnung (EU) 2016/679, soweit diese für das an den länderübergreifenden Onlinedienst angeschlossene Verwaltungsverfahren erforderlich sind. § 22 Absatz 2 des Bundesdatenschutzgesetzes gilt entsprechend.

(2) Die für die Unterstützung bei der Inanspruchnahme einer elektronischen Verwaltungsleistung erforderlichen Daten können im länderübergreifenden Onlinedienst zwischenge-

speichert werden, um dem Nutzer die Möglichkeit zu bieten, das Online-Formular zu einem späteren Zeitpunkt zu vervollständigen, zu korrigieren oder zu löschen. § 22 Absatz 2 des Bundesdatenschutzgesetzes gilt im Rahmen der Zwischenspeicherung besonderer Kategorien personenbezogener Daten im Sinne des Artikels 9 Absatz 1 Verordnung (EU) 2016/679 entsprechend.

(3) Die zwischengespeicherten Daten sind in der Regel nach Ablauf von 30 Tagen nach der letzten Bearbeitung des Online-Formulars durch den Nutzer automatisch zu löschen. Der Nutzer ist über die automatische Löschung der zwischengespeicherten Daten zu seinem Online-Formular vorab zu informieren. Die längerfristige Speicherung von Daten im länderübergreifenden Onlinedienst ist ausnahmsweise zulässig, wenn zu erwarten ist, dass dies für die Unterstützung des Nutzers bei der Inanspruchnahme einer elektronischen Verwaltungsleistung erforderlich ist. In solchen Fällen ist eine angemessene Löschfrist festzulegen. Der Nutzer ist über diese Löschfrist zu informieren.

(4) Verantwortlicher im Sinne von Artikel 4 Nummer 7 der Verordnung (EU) 2016/679 für die Verarbeitung personenbezogener Daten im länderübergreifenden Onlinedienst nach den Absätzen 1 bis 3 ist ausschließlich die den länderübergreifenden Onlinedienst betreibende Behörde. Die datenschutzrechtliche Verantwortlichkeit der Behörde, an die zum Zwecke der Durchführung des Verwaltungsverfahrens personenbezogene Daten übermittelt werden, bleibt unberührt.

§ 9 Bekanntgabe des Verwaltungsaktes

(1) Mit Einwilligung des Nutzers kann ein elektronischer Verwaltungsakt dadurch bekannt gegeben werden, dass er vom Nutzer oder seinem Bevollmächtigten über öffentlich zugängliche Netze von dessen Postfach nach § 2 Absatz 7, das Bestandteil eines Nutzerkontos nach § 2 Absatz 5 ist, abgerufen wird. Die Einwilligung nach Satz 1 gilt als erteilt, sofern der Nutzer nicht im Rahmen der Inanspruchnahme einer elektronischen Verwaltungsleistung eine elektronische Bekanntgabe über ein Postfach im Sinne des § 2 Absatz 7 ausschließt. Die Behörde hat zu gewährleisten, dass der Abruf nur nach Authentifizierung der berechtigten Person möglich ist und dass der elektronische Verwaltungsakt von dieser gespeichert werden kann. Der Verwaltungsakt gilt am vierten Tag nach der Bereitstellung zum Abruf als bekannt gegeben. Im Zweifel hat die Behörde für den Eintritt der Fiktionswirkung die Bereitstellung und den Zeitpunkt der Bereitstellung nachzuweisen. Der Nutzer oder sein Bevollmächtigter wird spätestens am Tag der Bereitstellung zum Abruf über die zu diesem Zweck von ihm angegebene Adresse über die Möglichkeit des Abrufs benachrichtigt. Erfolgt der Abruf vor einer erneuten Bekanntgabe des Verwaltungsaktes, bleibt der Tag des ersten Abrufs für den Zugang maßgeblich.

(2) Die Bundesregierung berichtet dem Deutschen Bundestag und dem Bundesrat bis spätestens 10. Dezember 2025 über die Erfahrungen in der Praxis mit der Bekanntgabe des Verwaltungsaktes über das Postfach.

§ 9a Grundsätze der elektronischen Abwicklung über Verwaltungsportale; Schriftformersatz

(1) Die Abwicklung einer elektronischen Verwaltungsleistung, die der Durchführung unmittelbar geltender Rechtsakte der Europäischen Union, für die dem Bund die Gesetzgebungskompetenz zusteht, oder der Ausführung von Bundesgesetzen dient, über ein Verwaltungsportal nach § 2 Absatz 2 erfolgt nach Maßgabe der Absätze 2 bis 4, soweit nicht durch Bundesgesetz etwas anderes bestimmt ist.

(2) Vor der Abgabe seiner Erklärung ist dem Nutzer Gelegenheit zu geben, die gesamte Erklärung auf Vollständigkeit und Richtigkeit zu prüfen.

(3) Der Nutzer ist durch geeignete Maßnahmen vor einer übereilten Abgabe der Erklärung zu warnen.

(4) Nach der Abgabe seiner Erklärung ist dem Nutzer eine Kopie seiner Erklärung zum Abruf bereitzustellen.

(5) Hat der Nutzer nach § 3 Absatz 4 über ein Nutzerkonto den Identitätsnachweis erbracht und gibt er über ein Verwaltungsportal mittels Online-Formular eine Erklärung ab, für die durch Rechtsvorschrift die Schriftform angeordnet ist, so wird dadurch zugleich die Schriftform ersetzt.

(6) Eine durch Rechtsvorschrift angeordnete Schriftform kann bei elektronischen Verwaltungsakten oder sonstigen elektronischen Dokumenten der Behörde, die an das Postfach eines Nutzerkontos übermittelt werden, auch dadurch ersetzt werden, dass diese mit dem qualifizierten elektronischen Siegel der Behörde versehen werden.

§ 10 Datenschutzcockpit; Verordnungsermächtigung

(1) Ein „Datenschutzcockpit" ist eine IT-Komponente, mit der sich natürliche Personen Auskünfte zu Datenübermittlungen zwischen öffentlichen Stellen anzeigen lassen können. Erfasst werden bis zum Vorliegen der technischen und rechtlichen Voraussetzungen für eine Erfassung weiterer Datenübermittlungen zunächst diejenigen Datenübermittlungen, bei denen eine Identifikationsnummer nach § 5 des Identifikationsnummerngesetzes zum Einsatz kommt.

(2) Im Datenschutzcockpit werden nach Maßgabe von Absatz 4 Satz 3 ausschließlich Protokolldaten nach § 9 des Identifikationsnummerngesetzes einschließlich der dazu durch die Registermodernisierungsbehörde und die Register übermittelten Inhaltsdaten sowie die Bestandsdaten der Register angezeigt. Diese Daten werden im Datenschutzcockpit nur für die Dauer des jeweiligen Nutzungsvorgangs gespeichert; nach Beendigung des Nutzungsvorgangs sind sie unverzüglich zu löschen. Der Auskunftsanspruch nach Artikel 15 der 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; L 314 vom 22.11.2016, S. 72; L 127 vom 23.5.2018, S. 2; L 74 vom 4.3.2021, S. 35) bleibt unberührt. Das Datenschutzcockpit ist aus Sicht des Nutzers einfach und zweckmäßig auszugestalten. Es sind technische und organisatorische Maßnahmen vorzusehen, damit staatliche Eingriffe zum Nachteil des Nutzers nicht möglich sind.

(3) Jede natürliche Person kann sich bei der öffentlichen Stelle, die das Datenschutzcockpit betreibt, für ein Datenschutzcockpit registrieren. Sie hat sich bei der Registrierung und Nutzung des Datenschutzcockpits mit einem Identifizierungsmittel auf dem Vertrauensniveau hoch zu identifizieren. Zur Feststellung der Identität darf bei Registrierung und Nutzung das dienste- und kartenspezifische Kennzeichen verarbeitet werden. Im Übrigen kann sich der Nutzer auch mit einem Nutzerkonto des Portalverbundes beim Datenschutzcockpit registrieren. In diesem Fall darf die für das Nutzerkonto zuständige Stelle das dienste- und kartenspezifische Kennzeichen an die für das Datenschutzcockpit zuständige Stelle übermitteln.

(4) Das Datenschutzcockpit darf die Identifikationsnummer nach § 139b der Abgabenordnung als Identifikator für die Anfrage zur Erhebung und Anzeige der Daten nach Absatz 2 verarbeiten. Zur Anfrage nach § 6 des Identifikationsnummerngesetzes erhebt das Datenschutzcockpit bei der Registrierung des Nutzers folgende Daten:

1. Namen,
2. Vornamen,
3. Anschrift,
4. Geburtsname und
5. Tag der Geburt.

Der Nutzer legt fest, in welchem Umfang das Datenschutzcockpit Protokolldaten einschließlich der übermittelten Inhaltsdaten sowie die Bestandsdaten der Register nach Absatz 2 erheben und anzeigen darf. Auf diese Daten hat nur der Nutzer Zugriff. Der Nutzer muss sein Konto im Datenschutzcockpit jederzeit selbst löschen können. Das Konto im Datenschutzcockpit wird automatisiert gelöscht, wenn es drei Jahre nicht verwendet wurde.

(5) Das Datenschutzcockpit wird von einer öffentlichen Stelle errichtet und betrieben, die durch Rechtsverordnung des Bundesministeriums des Innern und für Heimat im Benehmen mit dem IT-Planungsrat mit Zustimmung des Bundesrates bestimmt wird. Das Nähere zu den technischen Verfahren, den technischen Formaten der Datensätze und den Übertragungswegen legt das Bundesministerium des Innern und für Heimat im Benehmen mit dem IT-Planungsrat mit Zustimmung des Bundesrates durch Rechtsverordnung fest.

§ 11 Monitoring und Evaluierung; Ermittlung der Erfüllungsaufwände

Die für die Verwaltungsdigitalisierung zuständigen Ministerien der Länder und des Bundes

1. führen unter Einbeziehung des IT-Planungsrates beginnend mit dem 24. Juli 2024 fortlaufend ein Monitoring zu der Umsetzung der Vorschriften dieses Gesetzes durch und beauftragen eine fachunabhängige wissenschaftliche Einrichtung, dieses Gesetz alle drei Jahre, erstmals nach Ablauf von drei Jahren nach dem 24. Juli 2024, zu evaluieren und
2. ermitteln im Rahmen der Evaluierung nach Nummer 1 auf der Basis einer Erhebung des IT-Planungsrates zum 1. Januar 2026, zum 1. Januar 2028 und zum 1. Januar 2030 die sich aus diesem Gesetz, dem Gesetz über die Verbindung der informationstechnischen Netze des Bundes und der Länder – Gesetz zur Ausführung von Artikel 91c Absatz 4 des Grundgesetzes – und dem E-Government-Gesetz ergebenden Erfüllungsaufwände, soweit die Vorschriften auch für die Länder gelten. Dies gilt auch für die auf Basis der in diesen Gesetzen enthaltenen Rechtsverordnungsermächtigungen zu erlassenden Rechtsverordnungen mit zukünftiger Wirkung.

Die Evaluationsberichte werden elektronisch veröffentlicht.

§ 12 Übergangsregelungen zu § 3; Verordnungsermächtigungen

(1) Für einen Übergangszeitraum von drei Jahren kann die Identifizierung und Authentifizierung sowie die bidirektionale Kommunikation der Nutzer im Sinne des § 2 Absatz 4 Nummer 1 für elektronische Verwaltungsleistungen im Portalverbund auch über die bisheri-

gen Nutzerkonten und Postfächer der Länder oder eines Fachportals erfolgen. Die Frist nach Satz 1 beginnt an dem Tag, an dem das Bundesministerium des Innern und für Heimat im Einvernehmen mit dem IT-Planungsrat im Bundesgesetzblatt bekanntgibt, dass die Voraussetzungen für eine automatisierte Migration der Länderkonten auf das zentrale Bürgerkonto vorliegen. Das durch den Bund nach § 3 Absatz 1 Satz 1 bereitgestellte zentrale Bürgerkonto soll zu einer DeutschlandID weiterentwickelt werden.

(2) Die nach § 87a Absatz 6 der Abgabenordnung in der Steuerverwaltung bis einschließlich 31. Dezember 2019 eingesetzten sicheren Verfahren werden bundesweit zum Nachweis der Identität auf dem Vertrauensniveau „substantiell" anerkannt.

(3) Abweichend von § 3 Absatz 3 ist von der Verwendung des einheitlichen Organisationskontos abzusehen, wenn für die Inanspruchnahme einer elektronischen Verwaltungsleistung und die sonstige elektronische Kommunikation ausnahmsweise ein höheres Vertrauensniveau erforderlich ist.

(4) Öffentliche Stellen sind von der Verpflichtung nach § 3 Absatz 3 bis einschließlich 31. Dezember 2031 ausgenommen in Bezug auf elektronische Verwaltungsleistungen, die der Durchführung

1. der Verordnung (EU) 2021/1060 des Europäischen Parlaments und des Rates vom 24. Juni 2021 mit gemeinsamen Bestimmungen für den Europäischen Fonds für regionale Entwicklung, den Europäischen Sozialfonds Plus, den Kohäsionsfonds, den Fonds für einen gerechten Übergang und den Europäischen Meeres-, Fischerei- und Aquakulturfonds sowie mit Haushaltsvorschriften für diese Fonds und für den Asyl-, Migrations- und Integrationsfonds, den Fonds für die innere Sicherheit und das Instrument für finanzielle Hilfe im Bereich Grenzverwaltung und Visumpolitik (ABl. L 231 vom 30.6.2021, S. 159), die zuletzt durch die Verordnung (EU) 2023/435 des Europäischen Parlaments und des Rates vom 27. Februar 2023 zur Änderung der Verordnung (EU) 2021/241 in Bezug auf REPowerEU-Kapitel in den Aufbau- und Resilienzplänen und zur Änderung der Verordnungen (EU) Nr. 1303/2013, (EU) 2021/1060 und (EU) 2021/1755 sowie der Richtlinie 2003/87/EG (ABl. L 63 vom 28.2.2023, S. 1) geändert worden ist,
2. der Verordnung (EU) 2021/2115 des Europäischen Parlaments und des Rates vom 2. Dezember 2021 mit Vorschriften für die Unterstützung der von den Mitgliedstaaten im Rahmen der Gemeinsamen Agrarpolitik zu erstellenden und durch den Europäischen Garantiefonds für die Landwirtschaft (EGFL) und den Europäischen Landwirtschaftsfonds für die Entwicklung des ländlichen Raums (ELER) zu finanzierenden Strategiepläne (GAP-Strategiepläne) und zur Aufhebung der Verordnung (EU) Nr. 1305/2013 sowie der Verordnung (EU) Nr. 1307/2013 (ABl. L 435 vom 6.12.2021, S. 1), die zuletzt durch die Delegierte Verordnung (EU) 2022/648 der Kommission vom 15. Februar 2022 (ABl. L 119 vom 21.4.2022, S. 1) geändert worden ist, und
3. der Verordnung (EU) 2021/2116 des Europäischen Parlaments und des Rates vom 2. Dezember 2021 über die Finanzierung, Verwaltung und Überwachung der Gemeinsamen Agrarpolitik und zur Aufhebung der Verordnung (EU) Nr. 1306/2013 (ABl. L 435 vom 6.12.2021, S. 187), die zuletzt durch die Delegierte Verordnung (EU) 2022/1408 der Kommission vom 16. Juni 2022 (ABl. L 216 vom 19.8.2022, S. 1) geändert worden ist, dienen.

(5) Wird der Nachweis der Identität nach § 3 Absatz 4 Nummer 1 Buchstabe b erbracht, so kann die spätere Authentisierung des Nutzers auch durch Authentisierungsmittel nach § 10 Absatz 3a des Personalausweisgesetzes erfolgen.

VERORDNUNG (EU) 2018/1724 DES EUROPÄISCHEN PARLAMENTS UND DES RATES*

vom 2. Oktober 2018

über die Einrichtung eines einheitlichen digitalen Zugangstors zu Informationen, Verfahren, Hilfs- und Problemlösungsdiensten und zur Änderung der Verordnung (EU) Nr. 1024/2012

(Text von Bedeutung für den EWR)

Inhaltsübersicht

* Sog. „Single-Digital-Gateway-Verordnung" (SDG-VO).

[Vom Abdruck der Erwägungsgründe wurde abgesehen]

KAPITEL I
ALLGEMEINE BESTIMMUNGEN

Artikel 1
Gegenstand

(1) Mit dieser Verordnung werden Vorschriften festgelegt für

a) die Einrichtung und den Betrieb eines einheitlichen digitalen Zugangstors, um Bürgern und Unternehmen einfachen Zugang zu hochwertigen Informationen, effizienten Verfahren und wirksamen Hilfs- und Problemlösungsdiensten im Zusammenhang mit Unions- und nationalen Vorschriften für Bürger und Unternehmen, die ihre Rechte aus dem Unionsrecht im Bereich Binnenmarkt im Sinne von Artikel 26 Absatz 2 AEUV ausüben oder ausüben wollen, zu verschaffen;

b) die Inanspruchnahme von Verfahren durch grenzüberschreitende Nutzer und die Umsetzung des Grundsatzes der einmaligen Erfassung bei den in Anhang II dieser Verordnung aufgeführten Verfahren und den in den Richtlinien 2005/36/EG, 2006/123/EG, 2014/24/EU und 2014/25/EU vorgesehenen Verfahren;

c) die Berichterstattung über Hindernisse auf dem Binnenmarkt, beruhend auf der Einholung von Rückmeldungen der Nutzer und der Erhebung von Statistiken bei den Diensten, die von dem Zugangstor abgedeckt werden.

(2) Widerspricht diese Verordnung einer Bestimmung eines anderen Rechtsaktes der Union, der bestimmte Aspekte des Gegenstands dieser Verordnung regelt, so hat die Bestimmung des anderen Rechtsaktes der Union Vorrang.

(3) Diese Verordnung berührt nicht den Inhalt der Verfahren, die auf der Ebene der Union oder auf nationaler Ebene in irgendeinem der unter diese Verordnung fallenden Bereiche festgelegt sind, oder die Rechte, die im Rahmen dieser Verfahren gewährt werden. Ferner berührt diese Verordnung keine Maßnahmen, die gemäß dem Unionsrecht zur Gewährleistung der Cybersicherheit und zur Verhinderung von missbräuchlichem Verhalten ergriffen werden.

Artikel 2
Einrichtung des einheitlichen digitalen Zugangstors

(1) Die Kommission und die Mitgliedstaaten richten gemäß dieser Verordnung ein einheitliches digitales Zugangstor (im Folgenden „Zugangstor“) ein. Das Zugangstor besteht aus einer von der Kommission verwalteten gemeinsamen Nutzerschnittstelle (im Folgenden „gemeinsame Nutzerschnittstelle“), die in das Portal „Ihr Europa“ integriert wird und Zugang zu einschlägigen Unions- und nationalen Websites bietet.

(2) Das Zugangstor ermöglicht den Zugang zu:

a) Informationen über Rechte, Pflichten und Vorschriften nach dem Unionsrecht und nach nationalem Recht, die für Bürger und Unternehmen gelten, die ihre Rechte aus dem Unionsrecht im Bereich Binnenmarkt in den in Anhang I angegebenen Bereichen ausüben oder ausüben wollen;

b) Informationen über Online- und Offline-Verfahren und Links zu Online-Verfahren, einschließlich der Verfahren im Sinne des Anhangs II, auf der Ebene der Union oder auf nationaler Ebene, um die Bürger in die Lage zu versetzen, die Rechte im Zusammenhang mit dem Binnenmarkt in den in Anhang I angegebenen Bereichen, wahrzunehmen und die entsprechenden Pflichten und Vorschriften einzuhalten;

c) Informationen über und Links zu den in Anhang III aufgeführten oder in Artikel 7 genannten Hilfs- und Problemlösungsdiensten, und an die Bürger und Unternehmen sich bei Fragen oder Problemen im Zusammenhang mit ihren Rechten, Pflichten, Vorschriften oder den in Buchstabe a oder b des vorliegenden Absatzes genannten Verfahren wenden können.

(3) Die gemeinsame Nutzerschnittstelle ist in allen Amtssprachen der Union zugänglich.

Artikel 3
Begriffsbestimmungen

Für die Zwecke dieser Verordnung bezeichnet der Ausdruck:

1. „Nutzer“ einen Bürger der Union, eine natürliche Person, die in einem Mitgliedstaat ansässig ist oder eine juristische Person mit Sitz in einem Mitgliedstaat, der bzw. die über das Zugangstor auf die in Artikel 2 Absatz 2 genannten Informationen, Verfahren oder Hilfs- oder Problemlösungsdienste zugreift;

2. „grenzüberschreitender“ Nutzer einen Nutzer, der sich in einer Situation befindet, die nicht in jeder Hinsicht auf einen einzigen Mitgliedstaat begrenzt ist;

3. „Verfahren“ eine Abfolge von Maßnahmen, die die Nutzer ergreifen müssen, um den Anforderungen zu entsprechen oder einen Beschluss einer zuständigen Behörde zu erwirken, um ihre Rechte nach Artikel 2 Absatz 2 Buchstabe a ausüben zu können;

4. „zuständige Behörde“ jede Stelle oder Behörde eines Mitgliedstaats auf nationaler, regionaler oder lokaler Ebene mit bestimmten Zuständigkeiten für die unter diese Verordnung fallenden Informationen, Verfahren, Hilfs- und Problemlösungsdienste;

5. „Nachweis“ alle Unterlagen oder Daten, einschließlich Text- oder Ton-, Bild- oder audiovisuellen Aufzeichnungen, unabhängig vom verwendeten Medium, die von einer zuständigen Behörde verlangt werden, um Sachverhalte oder die Einhaltung der in Artikel 2 Absatz 2 Buchstabe b genannten Verfahrensvorschriften nachzuweisen.

KAPITEL II
ZUGANGSTOR-DIENSTE

Artikel 4
Zugang zu Informationen

(1) Die Mitgliedstaaten stellen sicher, dass die Nutzer auf ihren nationalen Internetseiten über einen einfachen Online-Zugang zu folgenden Informationen verfügen:

a) Informationen über die in Artikel 2 Absatz 2 Buchstabe a genannten Rechte, Pflichten und Vorschriften, die aus dem nationalen Recht abgeleitet sind;

b) Informationen über die in Artikel 2 Absatz 2 Buchstabe b genannten, auf nationaler Ebene eingerichteten Verfahren;

c) Informationen über die in Artikel 2 Absatz 2 Buchstabe c genannten, auf nationaler Ebene bereitgestellten Hilfs- und Problemlösungsdienste.

(2) Die Kommission stellt sicher, dass die Nutzer durch das Portal „Ihr Europa“ einen einfachen Online-Zugang zu folgenden Informationen verfügen:

a) Informationen über die in Artikel 2 Absatz 2 Buchstabe a genannten Rechte, Pflichten und Vorschriften, die aus dem Unionsrecht abgeleitet sind;

b) Informationen über die in Artikel 2 Absatz 2 Buchstabe b genannten, auf Unionsebene eingerichteten Verfahren;

c) Informationen über die in Artikel 2 Absatz 2 Buchstabe c genannten, auf Unionsebene bereitgestellten Hilfs- und Problemlösungsdienste.

Artikel 5
Zugang zu Informationen, die nicht in Anhang I enthalten sind

(1) Die Mitgliedstaaten und die Kommission können Links zu Informationen bereitstellen, die nicht in Anhang I aufgeführt sind und die von den zuständigen Behörden, der Kommis-

sion oder den Einrichtungen und sonstigen Stellen der Union angeboten werden, sofern diese Informationen in den Wirkungsbereich des Portals gemäß Artikel 1 Absatz 1 Buchstabe a fallen und den Qualitätsanforderungen des Artikels 9 entsprechen.

(2) Die Links zu den Informationen gemäß Absatz 1 des vorliegenden Artikels werden gemäß Artikel 19 Absätze 2 und 3 bereitgestellt.

(3) Bevor die Kommission die Links aktiviert prüft sie, ob die Bedingungen des Absatzes 1 erfüllt sind, und konsultiert die Koordinierungsgruppe für das Zugangstor.

Artikel 6
Verfahren, die vollständig online bereitzustellen sind

(1) Jeder Mitgliedstaat stellt sicher, dass die Nutzer vollständigen Online-Zugang zu allen in Anhang II aufgeführten Verfahren haben und diese vollständig online abwickeln können, sofern das jeweilige Verfahren in dem betreffenden Mitgliedstaat eingerichtet worden ist.

(2) Die in Absatz 1 genannten Verfahren gelten als vollständig online abzuwickeln, wenn

a) die Identifizierung der Nutzer, die Bereitstellung von Informationen und die Vorlage von Nachweisen, die Signierung und die endgültige Einreichung elektronisch aus der Ferne, sie über einen Dienstkanal erfolgen können, der die Nutzer in die Lage versetzt, die Anforderungen im Zusammenhang mit dem Verfahren in nutzerfreundlicher und strukturierter Weise zu erfüllen;

b) die Nutzer eine automatische Empfangsbestätigung erhalten, es sei denn, das Ergebnis des Verfahrens wird sofort übermittelt,

c) das Ergebnis des Verfahrens elektronisch oder — soweit zur Einhaltung geltender Vorschriften des Rechts der Union oder des nationalen Rechts erforderlich — physisch übermittelt wird, und

d) die Nutzer eine elektronische Benachrichtigung über den Abschluss des Verfahrens erhalten.

(3) Wenn der angestrebte Zweck in begründeten Ausnahmefällen aus übergeordneten Gründen des öffentlichen Interesses in den Bereichen öffentliche Sicherheit, öffentliche Gesundheit oder Bekämpfung missbräuchlichen Verhaltens, nicht vollständig online erreicht werden kann, können die Mitgliedstaaten verlangen, dass der Nutzer für einzelne Verfahrensschritte persönlich bei der zuständigen Behörde vorstellig wird. In solchen Ausnahmefällen beschränken die Mitgliedstaaten diese physische Anwesenheit auf das unbedingt notwendige objektiv gerechtfertigte Maß und stellen sicher, dass andere Verfahrensschritte vollständig online abgewickelt werden können. Die Mitgliedstaaten stellen auch sicher, dass diese Anforderungen der physischen Anwesenheit nicht zu einer Diskriminierung grenzüberschreitender Nutzer führen.

(4) Die Mitgliedstaaten übermitteln und erläutern in einer gemeinsamen, der Kommission und den anderen Mitgliedstaaten zugänglichen Ablage die Gründe, aus denen, und die Umstände unter denen die physische Anwesenheit für die in Absatz 3 genannten Verfahrensschritte erforderlich sein könnte sowie die Gründe, aus denen, und die Umstände unter denen eine physische Übermittlung gemäß Absatz 2 Buchstabe c erforderlich ist.

(5) Dieser Artikel hindert die Mitgliedstaaten nicht daran, Nutzern die zusätzliche Möglichkeit zu bieten, auf die in Artikel 2 Absatz 2 Buchstabe b genannten Verfahren anders als on-

line zuzugreifen und diese anders als online abzuwickeln, oder Nutzer direkt zu kontaktieren.

Artikel 7
Zugang zu Hilfs- und Problemlösungsdiensten

(1) Die Mitgliedstaaten und die Kommission stellen sicher, dass die Nutzer, einschließlich der grenzüberschreitenden Nutzer, online über verschiedene Kanäle leicht auf die in Artikel 2 Absatz 2 Buchstabe c genannten Hilfs- und Problemlösungsdienste zugreifen können.

(2) Die in Artikel 28 genannten nationalen Koordinatoren und die Kommission können gemäß Artikel 19 Absätze 2 und 3 Links zu Hilfs- und Problemlösungsdiensten bereitstellen, die von zuständigen Behörden, der Kommission oder von Einrichtungen und sonstigen Stellen der Union angeboten werden -und nicht in Anhang III aufgeführt sind, wenn diese Dienste den Qualitätsanforderungen der Artikel 11 und 16 entsprechen.

(3) Falls zur Erfüllung des Nutzerbedarfs erforderlich, kann der nationale Koordinator der Kommission vorschlagen, dass Links zu Hilfs- oder Problemlösungsdiensten, die von privaten oder halböffentlichen Einrichtungen bereitgestellt werden, in das Zugangstor einbezogen werden, sofern diese Dienste folgenden Anforderungen entsprechen:

a) sie bieten Informationen oder Hilfestellung in den Bereichen und für die Zwecke, die Gegenstand der vorliegenden Verordnung sind, und ergänzen die bereits in das Zugangstor einbezogenen Dienste;

b) sie werden kostenlos oder zu einem für Kleinstunternehmen, gemeinnützige Organisationen und Bürger erschwinglichen Preis angeboten; und

c) sie entsprechen den Anforderungen der Artikel 8, 11 und 16.

(4) Hat der nationale Koordinator die Einbeziehung eines Links gemäß Absatz 3 des vorliegenden Artikels vorgeschlagen und einen solchen Link gemäß Artikel 19 Absatz 3 bereitgestellt, so prüft die Kommission, ob die Bedingungen des Absatzes 3 des vorliegenden Artikels von dem zu verlinkenden Dienst erfüllt werden, und wenn das zutrifft, aktiviert sie den Link.

Stellt die Kommission fest, dass die in Absatz 3 genannten Bedingungen von dem zu verlinkenden Dienst nicht erfüllt werden, unterrichtet sie den nationalen Koordinator über die Gründe für die Nichtaktivierung des Links.

Artikel 8
Qualitätsanforderungen an die Webzugänglichkeit

Die Kommission macht diejenigen ihrer Websites und Webseiten, über die sie Zugang zu den Informationen nach Artikel 4 Absatz 2 und zu den Hilfs- und Problemlösungsdiensten nach Artikel 7 gewährt, besser zugänglich, indem sie diese wahrnehmbar, bedienbar, verständlich und robust gestaltet.

KAPITEL III
QUALITÄTSANFORDERUNGEN

ABSCHNITT 1
Qualitätsanforderungen im Zusammenhang mit Informationen über Rechte, Pflichten und Vorschriften, über Verfahren und über Hilfs- und Problemlösungsdienste

Artikel 9
Qualität von Informationen über Rechte, Pflichten und Vorschriften

(1) Sind die Mitgliedstaaten und die Kommission gemäß Artikel 4 für die Gewährleistung des Zugangs zu Informationen nach Artikel 2 Absatz 2 Buchstabe a zuständig, so stellen sie sicher, dass diese Informationen folgenden Anforderungen genügen:

a) Sie müssen nutzerfreundlich sein, damit die Nutzer die Informationen leicht finden und verstehen können und in der Lage sind zu erkennen, welche Informationen für ihre jeweilige Situation relevant sind;

b) Sie müssen genau und umfassend genug sein, um die Informationen abzudecken, die die Nutzer haben müssen, um ihre Rechte unter vollständiger Einhaltung der geltenden Vorschriften und Pflichten auszuüben;

c) gegebenenfalls enthalten sie Verweise auf bzw. Links zu Rechtsvorschriften, technischen Spezifikationen und Leitfäden;

d) sie enthalten die Bezeichnung der zuständigen Behörde oder Stelle, die für den Inhalt der Informationen verantwortlich ist;

e) sie enthalten die Kontaktangaben von allen relevanten Hilfs- oder Problemlösungsdiensten, wie z. B. eine Telefonnummer, eine E-Mail-Adresse, ein Online-Kontaktformular oder andere häufig verwendete elektronische Kommunikationsmittel, das für die Art des angebotenen Dienstes und die Zielgruppe dieses Dienstes am besten geeignet ist;

f) sie enthalten das Datum der letzten Aktualisierung der Informationen, falls vorhanden, oder wenn die Informationen nicht aktualisiert wurden, das Veröffentlichungsdatum der Informationen;

g) sie sind gut strukturiert und so dargestellt, dass die Nutzer die benötigten Informationen schnell finden können;

h) sie sind auf dem neuesten Stand; und

i) sie sind in klarer und verständlicher Sprache abgefasst, die dem Bedarf der potenziellen Nutzer angepasst ist.

(2) Die Mitgliedstaaten stellen die in Absatz 1 des vorliegenden Artikels genannten Informationen gemäß Artikel 12 in einer Amtssprache der Union zur Verfügung, die von der größtmöglichen Anzahl grenzüberschreitender Nutzer weitgehend verstanden wird.

Artikel 10
Qualität der Informationen über Verfahren

(1) Zur Erfüllung der Anforderungen des Artikels 4 stellen die Mitgliedstaaten und die Kommission sicher, dass Nutzer, gegebenenfalls bevor sie sich vor der Einleitung des Verfahrens ausweisen müssen, Zugang zu einer hinreichend umfassenden, klaren und nutzerfreundlichen Erklärung folgender Elemente der in Artikel 2 Absatz 2 Buchstabe b genannten Verfahren haben:

a) der relevanten Schritte des Verfahrens, die der Nutzer zu unternehmen hat, einschließlich etwaiger Ausnahmen gemäß Artikel 6 Absatz 3 von der Pflicht der Mitgliedstaaten, das Verfahren vollständig online bereitzustellen;

b) der Bezeichnung der zuständigen Behörde, die für das Verfahren zuständig ist, einschließlich ihrer Kontaktdaten;

c) der für das Verfahren zulässigen Mittel zur Authentifizierung, Identifizierung und Unterzeichnung;

d) der Art und des Formats der vorzulegenden Nachweise;

e) der Rechtsbehelfe, die im Falle von Streitigkeiten mit den zuständigen Behörden im Allgemeinen zur Verfügung stehen;

f) der anfallenden Gebühren und der Online-Zahlungsmethoden;

g) etwaiger Fristen, die vom Nutzer oder von der zuständigen Behörde einzuhalten sind, und wenn es keine Fristen gibt, der durchschnittlichen, geschätzten oder voraussichtlichen Zeit, die die zuständige Behörde zur Abwicklung des Verfahrens benötigt;

h) etwaiger Vorschriften über oder Rechtsfolgen für die Nutzer, die sich aus einer nicht erfolgten Antwort der zuständigen Behörde ergeben, einschließlich Reglungen zur Genehmigungsfiktion oder andere Verschweigensregelungen;

i) jeder zusätzlichen Sprache, in der das Verfahren abgewickelt werden kann.

(2) Liegen keine Regelungen zur Genehmigungsfiktion oder sonstige Verschweigensregelungen oder ähnliche Regelungen vor, so unterrichten die zuständigen Behörden die Nutzer gegebenenfalls über etwaige Verzögerungen und Fristverlängerungen oder die sich daraus ergebenden Folgen.

(3) Wenn die in Absatz 1 genannte Erklärung den nicht grenzüberschreitenden Nutzern bereits zur Verfügung steht, so kann sie für die Zwecke dieser Verordnung verwendet bzw. wiederverwendet werden, sofern sie gegebenenfalls auch die Situation der grenzüberschreitenden Nutzer berücksichtigt.

(4) Die Mitgliedstaaten stellen die in Absatz 1 des vorliegenden Artikels genannten Erklärungen gemäß Artikel 12 in einer Amtssprache der Union zur Verfügung, die von der größtmöglichen Anzahl grenzüberschreitender Nutzer weitgehend verstanden wird.

Artikel 11
Qualität der Informationen über Hilfs- und Problemlösungsdienste

(1) Zur Erfüllung der Anforderungen des Artikels 4 stellen die Mitgliedstaaten und die Kommission sicher, dass die Nutzer, bevor sie einen Antrag auf Erbringung eines Dienstes

nach Artikel 2 Absatz 2 Buchstabe c stellen, Zugang zu einer klaren und nutzerfreundlichen Erklärung folgender Elemente haben:

a) Art, Zweck und erwarteter Ergebnisse des angebotenen Dienstes;

b) Kontaktangaben der für den Dienst zuständigen Stellen, wie z. B. eine Telefonnummer, eine E-Mail-Adresse, ein Online-Formular oder ein anderes häufig verwendetes elektronisches Kommunikationsmittel, das für die Art des angebotenen Dienstes und die Zielgruppe dieses Dienstes am besten geeignet ist;

c) gegebenenfalls anfallende Gebühren und die Online-Zahlungsmethoden;

d) etwaige geltende Fristen, die einzuhalten sind, und wenn es keine Fristen gibt, die durchschnittlichen oder die für die Erbringung des Dienstes voraussichtlich erforderliche Zeit;

e) jede zusätzliche Sprache, in der die Anfrage gestellt werden kann und die für anschließende Kontakte verwendet werden kann.

(2) Die Mitgliedstaaten stellen die in Absatz 1 des vorliegenden Artikels genannten Erklärungen gemäß Artikel 12 in einer Amtssprache der Union zur Verfügung, die von der größtmöglichen Anzahl grenzüberschreitender Nutzer weitgehend verstanden wird.

Artikel 12
Übersetzung der Informationen

(1) Stellt ein Mitgliedstaat die in den Artikeln 9, 10 und 11 sowie die in Artikel 13 Absatz 2 Buchstabe a genannten Informationen, Erklärungen und Anweisungen nicht in einer Amtssprache der Union zur Verfügung, die von der größtmöglichen Anzahl grenzüberschreitender Nutzer weitgehend verstanden wird, so beantragt der Mitgliedstaat bei der Kommission Übersetzungen in diese Sprache im Rahmen der verfügbaren Haushaltsmittel der Union gemäß Artikel 32 Absatz 1 Buchstabe c.

(2) Die Mitgliedstaaten stellen sicher, dass die gemäß Absatz 1 des vorliegenden Artikels zur Übersetzung eingereichten Texte mindestens die grundlegenden Informationen in allen in Anhang I genannten Bereichen abdecken sowie, falls ausreichende Haushaltsmittel der Union verfügbar sind, alle weiteren Informationen, Erläuterungen und Anweisungen gemäß den Artikeln 9, 10 und 11 sowie Artikel 13 Absatz 2 Buchstabe a, unter Berücksichtigung der dringendsten Bedürfnisse der grenzüberschreitenden Nutzer. Die Mitgliedstaaten stellen die Links zu diesen übersetzten Informationen in der in Artikel 19 genannten Linkablage bereit.

(3) Die in Absatz 1 genannte Sprache ist die Amtssprache der Union, die von den Nutzern in der gesamten Union am häufigsten als Fremdsprache erlernt wird. Wenn die zu übersetzenden Informationen, Erläuterungen oder Anweisungen voraussichtlich von überwiegendem Interesse für grenzüberschreitende Nutzer aus einem anderen Mitgliedstaat sind, kann die in Absatz 1 genannte Sprache ausnahmsweise die Amtssprache der Union sein, die von diesen grenzüberschreitenden Nutzern als Erstsprache genutzt wird.

(4) Beantragt ein Mitgliedstaat eine Übersetzung in eine Amtssprache der Union, die nicht die von den Nutzern in der gesamten Union am häufigsten erlernte Fremdsprache ist, so begründet er seinen Antrag. Stellt die Kommission fest, dass die in Absatz 3 genannten Bedingungen für die Wahl einer solchen anderen Sprache nicht erfüllt sind, kann sie den Antrag ablehnen und setzt den Mitgliedstaat unter Angabe der Gründe in Kenntnis.

ABSCHNITT 2
Anforderungen an Online-Verfahren

Artikel 13
Grenzüberschreitender Zugang zu Online-Verfahren

(1) Die Mitgliedstaaten stellen sicher, dass ein auf nationaler Ebene festgelegtes Verfahren nach Artikel 2 Absatz 2 Buchstabe b, auf das nicht grenzüberschreitende Nutzer online zugreifen und das sie online abwickeln können, auch grenzüberschreitenden Nutzern auf nichtdiskriminierende Art mit Hilfe derselben oder einer alternativen technischen Lösung online zugänglich ist und von diesen online abgewickelt werden kann.

(2) Die Mitgliedstaaten stellen sicher, dass für die in Absatz 1 dieses Artikels genannten Verfahren mindestens die folgenden Anforderungen erfüllt werden:

a) Die Nutzer können auf die Anweisungen zur Abwicklung des Verfahrens in einer Amtssprache der Union zugreifen, die gemäß Artikel 12 von der größtmöglichen Anzahl grenzüberschreitender Nutzer weitgehend verstanden wird.

b) Grenzüberschreitenden Nutzern ist es möglich, die geforderten Informationen einzureichen, auch wenn die Struktur dieser Informationen von ähnlichen Informationen in dem betreffenden Mitgliedstaat abweicht.

c) Den grenzüberschreitenden Nutzern ist es möglich, sich in allen Fällen, in denen das auch für nicht grenzüberschreitende Nutzer möglich ist, gemäß der Verordnung (EU) Nr. 910/2014 elektronisch auszuweisen und zu authentifizieren, Unterlagen zu unterzeichnen oder mit einem Siegel zu versehen.

d) Den grenzüberschreitenden Nutzern ist es möglich, in allen Fällen, in denen das auch für nicht grenzüberschreitende Nutzer möglich ist, die Nachweise für die Erfüllung der geltenden Anforderungen in elektronischem Format zu erbringen und das Ergebnis der Verfahren in elektronischem Format zu erhalten.

e) Wenn zur Abwicklung eines Verfahrens eine Zahlung erforderlich ist, können die Nutzer alle Gebühren online über weithin verfügbare grenzüberschreitende Zahlungsdienste ohne Diskriminierung aufgrund des Niederlassungsorts des Zahlungsdienstleisters, des Ausstellungsorts des Zahlungsinstruments oder des Standorts des Zahlungskontos in der Union bezahlen.

(3) Erfordert das Verfahren keine elektronische Identifizierung oder Authentifizierung im Sinne von Absatz 2 Buchstabe c und dürfen die zuständigen Behörden gemäß den geltenden nationalen Rechtsvorschriften oder Verwaltungsgepflogenheiten digitalisierte Kopien nichtelektronischer Identitätsnachweise, etwa von Personalausweisen oder Pässen, bei nicht grenzüberschreitenden Nutzern zulassen, so lassen diese Behörden solche digitalisierten Kopien auch bei grenzüberschreitenden Nutzern zu.

Artikel 14
Technisches System für den grenzüberschreitenden automatisierten Austausch von Nachweisen und Anwendung des Grundsatzes der einmaligen Erfassung („Once Only Principle“)

(1) Zum Zwecke des Austauschs von Nachweisen für die in Anhang II dieser Verordnung aufgeführten Online-Verfahren sowie für die Verfahren nach den Richtlinien 2005/36/EG, 2006/123/EG, 2014/24/EU und 2014/25/EU richtet die Kommission in Zusammenarbeit mit den Mitgliedstaaten ein technisches System für den automatisierten Austausch von Nachweisen zwischen zuständigen Behörden in verschiedenen Mitgliedstaaten (im Folgenden „technisches System“) ein.

(2) Wenn die zuständigen Behörden in ihrem eigenen Mitgliedstaat rechtmäßig Nachweise, die für die in Absatz 1 genannten Online-Verfahren von Belang sind, in einem elektronischen Format ausstellen, das einen automatisierten Austausch ermöglicht,, stellen sie diese Nachweise auch den anfordernden zuständigen Behörden aus anderen Mitgliedstaaten in einem elektronischen Format zur Verfügung, das einen automatisierten Austausch ermöglicht.

(3) Das technische System muss insbesondere

a) auf ausdrückliches Ersuchen des Nutzers die Verarbeitung von Anträgen auf Ausstellung von Nachweisen ermöglichen,

b) die Verarbeitung von Anträgen auf Ausstellung von Nachweisen ermöglichen, die zugänglich gemacht oder ausgetauscht werden sollen,

c) die Übermittlung von Nachweisen zwischen den zuständigen Behörden zulassen,

d) die Verarbeitung der Nachweise durch die anfordernde zuständige Behörde zulassen,

e) die Vertraulichkeit und Integrität der Nachweise sicherstellen,

f) dem Nutzer die Möglichkeit bieten, die von der anfordernden zuständigen Behörde zu verwendenden Nachweise vorab einzusehen und zu entscheiden, ob er mit dem Austausch von Nachweisen fortfährt oder nicht,

g) ein angemessenes Maß an Interoperabilität mit anderen einschlägigen Systemen sicherstellen,

h) ein hohes Maß an Sicherheit für die Übermittlung und Verarbeitung von Nachweisen sicherstellen,

i) sicherstellen, dass Nachweise nicht über das für den Austausch von Nachweisen technisch notwendige Maß hinaus und auch dann nur solange verarbeitet werden, wie es der Zweck erfordert.

(4) Die Verwendung des technischen Systems ist für den Nutzer nicht verbindlich und ist nur auf sein ausdrückliches Ersuchen gestattet, sofern in den Rechtsvorschriften der Union oder der einzelnen Mitgliedstaaten nicht anders vorgesehen. Dem Nutzer wird gestattet, die Nachweise auf andere Weise als über das technische System und unmittelbar an die anfordernde zuständige Behörde zu übermitteln.

(5) Die Möglichkeit, den Nachweis gemäß Absatz 3 Buchstabe f des vorliegenden Artikels vorab einzusehen, ist nicht erforderlich bei Verfahren, bei denen der automatisierte grenzüberschreitende Datenaustausch ohne eine solche Vorschau gemäß den gelten Rechtsvorschriften der Union oder der Mitgliedstaaten erlaubt ist. Diese Möglichkeit einer Vorschau von Nachweisen berührt nicht die Pflicht, die Informationen gemäß den Artikeln 13 und 14 der Verordnung (EU) 2016/679 mitzuteilen/zu übermitteln.

(6) Die Mitgliedstaaten binden das voll funktionsfähige technische System in die in Absatz 1 genannten Verfahren ein.

(7) Die für die Online-Verfahren nach Absatz 1 zuständigen Behörden fordern — auf das freiwillig, für den konkreten Fall, nach Aufklärung und unmissverständlich bekundete ausdrückliche Ersuchen des betroffenen Nutzers — über das technische System Nachweise unmittelbar bei den zuständigen Behörden an, die in anderen Mitgliedstaaten Nachweise ausstellen. Die in Absatz 2 genannten ausstellenden zuständigen Behörden stellen diese Nachweise gemäß Absatz 3 Buchstabe e über dasselbe System bereit.

(8) Die der anfordernden zuständigen Behörde bereitgestellten Nachweise müssen auf das beschränkt sein, was angefordert wurde, und dürfen von dieser Behörde nur für die Zwecke des Verfahrens benutzt werden, für das die Nachweise ausgetauscht wurden. Die über das technische System ausgetauschten Nachweise gelten für die Zwecke der anfordernden zuständigen Behörde als echt.

(9) Die Kommission erlässt bis zum 12. Juni 2021 Durchführungsrechtsakte, um die technischen und operativen Spezifikationen des — für die Durchführung dieses Artikels erforderlichen — technischen Systems festzulegen. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 37 Absatz 2 genannten Prüfverfahren erlassen.

(10) Die Absätze 1 bis 8 gelten nicht für auf Unionsebene festgelegte Verfahren, die unterschiedliche Mechanismen für den Austausch von Nachweisen vorsehen, es sei denn das für die Umsetzung dieses Artikels erforderliche technische System ist gemäß den Vorschriften der Rechtsakte der Union, mit denen diese Verfahren festgelegt wurden, in sie eingebunden.

(11) Die Kommission und jeder Mitgliedstaat sind für die Entwicklung, die Verfügbarkeit, die Wartung, die Kontrolle, die Überwachung und das Sicherheitsmanagement ihrer jeweiligen Teile des technischen Systems verantwortlich.

Artikel 15
Überprüfung von Nachweisen zwischen den Mitgliedstaaten

Wenn das technische System oder andere für den Austausch oder die Überprüfung von Nachweisen zwischen den Mitgliedstaaten geeignete Systeme nicht verfügbar oder nicht anwendbar sind oder wenn der Nutzer nicht um die Verwendung des technischen Systems ersucht, arbeiten die zuständigen Behörden bei Bedarf über das Binnenmarkt-Informationssystem (IMI) zusammen, wenn das erforderlich ist, um die Echtheit der Nachweise zu überprüfen, die einer von ihnen für die Zwecke eines Online-Verfahrens vom Nutzer in elektronischem Format vorgelegt wurden.

ABSCHNITT 3
Qualitätsanforderungen an Hilfs- und Problemlösungsdienste

Artikel 16
Qualitätsanforderungen an Hilfs- und Problemlösungsdienste

Die zuständigen Behörden und die Kommission stellen im Rahmen ihrer jeweiligen Zuständigkeiten sicher, dass die in Anhang III aufgeführten Hilfe- und Problemlösungsdienste und diejenigen Dienste, die gemäß Artikel 7 Absätze 2, 3 und 4 in das Zugangstor einbezogen wurden, folgenden Qualitätsanforderungen entsprechen:

a) Sie werden innerhalb einer angemessenen Frist unter Berücksichtigung der Komplexität des Ersuchens erbracht.

b) Im Falle einer Fristverlängerung werden die Nutzer vorab über die Gründe hierfür und über die neue Frist informiert.

c) Ist zur Erbringung eines Dienstes eine Zahlung erforderlich, ist es Nutzern möglich, alle Gebühren ohne Diskriminierung aufgrund des Niederlassungsorts des Zahlungsdienstleisters, des Ausstellungsorts des Zahlungsinstruments oder des Standorts des Zahlungskontos in der Union online über weithin verfügbare grenzüberschreitende Zahlungsdienste zu bezahlen.

ABSCHNITT 4
Qualitätsüberwachung

Artikel 17
Qualitätsüberwachung

(1) Die in Artikel 28 genannten nationalen Koordinatoren und die Kommission überwachen im Rahmen ihrer jeweiligen Zuständigkeiten regelmäßig die Einhaltung der Qualitätsanforderungen der Artikel 8 bis 13 und 16 durch die über das Zugangstor bereitgestellten Informationen, Verfahren und Hilfs- und Problemlösungsdienste. Die Überwachung wird anhand der nach den Artikeln 24 und 25 gesammelten Daten durchgeführt.

(2) Im Falle einer Verschlechterung der Qualität der in Absatz 1 genannten, von den zuständigen Behörden bereitgestellten Informationen, Verfahren und Hilfs- und Problemlösungsdienste ergreift die Kommission unter Berücksichtigung der Schwere und des Fortbestehens der Verschlechterung mindestens eine der folgenden Maßnahmen:

a) Sie unterrichtet den entsprechenden nationalen Koordinator und ersucht ihn um Abhilfemaßnahmen.

b) Sie stellt in der Koordinierungsgruppe für das Zugangstor empfohlene Maßnahmen zur Verbesserung der Einhaltung der Qualitätsanforderungen zur Diskussion.

c) Sie sendet ein Schreiben mit Empfehlungen an den betreffenden Mitgliedstaat.

d) Sie nimmt die Information, das Verfahren oder den Hilfs- oder Problemlösungsdienst vorübergehend aus dem Zugangstor.

(3) Erfüllt ein Hilfs- oder Problemlösungsdienst, zu dem gemäß Artikel 7 Absatz 3 Links zur Verfügung gestellt werden, durchweg nicht die Anforderungen der Artikel 11 und 16 oder entspricht er nicht mehr dem Bedarf der Nutzer, der aus den gemäß den Artikeln 24 und 25 erhobenen Daten hervorgeht, kann die Kommission nach Rücksprache mit dem zuständigen nationalen Koordinator und erforderlichenfalls der Koordinierungsgruppe für das Zugangstor diesen Dienst von dem Zugangstor trennen.

KAPITEL IV
TECHNISCHE LÖSUNGEN

Artikel 18
Gemeinsame Nutzerschnittstelle

(1) Die Kommission stellt in enger Zusammenarbeit mit den Mitgliedstaaten eine in das Portal „Ihr Europa" integrierte gemeinsame Nutzerschnittstelle zur Verfügung, um das reibungslose Funktionieren des Zugangstors zu gewährleisten.

(2) Die gemeinsame Nutzerschnittstelle ermöglicht den Zugang zu den Informationen, Verfahren und Hilfs- oder Problemlösungsdiensten mithilfe von Links zu den entsprechenden Websites oder Webseiten auf Unions- oder nationaler Ebene, die in der in Artikel 19 genannten Linkablage enthalten sind.

(3) Die Mitgliedstaaten und die Kommission, die entsprechend ihren jeweiligen Rollen und Zuständigkeiten gemäß Artikel 4 tätig werden, stellen sicher, dass die Informationen über Vorschriften und Pflichten, über Verfahren und über Hilfs- und Problemlösungsdienste so organisiert und gekennzeichnet sind, dass sie über die gemeinsame Nutzerschnittstelle besser auffindbar sind.

(4) Die Kommission stellt sicher, dass die gemeinsame Nutzerschnittstelle die nachstehenden Qualitätsanforderungen erfüllt:

a) Sie ist leicht zu nutzen.

b) Sie ist online über verschiedene elektronische Geräte zugänglich.

c) Sie ist für verschiedene Internetbrowser entwickelt und optimiert.

d) Sie erfüllt folgende Anforderungen für einen barrierefreien Internetzugang: Wahrnehmbarkeit, Bedienbarkeit, Verständlichkeit und Robustheit.

(5) Die Kommission kann Durchführungsrechtsakte erlassen, in denen die Anforderungen an die Interoperabilität zur Verbesserung der Auffindbarkeit von Informationen über Vorschriften und Pflichten, über Verfahren und über Hilfs- und Problemlösungsdienste mit Hilfe der gemeinsamen Nutzerschnittstelle festgelegt sind. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 37 Absatz 2 genannten Prüfverfahren erlassen.

Artikel 19
Linkablage

(1) Die Kommission richtet in enger Zusammenarbeit mit den Mitgliedstaaten eine elektronische Linkablage zu den in Artikel 2 Absatz 2 genannten Informationen, Verfahren und Hilfs- und Problemlösungsdiensten ein, die die Verbindung zwischen solchen Diensten und der gemeinsamen Nutzerschnittstelle ermöglichen, und unterhält diese Ablage.

(2) Die Kommission stattet die Linkablage mit Links zu den Informationen, Verfahren und Hilfs- und Problemlösungsdiensten aus, die auf den auf Unionsebene verwalteten Internetseiten zur Verfügung stehen, und stellt sicher, dass diese Links korrekt und aktuell sind.

(3) Die nationalen Koordinatoren statten die Linkablage mit Links zu den Informationen, Verfahren und Hilfs- und Problemlösungsdiensten aus, die auf den von den zuständigen Behörden oder privaten oder halböffentlichen Einrichtungen gemäß Artikel 7 Absatz 3 verwalteten Internetseiten zur Verfügung stehen, und stellen sicher, dass diese Links korrekt und aktuell sind.

(4) Soweit technisch möglich, kann die Ausstattung mit Links gemäß Absatz 3 zwischen den einschlägigen Systemen der Mitgliedstaaten und der Linkablage automatisiert erfolgen.

(5) Die Kommission stellt die in der Linkablage enthaltenen Informationen in einem offenen und maschinenlesbaren Format öffentlich zur Verfügung.

(6) Die Kommission und die nationalen Koordinatoren stellen sicher, dass es bei den über das Zugangstor angebotenen Links zu Informationen, Verfahren und Hilfs- oder Problemlösungsdiensten nicht zu unnötigen teilweisen oder vollständigen Überschneidungen und Überlagerungen kommt, die Nutzer wahrscheinlich verwirren würden.

(7) Wenn die Bereitstellung von Informationen gemäß Artikel 4 in anderen Bestimmungen des Unionsrechts festgelegt ist, können die Kommission und die nationalen Koordinatoren Links zu diesen Informationen zur Verfügung stellen, um den Anforderungen des genannten Artikels zu entsprechen.

Artikel 20
Gemeinsame Suchmaschine für Hilfsdienste

(1) Um den Zugang zu den in Anhang III aufgeführten oder in Artikel 7 Absätze 2 und 3 genannten Hilfs- und Problemlösungsdiensten zu erleichtern, stellen die zuständigen Behörden und die Kommission sicher, dass die Nutzer über eine über das Zugangstor verfügbare gemeinsame Suchmaschine für Hilfs- und Problemlösungsdienste (im Folgenden „gemeinsame Suchmaschine für Hilfsdienste“) auf sie zugreifen können.

(2) Die Kommission entwickelt und verwaltet die gemeinsame Suchmaschine für Hilfsdienste und beschließt die Struktur und das Format, in dem die Beschreibungen und Kontaktangaben der Hilfs- und Problemlösungsdienste bereitgestellt werden müssen, um das reibungslose Funktionieren der gemeinsamen Suchmaschine für Hilfsdienste sicherzustellen.

(3) Die nationalen Koordinatoren stellen die in Absatz 2 genannten Beschreibungen und Kontaktangaben der Kommission zur Verfügung.

Artikel 21
Zuständigkeiten für die IKT-Anwendungen zur Unterstützung des Zugangstors

(1) Die Kommission ist verantwortlich für die Entwicklung, Verfügbarkeit, Überwachung, Aktualisierung, Wartung, Sicherheit und Bereitstellung folgender IKT-Anwendungen und Internetseiten:

a) das in Artikel 2 Absatz 1 genannte Portal „Ihr Europa“,

b) die in Artikel 18 Absatz 1 genannte gemeinsame Nutzerschnittstelle, einschließlich der Suchmaschine oder aller anderen IKT-Instrumente, die die Durchsuchbarkeit von Online-Informationen und -Diensten ermöglichen,

c) die in Artikel 19 Absatz 1 genannte Linkablage,

d) die in Artikel 20 Absatz 1 genannte gemeinsame Suchmaschine für Hilfsdienste,

e) die in Artikel 25 Absatz 1 und Artikel 26 Absatz 1 Buchstabe a genannten Instrumente für Rückmeldungen der Nutzer.

Die Kommission arbeitet in enger Zusammenarbeit mit den Mitgliedstaaten an der Entwicklung der IKT-Anwendungen.

(2) Die Mitgliedstaaten sind verantwortlich für die Entwicklung, Verfügbarkeit, Überwachung, Aktualisierung, Wartung und Sicherheit der IKT-Anwendungen im Zusammenhang mit den von ihnen verwalteten und mit der gemeinsamen Nutzerschnittstelle verbundenen nationalen Websites und Webseiten.

KAPITEL V
ÖFFENTLICHKEITSARBEIT

Artikel 22
Name, Logo und Qualitätssiegel

(1) Der Name, unter dem das Zugangstor in der Öffentlichkeit vorgestellt und bekannt gemacht werden soll, lautet „Your Europe".

Das Logo, unter dem das Zugangstor in der Öffentlichkeit vorgestellt und bekannt gemacht werden soll, wird von der Kommission in enger Zusammenarbeit mit der Koordinierungsgruppe für das Zugangstor festgelegt, und zwar spätestens bis zum 12. Juni 2019.

Das Logo des Zugangstors und ein Link zu dem Zugangstor werden auf den mit dem Zugangstor verbundenen einschlägigen Websites auf nationaler und auf Unionsebene sichtbar und verfügbar gemacht.

(2) Als Nachweis der Erfüllung der Qualitätsanforderungen der Artikel 9, 10 und 11 dienen der Name und das Logo des Zugangstors auch als Qualitätssiegel. Das Logo des Zugangstors wird jedoch ausschließlich als Qualitätssiegel von Webseiten und Websites, die in der in Artikel 19 genannten Linkablage enthalten sind, verwendet.

Artikel 23
Öffentlichkeitsarbeit

(1) Die Mitgliedstaaten und die Kommission fördern die Bekanntheit des Zugangstors und seine Nutzung bei Bürgern und Unternehmen und gewährleisten, dass das Zugangstor und seine Informationen, Verfahren und Hilfsdienste für die Öffentlichkeit sichtbar sind und über Suchmaschinen, die für die Öffentlichkeit zugänglich sind, leicht gefunden werden können.

(2) Die Mitgliedstaaten und die Kommission koordinieren ihre Öffentlichkeitsarbeit nach Absatz 1 und nehmen bei derartigen Maßnahmen gegebenenfalls mit Angabe anderer Markennamen Bezug auf das Zugangstor und verwenden sein Logo.

(3) Die Mitgliedstaaten und die Kommission stellen sicher, dass das Zugangstor über die verbundenen Websites, für die sie verantwortlich sind, leicht zu finden ist und dass eindeutige Links zur gemeinsamen Nutzerschnittstelle auf allen einschlägigen Websites auf nationaler und Unionsebene verfügbar sind.

(4) Die nationalen Koordinatoren machen das Zugangstor bei den zuständigen nationalen Behörden bekannt.

KAPITEL VI
EINHOLUNG VON RÜCKMELDUNGEN DER NUTZER UND ERHEBUNG VON STATISTIKEN

Artikel 24
Nutzerstatistiken

(1) Die zuständigen Behörden und die Kommission stellen sicher, dass Statistiken über die Aufrufe des Zugangstors und der mit dem Zugangstor verknüpften Internetseiten durch Nutzer — unter Wahrung von deren Anonymität- erhoben werden, um die Funktionsweise des Zugangstors zu verbessern.

(2) Die zuständigen Behörden, die Anbieter von Hilfs- und Problemlösungsdiensten nach Artikel 7 Absatz 3 und die Kommission erheben in aggregierter Form die Anzahl, den Ursprung und den Gegenstand von Anfragen nach Hilfs- und Problemlösungsdiensten sowie deren Antwortzeiten und tauschen sie aus.

(3) Die Statistiken, die gemäß den Absätzen 1 und 2 über Informationen, Verfahren und Hilfs- und Problemlösungsdienste, die mit dem Zugangstor verknüpft sind, erhoben werden, enthalten folgende Datenkategorien:

a) Daten zur Anzahl, Herkunft und Art der Nutzer des Zugangstors,

b) Daten zu Nutzerpräferenzen und Nutzerpfaden,

c) Daten zur Benutzerfreundlichkeit, Auffindbarkeit und Qualität der Informationen, Verfahren und Hilfs- und Problemlösungsdienste.

Diese Daten werden der Öffentlichkeit in einem offenen und weithin verwendeten maschinenlesbaren Format zur Verfügung gestellt.

(4) Die Kommission erlässt Durchführungsrechtsakte zur Festlegung der Erhebungs- und Austauschmethode für Nutzerstatistiken nach den Absätzen 1, 2 und 3 des vorliegenden Artikels. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 37 Absatz 2 genannten Prüfverfahren erlassen.

Artikel 25
Rückmeldungen der Nutzer zu den Diensten des Zugangstors

(1) Um Informationen über ihre Zufriedenheit mit den im Zugangstor bereitgestellten Diensten und Informationen unmittelbar von den Nutzern einzuholen, stellt die Kommission den Nutzern über das Zugangstor ein benutzerfreundliches Instrument für Rückmeldungen zur Verfügung, das es ihnen ermöglicht, unmittelbar nach der Nutzung eines der in Artikel 2 Absatz 2 genannten Dienste anonym zur Qualität und Verfügbarkeit der über das

Zugangstor erbrachten Dienste und der darin bereitgestellten Informationen sowie zur gemeinsamen Nutzerschnittstelle Stellung zu nehmen.

(2) Die zuständigen Behörden und die Kommission gewährleisten den Nutzern den Zugang zu dem in Absatz 1 genannten Instrument auf allen Internetseiten, die Teil des Zugangstors sind.

(3) Die Kommission, die zuständigen Behörden und die nationalen Koordinatoren haben unmittelbaren Zugang zu den Rückmeldungen, die über das in Absatz 1 genannte Instrument eingeholt werden, um auf alle angesprochenen Probleme einzugehen.

(4) Die zuständigen Behörden sind nicht verpflichtet, den Nutzern auf ihren Internetseiten, die Teil des Zugangstors sind, Zugang zu dem in Absatz 1 genannten Instrument für Nutzer-Rückmeldungen zu geben, wenn bereits ein anderes Instrument für Nutzer -Rückmeldungen mit ähnlichen Funktionen, wie das in Absatz 1 genannte Instrument für Rückmeldungen, auf ihren Internetseiten zur Überwachung der Qualität der Dienste zur Verfügung steht. Die zuständigen Behörden sammeln die über ihr eigenes Instrument eingeholten Rückmeldungen der Nutzer und stellen diese der Kommission und den nationalen Koordinatoren der anderen Mitgliedstaaten zur Verfügung.

(5) Die Kommission erlässt Durchführungsrechtsakte zur Festlegung der Vorschriften für die Einholung und den Austausch der Nutzer- Rückmeldungen. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 37 Absatz 2 genannten Prüfverfahren erlassen.

Artikel 26
Bericht über die Funktionsweise des Binnenmarkts

(1) Die Kommission

a) stellt für Nutzer des Zugangstors ein benutzerfreundliches Instrument bereit, damit sie jegliche Hindernisse, auf die sie bei der Ausübung ihrer Binnenmarktrechte gestoßen sind, anonym melden und dazu Rückmeldung geben können,

b) holt bei den Hilfs- und Problemlösungsdiensten, die Teil des Zugangstors sind, aggregierte Informationen über den Gegenstand von Anfragen und Antworten ein.

(2) Die Kommission, die zuständigen Behörden und die nationalen Koordinatoren haben unmittelbaren Zugang zu den gemäß Absatz 1 Buchstabe a eingeholten Rückmeldungen.

(3) Die Mitgliedstaaten und die Kommission analysieren und untersuchen die von den Nutzern gemäß diesem Artikel angesprochenen Probleme und gehen wo immer möglich mit geeigneten Mitteln auf sie ein.

Artikel 27
Online-Gesamtübersichten

Die Kommission veröffentlicht online anonymisierte Gesamtübersichten über die Probleme, die sich aus den nach Artikel 26 Absatz 1 eingeholten Informationen, den in Artikel 24 genannten wesentlichen Nutzerstatistiken und den in Artikel 25 genannten wichtigsten Rückmeldungen der Nutzer ergeben.

KAPITEL VII
VERWALTUNG DES ZUGANGSTORS

Artikel 28
Nationale Koordinatoren

(1) Jeder Mitgliedstaat ernennt einen nationalen Koordinator. Neben ihren Pflichten gemäß den Artikeln 7, 17, 19, 20, 23 und 25 üben die nationalen Koordinatoren folgende Funktionen aus:

a) Sie dienen als Kontaktstelle für ihre jeweiligen Verwaltungen für alle Fragen im Zusammenhang mit dem Zugangstor.

b) Sie fördern die einheitliche Anwendung der Artikel 9 bis 16 durch ihre jeweiligen zuständigen Behörden.

c) Sie stellen sicher, dass die in Artikel 17 Absatz 2 Buchstabe c genannten Empfehlungen korrekt umgesetzt werden.

(2) Jeder Mitgliedstaat kann entsprechend seiner internen Verwaltungsstruktur einen oder mehrere Koordinatoren zur Erfüllung der in Absatz 1 aufgeführten Aufgaben ernennen. Ein nationaler Koordinator je Mitgliedstaat ist für die Kontakte mit der Kommission in allen Fragen im Zusammenhang mit dem Zugangstor verantwortlich.

(3) Jeder Mitgliedstaat teilt den anderen Mitgliedstaaten und der Kommission den Namen und die Kontaktangaben seines nationalen Koordinators mit.

Artikel 29
Koordinierungsgruppe

Es wird eine Koordinierungsgruppe (im Folgenden „Koordinierungsgruppe für das Zugangstor“) eingerichtet. Sie besteht aus einem nationalen Koordinator aus jedem Mitgliedstaat unter Vorsitz eines Vertreters der Kommission. Sie gibt sich eine Geschäftsordnung. Die Sekretariatsgeschäfte werden von der Kommission geführt.

Artikel 30
Aufgaben der Koordinierungsgruppe für das Zugangstor

(1) Die Koordinierungsgruppe für das Zugangstor unterstützt die Ausführung dieser Verordnung. Insbesondere

a) erleichtert sie den Austausch über bewährte Verfahren und ihre regelmäßige Aktualisierung,

b) fördert sie die Akzeptanz von vollständig online abzuwickelnden Verfahren zusätzlich zu den in Anhang II der vorliegenden Verordnung aufgeführten Verfahren und von Online-Systemen für die Authentifizierung, die Identifizierung und für Signaturen, insbesondere gemäß der Verordnung (EU) Nr. 910/2014,

c) erörtert sie Verbesserungen der benutzerfreundlichen Darstellung von Informationen in den in Anhang I aufgeführten Bereichen, vor allem auf der Grundlage der gemäß den Artikeln 24 und 25 erhobenen Daten,

d) unterstützt sie die Kommission bei der Entwicklung gemeinsamer IKT-Lösungen für das Zugangstor,

e) erörtert sie den Entwurf des jährlichen Arbeitsprogramms,

f) unterstützt sie die Kommission bei der Überwachung der Durchführung des jährlichen Arbeitsprogramms,

g) erörtert sie zusätzliche Informationen, die gemäß Artikel 5 zur Verfügung gestellt werden, um andere Mitgliedstaaten darin zu bestärken, den Nutzern bei Bedarf ähnliche Informationen zur Verfügung zu stellen,

h) unterstützt sie die Kommission gemäß Artikel 17 bei der Überwachung der Erfüllung der Anforderungen der Artikel 8 bis 16,

i) informiert sie über die Umsetzung von Artikel 6 Absatz 1,

j) erörtert sie Maßnahmen und empfiehlt den zuständigen Behörden und der Kommission, um unnötige Überschneidungen bei den über das Zugangstor verfügbaren Diensten zu vermeiden oder zu beseitigen,

k) gibt sie Stellungnahmen zu Verfahren oder Maßnahmen ab, um wirkungsvoll auf Probleme mit der Qualität der Dienste, die von Nutzern zur Sprache gebracht wurden, einzugehen oder Vorschläge zu deren Verbesserung zu machen,

l) erörtert sie die Umsetzung der Grundsätze der eingebauten Sicherheit und des eingebauten Datenschutzes im Rahmen dieser Verordnung,

m) erörtert sie Probleme im Zusammenhang mit der Einholung der Rückmeldungen der Nutzer und der Erhebung von Statistiken gemäß den Artikeln 24 und 25, damit die von der Union und auf nationaler Ebene angebotenen Dienste stetig verbessert werden,

n) erörtert sie Fragen im Zusammenhang mit den Qualitätsanforderungen der über das Zugangstor angebotenen Dienste,

o) tauscht sie sich über bewährte Verfahren aus und unterstützt die Kommission bei der Organisation, Struktur und Darstellung der in Artikel 2 Absatz 2 genannten Dienste, damit für das reibungslose Funktionieren der gemeinsamen Nutzerschnittstelle gesorgt ist,

p) erleichtert sie die Entwicklung und Umsetzung der koordinierten Öffentlichkeitsarbeit,

q) arbeitet sie mit den Verwaltungsstellen oder Netzwerken von Informations-, Hilfs- oder Problemlösungsdiensten zusammen,

r) stellt sie Leitfäden zu der zusätzlichen Amtssprache bzw. den zusätzlichen Amtssprachen der Union für den Gebrauch durch die zuständigen Behörden gemäß Artikel 9 Absatz 2, Artikel 10 Absatz 4, Artikel 11 Absatz 2 und Artikel 13 Absatz 2 Buchstabe a zur Verfügung.

(2) Die Kommission kann die Koordinierungsgruppe für das Zugangstor zu allen Fragen im Zusammenhang mit der Anwendung dieser Verordnung konsultieren.

Artikel 31
Jährliches Arbeitsprogramm

(1) Die Kommission verabschiedet das jährliche Arbeitsprogramm, in dem insbesondere Folgendes festgelegt ist:

a) Maßnahmen zur Verbesserung der Darstellung von bestimmten Informationen in den in Anhang I aufgeführten Bereichen und Maßnahmen zur Erleichterung der raschen Erfüllung der Anforderung, Informationen bereitzustellen, durch die zuständigen Behörden auf allen Ebenen, auch auf Kommunalebene,

b) Maßnahmen zur Erleichterung der Einhaltung der Artikel 6 und 13,

c) Maßnahmen zur Sicherstellung der konsequenten Erfüllung der Anforderungen der Artikel 9 bis 12,

d) Tätigkeiten im Zusammenhang mit der Öffentlichkeitsarbeit für das Zugangstor gemäß Artikel 23.

(2) Bei der Erstellung des Entwurfs des jährlichen Arbeitsprogramms berücksichtigt die Kommission die gemäß den Artikeln 24 und 25 erstellten Nutzerstatistiken und eingeholten Rückmeldungen der Nutzer sowie etwaige Vorschläge der Mitgliedstaaten. Vor der Verabschiedung legt die Kommission den Entwurf des jährlichen Arbeitsprogramms der Koordinierungsgruppe für das Zugangstor zur Erörterung vor.

KAPITEL VIII
SCHLUSSBESTIMMUNGEN

Artikel 32
Kosten

(1) Der Gesamthaushalt der Europäischen Union deckt folgende Kosten ab:

a) Entwicklung und Wartung der IKT-Instrumente zur Unterstützung der Ausführung dieser Verordnung auf Unionsebene,

b) Öffentlichkeitsarbeit für das Zugangstor auf Unionsebene,

c) Übersetzung der Informationen, Erklärungen und Anweisungen gemäß Artikel 12 unter Einhaltung einer jährlichen Höchstmenge je Mitgliedstaat, unbeschadet einer möglichen Neuzuweisung, soweit erforderlich, um die vollständige Verwendung der verfügbaren Haushaltsmittel zu ermöglichen.

(2) Die Kosten im Zusammenhang mit nationalen Internetportalen, Informationsplattformen, Hilfsdiensten und Verfahren auf Ebene der Mitgliedstaaten werden aus den jeweiligen Haushalten der Mitgliedstaaten finanziert, sofern in Rechtsvorschriften der Union nicht anders vorgesehen.

Artikel 33
Schutz personenbezogener Daten

Die Verarbeitung personenbezogener Daten durch die zuständigen Behörden im Rahmen dieser Verordnung erfolgt gemäß der Verordnung (EU) 2016/679. Die Verarbeitung perso-

nenbezogener Daten durch die Kommission im Rahmen der vorliegenden Verordnung erfolgt gemäß der Verordnung (EU) 2018/1725.

Artikel 34
Zusammenarbeit mit anderen Informations- und Hilfsnetzen

(1) Nach Rücksprache mit den Mitgliedstaaten entscheidet die Kommission, welche bestehenden informellen Verwaltungsregelungen für die in Anhang III aufgeführten Hilfs- oder Problemlösungsdienste oder für die in Anhang I angegebenen Informationsbereiche in die Zuständigkeit der Koordinierungsgruppe für das Zugangstor fallen.

(2) Sind die Informations- und Hilfsdienste oder -netze durch einen verbindlichen Rechtsakt der Union für einen der in Anhang I aufgeführten Informationsbereiche geschaffen worden, so koordiniert die Kommission die Arbeit der Koordinierungsgruppe für das Zugangstor und der Verwaltungsgremien solcher Dienste oder Netze zum Zweck der Erzielung von Synergieeffekten und zur Vermeidung von Überschneidungen.

Artikel 35
Binnenmarkt-Informationssystem

(1) Für die Zwecke und nach Maßgabe von Artikel 6 Absatz 4 und Artikel 15 wird das mit der Verordnung (EU) Nr. 1024/2012 geschaffene Binnenmarkt-Informationssystem (IMI) genutzt.

(2) Die Kommission kann beschließen, das IMI als die in Artikel 19 Absatz 1 genannte elektronische Linkablage zu nutzen.

Artikel 36
Berichterstattung und Überprüfung

Spätestens am 12. Dezember 2022 und danach alle zwei Jahre überprüft die Kommission die Anwendung dieser Verordnung und legt dem Europäischen Parlament und dem Rat einen Bewertungsbericht über die Funktionsweise des Zugangstors und die Funktionsweise des Binnenmarktes auf der Grundlage der nach den Artikeln 24, 25 und 26 erhobenen Statistiken und eingeholten Rückmeldungen vor. In der Überprüfung wird insbesondere der Geltungsbereich von Artikel 14 überprüft, unter Berücksichtigung der technologischen, marktbezogenen und rechtlichen Entwicklungen im Zusammenhang mit dem Austausch von Nachweisen zwischen den zuständigen Behörden.

Artikel 37
Ausschussverfahren

(1) Die Kommission wird von einem Ausschuss unterstützt. Dieser Ausschuss ist ein Ausschuss im Sinne der Verordnung (EU) Nr. 182/2011.

(2) Wird auf diesen Absatz Bezug genommen, gilt Artikel 5 der Verordnung (EU) Nr. 182/2011.

Artikel 38
Änderung der Verordnung (EU) Nr. 1024/2012

[Vom Abdruck wurde abgesehen.]

Artikel 39
Inkrafttreten

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

Artikel 2, Artikel 4, Artikel 7 bis12, Artikel 16 Artikel 17, Artikel 18 Absätze 1 bis 4, Artikel 19, Artikel 20, Artikel 24 Absätze 1, 2 und 3, Artikel 25 Absätze 1 bis 4, Artikel 26 und Artikel 27 gelten ab dem 12. Dezember 2020.

Artikel 6, Artikel 13, Artikel 14 Absätze 1 bis 8 und 10 und Artikel 15 gelten ab dem 12. Dezember 2023.

Ungeachtet des Datums der Anwendung der Artikel 2, 9, 10 und 11 stellen die Kommunalbehörden die in diesen Artikeln genannten Informationen, Erklärungen und Anweisungen spätestens bis zum 12. Dezember 2022 zur Verfügung.

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

ANHANG I
Liste der in Artikel 2 Absatz 2 Buchstabe a genannten Informationsbereiche, die für Bürger und Unternehmen relevant sind, die ihre Binnenmarktrechte ausüben

Informationsbereiche im Zusammenhang mit Bürgern

Bereich	INFORMATIONEN ZU RECHTEN, PFLICHTEN UND VORSCHRIFTEN AUS DEM UNIONSRECHT UND DEM NATIONALEN RECHT
A. Reisen innerhalb der Union	1. Dokumente, die von Unionsbürgern, ihren Familienmitgliedern, die keine Unionsbürger sind, allein reisenden Minderjährigen und Nicht-Unionsbürgern bei grenzüberschreitenden Reisen innerhalb der Union verlangt werden (Personalausweis, Visum, Pass) 2. Rechte und Pflichten von Flug-, Zug-, Schiffs- und Busreisenden in und aus der Union und von Personen, die Pauschalreisen oder verbundene Reiseleistungen in Anspruch nehmen 3. Hilfeleistung bei eingeschränkter Mobilität bei Reisen in und aus der Union 4. Mitnahme von Tieren, Pflanzen,

	Alkohol, Tabak, Zigaretten und anderen Waren bei Reisen in der Union 5. Anrufe und Versand und Empfang von elektronischen Nachrichten und elektronischen Daten innerhalb der Union
B. Arbeit und Ruhestand innerhalb der Union	1. Arbeitssuche in einem anderen Mitgliedstaat 2. Aufnahme einer Beschäftigung in einem anderen Mitgliedstaat 3. Anerkennung von Qualifikationen zum Zwecke der Beschäftigung in einem anderen Mitgliedstaat 4. Besteuerung in einem anderen Mitgliedstaat 5. Haftungs- und Pflichtversicherungsbestimmungen im Zusammenhang mit der Niederlassung oder Beschäftigung in einem anderen Mitgliedstaat 6. Gesetzlich oder durch Rechtsverordnung geregelte Beschäftigungsbedingungen — auch für entsandte Arbeitnehmer — (einschließlich Informationen über Arbeitsstunden, bezahlten Urlaub, Urlaubsansprüche, Rechte und Pflichten bei Überstunden, Gesundheitskontrollen, Beendigung von Verträgen, Kündigung oder Entlassungen) 7. Gleichbehandlung (Vorschriften zum Verbot von Diskriminierung am Arbeitsplatz, über gleiche Entlohnung für Männer und Frauen und über gleiche Entlohnung für Beschäftigte mit befristeten oder unbefristeten Arbeitsverträgen) 8. Gesundheits- und Sicherheitsvorschriften im Zusammenhang mit verschiedenen Arten von Tätigkeiten 9. Rechte und Pflichten im Bereich der sozialen Sicherheit in der

	Union, auch im Zusammenhang mit Renten
C. Fahrzeuge in der Union	1. Vorübergehende oder dauerhafte Mitnahme eines Kraftfahrzeugs in einen anderen Mitgliedstaat 2. Erwerb und Verlängerung eines Führerscheins 3. Abschluss einer Kfz-Pflichtversicherung 4. Kauf und Verkauf eines Kraftfahrzeugs in einem anderen Mitgliedstaat 5. Nationale Verkehrsvorschriften und Anforderungen an Fahrer, einschließlich allgemeiner Vorschriften für die Nutzung der nationalen Straßenverkehrsinfrastruktur: zeitabhängige Gebühren (Vignette), entfernungsabhängige Gebühren (Maut), Emissionsplaketten
D. Wohnsitz in einem anderen Mitgliedstaat	1. Vorübergehender oder dauerhafter Umzug in einen anderen Mitgliedstaat 2. Kauf und Verkauf von Immobilien, einschließlich aller Bedingungen und Pflichten im Zusammenhang mit der Besteuerung, dem Eigentum oder der Nutzung von Immobilien (auch als Zweitwohnsitz) 3. Teilnahme an Kommunalwahlen und Wahlen zum Europäischen Parlament 4. Anforderungen in Bezug auf Aufenthaltskarten für Unionsbürger und ihre Familienmitglieder, einschließlich Familienmitglieder, die keine Unionsbürger sind 5. Voraussetzungen für die Einbürgerung von Staatsangehörigen eines anderen Mitgliedstaats

	6. Vorschriften für den Todesfall, einschließlich solcher über die Überführung der sterblichen Überreste in einen anderen Mitgliedstaat
E. Bildung oder Praktikum in einem anderen Mitgliedstaat	1. Bildungswesen in einem anderen Mitgliedstaat, einschließlich der frühkindlichen Betreuung, Bildung und Erziehung, der Primar- und Sekundarschulbildung, der Hochschulbildung und der Erwachsenenbildung 2. Freiwilligendienst in einem anderen Mitgliedstaat 3. Praktika in einem anderen Mitgliedstaat 4. Forschungstätigkeit in einem anderen Mitgliedstaat als Teil eines Bildungsprogramms
F. Medizinische Versorgung	1. Medizinische Behandlung in einem anderen Mitgliedstaat 2. Kauf von verordneten Arzneimitteln in einem anderen Mitgliedstaat als dem, in dem die Verordnung ausgestellt wurde, online oder vor Ort 3. Krankenversicherungsbestimmungen für kurze oder längere Aufenthalte in einem anderen Mitgliedstaat und Antrag auf Ausstellung einer Europäischen Krankenversicherungskarte 4. Allgemeine Informationen über Zugangsrechte zu verfügbaren öffentlichen Präventionsmaßnahmen im Gesundheitsbereich und über die Pflichten zur Teilnahme an diesen Maßnahmen 5. Dienste, die über die nationalen Notrufnummern (einschließlich 112 und 116) zur Verfügung gestellt werden 6. Rechte und Voraussetzungen für den Einzug in eine stationäre Pflegeeinrichtung

G. Bürger- und Familienrechte	1. Geburt, Sorgerecht für Minderjährige, elterliche Pflichten, Vorschriften für Leihmutterschaft und Adoption, einschließlich Stiefkindadoption, Unterhaltspflichten für Kinder bei grenzüberschreitenden familiären Gegebenheiten 2. Leben in einer binationalen Partnerschaft, auch einer gleichgeschlechtlichen Partnerschaft (Eheschließung, zivile/eingetragene Partnerschaft, Trennung, Scheidung, Güterrecht, Rechte von Lebenspartnern) 3. Vorschriften für die Anerkennung der Geschlechtszugehörigkeit 4. Erbansprüche und -pflichten in einem anderen Mitgliedstaat, einschließlich Steuervorschriften 5. Rechte und Vorschriften für Fälle der grenzüberschreitenden Kindesentführung durch einen Elternteil
H. Verbraucherrechte	1. Kauf von Waren, digitalen Inhalten oder entgeltliche Inanspruchnahme von Dienstleistungen aus einem anderen Mitgliedstaat (auch Finanzdienstleistungen), online oder vor Ort 2. Besitz eines Bankkontos in einem anderen Mitgliedstaat 3. Inanspruchnahme von öffentlichen Dienstleistungen, z. B. Gas-, Strom-, Wasserversorgung, Beseitigung von Haushaltsabfällen, Telekommunikationsdienstleistungen und Internet 4. Zahlungen, einschließlich Überweisungen, Verzögerungen bei grenzüberschreitenden Zahlungen 5. Verbraucherrechte und Garantien im Zusammenhang mit dem Kauf von Waren und Dienstleistungen, einschließlich Verfahren für die Beilegung von

	Verbraucherrechtsstreitigkeiten und die Verbraucherentschädigung 6. Sicherheit von Verbraucherprodukten 7. Mieten eines Kraftfahrzeugs
I. Schutz personenbezogener Daten	1. Ausübung der Rechte der Betroffenen im Zusammenhang mit dem Schutz personenbezogener Daten

Informationsbereiche im Zusammenhang mit Unternehmen

Bereich	INFORMATIONEN ZU RECHTEN, PFLICHTEN UND VORSCHRIFTEN
J. Gründung, Führung und Schließung eines Unternehmens	1. Eintragung, Änderung der Rechtsform oder Schließung eines Unternehmens (Registrierungsverfahren und Rechtsformen für geschäftliche Tätigkeiten) 2. Verlagerung eines Unternehmens in einen anderen Mitgliedstaat 3. Rechte des geistigen Eigentums (Antrag auf Erteilung eines Patents, Anmeldung einer Marke, einer Zeichnung oder eines Gebrauchsmusters, Erwerb einer Lizenz für die Vervielfältigung) 4. Fairness und Transparenz von Geschäftspraktiken, einschließlich Verbraucherrechte und Garantien im Zusammenhang mit dem Verkauf von Waren und Dienstleistungen 5. Angebot von Online-Verfahren für grenzüberschreitende Zahlungen beim Online-Verkauf von Waren und Dienstleistungen 6. Rechte und Pflichten aufgrund des Vertragsrechts, einschließlich Verzugszinsen 7. Insolvenzverfahren und Liquidation von Unternehmen 8. Kreditversicherung

	9. Unternehmensfusionen oder Verkauf eines Unternehmens 10. Zivilrechtliche Haftung der Direktoren eines Unternehmens 11. Vorschriften und Pflichten im Zusammenhang mit der Verarbeitung personenbezogener Daten
K. Arbeitnehmer	1. Gesetzlich oder durch Rechtsverordnung geregelte Beschäftigungsbedingungen einschließlich Arbeitsstunden, bezahlter Urlaub, Urlaubsansprüche, Rechte und Pflichten in Bezug auf Überstunden, Gesundheitskontrollen, Beendigung von Verträgen, Kündigung oder Entlassungen) 2. Rechte und Pflichten im Bereich der sozialen Sicherheit in der Union (Registrierung als Arbeitgeber, Registrierung von Beschäftigten, Mitteilung über das Ende eines Vertrags eines Beschäftigten, Zahlung von Sozialbeiträgen, Rechte und Pflichten im Zusammenhang mit Renten) 3. Beschäftigung von Arbeitnehmern in anderen Mitgliedstaaten (Entsendung von Arbeitnehmern, Vorschriften über den freien Dienstleistungsverkehr, Wohnsitzanforderungen für Arbeitnehmer) 4. Gleichbehandlung (Vorschriften gegen Diskriminierung am Arbeitsplatz, Vorschriften zur gleichen Entlohnung für Männer und Frauen, gleiche Entlohnung für Beschäftigte mit befristeten oder mit unbefristeten Arbeitsverträgen) 5. Vorschriften für die Arbeitnehmervertretung
L. Steuern	1. Mehrwertsteuer: Informationen

	über die allgemeinen Vorschriften, Sätze und Ausnahmeregelungen, MwSt.-Registrierung und -Zahlung, MwSt.-Erstattung 2. Verbrauchsteuern: Informationen über die allgemeinen Vorschriften, Sätze und Ausnahmeregelungen, Verbrauchsteuerregistrierung und -zahlung, Verbrauchsteuererstattung 3. Zölle und andere Steuern und Abgaben, die auf Einfuhren erhoben werden 4. Zollverfahren für Einfuhren und Ausfuhren gemäß dem Zollkodex der Union 5. Sonstige Steuern: Zahlung, Sätze, Steuererklärungen
M. Waren	1. Erlangung der CE-Kennzeichnung 2. Vorschriften für und Anforderungen an Erzeugnisse 3. Feststellung der geltenden Normen, technischen Spezifikationen und Zertifizierung der Produkte 4. Gegenseitige Anerkennung von Produkten, die keinen Unionsspezifikationen unterliegen 5. Anforderungen in Bezug auf die Einstufung, Kennzeichnung und Verpackung von gefährlichen Chemikalien 6. Verkäufe im Fernabsatz und außerhalb von Geschäftsräumen: Informationen, die Verbrauchern vorab zu erteilen sind, schriftliche Vertragsbestätigung, Rücktritt von einem Vertrag, Lieferung der Waren, sonstige spezifische Verpflichtungen 7. Fehlerhafte Produkte: Verbraucherrechte und Garantien, Verantwortlichkeiten nach dem Verkauf, Abhilfemöglichkeiten für eine geschädigte Partei 8. Zertifizierung, Gütezeichen

	(EMAS, Energieeffizienzkennzeichnung, Ökodesign, EU-Umweltzeichen) 9. Recycling und Abfallentsorgung
N. Dienstleistungen	1. Erlangung von Lizenzen, Genehmigungen oder Zulassungen im Hinblick auf die Gründung und Führung eines Unternehmens 2. Unterrichtung der Behörden über grenzüberschreitende Tätigkeiten 3. Anerkennung beruflicher Qualifikationen, einschließlich beruflicher Bildung
O. Finanzierung eines Unternehmens	1. Zugang zu Finanzmitteln auf Unionsebene, einschließlich Finanzierungsprogramme der Union und Finanzhilfen für Unternehmen 2. Zugang zu Finanzmitteln auf nationaler Ebene 3. Initiativen für Unternehmer (Austauschmaßnahmen für neue Unternehmer, Mentoring-Programme usw.)
P. Öffentliche Aufträge	1. Teilnahme an öffentlichen Ausschreibungen: Regeln und Verfahren 2. Online-Abgabe eines Gebots auf eine öffentliche Ausschreibung 3. Meldung von Unregelmäßigkeiten im Zusammenhang mit dem Ausschreibungsverfahren
Q. Gesundheit und Sicherheit am Arbeitsplatz	1. Gesundheits- und Sicherheitsvorschriften im Zusammenhang mit verschiedenen Arten von Tätigkeiten, einschließlich der Risikovermeidung, Information und Ausbildung
R. Projekte zur Fertigung von Netto-Null-Technologien	1. Informationen zum Genehmigungsverfahren, 2. Finanzierungs- und Investitionsdienstleistungen, 3. Finanzierungsmöglichkeiten auf

	Ebene der Union oder der Mitgliedstaaten, 4. Dienstleistungen zur Unterstützung von Unternehmen, darunter u. a. Körperschaftsteuererklärungen, lokale Steuergesetze und Arbeitsrecht.
AJ. Projekte im Bereich kritische Rohstoffe	1. die gemäß Artikel 9 Absatz 1 der Verordnung (EU) 2024/1252 des Europäischen Parlaments und des Rates eingerichteten zentralen Anlaufstellen 2. Informationen über das Genehmigungsverfahren 3. Informationen über Finanzierungs- und Investitionsdienstleistungen 4. Informationen über Finanzierungsmöglichkeiten auf Ebene der Union oder der Mitgliedstaaten 5. Informationen über Dienstleistungen zur Unterstützung von Unternehmen, darunter u. a. Körperschaftsteuererklärungen, lokale Steuergesetze oder Arbeitsrecht

ANHANG II
Verfahren nach Artikel 6 Absatz 1

Lebensereignisse	Verfahren	Erwartete Ergebnisse, gegebenenfalls vorbehaltlich einer Bewertung des Antrags durch die zuständige Behörde gemäß nationalen Rechtsvorschriften
Geburt	Beantragung des Nachweises über die Eintragung in das Geburtenregister	Nachweis über die Eintragung in das Geburtenregister oder Geburtsurkunde
Wohnsitz	Beantragung eines Wohnsitznachweises	Bestätigung der Meldung an der aktuellen Adresse
Studium	Beantragung einer Studienfinanzierung für ein	Entscheidung über den Antrag auf Studienfinanzierung oder

	Hochschulstudium, z. B. Studienbeihilfen oder -darlehen, bei einer öffentlichen Stelle oder Einrichtung	Empfangsbestätigung
	Einreichung eines ersten Antrags auf Zulassung zu einer öffentlichen Hochschuleinrichtung	Bestätigung des Eingangs des Antrags
	Beantragung der Anerkennung von akademischen Diplomen, Prüfungszeugnissen oder sonstigen Nachweisen über Studien oder Kurse	Entscheidung über den Antrag auf Anerkennung
Arbeit	Antrag auf Bestimmung des anwendbaren Rechts gemäß Titel II der Verordnung (EG) Nr. 883/2004	Beschluss über das anwendbare Recht
	Mitteilung einer Änderung der persönlichen oder beruflichen Situation des Empfängers von Sozialversicherungsleistungen, die für solche Leistungen relevant ist	Bestätigung des Eingangs der Mitteilung solcher Änderungen
	Antrag auf Ausstellung einer Europäischen Krankenversicherungskarte (EHIC)	Europäische Krankenversicherungskarte (EHIC)
	Einreichung einer Einkommensteuererklärung	Bestätigung des Eingangs der Erklärung
Umzug	Meldung einer Adressänderung	Bestätigung der Abmeldung von der früheren Adresse und der Anmeldung an der neuen Adresse
	Zulassung eines aus einem Mitgliedstaat stammenden oder bereits in einem EU-Mitgliedstaat zugelassenen Kraftfahrzeugs in Standardverfahren	Nachweis über die Zulassung eines Kraftfahrzeugs
	Beantragung von Plaketten für die Nutzung der nationalen Straßenverkehrsinfrastruktur: von einer öffentlichen Stelle oder Einrichtung ausgestellte zeitabhängige Gebühren (Vignette), entfernungsabhängige Gebühren (Maut),	Erhalt des Mautaufklebers oder der Vignette oder anderer Zahlungsbeleg
	Beantragung von Emissionsplaketten, die von einer öffentlichen Stelle oder Einrichtung ausgestellt werden	Erhalt der Emissionsplakette oder anderer Zahlungsbeleg

Ruhestand	Beantragung von Ruhestands- und Vorruhestandsleistungen aus obligatorischen Systemen	Bestätigung des Eingangs des Antrags oder Beschluss über den Antrag auf Ruhestands- oder Vorruhestandsleistungen
	Ersuchen um Informationen über die Daten im Zusammenhang mit Ruhestandsleistungen aus obligatorischen Systemen	Erklärung über die persönlichen Ruhestandsdaten
Gründung, Führung und Schließung eines Unternehmens	Meldung einer Geschäftstätigkeit, Zulassung zur Ausübung einer Geschäftstätigkeit, Änderung einer Geschäftstätigkeit und Einstellung einer Geschäftstätigkeit ausgenommen Insolvenz- oder Liquidationsverfahren, ausgenommen der erstmaligen Eintragung einer Geschäftstätigkeit in das Unternehmens-Register, und ausgenommen Eintragungen im Rahmen des Verfahren zur Gründung von — oder späteren Anmeldungen oder Einreichungen von Meldungen von — Gesellschaften oder Unternehmen im Sinne von Artikel 54 Absatz 2 AEUV	Bestätigung des Eingangs der Meldung oder Änderung einer Geschäftstätigkeit oder des Antrags auf Genehmigung der Geschäftstätigkeit
	Registrierung eines Arbeitgebers (einer natürlichen Person) bei obligatorischen Versorgungs- und Versicherungssystemen	Registrierung von Beschäftigten bei obligatorischen Versorgungs- und Versicherungssystemen
	Registrierung von Beschäftigten bei obligatorischen Versorgungs- und Versicherungssystemen	Bestätigung der Registrierung oder Sozialversicherungs-Kennnummer
	Einreichung einer Körperschaftsteuererklärung	Bestätigung des Eingangs der Erklärung
	Meldung an die Sozialversicherungssysteme bei Beendigung des Vertrags mit einem Beschäftigten, ausgenommen bei Verfahren zur kollektiven Beendigung von Arbeitnehmerverträgen	Bestätigung des Eingangs der Meldung
	Zahlung von Sozialbeiträgen für Beschäftigte	Empfangs- oder andere Art der Bestätigung der Zahlung der Sozialbeiträge für Beschäftigte
	Anmeldung eines Anbieters von	Bestätigung des Eingangs der

	Datenvermittlungsdiensten	Anmeldung
	Eintragung als in der Union anerkannte datenaltruistische Organisation	Bestätigung der Eintragung
Projekte im Bereich kritische Rohstoffe	Verfahren, das alle einschlägigen Genehmigungen für den Bau und den Betrieb von Projekten im Bereich kritische Rohstoffe umfasst, einschließlich Bau-, Chemie- und Netzanschlussgenehmigungen sowie Umweltverträglichkeitsprüfungen und -genehmigungen, sofern diese erforderlich sind, und das alle Anträge und Verfahren von der Bestätigung der Vollständigkeit des Antrags bis zur Mitteilung der umfassenden Entscheidung über das Ergebnis des Verfahrens durch die gemäß Artikel 9 der Verordnung (EU) 2024/1252 eingerichtete zuständige zentrale Anlaufstelle umfasst.	Alle Ergebnisse im Zusammenhang mit den Verfahren von der Bestätigung der Vollständigkeit des Antrags bis zur Mitteilung der umfassenden Entscheidung über das Ergebnis des Verfahrens durch die gemäß Artikel 9 der Verordnung (EU) 2024/1252 eingerichtete zentrale Anlaufstelle.

ANHANG III

Liste der in Artikel 2 Absatz 2 Buchstabe c genannten Hilfs- und Problemlösungsdienste

1. Einheitliche Ansprechpartner
2. Produktinfostellen
3. Produktinformationsstellen für das Bauwesen
4. Nationale Beratungszentren für Berufsqualifikationen
5. Nationale Kontaktstellen für die grenzüberschreitende Gesundheitsversorgung
6. Europäisches Netz der Arbeitsvermittlungen (EURES)
7. Die Liste der von der Kommission gemäß Artikel 20 Absatz 4 der Richtlinie 2013/11/EU des Europäischen Parlaments und des Rates eingerichteten alternativen Stellen zur Beilegung verbraucherrechtlicher Streitigkeiten.
8. Zentrale Kontaktstellen, die gemäß Artikel 6 Absatz 1 der Verordnung (EU) 2024/1735 des Europäischen Parlaments und des Rates — auch für die Zwecke von Artikel 18 Absatz 1 — der Netto-Null-Industrie-Verordnung eingerichtet oder benannt wurden, und Kontaktstellen, die gemäß Artikel 33 Absatz 1 der genannten Verordnung eingerichtet oder benannt wurden
9. Die zuständige zentrale Anlaufstelle gemäß Artikel 9 der Verordnung (EU) 2024/1252.

Verwaltungsverfahrensgesetz (VwVfG)

§ 1 Anwendungsbereich

(1) Dieses Gesetz gilt für die öffentlich-rechtliche Verwaltungstätigkeit der Behörden

1. des Bundes, der bundesunmittelbaren Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts,
2. der Länder, der Gemeinden und Gemeindeverbände, der sonstigen der Aufsicht des Landes unterstehenden juristischen Personen des öffentlichen Rechts, wenn sie Bundesrecht im Auftrag des Bundes ausführen,

soweit nicht Rechtsvorschriften des Bundes inhaltsgleiche oder entgegenstehende Bestimmungen enthalten.

(2) Dieses Gesetz gilt auch für die öffentlich-rechtliche Verwaltungstätigkeit der in Absatz 1 Nr. 2 bezeichneten Behörden, wenn die Länder Bundesrecht, das Gegenstände der ausschließlichen oder konkurrierenden Gesetzgebung des Bundes betrifft, als eigene Angelegenheit ausführen, soweit nicht Rechtsvorschriften des Bundes inhaltsgleiche oder entgegenstehende Bestimmungen enthalten. Für die Ausführung von Bundesgesetzen, die nach Inkrafttreten dieses Gesetzes erlassen werden, gilt dies nur, soweit die Bundesgesetze mit Zustimmung des Bundesrates dieses Gesetz für anwendbar erklären.

(3) Für die Ausführung von Bundesrecht durch die Länder gilt dieses Gesetz nicht, soweit die öffentlich-rechtliche Verwaltungstätigkeit der Behörden landesrechtlich durch ein Verwaltungsverfahrensgesetz geregelt ist.

(4) Behörde im Sinne dieses Gesetzes ist jede Stelle, die Aufgaben der öffentlichen Verwaltung wahrnimmt.

§ 3a Elektronische Kommunikation

(1) Die Übermittlung elektronischer Dokumente ist zulässig, soweit der Empfänger hierfür einen Zugang eröffnet.

(2) Eine durch Rechtsvorschrift angeordnete Schriftform kann, soweit nicht durch Rechtsvorschrift etwas anderes bestimmt ist, durch die elektronische Form ersetzt werden. Der elektronischen Form genügt ein elektronisches Dokument, das mit einer qualifizierten elektronischen Signatur versehen ist. Die Signierung mit einem Pseudonym, das die Identifizierung der Person des Signaturschlüsselinhabers nicht unmittelbar durch die Behörde ermöglicht, ist nicht zulässig.

(3) Die Schriftform kann auch ersetzt werden

1. durch unmittelbare Abgabe der Erklärung in einem elektronischen Formular, das von der Behörde in einem Eingabegerät oder über öffentlich zugängliche Netze zur Verfügung gestellt wird; bei einer Eingabe über öffentlich zugängliche Netze muss ein elektronischer Identitätsnachweis nach § 18 des Personalausweisgesetzes, nach § 12 des eID-Karte-Gesetzes oder nach § 78 Absatz 5 des Aufenthaltsgesetzes erfolgen;

2. durch Übermittlung einer von dem Erklärenden elektronisch signierten Erklärung an die Behörde

   a) aus einem besonderen elektronischen Anwaltspostfach nach den §§ 31a und 31b der Bundesrechtsanwaltsordnung oder aus einem entsprechenden, auf gesetzlicher Grundlage errichteten elektronischen Postfach;

   b) aus einem elektronischen Postfach einer Behörde oder einer juristischen Person des öffentlichen Rechts, das nach Durchführung eines Identifizierungsverfahrens nach den Regelungen der auf Grund des § 130a Absatz 2 Satz 2 der Zivilprozessordnung erlassenen Rechtsverordnung eingerichtet wurde;

   c) aus einem elektronischen Postfach einer natürlichen oder juristischen Person oder einer sonstigen Vereinigung, das nach Durchführung eines Identifizierungsverfahrens nach den Regelungen der auf Grund des § 130a Absatz 2 Satz 2 der Zivilprozessordnung erlassenen Rechtsverordnung eingerichtet wurde;

   d) mit der Versandart nach § 5 Absatz 5 des De-Mail-Gesetzes;

3. bei elektronischen Verwaltungsakten oder sonstigen elektronischen Dokumenten der Behörde,

   a) indem diese mit dem qualifizierten elektronischen Siegel der Behörde versehen werden;

   b) durch Versendung einer De-Mail-Nachricht nach § 5 Absatz 5 des De-Mail-Gesetzes, bei der die Bestätigung des akkreditierten Diensteanbieters die erlassende Behörde als Nutzer des De-Mail-Kontos erkennen lässt.

(4) Ist ein der Behörde übermitteltes elektronisches Dokument für sie zur Bearbeitung nicht geeignet, teilt sie dies dem Absender unter Angabe der für sie geltenden technischen Rahmenbedingungen unverzüglich mit. Macht ein Empfänger geltend, er könne das von der Behörde übermittelte elektronische Dokument nicht bearbeiten, hat sie es ihm erneut in einem geeigneten elektronischen Format oder als Schriftstück zu übermitteln.

(5) Ermöglicht die Behörde die unmittelbare Abgabe einer Erklärung in einem elektronischen Formular, das von der Behörde in einem Eingabegerät oder über öffentlich zugängliche Netze zur Verfügung gestellt wird, so hat sie dem Erklärenden vor Abgabe der Erklärung Gelegenheit zu geben, die gesamte Erklärung auf Vollständigkeit und Richtigkeit zu prüfen. Nach der Abgabe ist dem Erklärenden eine Kopie der Erklärung zur Verfügung zu stellen.

§ 9 Begriff des Verwaltungsverfahrens

Das Verwaltungsverfahren im Sinne dieses Gesetzes ist die nach außen wirkende Tätigkeit der Behörden, die auf die Prüfung der Voraussetzungen, die Vorbereitung und den Erlass eines Verwaltungsaktes oder auf den Abschluss eines öffentlich-rechtlichen Vertrags gerichtet ist; es schließt den Erlass des Verwaltungsaktes oder den Abschluss des öffentlich-rechtlichen Vertrags ein.

§ 10 Nichtförmlichkeit des Verwaltungsverfahrens

Das Verwaltungsverfahren ist an bestimmte Formen nicht gebunden, soweit keine besonderen Rechtsvorschriften für die Form des Verfahrens bestehen. Es ist einfach, zweckmäßig und zügig durchzuführen.

VwVfG (Auszug)

§ 27a Bekanntmachung im Internet

(1) Ist durch Rechtsvorschrift eine öffentliche oder ortsübliche Bekanntmachung angeordnet, so ist diese dadurch zu bewirken, dass der Inhalt der Bekanntmachung auch auf einer Internetseite der Behörde oder ihres Verwaltungsträgers zugänglich gemacht wird. Soweit durch Rechtsvorschrift nichts anderes bestimmt ist, ist für die Einhaltung einer vorgeschriebenen Frist die Zugänglichmachung im Internet nach Satz 1 maßgeblich.

(2) Absatz 1 gilt nicht, wenn eine Zugänglichmachung im Internet, insbesondere aus technischen Gründen, nicht möglich ist.

§ 27b Zugänglichmachung auszulegender Dokumente

(1) Ist durch Rechtsvorschrift die Auslegung von Dokumenten zur Einsicht angeordnet, so ist sie dadurch zu bewirken, dass die Dokumente zugänglich gemacht werden

1. auf einer Internetseite der für die Auslegung zuständigen Behörde oder ihres Verwaltungsträgers und
2. auf mindestens eine andere Weise.

Ist eine Veröffentlichung der auszulegenden Unterlagen im Internet, insbesondere aus technischen Gründen, nicht möglich, so wird die angeordnete Auslegung zur Einsicht durch die andere Zugangsmöglichkeit nach Satz 1 Nummer 2 bewirkt.

(2) In der Bekanntmachung der Auslegung sind anzugeben

1. der Zeitraum der Auslegung,
2. die Internetseite, auf der die Zugänglichmachung erfolgt, sowie
3. Art und Ort der anderen Zugangsmöglichkeit.

(3) Die Behörde kann verlangen, dass die Dokumente, die für die Auslegung einzureichen sind, in einem verkehrsüblichen elektronischen Format eingereicht werden.

(4) Sind in den auszulegenden Dokumenten Geheimnisse nach § 30 enthalten, so ist derjenige, der diese Dokumente einreichen muss, verpflichtet,

1. diese Geheimnisse zu kennzeichnen und
2. der Behörde zum Zwecke der Auslegung zusätzlich eine Darstellung vorzulegen, die den Inhalt der betreffenden Teile der Dokumente ohne Preisgabe der Geheimnisse beschreibt.

§ 27c Erörterung mit Verfahrensbeteiligten oder der Öffentlichkeit

(1) Ist durch Rechtsvorschrift eine Erörterung, insbesondere ein Erörterungstermin, eine mündliche Verhandlung oder eine Antragskonferenz angeordnet, kann sie ersetzt werden

1. durch eine Onlinekonsultation oder
2. mit Einwilligung der zur Teilnahme Berechtigten durch eine Video- oder Telefonkonferenz.

(2) Bei einer Onlinekonsultation ist den zur Teilnahme Berechtigten innerhalb einer vorher bekannt zu machenden Frist Gelegenheit zu geben, sich schriftlich oder elektronisch zu äu-

ßern. Die Frist soll mindestens eine Woche betragen. Werden für die Onlinekonsultation Informationen zur Verfügung gestellt, so gilt § 27b Absatz 4 entsprechend.

(3) Sonstige Regelungen, die die Durchführung einer Erörterung nach Absatz 1 betreffen, bleiben unberührt.

§ 29 Akteneinsicht durch Beteiligte

(1) Die Behörde hat den Beteiligten Einsicht in die das Verfahren betreffenden Akten zu gestatten, soweit deren Kenntnis zur Geltendmachung oder Verteidigung ihrer rechtlichen Interessen erforderlich ist. Satz 1 gilt bis zum Abschluss des Verwaltungsverfahrens nicht für Entwürfe zu Entscheidungen sowie die Arbeiten zu ihrer unmittelbaren Vorbereitung. Soweit nach den §§ 17 und 18 eine Vertretung stattfindet, haben nur die Vertreter Anspruch auf Akteneinsicht.

(2) Die Behörde ist zur Gestattung der Akteneinsicht nicht verpflichtet, soweit durch sie die ordnungsgemäße Erfüllung der Aufgaben der Behörde beeinträchtigt, das Bekanntwerden des Inhalts der Akten dem Wohl des Bundes oder eines Landes Nachteile bereiten würde oder soweit die Vorgänge nach einem Gesetz oder ihrem Wesen nach, namentlich wegen der berechtigten Interessen der Beteiligten oder dritter Personen, geheim gehalten werden müssen.

(3) Die Akteneinsicht erfolgt bei der Behörde, die die Akten führt. Im Einzelfall kann die Einsicht auch bei einer anderen Behörde oder bei einer diplomatischen oder berufskonsularischen Vertretung der Bundesrepublik Deutschland im Ausland erfolgen; weitere Ausnahmen kann die Behörde, die die Akten führt, gestatten.

§ 30 Geheimhaltung

Die Beteiligten haben Anspruch darauf, dass ihre Geheimnisse, insbesondere die zum persönlichen Lebensbereich gehörenden Geheimnisse sowie die Betriebs- und Geschäftsgeheimnisse, von der Behörde nicht unbefugt offenbart werden.

§ 33 Beglaubigung von Dokumenten

(1) Jede Behörde ist befugt, Abschriften von Urkunden, die sie selbst ausgestellt hat, zu beglaubigen. Darüber hinaus sind die von der Bundesregierung durch Rechtsverordnung bestimmten Behörden im Sinne des § 1 Abs. 1 Nr. 1 und die nach Landesrecht zuständigen Behörden befugt, Abschriften zu beglaubigen, wenn die Urschrift von einer Behörde ausgestellt ist oder die Abschrift zur Vorlage bei einer Behörde benötigt wird, sofern nicht durch Rechtsvorschrift die Erteilung beglaubigter Abschriften aus amtlichen Registern und Archiven anderen Behörden ausschließlich vorbehalten ist; die Rechtsverordnung bedarf nicht der Zustimmung des Bundesrates.

(2) Abschriften dürfen nicht beglaubigt werden, wenn Umstände zu der Annahme berechtigen, dass der ursprüngliche Inhalt des Schriftstücks, dessen Abschrift beglaubigt werden soll, geändert worden ist, insbesondere wenn dieses Schriftstück Lücken, Durchstreichungen, Einschaltungen, Änderungen, unleserliche Wörter, Zahlen oder Zeichen, Spuren der Beseitigung von Wörtern, Zahlen und Zeichen enthält oder wenn der Zusammenhang eines aus mehreren Blättern bestehenden Schriftstücks aufgehoben ist.

(3) Eine Abschrift wird beglaubigt durch einen Beglaubigungsvermerk, der unter die Abschrift zu setzen ist. Der Vermerk muss enthalten

1. die genaue Bezeichnung des Schriftstücks, dessen Abschrift beglaubigt wird,
2. die Feststellung, dass die beglaubigte Abschrift mit dem vorgelegten Schriftstück übereinstimmt,
3. den Hinweis, dass die beglaubigte Abschrift nur zur Vorlage bei der angegebenen Behörde erteilt wird, wenn die Urschrift nicht von einer Behörde ausgestellt worden ist,
4. den Ort und den Tag der Beglaubigung, die Unterschrift des für die Beglaubigung zuständigen Bediensteten und das Dienstsiegel.

(4) Die Absätze 1 bis 3 gelten entsprechend für die Beglaubigung von

1. Ablichtungen, Lichtdrucken und ähnlichen in technischen Verfahren hergestellten Vervielfältigungen,
2. auf fototechnischem Wege von Schriftstücken hergestellten Negativen, die bei einer Behörde aufbewahrt werden,
3. Ausdrucken elektronischer Dokumente,
4. elektronischen Dokumenten,
   a) die zur Abbildung eines Schriftstücks hergestellt wurden,
   b) die ein anderes technisches Format als das Ausgangsdokument, das verbunden ist mit einer qualifizierten elektronischen Signatur oder einem qualifizierten elektronischen Siegel einer Behörde, erhalten haben.

(5) Der Beglaubigungsvermerk muss zusätzlich zu den Angaben nach Absatz 3 Satz 2 bei der Beglaubigung

1. des Ausdrucks eines elektronischen Dokuments, das mit einer qualifizierten elektronischen Signatur oder einem qualifizierten elektronischen Siegel einer Behörde verbunden ist, die Feststellungen enthalten,
   a) wen die Signaturprüfung als Inhaber der Signatur ausweist oder welche Behörde die Signaturprüfung als Inhaber des Siegels ausweist,
   b) welchen Zeitpunkt die Signaturprüfung für die Anbringung der Signatur oder des Siegels ausweist und
   c) welche Zertifikate mit welchen Daten dieser Signatur oder diesem Siegel zu Grunde lagen;
2. eines elektronischen Dokuments den Namen des für die Beglaubigung zuständigen Bediensteten und die Bezeichnung der Behörde, die die Beglaubigung vornimmt, enthalten; die Unterschrift des für die Beglaubigung zuständigen Bediensteten und das Dienstsiegel nach Absatz 3 Satz 2 Nummer 4 werden durch eine dauerhaft überprüfbare qualifizierte elektronische Signatur oder durch ein dauerhaft überprüfbares qualifiziertes elektronisches Siegel der Behörde ersetzt.

Wird ein elektronisches Dokument, das ein anderes technisches Format erhalten hat als das Ausgangsdokument, das mit einer qualifizierten elektronischen Signatur oder mit einem qualifizierten elektronischen Siegel einer Behörde verbunden ist, nach Satz 1 Nummer 2 be-

glaubigt, so muss der Beglaubigungsvermerk zusätzlich die Feststellungen nach Satz 1 Nummer 1 für das Ausgangsdokument enthalten.

(6) Die nach Absatz 4 hergestellten Dokumente stehen, sofern sie beglaubigt sind, beglaubigten Abschriften gleich.

(7) Jede Behörde soll von Urkunden, die sie selbst ausgestellt hat, auf Verlangen ein elektronisches Dokument nach Absatz 4 Nummer 4 Buchstabe a oder eine elektronische Abschrift fertigen und beglaubigen.

§ 34 Beglaubigung von Unterschriften

(1) Die von der Bundesregierung durch Rechtsverordnung bestimmten Behörden im Sinne des § 1 Abs. 1 Nr. 1 und die nach Landesrecht zuständigen Behörden sind befugt, Unterschriften zu beglaubigen, wenn das unterzeichnete Schriftstück zur Vorlage bei einer Behörde oder bei einer sonstigen Stelle, der auf Grund einer Rechtsvorschrift das unterzeichnete Schriftstück vorzulegen ist, benötigt wird. Dies gilt nicht für

1. Unterschriften ohne zugehörigen Text,
2. Unterschriften, die der öffentlichen Beglaubigung (§ 129 des Bürgerlichen Gesetzbuchs) bedürfen.

(2) Eine Unterschrift soll nur beglaubigt werden, wenn sie in Gegenwart des beglaubigenden Bediensteten vollzogen oder anerkannt wird.

(3) Der Beglaubigungsvermerk ist unmittelbar bei der Unterschrift, die beglaubigt werden soll, anzubringen. Er muss enthalten

1. die Bestätigung, dass die Unterschrift echt ist,
2. die genaue Bezeichnung desjenigen, dessen Unterschrift beglaubigt wird, sowie die Angabe, ob sich der für die Beglaubigung zuständige Bedienstete Gewissheit über diese Person verschafft hat und ob die Unterschrift in seiner Gegenwart vollzogen oder anerkannt worden ist,
3. den Hinweis, dass die Beglaubigung nur zur Vorlage bei der angegebenen Behörde oder Stelle bestimmt ist,
4. den Ort und den Tag der Beglaubigung, die Unterschrift des für die Beglaubigung zuständigen Bediensteten und das Dienstsiegel.

(4) Die Absätze 1 bis 3 gelten für die Beglaubigung von Handzeichen entsprechend.

(5) Die Rechtsverordnungen nach Absatz 1 und 4 bedürfen nicht der Zustimmung des Bundesrates.

§ 35 Begriff des Verwaltungsaktes

Verwaltungsakt ist jede Verfügung, Entscheidung oder andere hoheitliche Maßnahme, die eine Behörde zur Regelung eines Einzelfalls auf dem Gebiet des öffentlichen Rechts trifft und die auf unmittelbare Rechtswirkung nach außen gerichtet ist. Allgemeinverfügung ist ein Verwaltungsakt, der sich an einen nach allgemeinen Merkmalen bestimmten oder bestimmbaren Personenkreis richtet oder die öffentlich-rechtliche Eigenschaft einer Sache oder ihre Benutzung durch die Allgemeinheit betrifft.

VwVfG (Auszug)

§ 35a Vollständig automatisierter Erlass eines Verwaltungsaktes

Ein Verwaltungsakt kann vollständig durch automatische Einrichtungen erlassen werden, sofern dies durch Rechtsvorschrift zugelassen ist und weder ein Ermessen noch ein Beurteilungsspielraum besteht.

§ 37 Bestimmtheit und Form des Verwaltungsaktes; Rechtsbehelfsbelehrung

(1) Ein Verwaltungsakt muss inhaltlich hinreichend bestimmt sein.

(2) Ein Verwaltungsakt kann schriftlich, elektronisch, mündlich oder in anderer Weise erlassen werden. Ein mündlicher Verwaltungsakt ist schriftlich oder elektronisch zu bestätigen, wenn hieran ein berechtigtes Interesse besteht und der Betroffene dies unverzüglich verlangt. Ein elektronischer Verwaltungsakt ist unter denselben Voraussetzungen schriftlich zu bestätigen; § 3a Absatz 2 und 3 findet insoweit keine Anwendung.

(3) Ein schriftlicher oder elektronischer Verwaltungsakt muss die erlassende Behörde erkennen lassen und die Unterschrift oder die Namenswiedergabe des Behördenleiters, seines Vertreters oder seines Beauftragten enthalten. Wird für einen Verwaltungsakt, für den durch Rechtsvorschrift die Schriftform angeordnet ist, die elektronische Form verwendet, muss auch das der Signatur zugrunde liegende qualifizierte Zertifikat oder ein zugehöriges qualifiziertes Attributzertifikat die erlassende Behörde erkennen lassen. Im Fall des § 3a Absatz 3 Nummer 3 Buchstabe b muss die Bestätigung nach § 5 Absatz 5 des De-Mail-Gesetzes die erlassende Behörde als Nutzer des De-Mail-Kontos erkennen lassen.

(4) Für einen Verwaltungsakt kann für die nach § 3a Absatz 2 erforderliche Signatur oder für das nach § 3a Absatz 3 Nummer 3 Buchstabe a erforderliche Siegel durch Rechtsvorschrift die dauerhafte Überprüfbarkeit vorgeschrieben werden.

(5) Bei einem schriftlichen Verwaltungsakt, der mit Hilfe automatischer Einrichtungen erlassen wird, können abweichend von Absatz 3 Unterschrift und Namenswiedergabe fehlen. Zur Inhaltsangabe können Schlüsselzeichen verwendet werden, wenn derjenige, für den der Verwaltungsakt bestimmt ist oder der von ihm betroffen wird, auf Grund der dazu gegebenen Erläuterungen den Inhalt des Verwaltungsaktes eindeutig erkennen kann.

(6) Einem schriftlichen oder elektronischen Verwaltungsakt, der der Anfechtung unterliegt, ist eine Erklärung beizufügen, durch die der Beteiligte über den Rechtsbehelf, der gegen den Verwaltungsakt gegeben ist, über die Behörde oder das Gericht, bei denen der Rechtsbehelf einzulegen ist, den Sitz und über die einzuhaltende Frist belehrt wird (Rechtsbehelfsbelehrung). Die Rechtsbehelfsbelehrung ist auch der schriftlichen oder elektronischen Bestätigung eines Verwaltungsaktes und der Bescheinigung nach § 42a Absatz 3 beizufügen.

§ 39 Begründung des Verwaltungsaktes

(1) Ein schriftlicher oder elektronischer sowie ein schriftlich oder elektronisch bestätigter Verwaltungsakt ist mit einer Begründung zu versehen. In der Begründung sind die wesentlichen tatsächlichen und rechtlichen Gründe mitzuteilen, die die Behörde zu ihrer Entscheidung bewogen haben. Die Begründung von Ermessensentscheidungen soll auch die Gesichtspunkte erkennen lassen, von denen die Behörde bei der Ausübung ihres Ermessens ausgegangen ist.

(2) Einer Begründung bedarf es nicht,

1. soweit die Behörde einem Antrag entspricht oder einer Erklärung folgt und der Verwaltungsakt nicht in Rechte eines anderen eingreift;
2. soweit demjenigen, für den der Verwaltungsakt bestimmt ist oder der von ihm betroffen wird, die Auffassung der Behörde über die Sach- und Rechtslage bereits bekannt oder auch ohne Begründung für ihn ohne weiteres erkennbar ist;
3. wenn die Behörde gleichartige Verwaltungsakte in größerer Zahl oder Verwaltungsakte mit Hilfe automatischer Einrichtungen erlässt und die Begründung nach den Umständen des Einzelfalls nicht geboten ist;
4. wenn sich dies aus einer Rechtsvorschrift ergibt;
5. wenn eine Allgemeinverfügung öffentlich bekannt gegeben wird.

§ 41 Bekanntgabe des Verwaltungsaktes

(1) Ein Verwaltungsakt ist demjenigen Beteiligten bekannt zu geben, für den er bestimmt ist oder der von ihm betroffen wird. Ist ein Bevollmächtigter bestellt, so kann die Bekanntgabe ihm gegenüber vorgenommen werden.

(2) Ein schriftlicher Verwaltungsakt, der im Inland durch die Post übermittelt wird, gilt am vierten Tag nach der Aufgabe zur Post als bekannt gegeben. Ein Verwaltungsakt, der im Inland oder in das Ausland elektronisch übermittelt wird, gilt am vierten Tag nach der Absendung als bekannt gegeben. Dies gilt nicht, wenn der Verwaltungsakt nicht oder zu einem späteren Zeitpunkt zugegangen ist; im Zweifel hat die Behörde den Zugang des Verwaltungsaktes und den Zeitpunkt des Zugangs nachzuweisen.

(2a) Mit Einwilligung des Beteiligten kann ein elektronischer Verwaltungsakt dadurch bekannt gegeben werden, dass er vom Beteiligten oder von seinem Bevollmächtigten über öffentlich zugängliche Netze abgerufen wird. Die Behörde hat zu gewährleisten, dass der Abruf nur nach Authentifizierung der berechtigten Person möglich ist und der elektronische Verwaltungsakt von ihr gespeichert werden kann. Der Verwaltungsakt gilt am Tag nach dem Abruf als bekannt gegeben. Wird der Verwaltungsakt nicht innerhalb von zehn Tagen nach Absendung einer Benachrichtigung über die Bereitstellung abgerufen, wird diese beendet. In diesem Fall ist die Bekanntgabe nicht bewirkt; die Möglichkeit einer erneuten Bereitstellung zum Abruf oder der Bekanntgabe auf andere Weise bleibt unberührt.

(3) Ein Verwaltungsakt darf öffentlich bekannt gegeben werden, wenn dies durch Rechtsvorschrift zugelassen ist. Eine Allgemeinverfügung darf auch dann öffentlich bekannt gegeben werden, wenn eine Bekanntgabe an die Beteiligten untunlich ist.

(4) Die öffentliche Bekanntgabe eines schriftlichen oder elektronischen Verwaltungsaktes wird dadurch bewirkt, dass sein verfügender Teil ortsüblich bekannt gemacht wird. In der ortsüblichen Bekanntmachung ist anzugeben, wo der Verwaltungsakt und seine Begründung eingesehen werden können. Der Verwaltungsakt gilt zwei Wochen nach der ortsüblichen Bekanntmachung als bekannt gegeben. In einer Allgemeinverfügung kann ein hiervon abweichender Tag, jedoch frühestens der auf die Bekanntmachung folgende Tag bestimmt werden.

(5) Vorschriften über die Bekanntgabe eines Verwaltungsaktes mittels Zustellung bleiben unberührt.

VwVfG (Auszug)

§ 43 Wirksamkeit des Verwaltungsaktes

(1) Ein Verwaltungsakt wird gegenüber demjenigen, für den er bestimmt ist oder der von ihm betroffen wird, in dem Zeitpunkt wirksam, in dem er ihm bekannt gegeben wird. Der Verwaltungsakt wird mit dem Inhalt wirksam, mit dem er bekannt gegeben wird.

(2) Ein Verwaltungsakt bleibt wirksam, solange und soweit er nicht zurückgenommen, widerrufen, anderweitig aufgehoben oder durch Zeitablauf oder auf andere Weise erledigt ist.

(3) Ein nichtiger Verwaltungsakt ist unwirksam.

Verwaltungszustellungsgesetz (VwZG)

§ 1 Anwendungsbereich

(1) Die Vorschriften dieses Gesetzes gelten für das Zustellungsverfahren der Bundesbehörden, der bundesunmittelbaren Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts und der Landesfinanzbehörden.

(2) Zugestellt wird, soweit dies durch Rechtsvorschrift oder behördliche Anordnung bestimmt ist.

§ 2 Allgemeines

(1) Zustellung ist die Bekanntgabe eines schriftlichen oder elektronischen Dokuments in der in diesem Gesetz bestimmten Form.

(2) Die Zustellung wird durch einen Erbringer von Postdienstleistungen (Post), einen nach § 17 des De-Mail-Gesetzes akkreditierten Diensteanbieter oder durch die Behörde ausgeführt. Daneben gelten die in den §§ 9 und 10 geregelten Sonderarten der Zustellung.

(3) Die Behörde hat die Wahl zwischen den einzelnen Zustellungsarten. § 5 Absatz 5 Satz 2 bleibt unberührt.

§ 5 Zustellung durch die Behörde gegen Empfangsbekenntnis; elektronische Zustellung

(1) Bei der Zustellung durch die Behörde händigt der zustellende Bedienstete das Dokument dem Empfänger in einem verschlossenen Umschlag aus. Das Dokument kann auch offen ausgehändigt werden, wenn keine schutzwürdigen Interessen des Empfängers entgegenstehen. Der Empfänger hat ein mit dem Datum der Aushändigung versehenes Empfangsbekenntnis zu unterschreiben. Der Bedienstete vermerkt das Datum der Zustellung auf dem Umschlag des auszuhändigenden Dokuments oder bei offener Aushändigung auf dem Dokument selbst.

(2) Die §§ 177 bis 181 der Zivilprozessordnung sind anzuwenden. Zum Nachweis der Zustellung ist in den Akten zu vermerken:

1. im Fall der Ersatzzustellung in der Wohnung, in Geschäftsräumen und Einrichtungen nach § 178 der Zivilprozessordnung der Grund, der diese Art der Zustellung rechtfertigt,
2. im Fall der Zustellung bei verweigerter Annahme nach § 179 der Zivilprozessordnung, wer die Annahme verweigert hat und dass das Dokument am Ort der Zustellung zurückgelassen oder an den Absender zurückgesandt wurde sowie der Zeitpunkt und der Ort der verweigerten Annahme,
3. in den Fällen der Ersatzzustellung nach den §§ 180 und 181 der Zivilprozessordnung der Grund der Ersatzzustellung sowie wann und wo das Dokument in einen Briefkasten eingelegt oder sonst niedergelegt und in welcher Weise die Niederlegung schriftlich mitgeteilt wurde.

Im Fall des § 181 Abs. 1 der Zivilprozessordnung kann das zuzustellende Dokument bei der Behörde, die den Zustellungsauftrag erteilt hat, niedergelegt werden, wenn diese Behörde

ihren Sitz am Ort der Zustellung oder am Ort des Amtsgerichts hat, in dessen Bezirk der Ort der Zustellung liegt.

(3) Zur Nachtzeit, an Sonntagen und allgemeinen Feiertagen darf nach den Absätzen 1 und 2 im Inland nur mit schriftlicher oder elektronischer Erlaubnis des Behördenleiters zugestellt werden. Die Nachtzeit umfasst die Stunden von 21 bis 6 Uhr. Die Erlaubnis ist bei der Zustellung abschriftlich mitzuteilen. Eine Zustellung, bei der diese Vorschriften nicht beachtet sind, ist wirksam, wenn die Annahme nicht verweigert wird.

(4) Das Dokument kann an Behörden, Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts, an Rechtsanwälte, Patentanwälte, Notare, Steuerberater, Steuerbevollmächtigte, Wirtschaftsprüfer, vereidigte Buchprüfer, Berufsausübungsgesellschaften im Sinne der Bundesrechtsanwaltsordnung, der Patentanwaltsordnung und des Steuerberatungsgesetzes, Wirtschaftsprüfungsgesellschaften und Buchprüfungsgesellschaften auch auf andere Weise, auch elektronisch, gegen Empfangsbekenntnis zugestellt werden.

(5) Ein elektronisches Dokument kann im Übrigen unbeschadet des Absatzes 4 elektronisch zugestellt werden, soweit der Empfänger hierfür einen Zugang eröffnet. Es ist elektronisch zuzustellen, wenn auf Grund einer Rechtsvorschrift ein Verfahren auf Verlangen des Empfängers in elektronischer Form abgewickelt wird. Für die Übermittlung ist das Dokument mit einer qualifizierten elektronischen Signatur zu versehen und gegen unbefugte Kenntnisnahme Dritter zu schützen.

(6) Bei der elektronischen Zustellung ist die Übermittlung mit dem Hinweis „Zustellung gegen Empfangsbekenntnis“ einzuleiten. Die Übermittlung muss die absendende Behörde, den Namen und die Anschrift des Zustellungsadressaten sowie den Namen des Bediensteten erkennen lassen, der das Dokument zur Übermittlung aufgegeben hat.

(7) Zum Nachweis der Zustellung nach den Absätzen 4 und 5 genügt das mit Datum und Unterschrift versehene Empfangsbekenntnis, das an die Behörde durch die Post oder elektronisch zurückzusenden ist. Ein elektronisches Dokument gilt in den Fällen des Absatzes 5 Satz 2 am vierten Tag nach der Absendung an den vom Empfänger hierfür eröffneten Zugang als zugestellt, wenn der Behörde nicht spätestens an diesem Tag ein Empfangsbekenntnis nach Satz 1 zugeht. Satz 2 gilt nicht, wenn der Empfänger nachweist, dass das Dokument nicht oder zu einem späteren Zeitpunkt zugegangen ist. Der Empfänger ist in den Fällen des Absatzes 5 Satz 2 vor der Übermittlung über die Rechtsfolgen nach den Sätzen 2 und 3 zu belehren. Zum Nachweis der Zustellung ist von der absendenden Behörde in den Akten zu vermerken, zu welchem Zeitpunkt und an welchen Zugang das Dokument gesendet wurde. Der Empfänger ist über den Eintritt der Zustellungsfiktion nach Satz 2 zu benachrichtigen.

§ 5a Elektronische Zustellung gegen Abholbestätigung über De-Mail-Dienste

(1) Die elektronische Zustellung kann unbeschadet des § 5 Absatz 4 und 5 Satz 1 und 2 durch Übermittlung der nach § 17 des De-Mail-Gesetzes akkreditierten Diensteanbieter gegen Abholbestätigung nach § 5 Absatz 9 des De-Mail-Gesetzes an das De-Mail-Postfach des Empfängers erfolgen. Für die Zustellung nach Satz 1 ist § 5 Absatz 4 und 6 mit der Maßgabe anzuwenden, dass an die Stelle des Empfangsbekenntnisses die Abholbestätigung tritt.

(2) Der nach § 17 des De-Mail-Gesetzes akkreditierte Diensteanbieter hat eine Versandbestätigung nach § 5 Absatz 7 des De-Mail-Gesetzes und eine Abholbestätigung nach § 5 Absatz 9 des De-Mail-Gesetzes zu erzeugen. Er hat diese Bestätigungen unverzüglich der absendenden Behörde zu übermitteln.

(3) Zum Nachweis der elektronischen Zustellung genügt die Abholbestätigung nach § 5 Absatz 9 des De-Mail-Gesetzes. Für diese gelten § 371 Absatz 1 Satz 2 und § 371a Absatz 3 der Zivilprozessordnung.

(4) Ein elektronisches Dokument gilt in den Fällen des § 5 Absatz 5 Satz 2 am vierten Tag nach der Absendung an das De-Mail-Postfach des Empfängers als zugestellt, wenn er dieses Postfach als Zugang eröffnet hat und der Behörde nicht spätestens an diesem Tag eine elektronische Abholbestätigung nach § 5 Absatz 9 des De-Mail-Gesetzes zugeht. Satz 1 gilt nicht, wenn der Empfänger nachweist, dass das Dokument nicht oder zu einem späteren Zeitpunkt zugegangen ist. Der Empfänger ist in den Fällen des § 5 Absatz 5 Satz 2 vor der Übermittlung über die Rechtsfolgen nach den Sätzen 1 und 2 zu belehren. Als Nachweis der Zustellung nach Satz 1 dient die Versandbestätigung nach § 5 Absatz 7 des De-Mail-Gesetzes oder ein Vermerk der absendenden Behörde in den Akten, zu welchem Zeitpunkt und an welches De-Mail-Postfach das Dokument gesendet wurde. Der Empfänger ist über den Eintritt der Zustellungsfiktion nach Satz 1 elektronisch zu benachrichtigen.

Vertrag über die Errichtung des IT-Planungsrats und über die Grundlagen der Zusammenarbeit beim Einsatz der Informationstechnologie in den Verwaltungen von Bund und Ländern – Vertrag zur Ausführung von Artikel 91c GG* (IT-Staatsvertrag)

Inhaltsübersicht

---

* Art 91c GG lautet:

(1) Bund und Länder können bei der Planung, der Errichtung und dem Betrieb der für ihre Aufgabenerfüllung benötigten informationstechnischen Systeme zusammenwirken.

(2) Bund und Länder können auf Grund von Vereinbarungen die für die Kommunikation zwischen ihren informationstechnischen Systemen notwendigen Standards und Sicherheitsanforderungen festlegen. Vereinbarungen über die Grundlagen der Zusammenarbeit nach Satz 1 können für einzelne nach Inhalt und Ausmaß bestimmte Aufgaben vorsehen, dass nähere Regelungen bei Zustimmung einer in der Vereinbarung zu bestimmenden qualifizierten Mehrheit für Bund und Länder in Kraft treten. Sie bedürfen der Zustimmung des Bundestages und der Volksvertretungen der beteiligten Länder; das Recht zur Kündigung dieser Vereinbarungen kann nicht ausgeschlossen werden. Die Vereinbarungen regeln auch die Kostentragung.

(3) Die Länder können darüber hinaus den gemeinschaftlichen Betrieb informationstechnischer Systeme sowie die Errichtung von dazu bestimmten Einrichtungen vereinbaren.

(4) Der Bund errichtet zur Verbindung der informationstechnischen Netze des Bundes und der Länder ein Verbindungsnetz. Das Nähere zur Errichtung und zum Betrieb des Verbindungsnetzes regelt ein Bundesgesetz mit Zustimmung des Bundesrates.

(5) Der übergreifende informationstechnische Zugang zu den Verwaltungsleistungen von Bund und Ländern wird durch Bundesgesetz mit Zustimmung des Bundesrates geregelt.

Präambel

Präambel

Das Land Baden-Württemberg,
der Freistaat Bayern,
das Land Berlin,
das Land Brandenburg,
die Freie Hansestadt Bremen,
die Freie und Hansestadt Hamburg,
das Land Hessen,
das Land Mecklenburg-Vorpommern,
das Land Niedersachsen,
das Land Nordrhein-Westfalen,
das Land Rheinland-Pfalz,
das Saarland,
der Freistaat Sachsen,
das Land Sachsen-Anhalt,
das Land Schleswig-Holstein und
der Freistaat Thüringen

sowie die

Bundesrepublik Deutschland (im Weiteren „der Bund“ genannt)

(im Folgenden „Vertragspartner“)

sehen übereinstimmend die wachsenden Herausforderungen als Folge der Entwicklungen in der Informationstechnik. Der reibungslose und sichere Betrieb informationstechnischer

Systeme stellt eine wesentliche Anforderung an die Aufrechterhaltung geordneter Abläufe in den Verwaltungen der Vertragspartner dar.

Der Bund und die Länder haben mit der Erarbeitung des im Anhang zu diesem Vertrag wiedergegebenen „Gemeinsamen Grundverständnis der technischen und organisatorischen Ausgestaltung der Bund-Länder-Zusammenarbeit bei dem Verbindungsnetz und der IT-Steuerung“ die Grundlage für ein neues System der Bund-Länder-IT-Koordinierung erarbeitet und in die Beratungen der Kommission zur Modernisierung der Bund-Länder-Finanzbeziehungen (Föderalismuskommission II) eingebracht (Arbeitsunterlage AG 3 – 08). Hieraus hat die Föderalismuskommission II mit Artikel 91c des Grundgesetzes eine Grundlage für die IT-Koordinierung von Bund und Ländern entwickelt und beschlossen.

Die Vertragspartner treffen daher auf der Grundlage des Artikel 91c des Grundgesetzes

- zur Einrichtung und Regelung der Arbeitsweise eines IT-Planungsrats als Steuerungsgremium der allgemeinen IT-Kooperation nach Artikel 91c Absatz 1 und 2 des Grundgesetzes,
- zu Planung, Errichtung, Betrieb und Weiterentwicklung von informationstechnischen Infrastrukturen, insbesondere auch zur Verbindung der informationstechnischen Netze von Bund und Ländern nach Maßgabe des gemäß Artikel 91c des Grundgesetzes erlassenen Bundesgesetzes, sowie
- zum Verfahren nach Artikel 91c Absatz 2 des Grundgesetzes zur Festlegung von IT-Standards und IT-Sicherheitsanforderungen, soweit dies der zur Erfüllung ihrer Aufgaben notwendige Datenaustausch erfordert,

folgende Vereinbarung:

Abschnitt I
Der IT-Planungsrat

§ 1 Einrichtung, Aufgaben, Beschlussfassung

(1) Der Planungsrat für die IT-Zusammenarbeit der öffentlichen Verwaltung zwischen Bund und Ländern (IT-Planungsrat)

1. koordiniert die Zusammenarbeit von Bund und Ländern in Fragen der Informationstechnik;
2. beschließt fachunabhängige und fachübergreifende IT-Interoperabilitäts- und IT-Sicherheitsstandards;
3. koordiniert und unterstützt die Zusammenarbeit von Bund und Ländern in Fragen der Digitalisierung von Verwaltungsleistungen;
4. steuert Projekte und Produkte des informations- und kommunikationstechnisch unterstützten Regierens und Verwaltens, die dem IT-Planungsrat zugewiesen werden;
5. übernimmt die in § 3 genannten Aufgaben für das Verbindungsnetz nach Maßgabe des dort angeführten Gesetzes.

Der IT-Planungsrat berichtet grundsätzlich an die Konferenz des Chefs des Bundeskanzleramtes mit den Chefs der Staats- und Senatskanzleien. Er vereint die bisherigen Gremien und Untergremien der gemeinsamen IT-Steuerung. Der IT-Planungsrat bedient sich zu seiner Unterstützung nach Maßgabe der §§ 5 bis 10 einer gemeinsamen Einrichtung.

(2) Dem IT-Planungsrat gehören als Mitglieder an:

1. der Beauftragte der Bundesregierung für Informationstechnik,
2. jeweils ein für Informationstechnik zuständiger Vertreter jedes Landes.

Der Bund und die Länder stellen sicher, dass ihre Vertreter über die erforderliche Entscheidungskompetenz verfügen. Drei Vertreter der Gemeinden und Gemeindeverbände, die von den kommunalen Spitzenverbänden auf Bundesebene entsandt werden, sowie der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit können an den Sitzungen des IT-Planungsrats beratend teilnehmen.

(3) Den Vorsitz im IT-Planungsrat übernehmen im jährlichen Wechsel der Bund und die Länder. Die Länder regeln die Reihenfolge ihres Vorsitzes untereinander.

(4) Der IT-Planungsrat tagt mindestens zweimal im Jahr oder auf Antrag des Bundes oder dreier Länder.

(5) Der IT-Planungsrat entscheidet durch Beschluss oder Empfehlung. Er entscheidet auf Antrag des Bundes oder dreier Länder. Entscheidungen des IT-Planungsrats werden im elektronischen Bundesanzeiger veröffentlicht.

(6) Der IT-Planungsrat beteiligt die jeweilige Fachministerkonferenz, soweit deren Fachplanungen von seinen Entscheidungen betroffen werden.

(7) Beschlüsse des IT-Planungsrats bedürfen, soweit in diesem Vertrag oder durch Gesetz nicht etwas anderes bestimmt ist, der Zustimmung des Bundes und einer Mehrheit von elf Ländern, welche mindestens zwei Drittel ihrer Finanzierungsanteile nach dem Königsteiner Schlüssel abbildet. Empfehlungen für die öffentliche Verwaltung kann der IT-Planungsrat mit einfacher Mehrheit der anwesenden Mitglieder aussprechen.

(8) Der IT-Planungsrat gibt sich eine Geschäftsordnung. Darin sind insbesondere Regelungen vorzusehen, die sicherstellen, dass, sofern erforderlich, eine Kabinettsbehandlung oder andere notwendige Abstimmungen über einen im IT-Planungsrat vorgesehenen Beschluss rechtzeitig durchgeführt werden können.

Abschnitt II
Gemeinsame Standards und Sicherheitsanforderungen, Informationsaustausch

§ 2 Festlegung von IT-Interoperabilitäts- und IT-Sicherheitsstandards

(1) Für den im Rahmen ihrer Aufgabenerfüllung notwendigen Austausch von Daten zwischen dem Bund und den Ländern sollen gemeinsame Standards für die auszutauschenden Datenobjekte, Datenformate und Standards für Verfahren, die zur Datenübertragung erforderlich sind, sowie IT-Sicherheitsstandards festgelegt werden, soweit nicht eine spezialgesetzliche Regelungsbefugnis vorliegt. Hierbei ist vorrangig auf bestehende Marktstandards abzustellen.

(2) Beschlüsse über Standards im Sinne des Absatz 1 werden vom IT-Planungsrat mit der Zustimmung des Bundes und einer Mehrheit von elf Ländern, welche mindestens zwei Drittel ihrer Finanzierungsanteile nach dem Königsteiner Schlüssel abbildet, gefasst, soweit dies zum bund-länderübergreifenden Datenaustausch oder zur Vereinheitlichung des Datenaustauschs der öffentlichen Verwaltung mit Bürgern und Wirtschaft notwendig ist. Diese Beschlüsse entfalten Bindungswirkung und werden vom Bund und den Ländern innerhalb jeweils vom IT-Planungsrat festzusetzender Fristen in ihren jeweiligen Verwaltungsräumen umgesetzt.

(3) Vor einer Beschlussfassung über verbindliche Standards im Sinne des Absatz 1 wird auf Antrag des Bundes oder dreier Länder grundsätzlich der Bedarf für einen solchen Beschluss sowie die IT-fachliche Qualität und Widerspruchsfreiheit des vorgesehenen Standards durch eine vom IT-Planungsrat bestimmte, unabhängige Einrichtung geprüft. Die Einrichtung kann in ihre Prüfung weitere Personen oder Einrichtungen, insbesondere Fachleute aus Wirtschaft und Wissenschaft, einbeziehen. Der IT-Planungsrat entscheidet unter Einbeziehung der Ergebnisse der Prüfung; er ist dabei nicht an die Ergebnisse der Prüfung gebunden.

§ 3 Aufgaben im Bereich Verbindungsnetz

Der IT-Planungsrat nimmt die Aufgaben des Koordinierungsgremiums nach Maßgabe des aufgrund von Artikel 91c Absatz 4 des Grundgesetzes ergangenen Bundesgesetzes wahr.

§ 4 Informationsaustausch

Der Bund und die Länder informieren sich möglichst frühzeitig über beabsichtigte Vorhaben zur Einrichtung und Entwicklung informationstechnischer Systeme, um eine bedarfsgerechte Zusammenarbeit zu ermöglichen.

Abschnitt III
Gemeinsame Einrichtung zur Unterstützung des IT-Planungsrats

§ 5 Errichtung und Aufgaben

(1) Die Vertragspartner errichten mit Wirkung zum 1. Januar 2020 eine rechtsfähige Anstalt des öffentlichen Rechts (gemeinsame Anstalt). Sie trägt die Bezeichnung „FITKO“ (Föderale IT-Kooperation) und hat ihren Sitz in Frankfurt am Main. Die gemeinsame Anstalt hat die Aufgabe, den IT-Planungsrat organisatorisch, fachlich und bei der Wahrnehmung der Aufgaben nach § 1 Absatz 1 zu unterstützen. Das Nähere regelt der IT-Planungsrat durch einstimmigen Beschluss und trifft dabei insbesondere Regelungen zu den Aufgaben, Befugnissen, der Wirtschaftsführung und Leitung der gemeinsamen Anstalt und ihrer Organe (Gründungsbeschluss).

(2) Der Gründungsbeschluss soll vorsehen, dass die gemeinsame Anstalt die Aufgaben bestehender Strukturen für Projekte und Produkte des IT-Planungsrats übernimmt. Er kann eine Rechtsnachfolge vorsehen und die hierzu bestehenden Verwaltungsabkommen außer Kraft setzen.

(3) Änderungen des Gründungsbeschlusses bedürfen der Zustimmung aller Mitglieder des IT-Planungsrats.

(4) Zur Wahrnehmung von Querschnittsaufgaben soll sich die gemeinsame Anstalt Dritter bedienen.

§ 6 Trägerschaft, Dienstherrnfähigkeit, anwendbares Recht

(1) Träger der gemeinsamen Anstalt sind die Vertragspartner zu gleichen Teilen. Die Anteile an der gemeinsamen Anstalt sind nicht übertragbar.

(2) Die gemeinsame Anstalt besitzt Dienstherrnfähigkeit.

(3) Für die Errichtung und den Betrieb der gemeinsamen Anstalt gilt das hessische Landesrecht, soweit in diesem Staatsvertrag, im Gründungsbeschluss oder in der Satzung der gemeinsamen Anstalt nichts anderes bestimmt ist. Für die Beamten der gemeinsamen Anstalt findet daneben das Beamtenstatusgesetz Anwendung. Für die Beschäftigten und Auszubildenden der gemeinsamen Anstalt gilt der Tarifvertrag für den Öffentlichen Dienst des Landes Hessen (TV-H) beziehungsweise der Tarifvertrag für Auszubildende des Landes Hessen in Ausbildungsberufen nach dem Berufsbildungsgesetz (TVA-H BBiG) einschließlich der diese Tarifverträge ergänzenden, ändernden und ersetzenden Tarifverträge in der jeweils geltenden Fassung. Beschäftigte nach Satz 3 können in einem außertariflichen Beschäftigungsverhältnis beschäftigt werden, soweit dies für die Durchführung der Aufgaben erforderlich ist und der Stellenplan eine entsprechende Ermächtigung enthält.

(4) Die gemeinsame Anstalt kann mit Zustimmung des Sitzlandes Aufgaben der Personalverwaltung und Personalwirtschaft einschließlich der Verarbeitung der hierfür erforderlichen Personalaktendaten auf Dienststellen des Sitzlandes übertragen. Diesen Stellen dürfen personenbezogene Daten der Beschäftigten übermittelt werden, soweit deren Kenntnis zur Erfüllung der übertragenen Aufgaben erforderlich ist.

(5) Der Versorgungslastenteilungs-Staatsvertrag über die Verteilung der Versorgungslasten bei bund- und länderübergreifenden Dienstherrenwechseln ist anzuwenden.

§ 7 Organe

(1) Die gemeinsame Anstalt wird von einem Präsidenten geleitet und vertreten. Er wird hierbei vom Verwaltungsrat beaufsichtigt.

(2) Der IT-Planungsrat nimmt die Funktion des Verwaltungsrats wahr. Entscheidungen des IT-Planungsrats, die er als Verwaltungsrat über Angelegenheiten der gemeinsamen Anstalt trifft, erfolgen nach Maßgabe des § 1 Absatz 7 Satz 1, soweit dieser Vertrag oder der Gründungsbeschluss keine abweichende Regelung enthält. Handelt es sich bei diesen Entscheidungen um die Satzung der gemeinsamen Anstalt und ihre Änderungen, so sind diese im elektronischen Bundesanzeiger zu veröffentlichen.

(3) Der Präsident wird vom IT-Planungsrat für die Dauer von höchstens fünf Jahren bestellt. Erneute Bestellungen sind zulässig. Der Präsident beruft einen Vertreter für den Fall seiner Abwesenheit.

§ 8 Aufsicht

Die gemeinsame Anstalt unterliegt der Rechtsaufsicht der Vertragspartner. Die Rechtsaufsicht wird vom Sitzland ausgeübt. Das Sitzland stellt vor der Ausübung von aufsichtlichen Maßnahmen mit den Vertragspartnern Einvernehmen her, sofern nicht ein Eilfall entgegensteht. Jeder Vertragspartner kann beim Sitzland aufsichtliche Maßnahmen beantragen. Zu-

ständige Stellen für Angelegenheiten der Rechtsaufsicht durch die Vertragspartner sind die Ministerien oder die Behörden, denen die jeweiligen Vertreter für Informationstechnik als Mitglieder des IT-Planungsrats (§ 1 Absatz 2) angehören.

§ 9 Finanzierung

(1) Die gemeinsame Anstalt erhält zur Erfüllung ihrer Aufgaben von den Vertragspartnern Finanzmittel nach Maßgabe des Wirtschaftsplans und der jeweiligen Haushalte des Bundes und der Länder.

(2) Für die Jahre 2020 bis 2022 verpflichten sich die Vertragspartner darüber hinaus, ein Digitalisierungsbudget im Umfang von bis zu 180 Millionen Euro zur Verfügung zu stellen. Mit dem Digitalisierungsbudget sollen Projekte und Produkte für die Digitalisierung von Verwaltungsleistungen, die auf allen föderalen Ebenen zum Einsatz kommen, unterstützt werden. Das Digitalisierungsbudget sowie die daraus zu finanzierenden Projekte und Produkte werden im Wirtschaftsplan gesondert ausgewiesen.

(3) Der Wirtschaftsplan und seine Änderungen werden durch den IT-Planungsrat gemäß § 1 Absatz 7 beschlossen. Der Wirtschaftsplan sowie eventuelle Änderungen bedürfen der Zustimmung der Finanzministerkonferenz und des Bundesministeriums des Innern, für Bau und Heimat im Einvernehmen mit dem Bundesministerium der Finanzen. Sie sind der Konferenz der Chefs des Bundekanzleramtes mit den Chefs der Staats- und Senatskanzleien nach § 1 Absatz 1 Satz 2 vorzulegen.

(4) Die Finanzierung der gemeinsamen Anstalt und ihrer Aufgaben erfolgt nach dem Königsteiner Schlüssel, erweitert um einen festen Finanzierungsanteil des Bundes in Höhe von 25 Prozent, soweit im Wirtschaftsplan für einzelne Projekte oder Produkte keine abweichende Regelung getroffen wird. Das Sitzland trägt vorweg eine Sitzlandquote. Diese beträgt 10 Prozent der Personal- und Verwaltungskosten der FITKO, ohne die auf das Digitalisierungsbudget entfallenden Beträge. Für die über das Digitalisierungsbudget nach Absatz 2 zu finanzierenden Projekte und Produkte wird der Königsteiner Schlüssel mit einem festen Finanzierungsanteil des Bundes in Höhe von 35 Prozent zugrunde gelegt.

(5) Die Ausführung des Wirtschaftsplans steht unter dem Vorbehalt der jeweiligen haushaltsrechtlichen Ermächtigung der Vertragspartner.

(6) Die Rechnungshöfe der Vertragspartner prüfen die Haushalts- und Wirtschaftsführung der gemeinsamen Anstalt.

(7) Die Zuweisung der Finanzmittel aus dem Wirtschaftsplan für das erste Halbjahr 2020 erfolgt zum 2. Januar 2020. Zur Sicherstellung der unterbrechungsfreien Auszahlung der Besoldung der Beamten, die zum 1. Januar 2020 von einem Dienstverhältnis bei einem der Vertragspartner in die gemeinsame Anstalt wechseln, wird der abgebende Vertragspartner die Besoldung für den Januar 2020 auszahlen. Er erlangt einen Rückzahlungsanspruch in voller Höhe der geleisteten Zahlungen gegenüber der gemeinsamen Anstalt.

§ 10 Unzulässigkeit eines Insolvenzverfahrens

Ein Insolvenzverfahren über das Vermögen der gemeinsamen Anstalt ist unzulässig.

Abschnitt IV
Schlussbestimmungen

§ 11 Änderung, Kündigung

(1) Änderungen dieses Vertrages bedürfen einer einstimmigen Entscheidung der Vertragspartner.

(2) Dieser Vertrag kann von jedem Vertragspartner unter Einhaltung einer zweijährigen Frist zum Jahresende gekündigt werden. Die Kündigung ist durch Kundgabe an die gemeinsame Anstalt für den IT-Planungsrat gegenüber den übrigen Vertragspartnern schriftlich zu erklären.

(3) Die Kündigung gilt auch für die auf der Grundlage dieses Vertrages geschlossenen Vereinbarungen. Mit Wirksamwerden der Kündigung endet die Trägerschaft an der gemeinsamen Anstalt. Die Kündigung lässt das Bestehen des Vertrages und der auf der Grundlage dieses Vertrages geschlossenen Vereinbarungen für die übrigen Vertragspartner vorbehaltlich der Regelung des § 12 Absatz 2 unberührt.

(4) Die gemeinsame Anstalt besteht unter der Trägerschaft der übrigen Vertragspartner weiter. Zwischen den verbleibenden Vertragspartnern und dem kündigenden Vertragspartner wird eine öffentlich-rechtliche Vereinbarung über die Auseinandersetzung, insbesondere über die Verteilung des Aktivvermögens sowie die Übernahme der bestehenden Verbindlichkeiten und Versorgungslasten, geschlossen. In der Auseinandersetzungsvereinbarung sind auch die Konsequenzen für das Personal der gemeinsamen Anstalt zu regeln. Eine Kündigung nach Absatz 2 wird erst wirksam, wenn die Auseinandersetzungsvereinbarung vorliegt.

§ 12 Inkrafttreten, Außerkrafttreten, Übergangsregelung

(1) Dieser Vertrag tritt am 1. April 2010 in Kraft. Sind bis zum 31. März 2010 nicht mindestens dreizehn Ratifikationsurkunden bei dem der Ministerpräsidentenkonferenz vorsitzenden Land hinterlegt, wird der Vertrag gegenstandslos.

(2) Der Vertrag tritt außer Kraft, wenn die Zahl der Vertragspartner zehn unterschreitet. Für diesen Fall enden seine Wirkungen mit dem Ablauf der Kündigungsfrist des zuletzt kündigenden Vertragspartners. Die gemeinsame Anstalt gilt mit dem Wirksamwerden der Kündigung des zuletzt kündigenden Vertragspartners als aufgelöst.

(3) Im Falle des Absatzes 2 gilt § 11 Absatz 4 Satz 2 entsprechend. Die Vertragspartner regeln die Übernahme von Beamten und Versorgungsempfängern der gemeinsamen Anstalt durch einen oder mehrere Vertragspartner im Rahmen der Auseinandersetzungsvereinbarung einvernehmlich, § 6 Absatz 5 ist entsprechend anzuwenden. Es gelten die Regelungen des dritten Abschnitts des Beamtenstatusgesetzes und des Hessischen Beamtengesetzes über den vollständigen Übergang der Aufgaben einer Körperschaft auf mehrere andere entsprechend. Die Vertragspartner sollen den Tarifbeschäftigten (einschließlich der Auszubildenden) der gemeinsamen Anstalt ein Übernahmeangebot zu einem oder mehreren der Vertragspartner stellen. Kündigungen der Vertragspartner, die zur Auflösung der gemeinsamen Anstalt nach Absatz 2 führen, werden erst wirksam, wenn die Auseinandersetzungsvereinbarung vorliegt.

(4) Bestehende Vereinbarungen der Vertragspartner über die gemeinschaftliche Aufgabenerledigung im Bereich informationstechnischer Systeme werden von den Bestimmungen dieses Vertrages, soweit sie diesen nicht widersprechen, nicht berührt. Mit dem Außerkrafttre-

ten bereits bestehender Vereinbarungen werden die Bestimmungen dieses Vertrages auf sie anwendbar.

(5) Die nach § 2 des IT-Staatsvertrags in der Fassung vom 1. April 2010 beim Bundesministerium des Innern, für Bau und Heimat eingerichtete Geschäftsstelle wird bis zum 30. Juni 2020 fortgeführt. Danach gehen die Aufgaben der Geschäftsstelle auf die gemeinsame Anstalt über. Die gemeinsame Anstalt tritt insoweit in die Rechtsnachfolge ein.

Anhang „Gemeinsames Grundverständnis der technischen und organisatorischen Ausgestaltung der Bund/Länder-Zusammenarbeit bei dem Verbindungsnetz und der IT-Steuerung"

A. Verbindungsnetz

1. Bund und Länder tragen gemeinsam die Verantwortung für ein künftiges Verbindungsnetz.
   a) Gemeinsam werden festgelegt:
      - die Anforderungen (z. B. hinsichtlich Datenschutz, Sicherheit), die vom Verbindungsnetz zu erfüllen sind,
      - die anzubietenden Anschlussklassen (inklusive beispielsweise Bandbreiten, Verfügbarkeiten),
      - das Minimum anzubietender Dienste,
      - die Anschlussbedingungen,
      - die Kostenhöhe und -verteilung,
      - das Verfahren bei Eilentscheidungen.

   b) In diesem Rahmen betreibt der Bund das Verbindungsnetz und setzt dabei die gemeinsamen Festlegungen um.
2. Die Länder haben gemeinsam mit dem Bund den DOI-Netz e. V. gegründet. Von diesem wird gegenwärtig ein Verbindungsnetz vergeben. Diese Lösung soll zum nächstmöglichen Zeitpunkt in die neuen Strukturen überführt werden.
3. Der Bund betreibt gegenwärtig die Neugestaltung seiner IT-Netze in einer modularen Architektur und auf der Grundlage eines Transportnetzes auf Basis von Dark Fibre. Dies geschieht in ausschließlicher Zuständigkeit des Bundes. Unter Nutzung des Transportnetzes dieser ohnehin im Aufbau befindlichen bundesweiten IT-Netzinfrastruktur kann das Verbindungsnetz als eigenes VPN (einschließlich Zugangsnetz) realisiert werden. Möglich ist außerdem die optionale Nutzung von Diensten aus dem Portfolio (Warenkorb) des Projektes „Netze des Bundes".
4. Der Bund ist die Vergabestelle für das Verbindungsnetz. Als Vergabestelle ist der Bund für die rechtlich korrekte Durchführung der Vergabe inklusive der Wahl des Vergabeverfahrens verantwortlich und wird nach dem Zuschlag Vertragspartner des Auftragnehmers.
5. Die Vergabeunterlagen werden vom Bund im Benehmen mit einem vom IT-Planungsrat eingesetzten Arbeitsgremium aus 3 Ländervertretern fertig gestellt.

6. Zur Beteiligung der Länder werden die Entwürfe der Vergabeunterlagen (inklusive Bewertungsmatrix) rechtzeitig vor der Veröffentlichung (z. B. in sogenannten „Leseräumen“[1]) zur Einsicht bereit gestellt. Dies dient zum einen der Information der Länder über die Umsetzung der gemeinsam festgelegten Anforderungen, zum anderen kann so der dort vorhandene Sachverstand in die Erstellung der Vergabeunterlagen einfließen.

7. Sollten durch Anforderungen des Bundes, die über die gemeinsam festgelegten Anforderungen hinausgehen, zusätzliche Kosten entstehen, so sind diese vom Bund zu tragen. Das Verfahren zur Feststellung der Zusatzkosten regelt der IT-Planungsrat[2].

8. Um auch im laufenden Betrieb eine Beteiligung der Länder sicher zu stellen, beauftragt der IT-Planungsrat das dreiköpfige Arbeitsgremium damit, die Interessen der Länder bei der Steuerung des Betriebs einzubringen. Dies betrifft insbesondere grundsätzlichere Fragen der Steuerung. Operative Fragen (z. B. die Bestellung eines neuen Anschlusses, die Veränderung einer Anschlussklasse, die Zubuchung eines optionalen Dienstes etc.) werden hingegen über dafür geschaffene Prozesse abgewickelt.

B. IT-Steuerung

1. Ein neues System der IT-Koordinierung von Bund und Ländern soll die bisherigen Gremien “Arbeitskreis der Staatssekretäre für E-Government in Bund und Ländern” (St-Runde Deutschland-Online) sowie “Kooperationsausschuss von Bund und Ländern für automatisierte Datenverarbeitung” (KoopA ADV) sowie alle Untergremien ablösen.

2. Die dauerhafte neue Struktur besteht aus einem „IT-Planungsrat“, in dem der Beauftragte der Bundesregierung für Informationstechnik, die für IT zuständigen Vertreter der Länder, Vertreter der drei kommunalen Spitzenverbände (ohne Stimmrecht) und der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (ohne Stimmrecht) vertreten sind. Der IT-Planungsrat berichtet an die Konferenz der Regierungschefs von Bund und Ländern.

3. Den Vorsitz übernehmen im jährlichen Wechsel Bund und Länder. Die Länder regeln die Rotation des Vorsitzes untereinander.

4. Die bisherige Geschäftsstelle Deutschland-Online im Bundesministerium des Innern wird Geschäftsstelle des IT-Planungsrates. Die Finanzierung der Geschäftsstelle übernimmt zur Hälfte der Bund, zur Hälfte übernehmen sie die Länder nach dem Königsteiner Schlüssel.

5. Der IT-Planungsrat hat folgende Aufgaben:

   a) Koordinierung der Zusammenarbeit von Bund und Ländern in Fragen der Informationstechnik,

   b) Beschlussfassung über fachunabhängige oder fachübergreifende IT-Interoperabilitäts- und IT-Sicherheitsstandards,

1) „Leseräume“ stellen angesichts der Zahl der Beteiligten sicher, dass die vertraulichen Dokumente nicht vor der Veröffentlichung bekannt werden und so das Vergabeverfahren gefährden.
2) Das Antragsrecht zur Durchführung dieses Verfahrens haben der Bund oder drei Länder.

c) Steuerung von E-Government-Projekten, die dem IT-Planungsrat von der Konferenz der Regierungschefs von Bund und Ländern zugewiesen werden,

d) Planung und Weiterentwicklung des Verbindungsnetzes inklusive gemeinsamer Festlegung gemäß Ziffer A. 1 a) und Überwachung der Umsetzung der gemeinsamen Festlegungen,

e) Einsetzen eines Arbeitsgremiums zur Befassung mit Vergabeunterlagen (Einzelheiten unter A. 6) und grundsätzlicher Steuerung (A. 9).

6. IT-Interoperabilitäts- und IT-Sicherheitsstandards

   – werden vom IT-Planungsrat mit einfacher Mehrheit als Empfehlung für die öffentliche Verwaltung beschlossen;

   – werden vom IT-Planungsrat mit noch auszugestaltender, qualifizierter Mehrheit beschlossen, soweit sie zum bund-länderübergreifenden Datenaustausch oder zur Vereinheitlichung des Datenaustausches der öffentlichen Verwaltung mit Bürgern und Wirtschaft erforderlich sind; sie entfalten Bindungswirkung, welche vom Bund und von den Ländern innerhalb von jeweils vom IT-Planungsrat festzusetzenden Fristen in ihren jeweiligen Verwaltungsräumen umgesetzt wird.

7. Der IT-Planungsrat beteiligt die jeweilige Fachministerkonferenz, soweit deren Fachplanungen betroffen sind.

8. Vor der Beschlussfassung im IT-Planungsrat stimmen die Vertreter von Bund und Ländern die zu fassenden Beschlüsse innerhalb ihrer Regierung ab bzw. führen – soweit erforderlich – eine Befassung des jeweiligen Kabinetts herbei.

9. Vor einer Beschlussfassung über verbindliche Standards wird grundsätzlich der Bedarf für einen solchen Beschluss sowie die IT-fachliche Qualität und Widerspruchsfreiheit des vorgesehenen Standards durch eine vom IT-Planungsrat bestimmte unabhängige Einrichtung geprüft, diese kann in ihre Prüfung Wirtschaft und Wissenschaft einbeziehen. Der IT-Planungsrat entscheidet unter Einbeziehung der Ergebnisse der Prüfung; er ist dabei nicht an die Ergebnisse der Prüfung gebunden.

Gesetz über die Verbindung der informationstechnischen Netze des Bundes und der Länder – Gesetz zur Ausführung von Artikel 91c Absatz 4 des Grundgesetzes – (IT-NetzG)

§ 1 Gegenstand der Zusammenarbeit; Koordinierungsgremium

(1) Der Bund errichtet zur Verbindung der informationstechnischen Netze des Bundes und der Länder ein Verbindungsnetz. Bund und Länder wirken hierfür nach Maßgabe dieses Gesetzes zusammen; insbesondere treffen sie die notwendigen gemeinsamen Festlegungen für das Verbindungsnetz.

(2) Die Zusammenarbeit erfolgt im Koordinierungsgremium für das Verbindungsnetz (Koordinierungsgremium). Dem Koordinierungsgremium gehören als stimmberechtigte Mitglieder an:

1. die oder der Beauftragte der Bundesregierung für Informationstechnik als Vertreter des Bundes,
2. die zuständigen Vertreterinnen oder Vertreter der Länder.

(3) Besteht aufgrund einer für den Bund und alle Länder wirksamen Vereinbarung nach Artikel 91c Absatz 2 des Grundgesetzes über die Zusammenarbeit ein Gremium, das entsprechend den Vorgaben des Absatzes 2 Satz 2 besetzt ist (IT-Planungsrat), übernimmt dieses Gremium auch die Aufgaben des Koordinierungsgremiums nach Maßgabe dieses Gesetzes. Die in der Vereinbarung getroffenen Regelungen finden in diesem Fall ergänzend Anwendung, soweit sie diesem Gesetz nicht widersprechen.

§ 2 Begriffsbestimmungen

(1) Informationstechnische Netze im Sinne dieses Gesetzes sind die Gesamtheit von Übertragungssystemen und gegebenenfalls Vermittlungs- und Leitwegeinrichtungen sowie anderweitigen Ressourcen, die die Übertragung von Signalen ermöglichen. Ausgenommen sind digitale Dienste nach § 1 Absatz 4 Nummer 1 des Digitale-Dienste-Gesetzes, Rundfunk sowie Sprechfunk- und Telefonnetze.

(2) Verbindungsnetz im Sinne dieses Gesetzes ist das informationstechnische Netz, welches die informationstechnischen Netze des Bundes und der Länder verbindet. Die Übergabepunkte zu den jeweils verbundenen Netzen werden gemeinsam vereinbart.

§ 3 Datenaustausch; Verordnungsermächtigung

(1) Der Datenaustausch zwischen dem Bund und den Ländern erfolgt über das Verbindungsnetz. Im Anwendungsbereich des Onlinezugangsgesetzes kann der Datenaustausch auch über andere Netze des Bundes, die einen dem beabsichtigten Datenaustausch entsprechenden IT-Sicherheitsstandard aufweisen, erfolgen.

(2) Das Bundesministerium des Innern und für Heimat wird ermächtigt, nach Prüfung durch das Bundesamt für Sicherheit in der Informationstechnik und im Benehmen mit dem Koordinierungsgremium durch Rechtsverordnung ohne Zustimmung des Bundesrates andere Netze nach Absatz 1 sowie deren Anschlussklassen und IT-Sicherheitsstandards festzulegen.

§ 4 Beschlüsse über das Verbindungsnetz

(1) Der Bund und die Länder beschließen gemeinsam im Koordinierungsgremium für das Verbindungsnetz die folgenden Festlegungen:

1. die vom Verbindungsnetz zu erfüllenden Anforderungen,
2. die anzubietenden Anschlussklassen,
3. das Minimum anzubietender Dienste,
4. die Anschlussbedingungen,
5. die Höhe der Anschlusskosten sowie das Verfahren zu ihrer Ermittlung,
6. das Verfahren bei Eilentscheidungen.

(2) Über Beschlüsse nach Absatz 1 entscheidet das Koordinierungsgremium auf Antrag des Bundes oder eines Viertels seiner Mitglieder.

(3) Beschlüsse nach Absatz 1 kommen mit Zustimmung des Bundes und einer Mehrheit von elf Ländern zustande, welche mindestens zwei Drittel ihrer Finanzierungsanteile nach dem Königsteiner Schlüssel abbildet.

§ 5 Vergabe

(1) Hinsichtlich des Verbindungsnetzes ist gemeinsame Vergabestelle des Bundes und der Länder einschließlich der mittelbaren Bundes- und Landesverwaltung eine vom Bundesministerium des Innern, für Bau und Heimat zu bestimmende Bundesbehörde. Der Bund kann Unternehmen mit dem Aufbau und dem Betrieb des Verbindungsnetzes beauftragen.

(2) Der Bund stellt die Vergabeunterlagen im Benehmen mit einem vom Koordinierungsgremium eingesetzten Arbeitsgremium aus drei Ländervertretern fertig. Den Ländern wird zu ihrer Beteiligung rechtzeitig vor der Veröffentlichung der Vergabeunterlagen Einsicht in die Entwürfe der Vergabeunterlagen gewährt; dabei ist der Schutz vertraulicher Dokumente durch geeignete Maßnahmen sicherzustellen.

§ 6 Betrieb

(1) Der Bund betreibt das Verbindungsnetz. Er setzt dabei die gemeinsamen Festlegungen nach § 4 Absatz 1 um.

(2) Das Koordinierungsgremium überwacht die Umsetzung der gemeinsamen Festlegungen und beauftragt hierzu ein von ihm eingesetztes Arbeitsgremium aus drei Ländervertretern, bei der Steuerung des Betriebs des Verbindungsnetzes die Interessen der Länder einzubringen.

§ 7 Kosten

(1) Der Bund trägt die Kosten der Errichtung und des Betriebs des Verbindungsnetzes.

(2) Der Bund und die Länder sowie gegebenenfalls angeschlossene weitere öffentliche Stellen tragen jeweils die Kosten für den jeweiligen Anschluss ihres Netzes an das Verbindungsnetz.

(3) Entstehen durch Anforderungen des Bundes, die über die gemeinsamen Festlegungen hinausgehen, zusätzliche Anschlusskosten, sind diese vom Bund zu tragen.

(4) Für andere Netze des Bundes nach § 3 Absatz 1 Satz 2 gelten die Absätze 2 und 3 entsprechend.

§ 8 Übergangsregelung

Den Übergang der gegenwärtig vom Deutschland Online Infrastruktur e. V. (DOI-Netz e. V.) wahrgenommenen Aufgaben auf den Bund nach diesem Gesetz einschließlich des Zeitpunkts des Übergangs legen Bund und Länder im DOI-Netz e. V. gemeinsam fest.

Verordnung zur Schaffung barrierefreier Informationstechnik nach dem Behindertengleichstellungsgesetz (Barrierefreie-Informationstechnik-Verordnung - BITV 2.0)

Eingangsformel

Auf Grund des § 11 Absatz 1 Satz 2 des Behindertengleichstellungsgesetzes, das zuletzt durch Artikel 12 des Gesetzes vom 19. Dezember 2007 (BGBl. I S. 3024) geändert worden ist, verordnet das Bundesministerium für Arbeit und Soziales:

§ 1 Ziele

(1) Die Barrierefreie-Informationstechnik-Verordnung dient dem Ziel, eine umfassend und grundsätzlich uneingeschränkt barrierefreie Gestaltung moderner Informations- und Kommunikationstechnik zu ermöglichen und zu gewährleisten.

(2) Informationen und Dienstleistungen öffentlicher Stellen, die elektronisch zur Verfügung gestellt werden, sowie elektronisch unterstützte Verwaltungsabläufe mit und innerhalb der Verwaltung, einschließlich der Verfahren zur elektronischen Aktenführung und zur elektronischen Vorgangsbearbeitung, sind für Menschen mit Behinderungen zugänglich und nutzbar zu gestalten.

§ 2 Anwendungsbereich

(1) Die Verordnung gilt unter Berücksichtigung der Umsetzungsfristen der §§ 12a bis 12c des Behindertengleichstellungsgesetzes für folgende Angebote, Anwendungen und Dienste:

1. Websites,
2. mobile Anwendungen,
3. elektronisch unterstützte Verwaltungsabläufe, einschließlich der Verfahren zur elektronischen Vorgangsbearbeitung und elektronischen Aktenführung,
4. grafische Programmoberflächen, die
   a) in die Angebote, Anwendungen und Dienste nach den Nummern 1 bis 3 integriert sind oder
   b) von den öffentlichen Stellen zur Nutzung bereitgestellt werden.

(2) Von der Anwendung dieser Verordnung ausgenommen sind folgende Inhalte von Websites und mobilen Anwendungen:

1. Reproduktionen von Stücken aus Kulturerbesammlungen, die nicht vollständig barrierefrei zugänglich gemacht werden können aufgrund
   a) der Unvereinbarkeit der Barrierefreiheitsanforderungen mit der Erhaltung des betreffenden Gegenstandes oder der Authentizität der Reproduktion oder
   b) der Nichtverfügbarkeit automatisierter und kosteneffizienter Lösungen, mit denen die betreffenden Stücke aus Kulturerbesammlungen in barrierefreie Inhalte umgewandelt werden können,

2. Archive, die weder Inhalte enthalten, die für aktive Verwaltungsverfahren benötigt werden, noch nach dem 23. September 2019 aktualisiert oder überarbeitet wurden, sowie
3. Inhalte von Websites und mobilen Anwendungen von Rundfunkanstalten des Bundesrechts, die der Wahrnehmung eines öffentlichen Sendeauftrags dienen.

(3) Für den Erhalt der Einsatzfähigkeit der Streitkräfte kann die Bundesministerin oder der Bundesminister der Verteidigung Ausnahmen von dieser Verordnung festlegen.

§ 2a Begriffsdefinitionen

(1) Websites im Sinne dieser Verordnung sind Auftritte, die

1. mit Webtechnologien, beispielsweise HTML, erstellt sind,
2. über eine individuelle Webadresse erreichbar sind und
3. mit einem Nutzeragenten, beispielsweise Browser, wiedergegeben werden können.

Zum Inhalt von Websites gehören textuelle und nicht textuelle Informationen sowie Interaktionen. Integrierte Inhalte in unterschiedlichen Formaten, beispielsweise Dokumente, Videos, Audiodateien, sowie integrierte Funktionalitäten, beispielsweise Formulare, Authentifizierungs-, Identifizierungs- und Zahlungsprozesse, sind Bestandteile von Websites. Von dieser Verordnung umfasst sind auch solche Websites, die sich ausschließlich an einen abgegrenzten Personenkreis richten, wie Intranets oder Extranets.

(2) Mobile Anwendungen im Sinne dieser Verordnung sind Programme, die auf mobilen Geräten, beispielsweise Smartphones und Tablets, installiert werden. Nicht dazu gehören Betriebssysteme und Hardware, auf denen die mobile Anwendung betrieben wird. Integrierte Inhalte in unterschiedlichen Formaten, beispielsweise Dokumente, Videos, Audiodateien, sind Bestandteile der mobilen Anwendungen.

(3) Elektronisch unterstützte Verwaltungsabläufe im Sinne dieser Verordnung sind Verfahren, die im Rahmen des Verwaltungshandelns intern oder extern angewandt werden und sich der Informations- und Kommunikationstechnik bedienen. Hierzu zählen insbesondere Verfahren zur elektronischen Vorgangsbearbeitung und elektronischen Aktenführung. Integrierte Inhalte in unterschiedlichen Formaten, beispielsweise Dokumente, Videos, Audiodateien, sind Bestandteile der elektronisch unterstützten Verwaltungsabläufe.

(4) Elektronische Vorgangsbearbeitung im Sinne dieser Verordnung ist die Unterstützung von Geschäftsprozessen und Verwaltungsabläufen durch Informations- und Kommunikationstechnik. Dazu zählen unter anderem

1. die Zuweisung und der Transport von Dokumenten an bearbeitende Personen,
2. die Bearbeitung dieser Dokumente,
3. die Darstellung von Prozessen, Organigrammen und Verantwortlichkeiten,
4. die Terminplanung und
5. die Protokollierung.

(5) Elektronische Aktenführung im Sinne dieser Verordnung ist die systematische und programmgestützte Vorhaltung und Nutzung von Dokumenten in elektronischer Form, beispielsweise mittels Dokumentenmanagementsystems.

(6) Grafische Programmoberflächen im Sinne dieser Verordnung sind webbasierte und nicht webbasierte Anwendungen einschließlich der

1. grafischen Nutzerschnittstellen auf zweidimensionalen Bildschirmen und Displays
2. grafischen Nutzerschnittstellen in dreidimensionalen virtuellen Repräsentationen oder in Echtzeit-Raum-Repräsentationen.

§ 3 Anzuwendende Standards

(1) Die in § 2 genannten Angebote, Anwendungen und Dienste der Informationstechnik sind barrierefrei zu gestalten. Dies erfordert, dass sie wahrnehmbar, bedienbar, verständlich und robust sind.

(2) Die Erfüllung der Anforderungen nach Absatz 1 wird vermutet, wenn diese Angebote, Anwendungen und Dienste

1. harmonisierten Normen oder Teilen dieser Normen entsprechen, und
2. die harmonisierten Normen oder Teile dieser Normen im Amtsblatt der Europäischen Union genannt worden sind.

(3) Soweit Nutzeranforderungen oder Teile von Angeboten, Diensten oder Anwendungen nicht von harmonisierten Normen abgedeckt sind, sind sie nach dem Stand der Technik barrierefrei zu gestalten.

(4) Für zentrale Navigations- und Einstiegsangebote sowie Angebote, die eine Nutzerinteraktion ermöglichen, beispielsweise Formulare und die Durchführung von Authentifizierungs-, Identifizierungs- und Zahlungsprozessen, soll ein höchstmögliches Maß an Barrierefreiheit angestrebt werden.

(5) Die Überwachungsstelle nach § 13 Absatz 3 des Behindertengleichstellungsgesetzes veröffentlicht auf ihrer Website regelmäßig alle zur Umsetzung dieser Verordnung erforderlichen Informationen in deutscher Sprache, insbesondere

1. aktuelle Informationen zu den zu beachtenden Standards, aus denen die Barrierefreiheitsanforderungen detailliert hervorgehen,
2. Konformitätstabellen, die einen Überblick zu den wichtigsten Barrierefreiheitsanforderungen geben,
3. Empfehlungen des Ausschusses für barrierefreie Informationstechnik nach § 5 sowie
4. weiterführende Erläuterungen.

§ 4 Erläuterungen in Deutscher Gebärdensprache und Leichter Sprache

Auf der Startseite einer Website einer öffentlichen Stelle sind nach Anlage 2 folgende Erläuterungen in Deutscher Gebärdensprache und in Leichter Sprache bereitzustellen:

1. Informationen zu den wesentlichen Inhalten,

2. Hinweise zur Navigation,
3. eine Erläuterung der wesentlichen Inhalte der Erklärung zur Barrierefreiheit,
4. Hinweise auf weitere in diesem Auftritt vorhandene Informationen in Deutscher Gebärdensprache und in Leichter Sprache.

§ 5 Ausschuss für barrierefreie Informationstechnik

(1) Bei der nach § 13 Absatz 3 des Behindertengleichstellungsgesetzes einzurichtenden Überwachungsstelle des Bundes für Barrierefreiheit von Informationstechnik wird ein Ausschuss für barrierefreie Informationstechnik eingerichtet. Der Ausschuss besteht aus fachkundigen Vertreterinnen und Vertretern aus der Überwachungsstelle, aus den Landes-Überwachungsstellen, aus Verbänden von Menschen mit Behinderungen und aus der Wirtschaft sowie weiteren fachkundigen Personen, insbesondere aus der Wissenschaft und aus öffentlichen Stellen im Sinne des § 12 des Behindertengleichstellungsgesetzes. An den Sitzungen des Ausschusses kann eine Vertreterin oder ein Vertreter des Bundesministeriums für Arbeit und Soziales teilnehmen.

(2) Zu den Aufgaben des Ausschusses gehört es,

1. den jeweils aktuellen Stand der Technik nach § 3 Absatz 2 und 3 zu ermitteln und zu dokumentieren,
2. sonstige gesicherte Erkenntnisse zur barrierefreien Informationstechnik zu ermitteln und zu dokumentieren, insbesondere Erkenntnisse bezüglich eines höchstmöglichen Maßes an Barrierefreiheit im Sinne von § 3 Absatz 4,
3. Empfehlungen zur praktischen Umsetzung der Anforderungen nach § 3 zu erarbeiten.

Veröffentlichungen des Ausschusses in Zusammenhang mit seinen Aufgaben bedürfen der vorherigen Zustimmung des Bundesministeriums für Arbeit und Soziales.

(3) Die Überwachungsstelle beruft die Mitglieder des Ausschusses in Abstimmung mit dem Bundesministerium für Arbeit und Soziales. Die Mitgliedschaft endet mit Ablauf des dritten Kalenderjahres nach der Berufung. Die Wiederberufung nach Beendigung der Mitgliedschaft ist zulässig. Die vorzeitige Abberufung aus wichtigem Grund ist zulässig.

(4) Der Ausschuss gibt sich zur Organisation seiner Arbeit eine Geschäftsordnung, die der Zustimmung des Bundesministeriums für Arbeit und Soziales bedarf.

(5) Der Ausschuss wird bei seiner Arbeit durch eine Geschäftsstelle unterstützt. Die Geschäftsstelle wird bei der Überwachungsstelle eingerichtet. Bei der Erfüllung seiner Aufgaben wird der Ausschuss darüber hinaus durch die Informationstechnik-Dienstleister des Bundes unterstützt.

§ 6 Beratung und Unterstützung durch die Bundesfachstelle für Barrierefreiheit und die Informationstechnik-Dienstleister des Bundes

Die Bundesfachstelle für Barrierefreiheit als zentrale Anlaufstelle zu Fragen der Barrierefreiheit berät die öffentlichen Stellen des Bundes im Rahmen der Erstberatung nach § 13 Absatz 2 Satz 3 Nummer 1 des Behindertengleichstellungsgesetzes zur barrierefreien Gestaltung nach Maßgabe dieser Rechtsverordnung. Das Informationstechnikzentrum Bund und die

BWI GmbH als zentrale Informationstechnik-Dienstleister der Bundesverwaltung beraten und unterstützen bei der technischen Umsetzung der IT-Barrierefreiheit.

§ 7 Erklärung zur Barrierefreiheit

(1) Die Erklärung zur Barrierefreiheit nach § 12b des Behindertengleichstellungsgesetzes ist in einem barrierefreien und maschinenlesbaren Format zu veröffentlichen und muss von der Startseite und von jeder Seite einer Website erreichbar sein. Für mobile Anwendungen ist die Erklärung an der Stelle, an der das Herunterladen der mobilen Anwendung ermöglicht wird, oder auf der Website der öffentlichen Stelle, zu veröffentlichen.

(2) Die nach § 12b Absatz 2 Nummer 2 des Behindertengleichstellungsgesetzes bereitzustellende Möglichkeit, elektronisch Kontakt aufzunehmen (Feedback-Mechanismus), soll von jeder Seite einer Website oder innerhalb der Navigation einer mobilen Anwendung unmittelbar zugänglich und einfach zu benutzen sein.

(3) Die Erklärung zur Barrierefreiheit muss umfassende, detaillierte und klar verständliche Angaben zur Vereinbarkeit der Website oder der mobilen Anwendung mit den Anforderungen zur Barrierefreiheit nach den §§ 3 und 4 enthalten.

(4) Die obligatorischen Inhalte, die im Abschnitt 1 des Anhangs zum Durchführungsbeschluss (EU) 2018/1523 der Kommission vom 11. Oktober 2018 zur Festlegung einer Mustererklärung zur Barrierefreiheit gemäß der Richtlinie (EU) 2016/2102 des Europäischen Parlaments und des Rates über den barrierefreien Zugang zu den Websites und mobilen Anwendungen öffentlicher Stellen (ABl. L 256 vom 12.10.2018, S. 103) festgelegt sind, sind in die Erklärung zur Barrierefreiheit aufzunehmen. Die öffentlichen Stellen sollen nach Möglichkeit auch Angaben zu den in Abschnitt 2 aufgeführten fakultativen Inhalten aufnehmen, insbesondere Angaben zu

1. Maßnahmen, die über die Mindestanforderungen an die barrierefreie Gestaltung hinausgehen, und
2. Maßnahmen, die zur Beseitigung von Barrieren ergriffen werden sollen.

Die Überwachungsstelle nach § 13 Absatz 3 des Behindertengleichstellungsgesetzes veröffentlicht auf ihrer Website eine Mustererklärung.

(5) Zur Erstellung der Erklärung zur Barrierefreiheit ist eine tatsächliche Bewertung der Vereinbarkeit der Website oder der mobilen Anwendung mit den in § 3 Absatz 1 bis 3 festgelegten Anforderungen vorzunehmen. In der Erklärung ist darzulegen, ob die Bewertung durch einen Dritten, beispielsweise in Form einer Zertifizierung, oder durch die öffentliche Stelle selbst vorgenommen wurde. Die Erklärung kann einen Link zu einem Bewertungsbericht enthalten.

(6) Die Erklärung zur Barrierefreiheit ist jährlich und bei jeder wesentlichen Änderung der Website oder der mobilen Anwendung zu aktualisieren.

§ 8 Überwachungsverfahren

(1) Das Überwachungsverfahren nach § 13 Absatz 3 Satz 2 Nummer 1 des Behindertengleichstellungsgesetzes ist durch die Überwachungsstelle nach § 13 Absatz 3 des Behindertengleichstellungsgesetzes durchzuführen unter Beachtung der Anforderungen der Artikel 1 bis 7 sowie des Anhangs I des Durchführungsbeschlusses (EU) 2018/1524 der Kommission vom 11. Oktober 2018 zur Festlegung einer Überwachungsmethodik und der Modalitäten für die

Berichterstattung der Mitgliedstaaten gemäß der Richtlinie (EU) 2016/2102 des Europäischen Parlaments und des Rates über den barrierefreien Zugang zu Websites und mobilen Anwendungen öffentlicher Stellen (ABl. L 256 vom 12.10.2018, S. 108).

(2) Die Überwachungsstelle erfasst im Rahmen ihrer Prüfungen die Erfüllung der Voraussetzungen nach Artikel 6 der Richtlinie (EU) 2016/2102 und die Erfüllung der sich ergänzend aus § 12a des Behindertengleichstellungsgesetzes und dieser Verordnung ergebenden Anforderungen getrennt. Sie kann ergänzend auch eine Prüfung der Benutzerfreundlichkeit vornehmen.

(3) Die Überwachungsstelle kann anlassbezogene Prüfungen und Wiederholungsprüfungen vornehmen.

(4) Die Verbände und Organisationen von Menschen mit Behinderungen sowie der Ausschuss nach § 5 werden in die Entwicklung und Evaluation der Überwachungsmethoden einbezogen. Die Überwachungsstelle konsultiert bei der Auswahl der zu überwachenden Websites und mobilen Anwendungen die Verbände und Organisationen von Menschen mit Behinderungen und berücksichtigt ihre Einschätzungen zu einzelnen Websites und mobilen Anwendungen.

§ 9 Berichterstattung

(1) Der Bericht an die Europäische Kommission wird durch die Überwachungsstelle nach § 13 Absatz 3 des Behindertengleichstellungsgesetzes erstellt unter Beachtung der Anforderungen der Artikel 8 bis 11 sowie des Anhangs II des Durchführungsbeschlusses (EU) 2018/1524 der Kommission vom 11. Oktober 2018 zur Festlegung einer Überwachungsmethodik und der Modalitäten für die Berichterstattung der Mitgliedstaaten gemäß der Richtlinie (EU) 2016/2102 des Europäischen Parlaments und des Rates über den barrierefreien Zugang zu Websites und mobilen Anwendungen öffentlicher Stellen (ABl. L 256 vom 12.10.2018, S. 108).

(2) Der Bericht enthält neben den obligatorischen Angaben insbesondere auch Angaben über:

1. die Nutzung des Durchsetzungsverfahrens nach § 12b Absatz 2 Nummer 3 in Verbindung mit § 16 des Behindertengleichstellungsgesetzes,
2. die Inanspruchnahme der Ausnahmeregelung nach § 12a Absatz 6 des Behindertengleichstellungsgesetzes, und
3. Ergebnisse der Konsultationen der Verbände und Organisationen von Menschen mit Behinderungen.

§ 10 Folgenabschätzung

Die Verordnung ist unter Berücksichtigung der technischen Entwicklung regelmäßig zu überprüfen.

Anlage 1 (weggefallen)

Anlage 2 (zu § 3 Absatz 2)

Teil 1

Für die Bereitstellung von Informationen in Deutscher Gebärdensprache im Internet oder Intranet gelten die folgenden Vorgaben:

1. Schatten auf dem Körper der Darstellerin oder des Darstellers sind zu vermeiden. Die Mimik und das Mundbild müssen gut sichtbar sein.
2. Der Hintergrund ist statisch zu gestalten. Ein schwarzer oder weißer Hintergrund ist zu vermeiden.
3. Der Hintergrund sowie die Kleidung und die Hände der Darstellerin oder des Darstellers stehen im Kontrast zueinander. Dabei soll die Kleidung dunkel und einfarbig sein.
4. Das Video ist durch das Logo für die Deutsche Gebärdensprache gekennzeichnet. Die farbliche Gestaltung des Logos kann dem jeweiligen Design des Auftritts angepasst werden.

Symbol für Deutsche Gebärdensprache 1

5. Die Auflösung beträgt mindestens 320 x 240 Pixel.
6. Die Bildfolge beträgt mindestens 25 Bilder je Sekunde.
7. Der Gebärdensprach-Film ist darüber hinaus als Datei zum Herunterladen verfügbar.

   Es sind Angaben zur Größe der Datei sowie zur Abspieldauer verfügbar.

Teil 2

Für die Bereitstellung von Informationen in Leichter Sprache im Internet oder Intranet gelten die folgenden Vorgaben:

1. Abkürzungen, Silbentrennung am Zeilenende, Verneinungen sowie Konjunktiv-, Passiv- und Genitiv-Konstruktionen sind zu vermeiden.
2. Die Leserinnen oder Leser sollten, soweit inhaltlich sinnvoll, persönlich angesprochen werden.
3. Begriffe sind durchgängig in gleicher Weise zu verwenden.
4. Es sind kurze, gebräuchliche Begriffe und Redewendungen zu verwenden. Abstrakte Begriffe und Fremdwörter sind zu vermeiden oder mit Hilfe konkreter Beispiele zu erläutern. Zusammengesetzte Substantive sind durch Bindestrich zu trennen.
5. Es sind kurze Sätze mit klarer Satzgliederung zu bilden.

6. Sonderzeichen und Einschübe in Klammern sind zu vermeiden.
7. Inhalte sind durch Absätze und Überschriften logisch zu strukturieren. Aufzählungen mit mehr als drei Punkten sind durch Listen zu gliedern.
8. Wichtige Inhalte sind voranzustellen.
9. Es sind klare Schriftarten mit deutlichem Kontrast und mit einer Schriftgröße von mindestens 1.2 em (120 Prozent) zu verwenden. Wichtige Informationen und Überschriften sind hervorzuheben. Es sind maximal zwei verschiedene Schriftarten zu verwenden.
10. Texte werden linksbündig ausgerichtet. Jeder Satz beginnt mit einer neuen Zeile. Der Hintergrund ist hell und einfarbig.
11. Es sind aussagekräftige Symbole und Bilder zu verwenden.
12. Anschriften sind nicht als Fließtext zu schreiben.
13. Tabellen sind übersichtlich zu gestalten.

Verordnung über die technischen Rahmenbedingungen des elektronischen Rechtsverkehrs und über das besondere elektronische Behördenpostfach (ERVV)

Eingangsformel

Auf Grund

- des § 130a Absatz 2 Satz 2 und Absatz 4 Nummer 3 der Zivilprozessordnung, der durch Artikel 1 Nummer 2 des Gesetzes vom 10. Oktober 2013 (BGBl. I S. 3786) neu gefasst worden ist,
- des § 46c Absatz 2 Satz 2 und Absatz 4 Nummer 3 des Arbeitsgerichtsgesetzes, der durch Artikel 3 Nummer 2 des Gesetzes vom 10. Oktober 2013 (BGBl. I S. 3786) neu gefasst worden ist,
- des § 65a Absatz 2 Satz 2 und Absatz 4 Nummer 3 des Sozialgerichtsgesetzes, der durch Artikel 4 Nummer 1 Buchstabe a des Gesetzes vom 10. Oktober 2013 (BGBl. I S. 3786) neu gefasst worden ist,
- des § 55a Absatz 2 Satz 2 und Absatz 4 Nummer 3 der Verwaltungsgerichtsordnung, der durch Artikel 5 Nummer 1 Buchstabe a des Gesetzes vom 10. Oktober 2013 (BGBl. I S. 3786) neu gefasst worden ist, und
- des § 52a Absatz 2 Satz 2 und Absatz 4 Nummer 3 der Finanzgerichtsordnung, der durch Artikel 6 Nummer 1 Buchstabe a des Gesetzes vom 10. Oktober 2013 (BGBl. I S. 3786) neu gefasst worden ist,

jeweils in Verbindung mit Artikel 25 des Gesetzes zur Förderung des elektronischen Rechtsverkehrs mit den Gerichten vom 10. Oktober 2013 (BGBl. I S. 3786), und auf Grund

- des § 14 Absatz 4 des Gesetzes über das Verfahren in Familiensachen und in den Angelegenheiten der freiwilligen Gerichtsbarkeit, der durch Artikel 13 Nummer 3 Buchstabe c des Gesetzes vom 5. Juli 2017 (BGBl. I S. 2208) geändert worden ist,
- des § 81 Absatz 4 der Grundbuchordnung, der durch Artikel 1 Nummer 13 des Gesetzes vom 11. August 2009 (BGBl. I S. 2713) neu gefasst worden ist, und
- des § 89 Absatz 4 der Schiffsregisterordnung, der durch Artikel 4 Absatz 5 Nummer 4 des Gesetzes vom 11. August 2009 (BGBl. I S. 2713) neu gefasst worden ist,

verordnet die Bundesregierung:

Kapitel 1
Allgemeine Vorschrift

§ 1 Anwendungsbereich

(1) Diese Verordnung gilt für die Übermittlung elektronischer Dokumente an die Gerichte der Länder und des Bundes sowie die Bearbeitung elektronischer Dokumente durch diese Gerichte nach § 130a der Zivilprozessordnung, § 46c des Arbeitsgerichtsgesetzes, § 65a des Sozialgerichtsgesetzes, § 55a der Verwaltungsgerichtsordnung und § 52a der Finanzgerichtsordnung. Sie gilt ferner nach Maßgabe des Kapitels 5 für die Übermittlung elektronischer

Dokumente an Strafverfolgungsbehörden und Strafgerichte der Länder und des Bundes nach § 32a der Strafprozessordnung sowie die Bearbeitung elektronischer Dokumente.

(2) Besondere bundesrechtliche Vorschriften über die Übermittlung elektronischer Dokumente und strukturierter maschinenlesbarer Datensätze bleiben unberührt.

Kapitel 2
Technische Rahmenbedingungen des elektronischen Rechtsverkehrs

§ 2 Anforderungen an elektronische Dokumente

(1) Das elektronische Dokument ist im Dateiformat PDF zu übermitteln. Wenn bildliche Darstellungen im Dateiformat PDF nicht verlustfrei wiedergegeben werden können, darf das elektronische Dokument zusätzlich im Dateiformat TIFF übermittelt werden. Die Dateiformate PDF und TIFF sollen den nach § 5 Absatz 1 Nummer 1 bekanntgemachten Versionen entsprechen.

(2) Das elektronische Dokument soll den nach § 5 Absatz 1 Nummer 1 und 6 bekanntgemachten technischen Standards entsprechen.

(3) Dem elektronischen Dokument soll ein strukturierter maschinenlesbarer Datensatz im Dateiformat XML beigefügt werden, der den nach § 5 Absatz 1 Nummer 2 bekanntgemachten Definitions- oder Schemadateien entspricht und mindestens enthält:

1. die Bezeichnung des Gerichts;
2. sofern bekannt, das Aktenzeichen des Verfahrens;
3. die Bezeichnung der Parteien oder Verfahrensbeteiligten;
4. die Angabe des Verfahrensgegenstandes;
5. sofern bekannt, das Aktenzeichen eines denselben Verfahrensgegenstand betreffenden Verfahrens und die Bezeichnung der die Akten führenden Stelle.

§ 3 Überschreitung der Höchstgrenzen

Wird glaubhaft gemacht, dass die nach § 5 Absatz 1 Nummer 3 bekanntgemachten Höchstgrenzen für die Anzahl oder das Volumen elektronischer Dokumente nicht eingehalten werden können, kann die Übermittlung als Schriftsatz nach den allgemeinen Vorschriften erfolgen, möglichst unter Beifügung des Schriftsatzes und der Anlagen als elektronische Dokumente auf einem nach § 5 Absatz 1 Nummer 4 bekanntgemachten zulässigen physischen Datenträger.

§ 4 Übermittlung elektronischer Dokumente mit qualifizierter elektronischer Signatur

(1) Ein elektronisches Dokument, das mit einer qualifizierten elektronischen Signatur der verantwortenden Person versehen ist, darf wie folgt übermittelt werden:

1. auf einem sicheren Übermittlungsweg oder
2. an das für den Empfang elektronischer Dokumente eingerichtete Elektronische Gerichts- und Verwaltungspostfach des Gerichts über eine Anwendung, die auf

OSCI oder einem diesen ersetzenden, dem jeweiligen Stand der Technik entsprechenden Protokollstandard beruht.

(2) Mehrere elektronische Dokumente dürfen nicht mit einer gemeinsamen qualifizierten elektronischen Signatur übermittelt werden.

§ 5 Bekanntmachung technischer Standards

(1) Die Bundesregierung macht folgende technische Standards für an die Übermittlung und Eignung zur Bearbeitung elektronischer Dokumente im Bundesanzeiger und auf der Internetseite www.justiz.de bekannt:

1. die Versionen der Dateiformate PDF und TIFF;
2. die Definitions- oder Schemadateien, die bei der Übermittlung eines strukturierten maschinenlesbaren Datensatzes im Format XML genutzt werden sollen;
3. die Höchstgrenzen für die Anzahl und das Volumen elektronischer Dokumente;
4. die zulässigen physischen Datenträger;
5. die Einzelheiten der Anbringung der qualifizierten elektronischen Signatur am elektronischen Dokument und
6. die technischen Eigenschaften der elektronischen Dokumente.

(2) Die technischen Standards müssen den aktuellen Stand der Technik und die Barrierefreiheit im Sinne der Barrierefreie-Informationstechnik-Verordnung vom 12. September 2011 (BGBl. I S. 1843), die zuletzt durch Artikel 4 der Verordnung vom 25. November 2016 (BGBl. I S. 2659) geändert worden ist, in der jeweils geltenden Fassung, berücksichtigen und mit einer Mindestgültigkeitsdauer bekanntgemacht werden. Die technischen Standards können mit einem Ablaufdatum nach der Mindestgültigkeitsdauer versehen werden, ab dem sie voraussichtlich durch neue bekanntgegebene Standards abgelöst sein müssen.

Kapitel 3
Besonderes elektronisches Behördenpostfach

§ 6 Besonderes elektronisches Behördenpostfach; Anforderungen

(1) Die Behörden sowie juristischen Personen des öffentlichen Rechts können zur Übermittlung elektronischer Dokumente auf einem sicheren Übermittlungsweg ein besonderes elektronisches Behördenpostfach verwenden,

1. das auf dem Protokollstandard OSCI oder einem diesen ersetzenden, dem jeweiligen Stand der Technik entsprechenden Protokollstandard beruht,
2. bei dem die Identität des Postfachinhabers in einem Identifizierungsverfahren geprüft und bestätigt wurde,
3. bei dem der Postfachinhaber in ein sicheres elektronisches Verzeichnis eingetragen ist und
4. bei dem feststellbar ist, dass das elektronische Dokument vom Postfachinhaber versandt wurde.

(2) Das besondere elektronische Behördenpostfach muss

1. über eine Suchfunktion verfügen, die es ermöglicht, andere Inhaber von besonderen elektronischen Postfächern aufzufinden,
2. für andere Inhaber von besonderen elektronischen Postfächern adressierbar sein und
3. barrierefrei sein im Sinne der Barrierefreie-Informationstechnik-Verordnung.

(3) Das Elektronische Gerichts- und Verwaltungspostfach eines Gerichts, einer Staatsanwaltschaft, einer Amtsanwaltschaft, einer Justizvollzugsanstalt oder einer Jugendarrestanstalt steht einem besonderen elektronischen Behördenpostfach gleich, soweit diese Stelle Aufgaben einer Behörde nach Absatz 1 wahrnimmt; § 7 findet keine Anwendung.

§ 7 Identifizierungsverfahren

(1) Die von den obersten Behörden des Bundes oder den Landesregierungen für ihren Bereich bestimmten öffentlich-rechtlichen Stellen prüfen die Identität der Behörden oder juristischen Personen des öffentlichen Rechts und bestätigen dies in einem sicheren elektronischen Verzeichnis. Die obersten Behörden des Bundes oder mehrere Landesregierungen können auch eine öffentlich-rechtliche Stelle gemeinsam für ihre Bereiche bestimmen.

(2) Bei der Prüfung der Identität ist zu ermitteln, ob

1. der Postfachinhaber eine inländische Behörde oder juristische Person des öffentlichen Rechts ist und
2. Name und Sitz des Postfachinhabers zutreffend bezeichnet sind.

§ 8 Zugang und Zugangsberechtigung; Verwaltung

(1) Der Postfachinhaber bestimmt die natürlichen Personen, die Zugang zum besonderen elektronischen Behördenpostfach erhalten sollen, und stellt ihnen das Zertifikat und das Zertifikats-Passwort zur Verfügung.

(2) Der Zugang zum besonderen elektronischen Behördenpostfach erfolgt ausschließlich mithilfe des Zertifikats und des Zertifikats-Passworts des Postfachinhabers. Die Zugangsberechtigten dürfen das Zertifikat nicht an Unbefugte weitergeben und haben das Zertifikats-Passwort geheim zu halten.

(3) Der Postfachinhaber kann die Zugangsberechtigungen zum besonderen elektronischen Behördenpostfach jederzeit aufheben oder einschränken.

(4) Der Postfachinhaber hat zu dokumentieren, wer zugangsberechtigt ist, wann das Zertifikat und das Zertifikats-Passwort zur Verfügung gestellt wurden und wann die Zugangsberechtigung aufgehoben wurde. Er stellt zugleich sicher, dass der Zugang zu seinem besonderen elektronischen Behördenpostfach nur den von ihm bestimmten Zugangsberechtigten möglich ist.

(5) Unbeschadet der Absätze 1, 3 und 4 kann die Verwaltung des besonderen elektronischen Behördenpostfachs behördenübergreifend automatisiert und an zentraler Stelle erfolgen.

§ 9 Änderung und Löschung

(1) Der Postfachinhaber hat Änderungen seines Namens oder Sitzes unverzüglich der nach § 7 Absatz 1 bestimmten Stelle anzuzeigen.

(2) Der Postfachinhaber kann jederzeit die Löschung seines besonderen elektronischen Behördenpostfachs veranlassen. Er hat die Löschung seines besonderen elektronischen Behördenpostfachs zu veranlassen, wenn seine Berechtigung zur Nutzung des besonderen elektronischen Behördenpostfachs endet.

Kapitel 4
Besonderes elektronisches Bürger- und Organisationenpostfach; Postfach- und Versanddienst eines Nutzerkontos

§ 10 Besonderes elektronisches Bürger- und Organisationenpostfach

(1) Natürliche Personen, juristische Personen sowie sonstige Vereinigungen können zur Übermittlung elektronischer Dokumente auf einem sicheren Übermittlungsweg ein besonderes elektronisches Bürger- und Organisationenpostfach verwenden,

1. das auf dem Protokollstandard OSCI oder einem diesen ersetzenden, dem jeweiligen Stand der Technik entsprechenden Protokollstandard beruht,
2. bei dem die Identität des Postfachinhabers festgestellt worden ist,
3. bei dem der Postfachinhaber in ein sicheres elektronisches Verzeichnis eingetragen ist,
4. bei dem sich der Postfachinhaber beim Versand eines elektronischen Dokuments authentisiert und
5. bei dem feststellbar ist, dass das elektronische Dokument vom Postfachinhaber versandt wurde.

(2) Das besondere elektronische Bürger- und Organisationenpostfach muss

1. über eine Suchfunktion verfügen, die es ermöglicht, Inhaber eines besonderen elektronischen Anwaltspostfachs, eines besonderen elektronischen Notarpostfachs, eines besonderen elektronischen Steuerberaterpostfachs oder eines besonderen elektronischen Behördenpostfachs aufzufinden,
2. für Inhaber besonderer elektronischer Anwaltspostfächer, besonderer elektronischer Notarpostfächer, besonderer elektronischer Steuerberaterpostfächer oder besonderer elektronischer Behördenpostfächer adressierbar sein und
3. barrierefrei sein im Sinne der Barrierefreie-Informationstechnik-Verordnung.

(3) Wird für eine rechtlich unselbständige Untergliederung einer juristischen Person oder sonstigen Vereinigung ein besonderes elektronisches Bürger- und Organisationenpostfach eingerichtet, so muss der Postfachinhaber so bezeichnet sein, dass eine Verwechslung mit der übergeordneten Organisationseinheit ausgeschlossen ist.

§ 11 Identifizierung und Authentisierung des Postfachinhabers

(1) Die Länder oder mehrere Länder gemeinsam bestimmen jeweils für ihren Bereich eine öffentlich-rechtliche Stelle, die die Freischaltung eines besonderen elektronischen Bürger- und Organisationenpostfachs veranlasst.

(2) Der Postfachinhaber hat im Rahmen der Identitätsfeststellung seinen Namen und seine Anschrift nachzuweisen. Der Nachweis kann nur durch eines der folgenden Identifizierungsmittel erfolgen:

1. den elektronischen Identitätsnachweis nach § 18 des Personalausweisgesetzes, nach § 12 des eID-Karte-Gesetzes oder nach § 78 Absatz 5 des Aufenthaltsgesetzes,
2. ein qualifiziertes elektronisches Siegel nach Artikel 38 der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG (ABl. L 257 vom 28.8.2014, S. 73; L 23 vom 29.1.2015, S. 19; L 155 vom 14.6.2016, S. 44),
3. bei öffentlich bestellten oder beeidigten Personen, die Dolmetscher- oder Übersetzungsleistungen erbringen, eine Bestätigung der nach dem Gerichtsdolmetschergesetz oder dem jeweiligen Landesrecht für die öffentliche Bestellung und Beeidigung dieser Personen zuständigen Stelle, auch hinsichtlich der Angaben zu Berufsbezeichnung sowie zur Sprache, für die die Bestellung erfolgt,
4. bei Gerichtsvollziehern eine Bestätigung der für ihre Ernennung zuständigen Stelle, auch hinsichtlich der Dienstbezeichnung, oder
5. eine in öffentlich beglaubigter Form abgegebene Erklärung über den Namen und die Anschrift des Postfachinhabers sowie die eindeutige Bezeichnung des Postfachs.

Eine nach Satz 2 Nummer 5 angegebene geschäftliche Anschrift ist durch eine Bescheinigung nach § 21 Absatz 1 der Bundesnotarordnung, einen amtlichen Registerausdruck oder eine beglaubigte Registerabschrift nachzuweisen. Geht eine angegebene geschäftliche Anschrift nicht aus einem öffentlichen Register hervor, so stellt die Stelle nach Absatz 1 diese durch geeignete Maßnahmen fest. Die Übermittlung von Daten nach Satz 2 Nummer 3 bis 5 an die in Absatz 1 genannte öffentlich-rechtliche Stelle erfolgt in strukturierter maschinenlesbarer Form. Im Fall des Satzes 2 Nummer 5 ist der öffentlich-rechtlichen Stelle zusätzlich eine öffentlich beglaubigte elektronische Abschrift der Erklärung zu übermitteln.

(3) Der Postfachinhaber hat sich beim Versand eines elektronischen Dokuments zu authentisieren durch

1. den elektronischen Identitätsnachweis nach § 18 des Personalausweisgesetzes, nach § 12 des eID-Karte-Gesetzes oder nach § 78 Absatz 5 des Aufenthaltsgesetzes,
2. ein Authentisierungszertifikat, das auf einer qualifizierten elektronischen Signaturerstellungseinheit nach dem Anhang II der Verordnung (EU) Nr. 910/2014 gespeichert ist, oder
3. ein nichtqualifiziertes Authentisierungszertifikat.

§ 12 Änderung von Angaben und Löschung des Postfachs

(1) Bei Änderung seiner Daten hat der Postfachinhaber unverzüglich die Anpassung seines Postfachs bei der nach § 11 Absatz 1 bestimmten Stelle zu veranlassen. Das betrifft insbesondere die Änderung seines Namens oder seiner Anschrift, bei juristischen Personen oder sonstigen Vereinigungen auch bei der Änderung des Sitzes.

(2) Der Postfachinhaber kann jederzeit die Löschung seines besonderen elektronischen Bürger- und Organisationenpostfachs veranlassen.

§ 13 Elektronische Kommunikation über den Postfach- und Versanddienst eines Nutzerkontos

(1) Zur Übermittlung elektronischer Dokumente auf einem sicheren Übermittlungsweg kann der Postfach- und Versanddienst eines Nutzerkontos im Sinne des § 2 Absatz 5 des Onlinezugangsgesetzes genutzt werden, wenn bei diesem Postfach- und Versanddienst

1. eine technische Vorrichtung besteht, die auf dem Protokollstandard OSCI oder einem diesen ersetzenden, dem jeweiligen Stand der Technik entsprechenden Protokollstandard beruht,
2. die Identität des Nutzers des Postfach- und Versanddienstes durch ein Identifizierungsmittel nach § 11 Absatz 2 Satz 2 Nummer 1 oder 2 oder für Nutzer des Organisationskontos im Sinne des § 2 Absatz 5 Satz 4 des Onlinezugangsgesetzes durch ein nach § 87a Absatz 6 der Abgabenordnung in der Steuerverwaltung eingesetztes sicheres Verfahren festgestellt ist,
3. der Nutzer des Postfach- und Versanddienstes sich beim Versand eines elektronischen Dokuments entsprechend § 11 Absatz 3 authentisiert und
4. feststellbar ist, dass das elektronische Dokument von dem Nutzer des Postfach- und Versanddienstes versandt wurde.

(2) Der Postfach- und Versanddienst muss barrierefrei sein im Sinne der Barrierefreie-Informationstechnik-Verordnung.

(3) Der Nutzer des Postfach- und Versanddienstes ist in ein sicheres elektronisches Verzeichnis einzutragen, soweit dies zum Betrieb des jeweiligen Postfach- und Versanddienstes erforderlich ist. In diesem Fall gilt § 10 Absatz 2 Nummer 1 und 2 entsprechend. Der Nutzer kann jederzeit die Löschung des Postfach- und Versanddienstes veranlassen.

§ 13a Datenverarbeitung

(1) Zur Auffindbarkeit und Adressierung eines Postfachinhabers dürfen folgende personenbezogene Daten im sicheren elektronischen Verzeichnis (§ 10 Absatz 1 Nummer 3 und § 13 Absatz 3 Satz 1) gespeichert und aus dem Verzeichnis abgerufen werden:

1. bei einer natürlichen Person:
   a) Vor- und Nachname,
   b) Anschrift,
   c) Staat,
   d) Nutzer-ID,

e) Verschlüsselungszertifikat;

2. bei einer juristischen Person:
   a) Name,
   b) Anschrift des Sitzes,
   c) Staat,
   d) Nutzer-ID,
   e) Verschlüsselungszertifikat.

(2) Für die Verarbeitung personenbezogener Daten im sicheren elektronischen Verzeichnis verantwortlich nach Artikel 4 Nummer 7 der 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; L 314 vom 22.11.2016, S. 72; L 127 vom 23.5.2018, S. 2; L 74 vom 4.3.2021, S. 35) sind die Stellen, in deren Auftrag das sichere elektronische Verzeichnis betrieben wird.

Kapitel 5
Elektronischer Rechtsverkehr mit Strafverfolgungsbehörden und Strafgerichten

§ 14 Schriftlich abzufassende, zu unterschreibende oder zu unterzeichnende Dokumente

Die Kapitel 2 bis 4 gelten im Bereich des elektronischen Rechtsverkehrs mit Strafverfolgungsbehörden und Strafgerichten für schriftlich abzufassende, zu unterschreibende oder zu unterzeichnende Dokumente, die gemäß § 32a Absatz 3 der Strafprozessordnung elektronisch eingereicht werden, mit der Maßgabe, dass der Datensatz nach § 2 Absatz 3 mindestens folgende Angaben enthält:

1. die Bezeichnung der Strafverfolgungsbehörde oder des Gerichts;
2. sofern bekannt, das Aktenzeichen des Verfahrens oder die Vorgangsnummer;
3. die Bezeichnung der beschuldigten Personen oder der Verfahrensbeteiligten; bei Verfahren gegen Unbekannt enthält der Datensatz anstelle der Bezeichnung der beschuldigten Personen die Bezeichnung „Unbekannt“ sowie, sofern bekannt, die Bezeichnung der geschädigten Personen;
4. die Angabe der den beschuldigten Personen zur Last gelegten Straftat oder des Verfahrensgegenstandes;
5. sofern bekannt, das Aktenzeichen eines denselben Verfahrensgegenstand betreffenden Verfahrens und die Bezeichnung der die Akten führenden Stelle.

§ 15 Sonstige verfahrensbezogene elektronische Dokumente

(1) Sonstige verfahrensbezogene elektronische Dokumente, die an Strafverfolgungsbehörden oder Strafgerichte übermittelt werden, sollen den Anforderungen des § 2 entsprechen. Entsprechen sie diesen Anforderungen nicht und sind sie zur Bearbeitung durch die Behörde oder das Gericht aufgrund der dortigen technischen Ausstattung oder der dort einzuhalten-

den Sicherheitsstandards nicht geeignet, so liegt ein wirksamer Eingang nicht vor. In der Mitteilung nach § 32a Absatz 6 Satz 1 der Strafprozessordnung ist auf die in § 2 geregelten technischen Rahmenbedingungen hinzuweisen.

(2) Die Übermittlung kann auch auf anderen als den in § 32a Absatz 4 der Strafprozessordnung genannten Übermittlungswegen erfolgen, wenn ein solcher Übermittlungsweg für die Entgegennahme verfahrensbezogener elektronischer Dokumente generell und ausdrücklich eröffnet ist.

Schlussformel

Der Bundesrat hat zugestimmt.

De-Mail-Gesetz

Abschnitt 1
Allgemeine Vorschriften

§ 1 De-Mail-Dienste

(1) De-Mail-Dienste sind Dienste auf einer elektronischen Kommunikationsplattform, die einen sicheren, vertraulichen und nachweisbaren Geschäftsverkehr für jedermann im Internet sicherstellen sollen.

(2) Ein De-Mail-Dienst muss eine sichere Anmeldung, die Nutzung eines Postfach- und Versanddienstes für sichere elektronische Post sowie die Nutzung eines Verzeichnisdienstes und kann zusätzlich auch Identitätsbestätigungs- und Dokumentenablagedienste ermöglichen. Ein De-Mail-Dienst wird von einem nach diesem Gesetz akkreditierten Diensteanbieter betrieben.

(3) Elektronische Kommunikationsinfrastrukturen und sonstige Anwendungen, die der sicheren Übermittlung von Nachrichten und Daten dienen, bleiben unberührt.

§ 2 Zuständige Behörde

Zuständige Behörde nach diesem Gesetz ist das Bundesamt für Sicherheit in der Informationstechnik.

Abschnitt 2
Pflichtangebote und optionale Angebote des Diensteanbieters

§ 3 Eröffnung eines De-Mail-Kontos

(1) Durch einen De-Mail-Konto-Vertrag verpflichtet sich ein akkreditierter Diensteanbieter, einem Nutzer ein De-Mail-Konto zur Verfügung zu stellen. Ein De-Mail-Konto ist ein Bereich in einem De-Mail-Dienst, der einem Nutzer so zugeordnet ist, dass er nur von ihm genutzt werden kann. Der akkreditierte Diensteanbieter hat durch technische Mittel sicherzustellen, dass nur der diesem De-Mail-Konto zugeordnete Nutzer Zugang zu dem ihm zugeordneten De-Mail-Konto erlangen kann.

(2) Der akkreditierte Diensteanbieter hat die Identität des Nutzers und bei juristischen Personen, rechtsfähigen Personengesellschaften oder öffentlichen Stellen zusätzlich die Identität ihrer gesetzlichen Vertreter oder Organmitglieder zuverlässig festzustellen. Dazu erhebt und speichert er folgende Angaben:

1. bei einer natürlichen Person Name, Geburtsort, Geburtsdatum und Anschrift;
2. bei einer juristischen Person oder rechtsfähigen Personengesellschaft oder öffentlichen Stelle Firma, Name oder Bezeichnung, Rechtsform, Registernummer, soweit vorhanden, Anschrift des Sitzes oder der Hauptniederlassung und Namen der Mitglieder des Vertretungsorgans oder der gesetzlichen Vertreter; ist ein Mitglied des Vertretungsorgans oder der gesetzliche Vertreter eine juristische Person, so wird

deren Firma, Name oder Bezeichnung, Rechtsform, Registernummer, soweit vorhanden, und Anschrift des Sitzes oder der Hauptniederlassung erhoben.

(3) Der akkreditierte Diensteanbieter hat die Angaben nach Absatz 2 vor Freischaltung des De-Mail-Kontos des Nutzers zu überprüfen:

1. bei natürlichen Personen
   a) anhand eines gültigen amtlichen Ausweises, der ein Lichtbild des Inhabers enthält und mit dem die Pass- und Ausweispflicht im Inland erfüllt wird, insbesondere anhand eines inländischen oder nach ausländerrechtlichen Bestimmungen anerkannten oder zugelassenen Passes, Personalausweises oder Pass- oder Ausweisersatzes,
   b) anhand von Dokumenten, die bezüglich ihrer Sicherheit einem Dokument nach Buchstabe a gleichwertig sind,
   c) anhand eines elektronischen Identitätsnachweises nach § 18 des Personalausweisgesetzes, nach § 12 des eID-Karte-Gesetzes oder nach § 78 Absatz 5 des Aufenthaltsgesetzes,
   d) anhand einer qualifizierten elektronischen Signatur oder
   e) anhand sonstiger geeigneter technischer Verfahren mit gleichwertiger Sicherheit zu einer Identifizierung anhand der Dokumente nach Buchstabe a;
2. bei juristischen Personen oder rechtsfähigen Personengesellschaften oder bei öffentlichen Stellen
   a) anhand eines Auszugs aus dem Handels- oder Genossenschaftsregister oder aus einem vergleichbaren amtlichen Register oder Verzeichnis,
   b) anhand der Gründungsdokumente,
   c) anhand von Dokumenten, die bezüglich ihrer Beweiskraft den Dokumenten nach den Buchstaben a oder b gleichwertig sind, oder
   d) durch Einsichtnahme in die Register- oder Verzeichnisdaten.

Soweit die Anschrift von natürlichen Personen nicht durch Verfahren nach Satz 1 Nummer 1 Buchstabe a bis e überprüft werden kann, ist sie anhand behördlicher Dokumente zu überprüfen, die zum Zweck der Anschriftsbescheinigung ausgestellt worden sind; sofern keine behördlichen Dokumente beigebracht werden können, ist die Anschrift anhand sonstiger geeigneter Verfahren zur Überprüfung der postalischen Erreichbarkeit zu überprüfen. Der akkreditierte Diensteanbieter kann von dem amtlichen Ausweis eine Kopie erstellen. Er hat die Kopie unverzüglich nach Feststellung der für die Identität erforderlichen Angaben des Teilnehmers zu vernichten. Der akkreditierte Diensteanbieter darf zur Identitätsfeststellung und -überprüfung mit Einwilligung des Nutzers auch personenbezogene Daten verarbeiten, die er zu einem früheren Zeitpunkt erhoben hat, sofern diese Daten die zuverlässige Identitätsfeststellung des Nutzers gewährleisten.

(4) Eine Nutzung der De-Mail-Dienste ist erst möglich, nachdem der akkreditierte Diensteanbieter das De-Mail-Konto des Nutzers freigeschaltet hat. Die Freischaltung erfolgt, sobald

1. der akkreditierte Diensteanbieter den Nutzer eindeutig identifiziert hat und die Identitätsdaten des Nutzers und bei Absatz 2 Nummer 2 auch dessen gesetzlichen Vertreters oder der Organmitglieder erhoben und erfolgreich überprüft worden sind,
2. der akkreditierte Diensteanbieter dem Nutzer dessen für die Erstanmeldung notwendigen Anmeldedaten auf geeignetem Wege übermittelt hat,
3. der Nutzer die Bestätigung nach § 9 Absatz 2 vorgenommen hat,
4. der Nutzer in die Prüfung seiner Nachrichten auf Schadsoftware durch den akkreditierten Diensteanbieter eingewilligt hat und
5. der Nutzer im Rahmen einer Erstanmeldung nachgewiesen hat, dass er die Anmeldedaten erfolgreich nutzen konnte.

(5) Der akkreditierte Diensteanbieter hat nach der Freischaltung des De-Mail-Kontos eines Nutzers die Richtigkeit der zu dem Nutzer gespeicherten Identitätsdaten sicherzustellen. Er hat die gespeicherten Identitätsdaten in angemessenen zeitlichen Abständen auf ihre Richtigkeit zu prüfen und soweit erforderlich zu berichtigen.

§ 4 Anmeldung zu einem De-Mail-Konto

(1) Der akkreditierte Diensteanbieter muss dem Nutzer den Zugang zu seinem De-Mail-Konto und den einzelnen Diensten mit einer sicheren Anmeldung oder auf Verlangen des Nutzers auch ohne eine solche sichere Anmeldung ermöglichen. Für die sichere Anmeldung hat der akkreditierte Diensteanbieter sicherzustellen, dass zum Schutz gegen eine unberechtigte Nutzung der Zugang zum De-Mail-Konto nur möglich ist, wenn zwei geeignete und voneinander unabhängige Sicherungsmittel eingesetzt werden; soweit bei den Sicherungsmitteln Geheimnisse verwendet werden, ist deren Einmaligkeit und Geheimhaltung sicherzustellen. Der Zugang zum De-Mail-Konto erfolgt ohne eine sichere Anmeldung, wenn nur ein Sicherungsmittel, in der Regel Benutzername und Passwort, verwendet wird. Der Nutzer kann verlangen, dass der Zugang zu seinem De-Mail-Konto ausschließlich mit einer sicheren Anmeldung möglich sein soll.

(2) Der akkreditierte Diensteanbieter hat zu gewährleisten, dass der Nutzer zwischen mindestens zwei Verfahren zur sicheren Anmeldung nach Absatz 1 Satz 2 wählen kann. Als ein Verfahren zur sicheren Anmeldung muss durch den Nutzer, soweit er eine natürliche Person ist, der elektronische Identitätsnachweis nach § 18 des Personalausweisgesetzes, nach § 12 des eID-Karte-Gesetzes oder nach § 78 Absatz 5 des Aufenthaltsgesetzes genutzt werden können.

(3) Der akkreditierte Diensteanbieter hat sicherzustellen, dass die Kommunikationsverbindung zwischen dem Nutzer und seinem De-Mail-Konto verschlüsselt erfolgt.

§ 5 Postfach- und Versanddienst

(1) Die Bereitstellung eines De-Mail-Kontos umfasst die Nutzung eines sicheren elektronischen Postfach- und Versanddienstes für elektronische Nachrichten. Hierzu wird dem Nutzer eine De-Mail-Adresse für elektronische Post zugewiesen, welche folgende Angaben enthalten muss:

1. im Domänenteil der De-Mail-Adresse eine Kennzeichnung, die ausschließlich für De-Mail-Dienste genutzt werden darf;

2. bei natürlichen Personen im lokalen Teil deren Nachnamen und einen oder mehrere Vornamen oder einen Teil des oder der Vornamen (Hauptadresse);

3. bei juristischen Personen, rechtsfähigen Personengesellschaften oder öffentlichen Stellen im Domänenteil eine Bezeichnung, welche in direktem Bezug zu ihrer Firma, Namen oder sonstiger Bezeichnung steht.

(2) Der akkreditierte Diensteanbieter kann Nutzern auf Verlangen auch pseudonyme De-Mail-Adressen zur Verfügung stellen, soweit es sich bei dem Nutzer um eine natürliche Person handelt. Die Inanspruchnahme eines Dienstes durch den Nutzer unter Pseudonym ist für Dritte erkennbar zu kennzeichnen.

(3) Der Postfach- und Versanddienst hat die Vertraulichkeit, die Integrität und die Authentizität der Nachrichten zu gewährleisten. Hierzu gewährleistet der akkreditierte Diensteanbieter, dass

1. die Kommunikation von einem akkreditierten Diensteanbieter zu jedem anderen akkreditierten Diensteanbieter über einen verschlüsselten gegenseitig authentisierten Kanal erfolgt (Transportverschlüsselung) und

2. der Inhalt einer De-Mail-Nachricht vom akkreditierten Diensteanbieter des Senders zum akkreditierten Diensteanbieter des Empfängers verschlüsselt übertragen wird.

Der Einsatz einer durchgängigen Verschlüsselung zwischen Sender und Empfänger (Ende-zu-Ende-Verschlüsselung) bleibt hiervon unberührt.

(4) Der Sender kann eine sichere Anmeldung nach § 4 für den Abruf der Nachricht durch den Empfänger bestimmen.

(5) Der akkreditierte Diensteanbieter muss dem Nutzer ermöglichen, seine sichere Anmeldung im Sinne von § 4 in der Nachricht so bestätigen zu lassen, dass die Unverfälschtheit der Bestätigung jederzeit nachprüfbar ist. Um dieses dem Empfänger der Nachricht kenntlich zu machen, bestätigt der akkreditierte Diensteanbieter des Senders die Verwendung der sicheren Anmeldung nach § 4. Hierzu versieht er im Auftrag des Senders die Nachricht mit einer dauerhaft überprüfbaren qualifizierten elektronischen Signatur; sind der Nachricht eine oder mehrere Dateien beigefügt, bezieht sich die qualifizierte elektronische Signatur auch auf diese. Die Bestätigung enthält bei natürlichen Personen den Namen und die Vornamen, bei juristischen Personen, rechtsfähigen Personengesellschaften oder öffentlichen Stellen die Firma, den Namen oder die Bezeichnung des Senders in der Form, in der diese nach § 3 Absatz 2 hinterlegt sind. Die Tatsache, dass der Absender diese Versandart genutzt hat, muss sich aus der Nachricht in der Form, wie sie beim Empfänger ankommt, ergeben. Die Bestätigung nach Satz 1 ist nicht zulässig bei Verwendung einer pseudonymen De-Mail-Adresse nach Absatz 2.

(6) Der akkreditierte Diensteanbieter mit Ausnahme der Diensteanbieter nach § 19 ist verpflichtet, elektronische Nachrichten nach den Vorschriften der Prozessordnungen und der Gesetze, die die Verwaltungszustellung regeln, förmlich zuzustellen. Im Umfang dieser Verpflichtung ist der akkreditierte Diensteanbieter mit Hoheitsbefugnissen ausgestattet (beliehener Unternehmer).

(7) Der akkreditierte Diensteanbieter bestätigt auf Antrag des Senders den Versand einer Nachricht. Die Versandbestätigung muss folgende Angaben enthalten:

1. die De-Mail-Adresse des Absenders und des Empfängers;

2. das Datum und die Uhrzeit des Versands der Nachricht vom De-Mail-Postfach des Senders;
3. den Namen und Vornamen oder die Firma des akkreditierten Diensteanbieters, der die Versandbestätigung erzeugt und
4. die Prüfsumme der zu bestätigenden Nachricht.

Der akkreditierte Diensteanbieter des Senders hat die Versandbestätigung mit einer qualifizierten elektronischen Signatur zu versehen.

(8) Auf Antrag des Senders wird der Eingang einer Nachricht im De-Mail-Postfach des Empfängers bestätigt. Hierbei wirken der akkreditierte Diensteanbieter des Senders und der akkreditierte Diensteanbieter des Empfängers zusammen. Der akkreditierte Diensteanbieter des Empfängers erstellt eine Eingangsbestätigung. Die Eingangsbestätigung enthält folgende Angaben:

1. die De-Mail-Adresse des Absenders und des Empfängers;
2. das Datum und die Uhrzeit des Eingangs der Nachricht im De-Mail-Postfach des Empfängers;
3. den Namen und Vornamen oder die Firma des akkreditierten Diensteanbieters, der die Eingangsbestätigung erzeugt und
4. die Prüfsumme der zu bestätigenden Nachricht.

Der akkreditierte Diensteanbieter des Empfängers hat die Eingangsbestätigung mit einer qualifizierten elektronischen Signatur zu versehen. Der akkreditierte Diensteanbieter des Empfängers sendet diesem ebenfalls die Eingangsbestätigung zu.

(9) Eine öffentliche Stelle, welche zur förmlichen Zustellung nach den Vorschriften der Prozessordnungen und der Gesetze, die die Verwaltungszustellung regeln, berechtigt ist, kann eine Abholbestätigung verlangen. Aus der Abholbestätigung ergibt sich, dass sich der Empfänger nach dem Eingang der Nachricht im Postfach an seinem De-Mail-Konto sicher im Sinne des § 4 angemeldet hat. Hierbei wirken der akkreditierte Diensteanbieter der öffentlichen Stelle als Senderin und der akkreditierte Diensteanbieter des Empfängers zusammen. Der akkreditierte Diensteanbieter des Empfängers erzeugt die Abholbestätigung. Die Abholbestätigung muss folgende Angaben enthalten:

1. die De-Mail-Adresse des Absenders und des Empfängers;
2. das Datum und die Uhrzeit des Eingangs der Nachricht im De-Mail-Postfach des Empfängers;
3. das Datum und die Uhrzeit der sicheren Anmeldung des Empfängers an seinem De-Mail-Konto im Sinne des § 4;
4. den Namen und Vornamen oder die Firma des akkreditierten Diensteanbieters, der die Abholbestätigung erzeugt und
5. die Prüfsumme der zu bestätigenden Nachricht.

Der akkreditierte Diensteanbieter des Empfängers hat die Abholbestätigung mit einer qualifizierten elektronischen Signatur zu versehen. Der akkreditierte Diensteanbieter des Empfängers sendet diesem ebenfalls die Abholbestätigung zu. Die in Satz 5 genannten Daten

dürfen ausschließlich zum Nachweis der förmlichen Zustellung im Sinne von § 5 Absatz 6 verarbeitet und genutzt werden.

(10) Der akkreditierte Diensteanbieter stellt sicher, dass Nachrichten, für die eine Eingangsbestätigung nach Absatz 8 oder eine Abholbestätigung nach Absatz 9 erteilt worden ist, durch den Empfänger ohne eine sichere Anmeldung an seinem De-Mail-Konto erst 90 Tage nach ihrem Eingang gelöscht werden können.

(11) Nutzern, die natürliche Personen sind, bietet der akkreditierte Diensteanbieter an, von allen an ihre De-Mail-Adresse adressierten Nachrichten eine Kopie an eine zuvor vom Nutzer angegebene De-Mail-Adresse (Weiterleitungsadresse) weiterzuleiten, ohne dass der Nutzer an seinem De-Mail-Konto angemeldet sein muss (automatische Weiterleitung). Der Nutzer kann ausschließen, dass im Sinne des Absatzes 4 an ihn gesendete Nachrichten weitergeleitet werden. Der Nutzer kann den Dienst der automatischen Weiterleitung jederzeit zurücknehmen. Um den Dienst der automatischen Weiterleitung nutzen zu können, muss der Nutzer sicher an seinem De-Mail-Konto angemeldet sein.

§ 6 Identitätsbestätigungsdienst

(1) Der akkreditierte Diensteanbieter kann einen Identitätsbestätigungsdienst anbieten. Ein solcher liegt vor, wenn sich der Nutzer der nach § 3 hinterlegten Identitätsdaten bedienen kann, um seine Identität gegenüber einem Dritten, der ebenfalls Nutzer eines De-Mail-Kontos ist, sicher elektronisch bestätigen zu lassen. Die Übermittlung der Identitätsdaten erfolgt mittels einer De-Mail-Nachricht, die der akkreditierte Diensteanbieter im Auftrag des Nutzers an den Dritten, welchem gegenüber er seine Identitätsdaten mitteilen möchte, sendet. Die De-Mail-Nachricht wird durch den akkreditierten Diensteanbieter mit einer qualifizierten elektronischen Signatur versehen.

(2) Der akkreditierte Diensteanbieter hat Vorkehrungen dafür zu treffen, dass Identitätsdaten nicht unbemerkt gefälscht oder verfälscht werden können.

(3) Die zuständige Behörde kann die Einschränkung der Verarbeitung eines Identitätsdatums anordnen, wenn Tatsachen die Annahme rechtfertigen, dass das Identitätsdatum auf Grund falscher Angaben ausgestellt wurde oder nicht ausreichend fälschungssicher ist.

§ 7 Verzeichnisdienst

(1) Der akkreditierte Diensteanbieter hat auf ausdrückliches Verlangen des Nutzers die De-Mail-Adressen, die nach § 3 hinterlegten Identitätsdaten Name und Anschrift, die für die Verschlüsselung von Nachrichten an den Nutzer notwendigen Informationen und die Information über die Möglichkeit der sicheren Anmeldung nach § 4 des Nutzers in einem Verzeichnisdienst zu veröffentlichen. Der akkreditierte Diensteanbieter darf die Eröffnung eines De-Mail-Kontos für den Nutzer nicht von dem Verlangen des Nutzers nach Satz 1 abhängig machen.

(2) Der akkreditierte Diensteanbieter hat eine De-Mail-Adresse, ein Identitätsdatum oder die für die Verschlüsselung von Nachrichten an den Nutzer notwendigen Informationen unverzüglich aus dem Verzeichnisdienst zu löschen, wenn

1. der Nutzer dies verlangt,
2. die Daten aufgrund falscher Angaben ausgestellt wurden,

3. der Diensteanbieter seine Tätigkeit beendet und diese nicht von einem anderen akkreditierten Diensteanbieter fortgeführt wird oder

4. die zuständige Behörde die Löschung aus dem Verzeichnisdienst anordnet.

Weitere Gründe für eine Löschung können vertraglich vereinbart werden.

(3) Die Veröffentlichung der De-Mail-Adresse im Verzeichnisdienst auf ein Verlangen des Nutzers als Verbraucher nach Absatz 1 allein gilt nicht als Eröffnung des Zugangs im Sinne von § 3a Absatz 1 des Verwaltungsverfahrensgesetzes, § 36a Absatz 1 des Ersten Buches Sozialgesetzbuch oder des § 87a Absatz 1 Satz 1 der Abgabenordnung. Auf Verlangen des Nutzers muss der akkreditierte Diensteanbieter durch einen geeigneten Zusatz die Erklärung des Nutzers im Verzeichnisdienst veröffentlichen, den Zugang im Sinne von § 3a des Verwaltungsverfahrensgesetzes, § 36a Absatz 1 des Ersten Buches Sozialgesetzbuch und des § 87a Absatz 1 Satz 1 der Abgabenordnung eröffnen zu wollen. Die Veröffentlichung der De-Mail-Adresse des Nutzers als Verbraucher mit diesem Zusatz im Verzeichnisdienst gilt als Zugangseröffnung. Satz 2 gilt entsprechend für die Entscheidung des Nutzers, die Zugangseröffnung zurückzunehmen.

(4) § 18 des Telekommunikation-Digitale-Dienste-Datenschutz-Gesetzes gilt entsprechend.

§ 8 Dokumentenablage

Der akkreditierte Diensteanbieter kann dem Nutzer eine Dokumentenablage zur sicheren Ablage von Dokumenten anbieten. Bietet er die Dokumentenablage an, so hat er dafür Sorge zu tragen, dass die Dokumente sicher abgelegt werden; Vertraulichkeit, Integrität und ständige Verfügbarkeit der abgelegten Dokumente sind zu gewährleisten. Der akkreditierte Diensteanbieter ist verpflichtet, alle Dokumente verschlüsselt abzulegen. Der Nutzer kann für jede einzelne Datei eine für den Zugriff erforderliche sichere Anmeldung nach § 4 festlegen. Auf Verlangen des Nutzers hat der akkreditierte Diensteanbieter ein Protokoll über die Einstellung und Herausnahme von Dokumenten bereitzustellen, das mit einer qualifizierten elektronischen Signatur gesichert ist.

Abschnitt 3
De-Mail-Dienste-Nutzung

§ 9 Aufklärungs- und Informationspflichten

(1) Der akkreditierte Diensteanbieter hat den Nutzer vor der erstmaligen Nutzung des De-Mail-Kontos über die Rechtsfolgen und Kosten der Nutzung von De-Mail-Diensten, insbesondere der Nutzung des Postfach- und Versanddienstes nach § 5, des Verzeichnisdienstes nach § 7 und der Dokumentenablage nach § 8, über die Rechtsfolgen und Kosten der Sperrung und Auflösung des De-Mail-Kontos nach § 10, der Einstellung der Tätigkeit nach § 11 und der Vertragsbeendigung nach § 12 sowie über die Maßnahmen zu informieren, die notwendig sind, um einen unbefugten Zugang zum De-Mail-Konto zu verhindern. Dies umfasst insbesondere auch Informationen

1. über die Möglichkeit und Bedeutung einer sicheren Anmeldung nach § 4 Absatz 1 Satz 2 sowie einen Hinweis dazu, dass ein Zugang zum De-Mail-Konto ohne sichere Anmeldung nicht den gleichen Schutz bietet wie mit einer sicheren Anmeldung und

2. über den Inhalt und die Bedeutung der Transportverschlüsselung nach § 5 Absatz 3 Satz 2 sowie der Verschlüsselung nach § 4 Absatz 3 sowie über die Unterschiede dieser Verschlüsselungen zu einer Ende-zu-Ende-Verschlüsselung nach § 5 Absatz 3 Satz 3.

Der akkreditierte Diensteanbieter muss den Nutzer außerdem darüber informieren, wie mit schadsoftwarebehafteten De-Mail-Nachrichten umgegangen wird.

(2) Der akkreditierte Diensteanbieter darf die erstmalige Nutzung des De-Mail-Kontos nur zulassen, wenn der Nutzer die erforderlichen Informationen in Textform erhalten und in Textform bestätigt hat, dass er die Informationen nach Absatz 1 erhalten und zur Kenntnis genommen hat.

(3) Informationspflichten nach anderen Gesetzen bleiben unberührt.

§ 10 Sperrung und Auflösung des De-Mail-Kontos

(1) Der akkreditierte Diensteanbieter hat den Zugang zu einem De-Mail-Konto unverzüglich zu sperren, wenn

1. der Nutzer es verlangt,
2. Tatsachen die Annahme rechtfertigen, dass die zur eindeutigen Identifizierung des Nutzers beim akkreditierten Diensteanbieter gespeicherten Daten nicht ausreichend fälschungssicher sind oder dass die sichere Anmeldung gemäß § 4 Mängel aufweist, die eine unbemerkte Fälschung oder Kompromittierung des Anmeldevorgangs zulassen,
3. die zuständige Behörde die Sperrung gemäß Absatz 2 anordnet oder
4. die Voraussetzungen eines vertraglich zwischen dem akkreditierten Diensteanbieter und dem Nutzer vereinbarten Sperrgrundes vorliegen.

Im Fall des Satzes 1 Nummer 4 hat der akkreditierte Diensteanbieter die Sperrung so vorzunehmen, dass der Abruf von Nachrichten möglich bleibt; dies gilt nicht, soweit der vertraglich vereinbarte Sperrgrund den Abruf von Nachrichten ausschließt. Der akkreditierte Diensteanbieter hat den zur Sperrung berechtigten Nutzern eine Rufnummer bekannt zu geben, unter der diese unverzüglich eine Sperrung des Zugangs veranlassen können.

(2) Die zuständige Behörde kann die Sperrung eines De-Mail-Kontos anordnen, wenn Tatsachen die Annahme rechtfertigen, dass das De-Mail-Konto auf Grund falscher Angaben eröffnet wurde oder die zur eindeutigen Identifizierung des Nutzers beim akkreditierten Diensteanbieter vorgehaltenen Daten nicht ausreichend fälschungssicher sind oder die sichere Anmeldung gemäß § 4 Absatz 1 Mängel aufweist, die eine unbemerkte Fälschung oder Kompromittierung des Anmeldevorgangs zulassen.

(3) Der akkreditierte Diensteanbieter hat dem Nutzer nach Wegfall des Sperrgrundes den Zugang zum De-Mail-Konto erneut zu gewähren.

(4) Der akkreditierte Diensteanbieter hat ein De-Mail-Konto unverzüglich aufzulösen, wenn

1. der Nutzer dies verlangt oder
2. die zuständige Behörde die Auflösung anordnet.

Die zuständige Behörde kann die Auflösung anordnen, wenn die Voraussetzungen des Absatzes 2 vorliegen und eine Sperrung nicht ausreichend ist. Eine Vereinbarung über weitere Auflösungsgründe ist unwirksam.

(5) Der akkreditierte Diensteanbieter hat sich vor einer Sperrung nach Absatz 1 oder einer Auflösung nach Absatz 4 auf geeignete Weise von der Identität des zur Sperrung oder Auflösung berechtigten Nutzers zu überzeugen.

(6) Im Fall einer Sperrung nach Absatz 1 Satz 1 Nummer 1 bis 3 oder Absatz 1 Satz 1 Nummer 4 in Verbindung mit Absatz 1 Satz 2 zweiter Halbsatz sowie einer Auflösung nach Absatz 4 hat der akkreditierte Diensteanbieter den Eingang von Nachrichten in das Postfach eines gesperrten oder aufgelösten De-Mail-Kontos zu unterbinden und den Absender unverzüglich davon zu informieren.

(7) Sofern die Sperrung oder Auflösung des De-Mail-Kontos auf Veranlassung des akkreditierten Diensteanbieters oder der zuständigen Behörde erfolgt, ist der Nutzer über die Sperrung oder Auflösung zu informieren. In den Fällen des Absatzes 1 Satz 2 erster Halbsatz ist der akkreditierte Diensteanbieter verpflichtet, den Nutzer darüber zu informieren, dass er trotz Sperrung Nachrichten empfangen und abrufen kann.

§ 11 Einstellung der Tätigkeit

(1) Der akkreditierte Diensteanbieter hat die Einstellung seiner Tätigkeit unverzüglich der zuständigen Behörde anzuzeigen. Er hat dafür zu sorgen, dass das De-Mail-Konto von einem anderen akkreditierten Diensteanbieter übernommen werden kann. Er hat die betroffenen Nutzer unverzüglich über die Einstellung seiner Tätigkeit zu benachrichtigen und deren Zustimmung zur Übernahme des De-Mail-Kontos durch einen anderen akkreditierten Diensteanbieter einzuholen.

(2) Übernimmt kein anderer akkreditierter Diensteanbieter das De-Mail-Konto, muss der akkreditierte Diensteanbieter sicherstellen, dass die im Postfach und in der Dokumentenablage gespeicherten Daten für wenigstens drei Monate ab dem Zeitpunkt der Benachrichtigung des Nutzers abrufbar bleiben.

(3) Der akkreditierte Diensteanbieter hat die Dokumentation nach § 13 an den akkreditierten Diensteanbieter, der das De-Mail-Konto nach Absatz 1 übernimmt, zu übergeben. Übernimmt kein anderer akkreditierter Diensteanbieter das De-Mail-Konto, übernimmt die zuständige Behörde die Dokumentation. In diesem Fall erteilt die zuständige Behörde bei Vorliegen eines berechtigten Interesses Auskunft daraus, soweit dies ohne unverhältnismäßigen Aufwand möglich ist.

(4) Der akkreditierte Diensteanbieter hat einen Antrag auf Eröffnung eines Insolvenzverfahrens der zuständigen Behörde unverzüglich anzuzeigen.

§ 12 Vertragsbeendigung

Der akkreditierte Diensteanbieter ist verpflichtet, dem Nutzer für einen Zeitraum von drei Monaten nach Vertragsende den Zugriff auf die im Postfach und in der Dokumentenablage abgelegten Daten zu ermöglichen und ihn auf ihre Löschung mindestens einen Monat vor dieser in Textform hinzuweisen.

§ 13 Dokumentation

(1) Der akkreditierte Diensteanbieter hat alle Maßnahmen zur Sicherstellung der Voraussetzungen der Akkreditierung und zur Erfüllung der in §§ 3 bis 12 genannten Pflichten so zu dokumentieren, dass die Daten und ihre Unverfälschtheit jederzeit nachprüfbar sind. Die Dokumentationspflicht umfasst den Vorgang der Eröffnung eines De-Mail-Kontos, jede Änderung von Daten, die hinsichtlich der Führung eines De-Mail-Kontos relevant sind, sowie jede Änderung hinsichtlich des Status eines De-Mail-Kontos. Für angefertigte Kopien von amtlichen Ausweisen gilt § 3 Absatz 3 Satz 3.

(2) Der akkreditierte Diensteanbieter hat die Dokumentation nach Absatz 1 während der Dauer des zwischen ihm und dem Nutzer bestehenden Vertragsverhältnisses sowie zehn weitere Jahre ab dem Schluss des Jahres aufzubewahren, in dem das Vertragsverhältnis endet.

(3) (weggefallen)

§ 14 Jugend- und Verbraucherschutz

Der akkreditierte Diensteanbieter hat bei Gestaltung und Betrieb der De-Mail-Dienste die Belange des Jugendschutzes und des Verbraucherschutzes zu beachten.

§ 15 Datenschutz

Der akkreditierte Diensteanbieter darf personenbezogene Daten des Nutzers eines De-Mail-Kontos nur verarbeiten, soweit dies zur Bereitstellung der De-Mail-Dienste und deren Durchführung erforderlich ist; im Übrigen gelten die Regelungen des Digitale-Dienste-Gesetzes, des Telekommunikationsgesetzes, des Telekommunikation-Digitale-Dienste-Datenschutz-Gesetzes und des Bundesdatenschutzgesetzes. Die datenschutzrechtlichen Regelungen dieser Gesetze gelten ergänzend zu der 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; L 314 vom 22.11.2016, S. 72; L 127 vom 23.5.2018, S. 2) in der jeweils geltenden Fassung.

§ 16 Auskunftsanspruch

(1) Ein akkreditierter Diensteanbieter erteilt Dritten Auskunft über Namen und Anschrift eines Nutzers, wenn

1. der Dritte glaubhaft macht, die Auskunft zur Verfolgung eines Rechtsanspruches gegen den Nutzer zu benötigen,
2. sich die Auskunft auf ein Rechtsverhältnis zwischen dem Dritten und dem Nutzer bezieht, das unter Nutzung von De-Mail zustande gekommen ist,
3. der Dritte die zur Feststellung seiner Identität notwendigen Angaben im Sinne von § 3 Absatz 2 macht,
4. der akkreditierte Diensteanbieter die Richtigkeit der Angaben nach § 3 Absatz 3 überprüft hat,
5. das Verlangen nicht rechtsmissbräuchlich ist, insbesondere nicht allein dem Zweck dient, ein Pseudonym aufzudecken, und

6. die schutzwürdigen Interessen des Nutzers im Einzelfall nicht überwiegen.

(2) Der Dritte hat dem akkreditierten Diensteanbieter zur Glaubhaftmachung nach Absatz 1 Nummer 1 elektronische Nachrichten oder Schriftstücke zu übermitteln, aus denen sich das Rechtsverhältnis zum Nutzer ergibt, sofern diese angefallen sind. Der akkreditierte Diensteanbieter hat den Nutzer von dem Auskunftsersuchen unverzüglich und unter Benennung des Dritten zu informieren und ihm Gelegenheit zur Stellungnahme zum Auskunftsersuchen zu gewähren, soweit dies die Verfolgung des Rechtsanspruchs des Dritten nicht im Einzelfall gefährdet.

(3) Der akkreditierte Diensteanbieter kann den Ersatz der für die Auskunftserteilung erforderlichen Aufwendungen verlangen.

(4) Die durch die Auskunftserteilung erlangten Daten dürfen nur zu dem bei dem Ersuchen angegebenen Zweck verwendet werden.

(5) Der akkreditierte Diensteanbieter hat die Auskunftserteilung nach Absatz 1 zu dokumentieren und den Nutzer von der Erteilung der Auskunft zu informieren. Die Dokumentationspflicht nach Satz 1 umfasst den Antrag zur Auskunftserteilung samt Angabe des Dritten nach Absatz 1, die Entscheidung des akkreditierten Diensteanbieters, die Identifizierungsdaten des bearbeitenden Mitarbeiters des akkreditierten Diensteanbieters, die Mitteilung des Ergebnisses an den auskunftsersuchenden Dritten, die Mitteilung über die Auskunftserteilung an den Nutzer und die jeweilige gesetzliche Zeit bei einzelnen Prozessen innerhalb der Auskunftserteilung. Die Dokumentation ist drei Jahre aufzubewahren.

(6) Die §§ 13 und 13a des Gesetzes über Unterlassungsklagen bei Verbraucherrechts- und anderen Verstößen bleiben unberührt.

(7) Die nach anderen Rechtsvorschriften bestehenden Regelungen zu Auskünften gegenüber öffentlichen Stellen bleiben unberührt.

Abschnitt 4
Akkreditierung

§ 17 Akkreditierung von Diensteanbietern

(1) Diensteanbieter, die De-Mail-Dienste anbieten wollen, müssen sich auf schriftlichen Antrag von der zuständigen Behörde akkreditieren lassen. Die Akkreditierung ist zu erteilen, wenn der Diensteanbieter nachweist, dass er die Voraussetzungen nach § 18 erfüllt und wenn die Ausübung der Aufsicht über den Diensteanbieter durch die zuständige Behörde gewährleistet ist. Akkreditierte Diensteanbieter erhalten ein Gütezeichen der zuständigen Behörde. Das Gütezeichen dient als Nachweis für die umfassend geprüfte technische und administrative Sicherheit der De-Mail-Dienste. Sie dürfen sich als akkreditierte Diensteanbieter bezeichnen. Nur akkreditierte Diensteanbieter dürfen sich im Geschäftsverkehr auf die nachgewiesene Sicherheit berufen und das Gütezeichen führen. Weitere Kennzeichnungen können akkreditierten Diensteanbietern vorbehalten sein.

(2) Über den Antrag nach § 17 Absatz 1 Satz 1 ist innerhalb einer Frist von drei Monaten zu entscheiden; § 42a Absatz 2 Satz 2 bis 4 des Verwaltungsverfahrensgesetzes findet Anwendung.

(3) Die Akkreditierung ist nach wesentlichen Veränderungen, spätestens jedoch nach drei Jahren zu erneuern.

§ 18 Voraussetzungen der Akkreditierung; Nachweis

(1) Als Diensteanbieter kann nur akkreditiert werden, wer

1. die für den Betrieb von De-Mail-Diensten erforderliche Zuverlässigkeit und Fachkunde besitzt,
2. eine geeignete Deckungsvorsorge trifft, um seinen gesetzlichen Verpflichtungen zum Ersatz von Schäden nachzukommen,
3. die technischen und organisatorischen Anforderungen an die Pflichten nach den §§ 3 bis 13 sowie nach § 16 in der Weise erfüllt, dass er die Dienste zuverlässig und sicher erbringt, er mit den anderen akkreditierten Diensteanbietern zusammenwirkt und für die Erbringung der Dienste ausschließlich technische Geräte verwendet, die sich im Gebiet der Mitgliedstaaten der Europäischen Union oder eines anderen Vertragsstaates des Abkommens über den Europäischen Wirtschaftsraum befinden,
4. bei der Gestaltung und dem Betrieb der De-Mail-Dienste die datenschutzrechtlichen Anforderungen erfüllt.

(2) Die Diensteanbieter haben die technischen und organisatorischen Anforderungen nach den §§ 3 bis 13 sowie nach § 16 nach dem Stand der Technik zu erfüllen. Die Einhaltung des Standes der Technik wird vermutet, wenn die Technische Richtlinie 01201 De-Mail des Bundesamtes für Sicherheit in der Informationstechnik vom 23. März 2011 (eBAnz AT40 2011 B1) in der jeweils im Bundesanzeiger veröffentlichten Fassung eingehalten wird. Bevor das Bundesamt für Sicherheit in der Informationstechnik wesentliche Änderungen an der Technischen Richtlinie vornimmt, hört es den Ausschuss De-Mail-Standardisierung im Sinne des § 22 an, und dem oder der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit wird hierbei Gelegenheit zur Stellungnahme gegeben, sofern Fragen des Datenschutzes berührt sind.

(3) Die Voraussetzungen nach Absatz 1 werden wie folgt nachgewiesen:

1. die erforderliche Zuverlässigkeit und Fachkunde durch Nachweise über die persönlichen Eigenschaften, das Verhalten und die entsprechenden Fähigkeiten seiner oder der in seinem Betrieb tätigen Personen; als Nachweis der erforderlichen Fachkunde ist es in der Regel ausreichend, wenn für die jeweilige Aufgabe im Betrieb entsprechende Zeugnisse oder Nachweise über die dafür notwendigen Kenntnisse, Erfahrungen und Fertigkeiten vorgelegt werden;
2. eine ausreichende Deckungsvorsorge durch den Abschluss einer Versicherung oder die Freistellungs- oder Gewährleistungsverpflichtung eines Kreditunternehmens mit einer Mindestdeckungssumme von jeweils 250 000 Euro für einen verursachten Schaden. Die Deckungsvorsorge kann erbracht werden durch
   a) eine Haftpflichtversicherung bei einem innerhalb der Mitgliedstaaten der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum zum Geschäftsbetrieb befugten Versicherungsunternehmen oder

b) eine Freistellungs- oder Gewährleistungsverpflichtung eines in einem der Mitgliedstaaten der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum zum Geschäftsbetrieb befugten Kreditinstituts, wenn gewährleistet ist, dass sie einer Haftpflichtversicherung vergleichbare Sicherheit bietet.

Soweit die Deckungsvorsorge durch eine Versicherung erbracht wird, gilt Folgendes:

a) Auf diese Versicherung finden § 113 Absatz 2 und 3 und die §§ 114 bis 124 des Versicherungsvertragsgesetzes Anwendung.

b) Die Mindestversicherungssumme muss 2,5 Millionen Euro für den einzelnen Versicherungsfall betragen. Versicherungsfall ist jede Pflichtverletzung des Diensteanbieters, unabhängig von der Anzahl der dadurch ausgelösten Schadensfälle. Wird eine Jahreshöchstleistung für alle in einem Versicherungsjahr verursachten Schäden vereinbart, muss sie mindestens das Vierfache der Mindestversicherungssumme betragen.

c) Von der Versicherung kann die Leistung nur ausgeschlossen werden für Ersatzansprüche aus vorsätzlich begangener Pflichtverletzung des akkreditierten Diensteanbieters oder der Personen, für die er einzustehen hat.

d) Die Vereinbarung eines Selbstbehaltes bis zu 1 Prozent der Mindestversicherungssumme ist zulässig;

3. die Erfüllung der technischen und organisatorischen Anforderungen an die Pflichten im Sinne des Absatzes 1 Nummer 3 durch vom Bundesamt für Sicherheit in der Informationstechnik nach § 9 Absatz 2 Satz 1 des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik zertifizierten IT-Sicherheitsdienstleistern erteilte Testate; das Zusammenwirken mit den anderen akkreditierten Diensteanbietern kann nur nach ausreichenden Prüfungen bestätigt werden; die Sicherheit der Dienste kann nur nach einer umfassenden im Rahmen der Vergabe der Testate stattfindenden Prüfung des Sicherheitskonzepts und der eingesetzten IT-Infrastrukturen bestätigt werden; zum Zeitpunkt des Inkrafttretens des Gesetzes erteilte Zertifikate können berücksichtigt werden;

4. die Erfüllung der datenschutzrechtlichen Anforderungen an das Datenschutzkonzept für die eingesetzten Verfahren und die eingesetzten informationstechnischen Einrichtungen durch Vorlage geeigneter Nachweise; der Nachweis wird dadurch geführt, dass der antragstellende Diensteanbieter ein Zertifikat des oder der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit vorlegt; der oder die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit erteilt auf schriftlichen Antrag des Diensteanbieters ein Zertifikat, wenn die datenschutzrechtlichen Kriterien erfüllt sind; die Erfüllung der datenschutzrechtlichen Kriterien wird nachgewiesen durch ein Gutachten, welches von einer vom Bund oder einem Land anerkannten oder öffentlich bestellten oder beliehenen sachverständigen Stelle für Datenschutz erstellt wurde; der oder die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit kann ergänzende Angaben anfordern; die datenschutzrechtlichen Kriterien sind in einem Kriterienkatalog definiert, der in der Verantwortung des oder der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit liegt und durch ihn oder sie im Bundesanzei-

ger und zusätzlich im Internet oder in sonstiger geeigneter Weise veröffentlicht wird; dem Bundesamt für Sicherheit in der Informationstechnik wird Gelegenheit zur Stellungnahme gegeben, sofern Fragen der IT-Sicherheit berührt sind.

(4) Der Diensteanbieter kann, unter Einbeziehung in seine Konzepte zur Umsetzung der Anforderungen des Absatzes 1, zur Erfüllung von Pflichten nach diesem Gesetz Dritte beauftragen.

§ 19 Gleichstellung ausländischer Dienste

(1) Vergleichbare Dienste aus einem anderen Mitgliedstaat der Europäischen Union oder aus einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum sind den Diensten eines akkreditierten Diensteanbieters, mit Ausnahme solcher Dienste, die mit der Ausübung hoheitlicher Tätigkeit verbunden sind, gleichgestellt, wenn ihre Anbieter dem § 18 gleichwertige Voraussetzungen erfüllen, diese gegenüber einer zuständige Stelle nachgewiesen sind und das Fortbestehen der Erfüllung dieser Voraussetzungen durch eine in diesem Mitglied- oder Vertragsstaat bestehende Kontrolle gewährleistet wird.

(2) Die Prüfung der Gleichwertigkeit des ausländischen Diensteanbieters nach Absatz 1 obliegt der zuständigen Behörde. Die Gleichwertigkeit ausländischer Diensteanbieter ist gegeben, wenn die zuständige Behörde festgestellt hat, dass im Herkunftsland des jeweiligen Diensteanbieters

1. die Sicherheitsanforderungen an Diensteanbieter,
2. die Prüfungsmodalitäten für Diensteanbieter sowie die Anforderungen an die für die Prüfung der Dienste zuständigen Stellen und
3. das Kontrollsystem

eine gleichwertige Sicherheit bieten.

Abschnitt 5
Aufsicht

§ 20 Aufsichtsmaßnahmen

(1) Die Aufsicht über die Einhaltung dieses Gesetzes obliegt der zuständigen Behörde. Mit der Akkreditierung unterliegen Diensteanbieter der Aufsicht der zuständigen Behörde.

(2) Die zuständige Behörde kann gegenüber Diensteanbietern Maßnahmen treffen, um die Einhaltung dieses Gesetzes sicherzustellen.

(3) Ungeachtet des Vorliegens von Testaten im Sinne des § 18 Absatz 3 Nummer 3 kann die zuständige Behörde einem akkreditierten Diensteanbieter den Betrieb vorübergehend ganz oder teilweise untersagen, wenn Tatsachen die Annahme rechtfertigen, dass

1. eine Voraussetzung für die Akkreditierung nach § 17 Absatz 1 weggefallen ist,
2. ungültige Einzelnachweise für das Angebot von De-Mail-Diensten verwendet oder bestätigt werden,
3. nachhaltig, erheblich oder dauerhaft gegen Pflichten verstoßen wird oder

4. sonstige Voraussetzungen für die Akkreditierung oder für die Anerkennung nach diesem Gesetz nicht erfüllt werden.

(4) Die Gültigkeit der von einem akkreditierten Diensteanbieter im Rahmen des Postfach- und Versanddienstes ausgestellten Eingangsbestätigungen und Abholbestätigungen bleibt von der Untersagung des Betriebs, der Einstellung der Tätigkeit, der Rücknahme oder dem Widerruf einer Akkreditierung unberührt.

(5) Soweit es zur Erfüllung der der zuständigen Behörde als Aufsichtsbehörde übertragenen Aufgaben erforderlich ist, haben die akkreditierten Diensteanbieter und die für diese nach § 18 Absatz 4 tätigen Dritten der zuständigen Behörde und den in ihrem Auftrag handelnden Personen das Betreten der Geschäftsräume während der üblichen Betriebszeiten zu gestatten, auf Verlangen die in Betracht kommenden Bücher, Aufzeichnungen, Belege, Schriftstücke und sonstigen Unterlagen in geeigneter Weise zur Einsicht vorzulegen, auch soweit sie elektronisch geführt werden, Auskunft zu erteilen und die erforderliche Unterstützung zu gewähren. Ein Zugriff auf De-Mail-Nachrichten von Nutzern durch die zuständige Behörde als Aufsichtsbehörde findet nicht statt. Der zur Erteilung einer Auskunft Verpflichtete kann die Auskunft verweigern, wenn er sich damit selbst oder einen der in § 383 Absatz 1 Nummer 1 bis 3 der Zivilprozessordnung bezeichneten Angehörigen der Gefahr der Verfolgung wegen einer Straftat oder eines Verfahrens nach dem Gesetz über Ordnungswidrigkeiten aussetzen würde. Er ist auf dieses Recht hinzuweisen.

§ 21 Informationspflicht

Die zuständige Behörde hat die Namen der akkreditierten Diensteanbieter sowie der ausländischen Diensteanbieter nach § 19 jeweils unter Angabe der ausschließlich für die De-Mail-Dienste verwendeten Kennzeichnungen gemäß § 5 Absatz 1 Satz 2 Nummer 1 für jeden über öffentlich erreichbare Kommunikationsverbindungen abrufbar zu halten.

Abschnitt 6
Schlussbestimmungen

§ 22 Ausschuss De-Mail-Standardisierung

Die technischen und organisatorischen Anforderungen an die Pflichten nach den §§ 3 bis 13 sowie nach § 16 werden unter Beteiligung der akkreditierten Diensteanbieter weiterentwickelt; dies gilt nicht für Anforderungen, die das Zusammenwirken zwischen den akkreditierten Diensteanbietern als solches oder die Sicherheit betreffen. Zu diesem Zweck wird ein Ausschuss De-Mail-Standardisierung gegründet, dem mindestens alle akkreditierten Diensteanbieter, je ein Vertreter von zwei auf Bundesebene bestehenden Gesamtverbänden, deren Belange berührt sind, das Bundesamt für Sicherheit in der Informationstechnik, der oder die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, ein vom IT-Planungsrat beauftragter Vertreter der Länder sowie ein Vertreter des Rates der IT-Beauftragten der Bundesregierung angehören. Die Entscheidung, welche beiden Verbände dem Ausschuss angehören sollen, liegt im Ermessen der zuständigen Behörde. Wird der Rat der IT-Beauftragten der Bundesregierung aufgelöst, tritt an dessen Stelle die von der Bundesregierung bestimmte Nachfolgeorganisation. Der Ausschuss tagt mindestens einmal im Jahr.

§ 23 Bußgeldvorschriften

(1) Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig

1. entgegen § 3 Absatz 1 Satz 3 nicht sicherstellt, dass nur der Nutzer Zugang erlangen kann,
2. entgegen § 3 Absatz 3 Satz 1 Nummer 1 erster Halbsatz oder Nummer 2 eine dort genannte Angabe nicht oder nicht rechtzeitig überprüft,
3. entgegen § 4 Absatz 1 Satz 2 nicht sicherstellt, dass eine sichere Anmeldung nur in den dort genannten Fällen erfolgt,
4. entgegen § 4 Absatz 3 nicht sicherstellt, dass eine Kommunikationsverbindung verschlüsselt erfolgt,
5. entgegen § 7 Absatz 2 Satz 1 Nummer 2 oder 4 dort genannte Daten nicht oder nicht rechtzeitig löscht,
6. entgegen § 10 Absatz 1 Satz 1 oder Absatz 4 Satz 1 Nummer 2 den Zugang zu einem De-Mail-Konto nicht oder nicht rechtzeitig sperrt oder das De-Mail-Konto nicht oder nicht rechtzeitig auflöst,
7. entgegen § 11 Absatz 1 Satz 1 eine Anzeige nicht, nicht richtig oder nicht rechtzeitig erstattet,
8. entgegen § 11 Absatz 1 Satz 3 einen Nutzer nicht, nicht richtig oder nicht rechtzeitig benachrichtigt,
9. entgegen § 11 Absatz 2 nicht sicherstellt, dass die dort genannten Daten abrufbar bleiben,
10. entgegen § 12 den Zugriff auf dort genannte Daten nicht ermöglicht oder einen Hinweis nicht, nicht richtig oder nicht rechtzeitig gibt,
11. entgegen § 13 Absatz 1 eine Dokumentation nicht oder nicht richtig erstellt,
12. entgegen § 13 Absatz 2 eine Dokumentation nicht oder nicht mindestens zehn Jahre aufbewahrt oder
13. entgegen § 17 Absatz 1 Satz 6 sich auf die nachgewiesene Sicherheit beruft oder das Gütezeichen führt.

(2) Die Ordnungswidrigkeit kann in den Fällen des Absatzes 1 Nummer 5 und 6 mit einer Geldbuße bis zu dreihunderttausend Euro und in den übrigen Fällen mit einer Geldbuße bis zu fünfzigtausend Euro geahndet werden.

(3) Verwaltungsbehörde im Sinne des § 36 Absatz 1 Nummer 1 des Gesetzes über Ordnungswidrigkeiten ist das Bundesamt für Sicherheit in der Informationstechnik.

§ 24 (weggefallen)

§ 25 Verfahren über eine einheitliche Stelle

Verwaltungsverfahren nach diesem Gesetz können über eine einheitliche Stelle abgewickelt werden.

Gesetz zur Einführung und Verwendung einer Identifikationsnummer in der öffentlichen Verwaltung (Identifikationsnummerngesetz - IDNrG)

§ 1 Ziele des Gesetzes

Die Identifikationsnummer nach § 139b der Abgabenordnung (Identifikationsnummer) wird als zusätzliches Ordnungsmerkmal in die sich aus der Anlage zu diesem Gesetz ergebenden Register des Bundes und der Länder eingeführt, um

1. Daten einer natürlichen Person in einem Verwaltungsverfahren eindeutig zuzuordnen,
2. die Datenqualität der zu einer natürlichen Person gespeicherten Daten zu verbessern sowie
3. die erneute Beibringung von bei öffentlichen Stellen bereits vorhandenen Daten durch die betroffene Person zu verringern.

§ 2 Aufgaben registerführender Stellen

Öffentliche Stellen in Bund und Ländern, welche Register nach § 1 führen (registerführende Stellen), sind zur Erreichung der Ziele nach § 1 verpflichtet

1. bis spätestens zum Ablauf des fünften auf das Inkrafttreten dieses Gesetzes folgenden Kalenderjahres die Identifikationsnummer als zusätzliches Ordnungsmerkmal zu Personendaten in die sich aus der Anlage zu diesem Gesetz ergebenden Register zu speichern,
2. die in diesen Registern gespeicherten Daten, die den Datenkategorien in § 4 Absatz 2 und 3 entsprechen, durch die beim Bundeszentralamt für Steuern gespeicherten Daten nach § 4 Absatz 2 und 3 zu ersetzen und diese im Vergleich zu den beim Bundeszentralamt für Steuern gespeicherten Daten nach § 4 Absatz 2 und 3 nach fachlichem Bedarf aktuell zu halten; hierbei bleiben besondere Vorschriften über die Berichtigung von Daten unberührt; ein automatisierter Abgleich ist zulässig; sowie
3. natürlichen Personen die Übermittlung ihrer Daten unter Verwendung der Identifikationsnummer digital über eine zentrale Stelle transparent zu machen (Datenschutzcockpit).

§ 3 Einrichtung und Aufgaben der Registermodernisierungsbehörde

(1) Die Registermodernisierungsbehörde hat folgende Aufgaben:

1. Erstellen einer Übersicht über bestehende Register,
2. Übermittlung der Identifikationsnummer sowie der übrigen Daten nach § 4 Absatz 2 und 3 an
   a) registerführende Stellen in Bund und Ländern zur Erfüllung der Aufgaben nach § 2 sowie
   b) öffentliche Stellen nach § 6 Absatz 2,

3. übergeordnete Steuerung
   a) der einzelnen Projekte zur Umsetzung dieses Gesetzes sowie
   b) von registerübergreifenden Maßnahmen zur Verbesserung der Datenqualität.

Das Bundesverwaltungsamt nimmt die Aufgaben der Registermodernisierungsbehörde wahr.

(2) Die Registermodernisierungsbehörde darf zur Aufgabenerfüllung nach Maßgabe dieses Gesetzes sowie in entsprechender Anwendung von § 30 Absatz 6 und 11 der Abgabenordnung und der Steuerdaten-Abrufverordnung in der jeweils geltenden Fassung beim Bundeszentralamt für Steuern nach § 139b Absatz 3 Nummer 1, 3 bis 10 und 12 bis 16 der Abgabenordnung gespeicherte Daten im automatisierten Verfahren abrufen und an

1. registerführende Stellen zur Erfüllung der Aufgaben nach § 2 sowie
2. öffentliche Stellen zum Zwecke der Erbringung von Verwaltungsleistungen nach dem Onlinezugangsgesetz

übermitteln. Die Erfüllung der sonstigen Aufgaben des Bundesverwaltungsamts bleibt unberührt.

§ 4 Zu einer Person gespeicherte Daten

(1) Die Daten nach den Absätzen 2 und 3 einer natürlichen Person werden vom Bundeszentralamt für Steuern gespeichert, wenn diese Person eine Identifikationsnummer nach § 139b der Abgabenordnung erhalten hat.

(2) Die zur Identifizierung einer natürlichen Person erforderlichen personenbezogenen Daten sind die Basisdaten. Einer natürlichen Person werden folgende Daten als Basisdaten zugeordnet:

1. Identifikationsnummer,
2. Familienname,
3. frühere Namen,
4. Vornamen,
5. Doktorgrad,
6. Tag und Ort der Geburt,
7. Geschlecht,
8. Staatsangehörigkeiten,
9. gegenwärtige oder letzte bekannte Anschrift,
10. Sterbetag sowie
11. Tag des Einzugs und des Auszugs.

(3) Einer natürlichen Person werden zudem folgende weitere Daten zugeordnet:

1. Auskunftssperren nach dem Bundesmeldegesetz sowie
2. Datum des letzten Verwaltungskontakts (Monat, Jahr).

(4) Das Datum nach Absatz 3 Nummer 2 wird der Registermodernisierungsbehörde von gesetzlich bestimmten Registern bei Vorliegen eines Verwaltungskontakts automatisiert übermittelt und an das Bundeszentralamt für Steuern weitergeleitet.

§ 5 Zweck und Vergabe der Identifikationsnummer

(1) Die Identifikationsnummer dient im Rahmen dieses Gesetzes

1. der Zuordnung der Datensätze zu einer Person sowie
2. dem Abgleich von Datensätzen einer natürlichen Person, die den Datenkategorien in § 4 Absatz 2 und 3 entsprechen, in verschiedenen Registern untereinander, soweit eine andere gesetzliche Vorschrift dies erlaubt.

Die Verarbeitung der Identifikationsnummer nach diesem Gesetz durch öffentliche und nicht-öffentliche Stellen zu anderen Zwecken ist außer zu Verarbeitungen zur Erbringung von Verwaltungsleistungen nach dem Onlinezugangsgesetz auf Grund von Rechtsvorschriften oder mit Einwilligung der betroffenen Person sowie zum Zwecke eines registerbasierten Zensus unzulässig. Die Verarbeitung der Identifikationsnummer nach § 139b der Abgabenordnung bleibt unberührt.

(2) Hinsichtlich der Vergabe der Identifikationsnummer durch das Bundeszentralamt für Steuern gilt § 139b der Abgabenordnung in Verbindung mit der Steueridentifikationsnummerverordnung.

(3) Die Registermodernisierungsbehörde stellt sicher, dass bei einer Verarbeitung der Identifikationsnummer für Datenübermittlungen an die Registermodernisierungsbehörde oder bei Datenabrufen von der Registermodernisierungsbehörde fehlerhafte Angaben der Identifikationsnummer erkannt werden und in solchen Fällen keine weitere Datenverarbeitung erfolgt.

§ 6 Automatisierter Datenabruf bei der Registermodernisierungsbehörde

(1) Registerführende Stellen rufen zur Erfüllung der Aufgaben nach § 2 die Daten nach § 4 Absatz 2 und 3 bei der Registermodernisierungsbehörde ab, es sei denn, dass der Abruf bei der Meldebehörde erfolgt. Die registerführenden Stellen dürfen die abgerufenen Daten zur Erfüllung der Aufgaben nach § 2 Nummer 1 und 2 verarbeiten.

(2) Die Daten nach § 4 Absatz 2 und 3 sollen von einer öffentlichen Stelle bei der Registermodernisierungsbehörde zum Zwecke der Erbringung von Verwaltungsleistungen nach dem Onlinezugangsgesetz abgerufen werden. Die Verarbeitung erfolgt nach Maßgabe der für die öffentliche Stelle jeweils anwendbaren Rechtsgrundlage.

(3) Datenabrufe bei der Registermodernisierungsbehörde nach diesem Gesetz erfolgen ausschließlich im automatisierten Verfahren wie folgt:

1. Enthält das Datenabrufersuchen mindestens den Familiennamen, den Wohnort, die Postleitzahl sowie das Geburtsdatum der betroffenen Person, übermittelt die Registermodernisierungsbehörde der ersuchenden Stelle die Identifikationsnummer sowie die weiteren zur betroffenen Person gespeicherten Daten nach § 4 Absatz 2 und 3, soweit sie zur Erfüllung der Aufgaben der ersuchenden Stelle erforderlich sind.

2. Sofern ein Datenabrufersuchen nach Nummer 1 nicht veranlasst werden kann, weil Wohnort und Postleitzahl nicht vorliegen, kann ein Datenabrufersuchen durchgeführt werden, wenn das Datenabrufersuchen mindestens den Familiennamen, den Vornamen und das Geburtsdatum enthält.

3. Enthält das Datenabrufersuchen mindestens die Identifikationsnummer und das Geburtsdatum der betroffenen Person, übermittelt die Registermodernisierungsbehörde der ersuchenden Stelle die übrigen zur Person gespeicherten Daten nach § 4 Absatz 2 und 3, soweit sie zur Erfüllung der Aufgaben der ersuchenden Stelle erforderlich sind.

(4) Daten dürfen von der Registermodernisierungsbehörde den ersuchenden Stellen nur übermittelt werden, wenn sichergestellt ist, dass die Voraussetzung zum Datenabruf vorliegt. Das Datenabrufersuchen darf keine Daten enthalten, die nicht in § 4 Absatz 2 bezeichnet sind. Ist eine eindeutige Identifizierung der betroffenen Person nicht möglich, teilt die Registermodernisierungsbehörde dies der ersuchenden Stelle mit und übermittelt keine Daten nach § 4 Absatz 2 und 3.

(5) Liegt zu Daten einer Person eine Auskunftssperre nach dem Bundesmeldegesetz vor, übermittelt die Registermodernisierungsbehörde an registerführende Stellen die Daten ausschließlich im Rahmen der erstmaligen Datenübermittlung der Identifikationsnummer nach Absatz 1 in Verbindung mit § 2 Nummer 1 und 2. Bei Abrufen zur Aktualisierung und übrigen Abrufen erhält die abrufende öffentliche Stelle von der Registermodernisierungsbehörde eine Mitteilung, die keine Rückschlüsse darauf zulassen darf, ob zu der betroffenen Person keine Daten vorhanden sind oder ob eine Auskunftssperre besteht.

§ 7 Verfahren der Datenübermittlungen mit der Registermodernisierungs- behörde und zwischen öffentlichen Stellen

(1) Die Verfahren der Datenabrufe öffentlicher Stellen bei der Registermodernisierungsbehörde, Antworten der Registermodernisierungsbehörde an die ersuchenden Stellen sowie Datenersetzungen nach § 2 Nummer 2 sind elektronisch unter Nutzung eines vom Bundesministerium des Innern, für Bau und Heimat im Einvernehmen mit dem Bundesministerium der Finanzen im Bundesanzeiger bekannt zu machenden Datenaustauschstandards zu führen. Die Registermodernisierungsbehörde führt eine automatisierte Prüfung der übermittelten Daten daraufhin durch, ob sie der richtigen Identifikationsnummer zugeordnet, vollständig und schlüssig sind und ob sie dem Datenaustauschstandard nach Satz 1 entsprechen. Der elektronische Datenaustausch zwischen Bund und Ländern ist gemäß § 3 des Gesetzes über die Verbindung der informationstechnischen Netze des Bundes und der Länder – Gesetz zur Ausführung von Artikel 91c Absatz 4 des Grundgesetzes – vom 10. August 2009 (BGBl. I S. 2702, 2706), das durch Artikel 72 der Verordnung vom 19. Juni 2020 (BGBl. I S. 1328) geändert worden ist, ausschließlich über das Verbindungsnetz zu führen.

(2) Datenübermittlungen unter Nutzung einer Identifikationsnummer nach diesem Gesetz zwischen öffentlichen Stellen verschiedener Bereiche erfolgen über Vermittlungsstellen verschlüsselt in gesicherten Verfahren, die dem aktuellen Stand von Sicherheit und Technik entsprechen müssen. Es werden mindestens sechs Bereiche gebildet, die durch die Rechtsverordnung nach § 12 Absatz 1 Satz 1 näher bestimmt werden. Die Vermittlungsstellen müssen öffentliche Stellen sein. Sie sind für den sicheren, verlässlichen und nachvollziehbaren Transport elektronischer Nachrichten zuständig und müssen diese Aufgabe ohne Kenntnis der Nachrichteninhalte erbringen können. Sie kontrollieren und protokollieren abstrakt die Übermittlungsberechtigung. Liegt die Übermittlungsberechtigung abstrakt nicht vor, wer-

den keine personenbezogenen Daten übermittelt. Die bestehende Anwendung des Verfahrens nach Satz 1 innerhalb von Bereichen bleibt unberührt.

(3) Gemeinde und Gemeindeverbände sind zur Umsetzung der Verpflichtungen nach Absatz 2 bei Datenübermittlungen innerhalb einer Gemeinde oder eines Gemeindeverbands sieben Jahre nach Inkrafttreten dieses Gesetzes verpflichtet.

§ 8 Befugnisse und Verantwortlichkeiten

(1) Die datenschutzrechtliche Verantwortung des einzelnen Datenabrufs trägt die jeweilige abrufende Stelle.

(2) Die Registermodernisierungsbehörde hat durch geeignete technische und organisatorische Maßnahmen nach den Artikeln 24, 25 und 32 der 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; L 314 vom 22.11.2016, S. 72; L 127 vom 23.5.2018, S. 2) sicherzustellen, dass die Daten nach § 4 Absatz 2 und 3 nicht unbefugt verarbeitet werden können. Die abrufende Stelle hat bei Einrichtung eines automatisierten Abrufverfahrens durch geeignete technische und organisatorische Maßnahmen nach den Artikeln 24, 25 und 32 der Verordnung (EU) 2016/679 sicherzustellen, dass Daten nur von hierzu befugten Personen abgerufen werden können.

(3) Bei Datenabrufen prüft die Registermodernisierungsbehörde automatisiert bei jedem Aufbau einer Verbindung anhand sicherer Authentifizierungsverfahren die Identität der abrufenden Stelle; über die Identität der abrufenden Stelle darf kein Zweifel bestehen. Andernfalls werden keine personenbezogenen Daten übermittelt.

(4) Die Registermodernisierungsbehörde überprüft die Zulässigkeit der Abrufe über Absatz 3 hinaus durch geeignete Stichprobenverfahren sowie wenn dazu Anlass besteht. Die abrufende Stelle hat ein Berechtigungskonzept zu erstellen, welches mit dem jeweiligen Datenschutzbeauftragten der abrufenden Stelle abzustimmen ist.

§ 9 Protokollierung

(1) Alle Datenübermittlungen zwischen öffentlichen Stellen unter Nutzung einer Identifikationsnummer nach diesem Gesetz sind durch die jeweiligen Stellen in einer Weise zu protokollieren, die die Kontrolle der Zulässigkeit von Datenabrufen technisch unterstützt. Die Datenübermittlungen zwischen der Registermodernisierungsbehörde und dem Bundeszentralamt für Steuern sowie Datenabrufe bei der Registermodernisierungsbehörde werden bei der Registermodernisierungsbehörde protokolliert.

(2) Die Protokolldaten nach Absatz 1 dürfen nur zur datenschutzrechtlichen Prüfung sowie zur Gewährleistung der datenschutzrechtlichen Rechte der betroffenen Person, einschließlich der Übermittlung an das Datenschutzcockpit der betroffenen Person nach § 10 des Onlinezugangsgesetzes, verwendet werden.

(3) Die Protokolldaten sind zwei Jahre aufzubewahren und danach unverzüglich zu löschen, soweit ihre längere Aufbewahrung nicht zur Erfüllung eines Zwecks nach Absatz 2 erforderlich ist. Ist eine längere Aufbewahrung erforderlich, so sind die Gründe der Erforderlichkeit zu dokumentieren. Abweichende gesetzliche Regelungen bleiben unberührt.

§ 10 Qualitätssicherung

(1) Das Bundeszentralamt für Steuern ist für die Qualitätssicherung der nach § 4 Absatz 2 und 3 gespeicherten Daten verantwortlich.

(2) Die Registermodernisierungsbehörde ist für die Koordinierung der registerübergreifenden Qualitätssicherung verantwortlich. Hierzu etabliert sie Verfahren, die eine hohe Aktualität, Validität und Konsistenz der Daten, einschließlich einer Bereinigung um Mehrfach-, Über- und Untererfassungen, gewährleisten, und wirkt mit registerführenden Stellen zusammen.

(3) Die Entscheidung über die Änderung eines Datums trifft

1. für Daten, die von einer inländischen Personenstandsbehörde beurkundet wurden, die zuständige Personenstandsbehörde,
2. hinsichtlich des Bestehens der deutschen Staatsangehörigkeit die zuständige Staatsangehörigkeitsbehörde,
3. für andere Daten einer im Inland gemeldeten Person die zuständige Meldebehörde, es sei denn, dass eine andere Behörde befugt ist, die Richtigkeit des Datums mit Wirkung für Dritte verbindlich festzustellen,
4. für andere Daten einer nicht im Inland gemeldeten Person die Behörde, die die Daten an das Bundeszentralamt für Steuern übermittelt hat, es sei denn, dass eine andere Behörde befugt ist, die Richtigkeit des Datums mit Wirkung für Dritte verbindlich festzustellen.

(4) Jede nach § 6 Absatz 1 oder 2 zum Abruf von Daten berechtigte öffentliche Stelle, die konkrete Anhaltspunkte für die Unrichtigkeit oder Unvollständigkeit der Daten nach § 4 Absatz 2 und 3 erlangt hat, hat die Registermodernisierungsbehörde unverzüglich hierüber zu unterrichten. Nach Überprüfung der Information nach Satz 1 hat die Registermodernisierungsbehörde das Bundeszentralamt für Steuern über das Prüfergebnis zu informieren. Die Verfahren nach § 139b Absatz 8 und 9 der Abgabenordnung sowie nach § 139d der Abgabenordnung in Verbindung mit § 6 Absatz 2 der Steueridentifikationsnummerverordnung bleiben unberührt.

(5) Jede nach § 6 Absatz 1 oder 2 zum Abruf von Daten berechtigte öffentliche Stelle, in deren Dateisystemen oder Registern Daten nach § 4 Absatz 2 und 3 zu einer natürlichen Person gespeichert sind, ist verpflichtet, auf Verlangen der Registermodernisierungsbehörde an der Aufklärung von Unrichtigkeiten oder Unvollständigkeiten dieser Daten in ihrem eigenen oder dem Datenbestand einer anderen öffentlichen Stelle mitzuwirken.

(6) Jede öffentliche Stelle, die beim Abgleich der bei ihr gespeicherten Daten mit den von der Registermodernisierungsbehörde auf ihr Datenabrufersuchen übermittelten Daten eine Unrichtigkeit oder Unvollständigkeit in ihren Registern festgestellt hat, ist verpflichtet, ihren Datenbestand von Amts wegen zu berichtigen oder zu ergänzen. Besondere Vorschriften über die Berichtigung von Daten bleiben unberührt.

§ 11 Löschung

Die Registermodernisierungsbehörde hat die Daten nach § 4 Absatz 2 und 3 unverzüglich nach der Übermittlung und Protokollierung nach § 9 zu löschen.

§ 12 Verordnungsermächtigung

(1) Die Bundesregierung wird ermächtigt, durch Rechtsverordnung mit Zustimmung des Bundesrates die Anzahl und die Abgrenzung der Bereiche nach § 7 Absatz 2 Satz 2 zu bestimmen. Die Anzahl und die Abgrenzung der Bereiche hat dabei so zu erfolgen, dass das Risiko, bezogen auf die einzelne Person ein vollständiges Persönlichkeitsprofil durch Datenübermittlungen innerhalb eines Bereichs zu erstellen, wirksam begrenzt wird.

(2) Das Bundesministerium des Innern, für Bau und Heimat wird ermächtigt, im Einvernehmen mit dem Bundesministerium der Finanzen durch Rechtsverordnung mit Zustimmung des Bundesrates Näheres zu den technischen Verfahren der Datenübermittlungen nach § 7 Absatz 2 zu bestimmen.

(3) Das Bundesministerium des Innern, für Bau und Heimat wird ermächtigt, im Einvernehmen mit dem Bundesministerium der Finanzen und im Benehmen mit dem IT-Planungsrat durch Rechtsverordnung, die nicht der Zustimmung des Bundesrates bedarf, Näheres zu bestimmen

1. zu dem technischen Verfahren der Datenübermittlung zwischen der Registermodernisierungsbehörde und dem Bundeszentralamt für Steuern nach § 3,
2. zu dem technischen Format der Daten nach § 4 Absatz 2 und 3,
3. zu den technischen Verfahren der Datenübermittlung an und durch die Registermodernisierungsbehörde nach § 7 Absatz 1 und § 10 Absatz 4,
4. zu den spezifischen technischen und organisatorischen Maßnahmen der Registermodernisierungsbehörde nach den Artikeln 24, 25 und 32 der Verordnung (EU) 2016/679 und der Authentifizierungsverfahren nach § 8 Absatz 3 sowie
5. zu den technischen Standards und Verantwortlichkeiten der Protokollierung nach § 9 Absatz 1 Satz 2.

(4) Das jeweils zuständige Bundesministerium wird ermächtigt, die Anwendung des Verfahrens nach § 7 Absatz 2 auch innerhalb eines Verwaltungsbereichs durch Rechtsverordnung mit Zustimmung des Bundesrates zu bestimmen.

§ 13 Prüfung durch den oder die Bundesbeauftragten für den Datenschutz und die Informationsfreiheit

Der oder die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit soll die Registermodernisierungsbehörde hinsichtlich der Datenverarbeitungen nach diesem Gesetz zwei Jahre nach Inkrafttreten dieses Gesetzes und dann erneut zweimal alle zwei Jahre prüfen.

§ 14 Verhältnis zu anderen Vorschriften

(1) Der Datenaustausch nach § 139b Absatz 6 bis 9 der Abgabenordnung bleibt unberührt.

(2) Andere gesetzliche Vorschriften zur Verarbeitung personenbezogener Daten bleiben unberührt.

§ 15 Ausschluss abweichenden Landesrechts

Von den in diesem Gesetz oder auf Grundlage dieses Gesetzes getroffenen Regelungen kann durch Landesrecht nicht abgewichen werden.

§ 16 Evaluierung

(1) Das Bundesministerium des Innern, für Bau und Heimat berichtet dem Deutschen Bundestag im dritten Jahr nach Inkrafttreten dieses Gesetzes und dann fortlaufend alle drei Jahre jeweils über die Datenverarbeitungen durch die Registermodernisierungsbehörde. Hierbei ist insbesondere über die Ergebnisse der Überprüfungen nach § 8 Absatz 4 zu berichten.

(2) Das Bundesministerium des Innern, für Bau und Heimat berichtet dem Deutschen Bundestag unter Einbeziehung von wissenschaftlichem Sachverstand im fünften Jahr nach Inkrafttreten dieses Gesetzes über die Wirksamkeit der in diesem Gesetz enthaltenen Maßnahmen für die Erreichung der in § 1 genannten Ziele. Der Bericht hat insbesondere Empfehlungen zu enthalten, ob

1. für andere Bereiche weitere, bereichsspezifische Identifikationsnummern eingeführt werden oder eine einheitliche Identifikationsnummer für alle Register umgesetzt wird und
2. das Verfahren nach § 7 Absatz 2 auch innerhalb von Verwaltungsbereichen Anwendung finden sollte.

§ 17 Strafvorschriften

(1) Mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe wird bestraft, wer die Identifikationsnummer

1. wissentlich, ohne hierzu berechtigt zu sein, erhebt, speichert, übermittelt oder verbreitet oder
2. ohne hierzu berechtigt zu sein, verwendet, um personenbezogene Daten, die nicht offenkundig sind, zu erheben, zu speichern oder zu übermitteln.

(2) Die Tat wird nur auf Antrag verfolgt. Antragsberechtigt sind die betroffene Person, der Verantwortliche und die Datenschutzaufsichtsbehörden.

Anlage (zu § 1)
Register nach § 1 dieses Gesetzes

Register im Sinne des § 1 dieses Gesetzes sind:

1. Melderegister
2. elektronisch geführte Personenstandsregister
3. Ausländerzentralregister
4. Stammsatzdatei der Datenstelle der Rentenversicherung gemäß § 150 des Sechsten Buches Sozialgesetzbuch
5. Versichertenkonten der Rentenversicherungsträger gemäß § 149 des Sechsten Buches Sozialgesetzbuch

6. Rentenzahlbestandsregister des Renten-Services der Deutschen Post AG
7. die Stammsatzdatei der landwirtschaftlichen Sozialversicherung nach § 62 des Gesetzes über die Alterssicherung der Landwirte
8. bei den berufsständischen Versorgungswerken systematisch geführte personenbezogene Datenbestände zu Leistungsberechtigten
9. bei der Künstlersozialkasse systematisch geführte personenbezogene Datenbestände zu den nach näherer Bestimmung des Künstlersozialversicherungsgesetzes versicherten Künstlern und Publizisten
10. bei der Bundesagentur für Arbeit systematisch geführte personenbezogene Datenbestände nach dem Dritten Buch Sozialgesetzbuch
11. bei den Trägern der Grundsicherung für Arbeitsuchende systematisch geführte personenbezogene Datenbestände nach dem Zweiten Buch Sozialgesetzbuch
12. Dateisystem der Beschäftigungsbetriebe nach § 18i des Vierten Buches Sozialgesetzbuch
13. eID-Karte-Register
14. Zentrales Unternehmerverzeichnis der gesetzlichen Unfallversicherung
15. Zentrales Fahrzeugregister
16. Zentrales Fahrerlaubnisregister
17. Fahreignungsregister
18. Lehrlingsrolle gemäß § 28 der Handwerksordnung
19. Handwerksrolle gemäß § 6 der Handwerksordnung
20. Verzeichnis der Inhaber von Betrieben eines zulassungsfreien oder eines handwerksähnlichen Gewerbes gemäß § 19 der Handwerksordnung
21. Personalausweisregister
22. Passregister
23. Ausländerdateien nach § 62 der Aufenthaltsverordnung
24. Verzeichnis der Berufsausbildungsverhältnisse nach § 34 des Berufsbildungsgesetzes
25. bei den allgemeinbildenden und beruflichen Schulen, Schulbehörden, Bildungseinrichtungen nach § 2 des Hochschulstatistikgesetzes systematisch geführte personenbezogene Datenbestände zu Bildungsteilnehmenden
26. Versichertenverzeichnis der Krankenkassen
27. Bundeszentralregister
28. Nationales Waffenregister
29. bei den Elterngeldstellen nach § 12 des Bundeselterngeld- und Elternzeitgesetzes systematisch geführte personenbezogene Datenbestände zu Leistungsempfängern

30. Verzeichnis der gemäß § 14 der Gewerbeordnung angezeigten Gewerbebetriebe
31. Gewerbezentralregister
32. Versichertenverzeichnis der Pflegekassen
33. Register für Grundsicherung im Alter
34. Register für ergänzende Hilfe zum Lebensunterhalt
35. bei den Wohngeldbehörden nach § 24 des Wohngeldgesetzes systematisch geführte personenbezogene Datenbestände zu Leistungsempfängern
36. bei den Ämtern für Ausbildungsförderung und dem Bundesverwaltungsamt nach den §§ 39 und 40 des Bundesausbildungsförderungsgesetzes systematisch geführte personenbezogene Datenbestände zu Leistungsempfängern
37. Register der Versorgungsämter
38. bei den für die Durchführung des Asylbewerberleistungsgesetzes zuständigen Behörden nach den §§ 10 und 10a des Asylbewerberleistungsgesetzes systematisch geführte personenbezogene Datenbestände zu Leistungsempfängern
39. Vermittlerregister nach § 11a der Gewerbeordnung
40. Berufsregister der Steuerberater und Wirtschaftsprüfer
41. Beitragskontendatenbank
42. bei den öffentlichen Arbeitgebern in Bund, Ländern und Kommunen nach § 2 Absatz 1 des Finanz- und Personalstatistikgesetzes systematisch geführte personenbezogene Datenbestände über die Beschäftigten
43. sämtliche von den Architekten- und Ingenieurkammern der Länder auf gesetzlicher Grundlage zu führenden Listen, Verzeichnisse oder Register
44. bei den Industrie- und Handelskammern geführten Verzeichnisse ihrer Mitglieder nach § 2 des Gesetzes zur vorläufigen Regelung des Rechts der Industrie- und Handelskammern
45. Krisenvorsorgeliste nach § 6 Absatz 3 des Konsulargesetzes
46. Zentrale Luftfahrerdatei
47. Register für Betreiber von unbemannten und zulassungspflichtigen Fluggeräten
48. Luftfahrzeugrolle nach § 64 Absatz 1 Nummer 1 des Luftverkehrsgesetzes
49. Zulassungsregister nach § 14 des Umweltauditgesetzes
50. Verzeichnis über die Bescheinigungen über die Fahrzeugführerschulung nach Abschnitt 8.2.2 der Vorschriften für die Ausbildung der Fahrzeugbesatzung (sog. ADR-Infodatenbank) gemäß § 14 Absatz 3 der Gefahrgutverordnung Straße, Eisenbahn und Binnenschifffahrt

Gesetz über Personalausweise und den elektronischen Identitätsnachweis (Personalausweisgesetz – PAuswG)*

Inhaltsübersicht

* Vom Abdruck des parallel gelagerten Passgesetzes (online unter https://www.gesetze-im-internet.de/pa_g_1986/) wurde abgesehen

Abschnitt 8
Verordnungsermächtigung; Übergangsvorschrift

Abschnitt 1
Allgemeine Vorschriften

§ 1 Ausweispflicht; Ausweisrecht

(1) Deutsche im Sinne des Artikels 116 Abs. 1 des Grundgesetzes sind verpflichtet, einen gültigen Ausweis zu besitzen, sobald sie 16 Jahre alt sind und der allgemeinen Meldepflicht unterliegen oder, ohne ihr zu unterliegen, sich überwiegend in Deutschland aufhalten. Sie müssen ihn auf Verlangen einer zur Feststellung der Identität berechtigten Behörde vorlegen und es ihr ermöglichen, ihr Gesicht mit dem Lichtbild des Ausweises abzugleichen. Vom Ausweisinhaber darf nicht verlangt werden, den Personalausweis zu hinterlegen oder in sonstiger Weise den Gewahrsam aufzugeben. Dies gilt nicht für zur Identitätsfeststellung berechtigte Behörden sowie in den Fällen der Einziehung und Sicherstellung.

(2) Die Ausweispflicht gilt auch für Personen, die als Binnenschiffer oder Seeleute nach dem Bundesmeldegesetz einer besonderen Meldepflicht unterliegen. Sie gilt nicht für Personen, gegen die eine Freiheitsstrafe vollzogen wird, wenn deren Vollzug noch länger als drei Monate andauert. Die Ausweispflicht nach Absatz 1 Satz 1 und 2 erfüllt auch, wer einen gültigen Pass im Sinne des § 1 Absatz 2 des Passgesetzes besitzt, ihn auf Verlangen vorlegt und den Lichtbildabgleich ermöglicht.

(3) Die zuständige Personalausweisbehörde nach § 7 Abs. 1 und 2 kann Personen von der Ausweispflicht befreien,

1. für die ein Betreuer oder eine Betreuerin nicht nur durch einstweilige Anordnung bestellt ist oder die handlungs- oder einwilligungsunfähig sind und von einem oder von einer mit öffentlich beglaubigter Vollmacht Bevollmächtigten vertreten werden,
2. die voraussichtlich dauerhaft in einem Krankenhaus, einem Pflegeheim oder einer ähnlichen Einrichtung untergebracht sind oder
3. die sich wegen einer dauerhaften Behinderung nicht allein in der Öffentlichkeit bewegen können.

(4) Auf Antrag ist ein Ausweis auch auszustellen, wenn Personen

1. noch nicht 16 Jahre alt sind oder
2. Deutsche im Sinne des Artikels 116 Abs. 1 des Grundgesetzes sind, die der Meldepflicht deswegen nicht unterliegen, weil sie keine Wohnung in Deutschland haben.

§ 2 Begriffsbestimmungen

(1) Ausweise im Sinne dieses Gesetzes sind der Personalausweis, der vorläufige Personalausweis und der Ersatz-Personalausweis.

(2) Zur Identitätsfeststellung berechtigte Behörden im Sinne dieses Gesetzes sind öffentliche Stellen, die befugt sind, zur Erfüllung ihrer gesetzlichen Aufgaben als hoheitliche Maßnahme die Identität von Personen festzustellen.

(3) Diensteanbieter sind natürliche und juristische Personen, die zur Wahrnehmung von Aufgaben der öffentlichen Verwaltung oder zur Erfüllung eigener Geschäftszwecke den Nachweis der Identität oder einzelner Identitätsmerkmale des Ausweisinhabers benötigen und ihren Wohn-, Geschäfts- oder Dienstsitz innerhalb der Europäischen Union sowie in Staaten, in denen ein vergleichbarer Datenschutzstandard besteht, haben.

(3a) Identifizierungsdiensteanbieter sind Diensteanbieter, deren Dienst darin besteht, für einen Dritten eine einzelfallbezogene Identifizierungsdienstleistung mittels des elektronischen Identitätsnachweises nach § 18 zu erbringen.

(4) Ein Berechtigungszertifikat ist eine elektronische Bescheinigung, die es einem Diensteanbieter ermöglicht,

1. seine Identität dem Personalausweisinhaber nachzuweisen und
2. die Übermittlung personen- und ausweisbezogener Daten aus dem Personalausweis anzufragen.

(5) Ein dienste- und kartenspezifisches Kennzeichen ist eine Zeichenfolge, die im Speicher- und Verarbeitungsmedium des Personalausweises oder eines mobilen Endgeräts berechnet wird. Es dient der eindeutigen elektronischen Wiedererkennung eines elektronischen Identitätsnachweises mit dem Personalausweis oder mit einem mobilen Endgerät durch den Diensteanbieter, für den es errechnet wurde, ohne dass weitere personenbezogene Daten übermittelt werden müssen.

(6) Das Sperrkennwort ist eine Zeichenfolge, die ausschließlich der Sperrung eines elektronischen Identitätsnachweises dient.

(6a) Die Sperrsumme ist ein eindeutiges Merkmal, das aus dem Sperrkennwort, dem Familiennamen, den Vornamen und dem Tag der Geburt eines Ausweisinhabers errechnet wird. Es dient der Übermittlung einer Sperrung vom Sperrnotruf oder einer Personalausweisbehörde an den Sperrlistenbetreiber. Mithilfe der Sperrsumme ermittelt der Sperrlistenbetreiber anhand der Referenzliste den Sperrschlüssel eines zu sperrenden elektronischen Identitätsnachweises.

(7) Sperrmerkmale eines elektronischen Identitätsnachweises mit dem Personalausweis oder mit einem mobilen Endgerät sind dienste- und kartenspezifische Zeichenfolgen, die ausschließlich der Erkennung abhandengekommener Personalausweise oder mobiler Endgeräte durch den Diensteanbieter dienen, für den sie errechnet wurden.

(8) Jeder Ausweis erhält eine neue Seriennummer. Die Seriennummer eines Personalausweises setzt sich aus einer vierstelligen Behördenkennzahl und einer fünfstelligen, zufällig vergebenen Nummer zusammen und kann Ziffern und Buchstaben enthalten. Die Seriennummer des vorläufigen Personalausweises und des Ersatz-Personalausweises besteht aus einem Buchstaben und sieben Ziffern.

(9) Die Prüfziffern werden aus den Daten des maschinenlesbaren Bereichs errechnet und dienen zur Feststellung seiner Unversehrtheit.

(10) Die Geheimnummer besteht aus einer sechsstelligen Ziffernfolge und dient der Freigabe der Datenübermittlung aus dem Personalausweis oder aus einem mobilen Endgerät im Rahmen des elektronischen Identitätsnachweises.

(11) Die Zugangsnummer ist eine zufällig erzeugte, ausschließlich auf der Karte sichtbar aufgebrachte sechsstellige Ziffernfolge, die zur Absicherung gegen unberechtigten Zugriff auf die Kommunikation zwischen Personalausweis und Lesegeräten dient.

(12) Die Entsperrnummer ist eine zufällig erzeugte Ziffernfolge, die die Freischaltung der Geheimnummer ermöglicht, wenn diese nach dreimaliger Fehleingabe gesperrt worden ist.

(13) Im Sinne dieses Gesetzes ist ein mobiles Endgerät ein solches Gerät, das dem Stand der Technik entspricht, um einen elektronischen Identitätsnachweis nach § 18 Absatz 2 Satz 1 Nummer 2 durchführen zu können.

§ 3 Vorläufiger Personalausweis

(1) Macht die antragstellende Person glaubhaft, dass sie sofort einen Ausweis benötigt, ist ihr ein vorläufiger Personalausweis auszustellen.

(2) Hierfür sind ausschließlich die in § 7 Abs. 1 genannten Behörden zuständig.

§ 4 Eigentum am Ausweis; Ausweishersteller; Vergabestelle für Berechtigungszertifikate

(1) Niemand darf mehr als einen auf seine Person ausgestellten gültigen Ausweis der Bundesrepublik Deutschland besitzen.

(2) Ausweise sind Eigentum der Bundesrepublik Deutschland.

(3) Das Bundesministerium des Innern und für Heimat bestimmt

1. den Ausweishersteller,
2. den Lieferanten von Geräten zur Aufnahme und elektronischen Erfassung von Lichtbildern, sofern diese durch die Personalausweisbehörde gefertigt werden, und von Fingerabdrücken,
3. die Vergabestelle für Berechtigungszertifikate sowie
4. den Sperrlistenbetreiber

und macht deren Namen jeweils im Bundesanzeiger bekannt. Dies gilt nicht für Geräte zur Aufnahme und elektronischen Erfassung von Lichtbildern nach Satz 1 Nummer 2, die im Rahmen einer Antragstellung beim Auswärtigen Amt gefertigt werden.

§ 5 Ausweismuster; gespeicherte Daten

(1) Ausweise sind nach einheitlichen Mustern auszustellen.

(2) Der Personalausweis enthält neben der Angabe der ausstellenden Behörde, dem Tag der Ausstellung, dem letzten Tag der Gültigkeitsdauer, der Zugangsnummer und den in Absatz 4 Satz 2 genannten Daten ausschließlich folgende sichtbar aufgebrachte Angaben über den Ausweisinhaber:

1. Familienname und Geburtsname,
2. Vornamen,

3. Doktorgrad,
4. Tag und Ort der Geburt,
5. Lichtbild,
6. Unterschrift,
7. Größe,
8. Farbe der Augen,
9. Anschrift; hat der Ausweisinhaber keine Wohnung in Deutschland, kann die Angabe „keine Wohnung in Deutschland“ eingetragen werden,
10. Staatsangehörigkeit,
11. Seriennummer und
12. Ordensname, Künstlername.

(3) Der vorläufige Personalausweis enthält die in Absatz 2 Nr. 1 bis 12 und die in Absatz 4 Satz 2 genannten Angaben sowie die Angabe der ausstellenden Behörde, den Tag der Ausstellung und den letzten Tag der Gültigkeitsdauer.

(3a) Der Ersatz-Personalausweis enthält die in Absatz 2 Nummer 1 bis 12 und die in Absatz 4 Satz 2 genannten Angaben sowie die Angabe der ausstellenden Behörde, den Tag der Ausstellung, den letzten Tag der Gültigkeitsdauer und den Vermerk, dass der Ersatz-Personalausweis nicht zum Verlassen Deutschlands berechtigt. Abweichend von Absatz 2 Nummer 9 ist die Eintragung „keine Wohnung in Deutschland“ nicht zulässig.

(4) Ausweise haben einen Bereich für das automatisierte Auslesen. Dieser darf ausschließlich die folgenden sichtbar aufgedruckten Angaben enthalten:

1. Abkürzungen
   a) „IDD“ für Personalausweis der Bundesrepublik Deutschland,
   b) „ITD“ für vorläufigen Personalausweis der Bundesrepublik Deutschland oder
   c) „IXD“ für Ersatz-Personalausweis der Bundesrepublik Deutschland,
2. Familienname,
3. Vornamen,
4. Seriennummer,
5. Abkürzung „D“ für deutsche Staatsangehörigkeit,
6. Tag der Geburt,
7. letzter Tag der Gültigkeitsdauer,

7a. Versionsnummer des Ausweismusters,

8. Prüfziffern und
9. Leerstellen.

Bei einer Identitätsüberprüfung nach § 16 darf auch die aufgedruckte Zugangsnummer automatisiert gelesen werden.

(5) Der Personalausweis enthält ein elektronisches Speicher- und Verarbeitungsmedium, auf dem folgende Daten gespeichert werden:

1. die Daten nach Absatz 2 Nummer 1 bis 5, 9, 10 und 12,
1a. der im amtlichen Gemeindeverzeichnis verwendete eindeutige Gemeindeschlüssel,
2. die Daten des maschinenlesbaren Bereichs nach Absatz 4 Satz 2 und
3. die Fingerabdrücke nach Absatz 9, die Bezeichnung der erfassten Finger, die Angaben zur Qualität der Abdrücke.

(5a) Zur Einrichtung eines elektronischen Identitätsnachweises nach § 10a Absatz 1 Satz 1 dürfen auf einem elektronischen Speicher- und Verarbeitungsmedium in einem mobilen Endgerät folgende Daten gespeichert werden:

1. die Daten nach Absatz 2 Nummer 1 bis 4, 9, 10 und 12,
2. die Dokumentenart,
3. der letzte Tag der Gültigkeitsdauer des elektronischen Identitätsnachweises,
4. die Abkürzung „D“ für Bundesrepublik Deutschland und
5. der im amtlichen Gemeindeverzeichnis verwendete eindeutige Gemeindeschlüssel.

(6) Die gespeicherten Daten sind gegen unbefugtes Verändern, Löschen und Auslesen zu sichern.

(7) Abweichend von Absatz 5 erhalten Kinder, solange sie noch nicht sechs Jahre alt sind, einen Personalausweis mit einem elektronischen Speicher- und Verarbeitungsmedium, auf dem nur das Lichtbild und die Daten des maschinenlesbaren Bereichs nach Absatz 4 Satz 2 gespeichert sind.

(8) Die Seriennummer, die Prüfziffern, das Sperrkennwort und Sperrmerkmale dürfen keine Daten über die Person des Ausweisinhabers oder Hinweise auf solche Daten enthalten.

(9) Die auf Grund der Verordnung (EU) 2019/1157 des Europäischen Parlaments und des Rates vom 20. Juni 2019 zur Erhöhung der Sicherheit der Personalausweise von Unionsbürgern und der Aufenthaltsdokumente, die Unionsbürgern und deren Familienangehörigen ausgestellt werden, die ihr Recht auf Freizügigkeit ausüben (ABl. L 188 vom 12.7.2019, S. 67), auf dem elektronischen Speichermedium zu speichernden zwei Fingerabdrücke der antragstellenden Person werden in Form des flachen Abdrucks des linken und rechten Zeigefingers im elektronischen Speicher- und Verarbeitungsmedium des Personalausweises gespeichert. Bei Fehlen eines Zeigefingers, ungenügender Qualität des Fingerabdrucks oder Verletzungen der Fingerkuppe wird ersatzweise der flache Abdruck entweder des Daumens, des Mittelfingers oder des Ringfingers gespeichert. Fingerabdrücke sind nicht zu speichern, wenn die Abnahme der Fingerabdrücke aus medizinischen Gründen, die nicht nur vorübergehender Art sind, unmöglich ist.

(10) Die im elektronischen Speicher- und Verarbeitungsmedium des Personalausweises oder eines mobilen Endgeräts gespeicherten Daten ermöglichen auch die Funktion des elektronischen Identitätsnachweises nach § 18.

§ 6 Gültigkeitsdauer des Ausweises; vorzeitige Beantragung; räumliche Beschränkungen

(1) Personalausweise werden für eine Gültigkeitsdauer von zehn Jahren ausgestellt.

(2) Vor Ablauf der Gültigkeit eines Personalausweises kann ein neuer Personalausweis beantragt werden, wenn ein berechtigtes Interesse an der Neuausstellung dargelegt wird.

(3) Bei Personen, die noch nicht 24 Jahre alt sind, beträgt die Gültigkeitsdauer des Personalausweises sechs Jahre.

(4) Die Gültigkeitsdauer eines vorläufigen Personalausweises ist unter Berücksichtigung des Nutzungszwecks festzulegen; sie darf einen Zeitraum von drei Monaten nicht überschreiten.

(4a) Die Gültigkeitsdauer des Ersatz-Personalausweises ist auf den Zeitraum zu beschränken, der für das Erreichen des Zweckes nach § 6a erforderlich ist; sie darf einen Zeitraum von drei Jahren nicht überschreiten.

(5) Eine Verlängerung der Gültigkeitsdauer ist nicht zulässig.

(6) (weggefallen)

(7) Unter den Voraussetzungen des § 7 Abs. 1 des Passgesetzes kann die zuständige Behörde im Einzelfall anordnen, dass der Ausweis nicht zum Verlassen Deutschlands berechtigt.

(8) Anordnungen nach Absatz 7 dürfen im polizeilichen Grenzfahndungsbestand gespeichert werden.

§ 6a Versagung und Entziehung; Ersatz-Personalausweis

(1) Ein Personalausweis oder ein vorläufiger Personalausweis kann unter den Voraussetzungen des § 7 Absatz 1 Nummer 1 oder Nummer 10 des Passgesetzes versagt werden. Im Falle des § 7 Absatz 1 Nummer 1 des Passgesetzes gilt dies nur, wenn die Gefährdung darin besteht, dass bestimmte Tatsachen die Annahme begründen, dass der Ausweisbewerber

1. einer terroristischen Vereinigung nach § 129a des Strafgesetzbuchs oder einer terroristischen Vereinigung nach § 129a in Verbindung mit § 129b Absatz 1 Satz 1 des Strafgesetzbuchs mit Bezug zur Bundesrepublik Deutschland angehört oder diese unterstützt oder
2. rechtswidrig Gewalt gegen Leib oder Leben als Mittel zur Durchsetzung international ausgerichteter politischer oder religiöser Belange anwendet oder eine solche Gewaltanwendung unterstützt oder vorsätzlich hervorruft.

(2) Dem Ausweisinhaber kann ein Personalausweis oder ein vorläufiger Personalausweis entzogen werden, wenn gegen ihn eine vollziehbare Anordnung nach § 6 Absatz 7 in Verbindung mit § 7 Absatz 1 Nummer 1 oder Nummer 10 des Passgesetzes besteht. Im Falle einer Anordnung nach § 6 Absatz 7 in Verbindung mit § 7 Absatz 1 Nummer 1 des Passgesetzes gilt dies nur, wenn die Gefährdung darin besteht, dass bestimmte Tatsachen die Annahme begründen, dass der Ausweisinhaber

1. einer terroristischen Vereinigung nach § 129a des Strafgesetzbuchs oder einer terroristischen Vereinigung nach § 129a in Verbindung mit § 129b Absatz 1 Satz 1 des Strafgesetzbuchs mit Bezug zur Bundesrepublik Deutschland angehört oder diese unterstützt oder

2. rechtswidrig Gewalt gegen Leib oder Leben als Mittel zur Durchsetzung international ausgerichteter politischer oder religiöser Belange anwendet oder eine solche Gewaltanwendung unterstützt oder vorsätzlich hervorruft.

(3) Ist ein Personalausweis oder vorläufiger Personalausweis versagt oder entzogen worden, ist ein Ersatz-Personalausweis auszustellen.

(4) Liegen die Voraussetzungen des Absatzes 1 oder des Absatzes 2 nicht mehr vor, ist dies dem Inhaber eines Ersatz-Personalausweises unverzüglich mitzuteilen und ihm auf Antrag ein Personalausweis oder ein vorläufiger Personalausweis auszustellen.

(5) Für Maßnahmen nach den Absätzen 1 bis 3 sowie Mitteilungen nach Absatz 4 sind ausschließlich die in § 7 Absatz 1 genannten Behörden zuständig.

§ 7 Sachliche Zuständigkeit

(1) Für Ausweisangelegenheiten in Deutschland sind die von den Ländern bestimmten Behörden zuständig (Personalausweisbehörden).

(2) Für Personalausweisangelegenheiten im Ausland ist das Auswärtige Amt mit den von ihm bestimmten Auslandsvertretungen zuständig (Personalausweisbehörde).

(3) Für die Einziehung nach § 29 Abs. 1 und die Sicherstellung nach § 29 Abs. 2 sind die Personalausweisbehörden, die Auslandsvertretungen und die zur hoheitlichen Identitätsfeststellung berechtigten Behörden zuständig.

(3a) Für das elektronisch beantragte Neusetzen der Geheimnummer sowie für die elektronische Beantragung des nachträglichen Einschaltens der Funktion zum elektronischen Identitätsnachweis ist der Ausweishersteller zuständig.

(3b) Für die Übermittlung von Daten nach § 5 Absatz 5a aus dem elektronischen Speicher- und Verarbeitungsmedium des Personalausweises auf ein elektronisches Speicher- und Verarbeitungsmedium in einem mobilen Endgerät nach § 10a Absatz 1 sowie für die Auskunft nach § 10a Absatz 5 ist der Ausweishersteller zuständig.

(4) Für die Erteilung und Aufhebung von Berechtigungen nach § 21 ist die Vergabestelle für Berechtigungszertifikate nach § 4 Abs. 3 zuständig. Für das Führen einer Sperrliste nach § 10 Abs. 4 Satz 1 ist der Sperrlistenbetreiber nach § 4 Abs. 3 zuständig.

(5) Für Diensteanbieter in Deutschland sind die für die Einhaltung der Vorgaben des Datenschutzes zuständigen Stellen zuständig. Haben Diensteanbieter ihren Wohn-, Geschäfts- oder Dienstsitz nicht in Deutschland, so ist der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit zuständige Datenschutzaufsichtsbehörde im Sinne des § 21 Absatz 4 Satz 3.

§ 7a Beleihung

(1) Das Bundesministerium des Innern und für Heimat kann teilrechtsfähigen Vereinigungen sowie juristischen Personen des Privatrechts zur Wahrnehmung der Aufgabe des elektronisch beantragten Neusetzens der Geheimnummer nach § 20 Absatz 2 der Personalausweisverordnung Hoheitsbefugnisse übertragen (Beleihung). Der Beliehene tritt insoweit an die Stelle des Ausweisherstellers; er ist Träger der öffentlichen Verwaltung.

(2) Die Beleihung ist nur zulässig, wenn

1. der zu Beleihende den Stand der Technik für die zu übertragende Aufgabe einhält,
2. die ordnungsgemäße Erfüllung der zu übertragenden Aufgabe durch den zu Beleihenden sichergestellt wird,
3. die Erfüllung der zu übertragenden Aufgabe durch den zu Beleihenden voraussichtlich Wirtschaftlichkeitsvorteile gegenüber einer staatlichen Aufgabenwahrnehmung aufweisen wird und
4. keine überwiegenden öffentlichen Interessen entgegenstehen.

Die Beleihung ist im Bundesanzeiger bekannt zu machen. Das Vorliegen der Voraussetzungen nach Satz 1 ist in regelmäßigen Abständen zu prüfen.

(3) Die Beleihung kann jederzeit ganz oder teilweise zurückgenommen, widerrufen oder mit Nebenbestimmungen verbunden werden; der Zeitpunkt der Maßnahme hat die Interessen des Beliehenen angemessen zu berücksichtigen. Liegen die Voraussetzungen nach Absatz 2 Satz 1 nicht mehr vor, so ist die Beleihung zu widerrufen. Soweit die Beleihung zurückgenommen oder widerrufen wurde, ist dies im Bundesanzeiger bekannt zu machen.

(4) Der Beliehene untersteht im Umfang der ihm übertragenen Aufgabe der Rechts- und Fachaufsicht des Bundesministeriums des Innern und für Heimat.

(5) Im Umfang der übertragenen Aufgabe findet § 31 Absatz 1 auf den Beliehenen entsprechend Anwendung.

(6) Wird der Bund von einem Dritten wegen eines Schadens in Anspruch genommen, den der Beliehene in Ausübung des ihm anvertrauten Amtes dem Dritten durch eine Amtspflichtverletzung zugefügt hat, so kann der Bund bei Vorsatz oder grober Fahrlässigkeit beim Beliehenen Rückgriff nehmen.

§ 8 Örtliche Zuständigkeit; Tätigwerden bei örtlicher Unzuständigkeit

(1) In Deutschland ist die Personalausweisbehörde zuständig, in deren Bezirk die antragstellende Person oder der Ausweisinhaber für seine Wohnung, bei mehreren Wohnungen für seine Hauptwohnung, meldepflichtig ist. Hat die antragstellende Person keine Wohnung, so ist die Personalausweisbehörde zuständig, in deren Bezirk sie sich vorübergehend aufhält.

(1a) Für das Führen des Personalausweisregisters nach § 23 ist die Personalausweisbehörde zuständig, welche den Ausweis ausgestellt hat.

(2) Im Ausland sind die vom Auswärtigen Amt bestimmten Auslandsvertretungen zuständig, in deren Bezirk sich die antragstellende Person oder der Ausweisinhaber gewöhnlich aufhält. Der Ausweisinhaber hat den Nachweis über den gewöhnlichen Aufenthaltsort zu erbringen.

(3) Für Binnenschiffer, die keine Wohnung in Deutschland haben, ist die Personalausweisbehörde am Heimatort des Binnenschiffes, für Seeleute, die keine Wohnung in Deutschland haben, die Personalausweisbehörde am Sitz des Reeders zuständig.

(4) Der Antrag auf Ausstellung eines Ausweises muss auch von einer örtlich nicht zuständigen Personalausweisbehörde bearbeitet werden, wenn ein wichtiger Grund dargelegt wird. Ein Ausweis darf nur mit Ermächtigung der örtlich zuständigen Personalausweisbehörde ausgestellt werden.

Abschnitt 2
Ausstellung und Sperrung des Ausweises; elektronischer Identitätsnachweis

§ 9 Ausstellung des Ausweises

(1) Personalausweise und vorläufige Personalausweise werden auf Antrag für Deutsche im Sinne des Artikels 116 Abs. 1 des Grundgesetzes ausgestellt. § 3a Abs. 1 des Verwaltungsverfahrensgesetzes ist nicht anzuwenden. Im Antragsverfahren nachzureichende Erklärungen können mittels Datenübertragung abgegeben werden. Die antragstellende Person und ihr gesetzlicher Vertreter können sich bei der Stellung des Antrags nicht durch einen Bevollmächtigten vertreten lassen. Dies gilt nicht für eine handlungs- oder einwilligungsunfähige antragstellende Person, wenn eine für diesen Fall erteilte, öffentlich beglaubigte oder beurkundete Vollmacht vorliegt. Die antragstellende Person und ihr gesetzlicher oder bevollmächtigter Vertreter sollen persönlich erscheinen.

(2) Für Minderjährige, die noch nicht 16 Jahre alt sind, und für Personen, die geschäftsunfähig sind und sich nicht nach Absatz 1 Satz 5 durch einen Bevollmächtigten vertreten lassen, kann nur diejenige Person den Antrag stellen, die sorgeberechtigt ist oder als Betreuer ihren Aufenthalt bestimmen darf. Sie ist verpflichtet, für Jugendliche, die 16, aber noch nicht 18 Jahre alt sind, innerhalb von sechs Wochen, nachdem der Jugendliche 16 Jahre alt geworden ist, den Antrag auf Ausstellung eines Ausweises zu stellen, falls dies der Jugendliche unterlässt. Jugendliche, die mindestens 16 Jahre alt sind, dürfen Verfahrenshandlungen nach diesem Gesetz vornehmen.

(3) In dem Antrag sind alle Tatsachen anzugeben, die zur Feststellung der Person des Antragstellers und seiner Eigenschaft als Deutscher notwendig sind. Die Angaben zum Doktorgrad und zu den Ordens- und Künstlernamen sind freiwillig. Die antragstellende Person hat die erforderlichen Nachweise zu erbringen. Fingerabdrücke von Kindern sind nicht abzunehmen, solange die Kinder noch nicht sechs Jahre alt sind.

(4) Bestehen Zweifel über die Person des Antragstellers, sind die zur Feststellung seiner Identität erforderlichen Maßnahmen zu treffen. Die Personalausweisbehörde kann die Durchführung erkennungsdienstlicher Maßnahmen veranlassen, wenn die Identität der antragstellenden Person auf andere Weise nicht oder nur unter erheblichen Schwierigkeiten festgestellt werden kann. Ist die Identität festgestellt, so sind die im Zusammenhang mit der Feststellung angefallenen Unterlagen zu vernichten. Die Vernichtung ist zu protokollieren.

(5) Die Unterschrift durch ein Kind ist zu leisten, wenn es zum Zeitpunkt der Beantragung des Ausweises zehn Jahre oder älter ist.

(6) Für Deutsche im Sinne des Artikels 116 Absatz 1 des Grundgesetzes werden nach Maßgabe des § 6a Ersatz-Personalausweise von Amts wegen ausgestellt. Absatz 1 Satz 2 bis 6, Absatz 2 Satz 3, Absatz 3 Satz 1 bis 3 sowie die Absätze 4 und 5 gelten entsprechend.

§ 10 Einschaltung, Sperrung und Entsperrung der Funktion des elektronischen Identitätsnachweises mit dem Personalausweis

(1) Der Personalausweis wird mit einer Funktion zum elektronischen Identitätsnachweis nach § 18 ausgegeben.

(2) Der Ausweishersteller schaltet die Funktion aus, wenn die antragstellende Person zum Zeitpunkt der Antragstellung noch nicht 16 Jahre alt ist.

(3) Auf Antrag des Ausweisinhabers und unter Vorlage des Personalausweises kann ein ausgeschalteter elektronischer Identitätsnachweis während der Gültigkeitsdauer des Personalausweises eingeschaltet werden, wenn der Ausweisinhaber zum Zeitpunkt der Antragstellung bereits 16 Jahre alt ist.

(3a) Das Bundesministerium des Innern und für Heimat soll nach Prüfung durch das Bundesamt für Sicherheit in der Informationstechnik für Fälle, in denen der Nachweis der Identität durch einen elektronischen Identitätsnachweis nach § 18 dieses Gesetzes, nach § 12 des eID-Karte-Gesetzes oder nach § 78 Absatz 5 des Aufenthaltsgesetzes erbracht wurde, für die spätere Authentisierung des Inhabers des elektronischen Identitätsnachweises auch andere Authentisierungsmittel befristet zulassen. Das Bundesministerium des Innern und für Heimat gibt die Zulassung und die Dauer der Befristung im Bundesanzeiger bekannt.

(4) Der Sperrlistenbetreiber nach § 7 Abs. 4 Satz 2 stellt jedem Diensteanbieter über jederzeit öffentlich erreichbare Kommunikationsverbindungen eine für ihn errechnete, aktuelle Liste bereit, die ausschließlich die Sperrmerkmale von Personalausweisen mit gesperrtem elektronischen Identitätsnachweis enthält (Sperrliste). Die Diensteanbieter rufen die für sie errechnete Sperrliste regelmäßig ab und gleichen sie im Rahmen des elektronischen Identitätsnachweises lokal mit zu akzeptierenden Personalausweisen ab.

(5) Die zuständige Personalausweisbehörde hat unverzüglich zur Aktualisierung der Sperrliste die Sperrsumme des Personalausweises an den Sperrlistenbetreiber nach § 7 Absatz 4 Satz 2 zu übermitteln, wenn sie Kenntnis erlangt von

1. dem Abhandenkommen eines Personalausweises mit elektronischem Identitätsnachweis,
2. dem Versterben eines Ausweisinhabers oder
3. der Ungültigkeit eines nicht im Besitz der Behörde befindlichen Ausweises nach § 28 Absatz 1 oder Absatz 2.

(6) Der Personalausweisinhaber kann durch Mitteilung des Sperrkennworts an den Sperrlistenbetreiber nach § 7 Abs. 4 Satz 2 eine sofortige Sperrung des elektronischen Identitätsnachweises veranlassen. Davon unberührt bleibt die Pflicht, den Verlust oder das Abhandenkommen des Personalausweises der Personalausweisbehörde nach § 27 Abs. 1 Nr. 3 anzuzeigen.

(7) Der Sperrlistenbetreiber nach § 7 Abs. 4 Satz 2 stellt den Personalausweisbehörden für die Fälle nach Absatz 5 und den Personalausweisinhabern für die Fälle nach Absatz 6 einen Sperrdienst über jederzeit öffentlich erreichbare Kommunikationsverbindungen zur Verfügung.

(8) Teilt nach erfolgter Sperrung nach Absatz 5 der Personalausweisinhaber das Wiederauffinden seines Personalausweises unter den Voraussetzungen des § 9 Absatz 1 Satz 6 und unter Vorlage seines Personalausweises mit oder bittet er nach einer Sperrung nach Absatz 6 unter den Voraussetzungen des § 9 Absatz 1 Satz 6 und unter Vorlage seines Personalausweises um Entsperrung, so ersucht die Personalausweisbehörde den Sperrlistenbetreiber nach § 7 Absatz 4 Satz 2 um Löschung des Sperreintrags zu diesem Personalausweis. Die Pflicht des Personalausweisinhabers, den Ausweis bei Wiederauffinden nach § 27 Abs. 1 Nr. 3 vorzulegen, bleibt hiervon unberührt.

(9) Der Zeitpunkt der Meldung des Abhandenkommens eines Ausweises ist von der Personalausweisbehörde oder Polizeibehörde zu dokumentieren und der ausstellenden Personalausweisbehörde mitzuteilen.

§ 10a Einrichtung des elektronischen Identitätsnachweises mit einem mobilen Endgerät

(1) Auf elektronische Veranlassung durch den Ausweisinhaber übermittelt der Ausweishersteller die Daten nach § 5 Absatz 5a aus dem elektronischen Speicher- und Verarbeitungsmedium des Personalausweises in einem sicheren Verfahren auf ein elektronisches Speicher- und Verarbeitungsmedium in einem mobilen Endgerät. Der Ausweisinhaber weist seine Identität gegenüber dem Ausweishersteller mit einem elektronischen Identitätsnachweis nach § 18 nach. Ferner hat der Ausweishersteller Maßnahmen gegen eine missbräuchliche Verwendung der Daten im Anschluss an die Übermittlung der Daten auf das elektronische Speicher- und Verarbeitungsmedium in dem mobilen Endgerät vorzusehen. Der Ausweisinhaber ist auf seine Pflichten nach § 27 Absatz 2 sowie darauf hinzuweisen, dass das mobile Endgerät hinsichtlich der in seinem elektronischen Speicher- und Verarbeitungsmedium nach Absatz 1 gespeicherten Daten mit besonderer Sorgfalt zu behandeln ist.

(2) Die Gültigkeitsdauer eines elektronischen Identitätsnachweises nach § 18 Absatz 2 Satz 1 Nummer 2 auf Grundlage einer Übermittlung der Daten nach Absatz 1 beträgt fünf Jahre. Eine Verlängerung der Gültigkeitsdauer ist nicht zulässig. Durch Rechtsverordnung nach § 34 Satz 1 Nummer 8a kann eine kürzere Gültigkeitsdauer festgelegt werden. Eine Übermittlung nach Absatz 1 Satz 1 kann mehrfach durchgeführt werden.

(3) Im Zuge der Übermittlung nach Absatz 1 Satz 1 erzeugt der Ausweishersteller einen neuen Sperrschlüssel sowie eine neue Sperrsumme und übermittelt diese Daten sowie den letzten Tag der Gültigkeit an den Sperrlistenbetreiber. § 10 Absatz 4 und Absatz 6 Satz 1 gilt entsprechend. Der Ausweisinhaber kann die Daten auf dem mobilen Endgerät selbst löschen.

(4) Werden die auf das elektronische Speicher- und Verarbeitungsmedium des mobilen Endgeräts übermittelten Daten nach Absatz 1 Satz 1 unrichtig, darf ein elektronischer Identitätsnachweis nach § 18 Absatz 2 Satz 1 Nummer 2 nicht durchgeführt werden. Vor einer weiteren Nutzung ist erneut eine Übermittlung nach Absatz 1 unter Verwendung des elektronischen Speicher- und Verarbeitungsmediums des Personalausweises mit den richtigen Daten durchzuführen.

(5) Auf elektronischen Antrag des Ausweisinhabers hat der Ausweishersteller diesem Auskunft zu erteilen darüber, jeweils zu welchem Datum und zu welcher Uhrzeit eine Übermittlung nach Absatz 1 Satz 1 der Daten des Personalausweises des Ausweisinhabers auf ein elektronisches Speicher- und Verarbeitungsmedium in einem mobilen Endgerät durchgeführt wurde, sowie über jeweils den letzten Tag der Gültigkeitsdauer, das Sperrkennwort und den Hersteller und die Modellbezeichnung des mobilen Endgeräts. Zur Identifizierung der antragstellenden Person hat der Ausweishersteller zur Person des Ausweisinhabers einen elektronischen Identitätsnachweis nach § 18 durchzuführen.

§ 11 Informationspflichten

(1) Auf Verlangen des Personalausweisinhabers hat die Personalausweisbehörde ihm Einsicht in die im elektronischen Speicher- und Verarbeitungsmedium des Personalausweises gespeicherten auslesbaren Daten zu gewähren.

(2) (weggefallen)

(3) Die Personalausweisbehörde hat die antragstellende Person bei Antragstellung über den elektronischen Identitätsnachweis nach § 18, einschließlich des elektronischen Identitätsnachweises mit einem mobilen Endgerät, und das Vor-Ort-Auslesen nach § 18a sowie über Maßnahmen zu unterrichten, die erforderlich sind, um die Sicherheit der Nutzung des elektronischen Identitätsnachweises zu gewährleisten. Sie hat der antragstellenden Person die Übergabe von entsprechendem Informationsmaterial anzubieten, in dem auch auf die Möglichkeit einer Sperrung nach § 10 Absatz 6 hingewiesen wird.

(4) (weggefallen)

(5) Personalausweisbehörden, die Kenntnis von dem Abhandenkommen eines Ausweises erlangen, haben die zuständige Personalausweisbehörde, die ausstellende Personalausweisbehörde und eine Polizeibehörde unverzüglich in Kenntnis zu setzen; eine Polizeibehörde, die anderweitig Kenntnis vom Abhandenkommen eines Ausweises erlangt, hat die zuständige und die ausstellende Personalausweisbehörde unverzüglich zu unterrichten. Dabei sollen Angaben zum Familiennamen, den Vornamen, zur Seriennummer, zur ausstellenden Personalausweisbehörde, zum Ausstellungsdatum und zur Gültigkeitsdauer des Ausweises übermittelt werden. Die Polizeibehörde hat die Einstellung in die polizeiliche Sachfahndung vorzunehmen.

(6) Stellt eine nicht zuständige Personalausweisbehörde nach § 8 Abs. 4 einen Ausweis aus, so hat sie der zuständigen Personalausweisbehörde den Familiennamen, die Vornamen, den Tag und Ort der Geburt, die ausstellende Personalausweisbehörde, das Ausstellungsdatum, die Gültigkeitsdauer und die Seriennummer des Ausweises zu übermitteln.

(7) Schaltet eine Personalausweisbehörde den elektronischen Identitätsnachweis eines Personalausweises ein, so hat sie unverzüglich die ausstellende Personalausweisbehörde davon in Kenntnis zu setzen. Das Gleiche gilt für den Ausweishersteller im Falle der elektronischen Beantragung des nachträglichen Einschaltens der Funktion zum elektronischen Identitätsnachweis.

§ 12 Form und Verfahren der Datenerfassung, -prüfung und -übermittlung

(1) Die Datenübermittlung von den Personalausweisbehörden an den Ausweishersteller zum Zweck der Ausweisherstellung, insbesondere die Übermittlung sämtlicher Ausweisantragsdaten, erfolgt durch Datenübertragung. Die Datenübertragung kann auch über Vermittlungsstellen erfolgen. Die beteiligten Stellen haben dem jeweiligen Stand der Technik entsprechende Maßnahmen zur Sicherstellung von Datenschutz und Datensicherheit zu treffen, die insbesondere die Vertraulichkeit und Unversehrtheit der Daten sowie die Feststellbarkeit der übermittelnden Stelle gewährleisten; im Falle der Nutzung allgemein zugänglicher Netze sind Verschlüsselungsverfahren anzuwenden, die dem jeweiligen Stand der Technik entsprechen.

(2) Zur elektronischen Erfassung, Echtheitsbewertung und Qualitätssicherung des Lichtbildes und der Fingerabdrücke sowie zur Übermittlung der Ausweisdaten von der Personalausweisbehörde an den Ausweishersteller dürfen ausschließlich solche technischen Systeme und Bestandteile eingesetzt werden, die den Anforderungen der Rechtsverordnung nach § 34 Satz 1 Nummer 3 entsprechen. Die Einhaltung der Anforderungen ist vom Bundesamt für Sicherheit in der Informationstechnik gemäß der Rechtsverordnung nach § 34 Satz 1 Nummer 4 festzustellen.

§ 13 (weggefallen)

Abschnitt 3
Umgang mit personenbezogenen Daten

§ 14 Erhebung und Verwendung personenbezogener Daten

Die Erhebung und Verwendung personenbezogener Daten aus dem Ausweis oder mithilfe des Ausweises darf ausschließlich erfolgen durch

1. zur Identitätsfeststellung berechtigte Behörden nach Maßgabe der §§ 15 bis 17,
2. öffentliche Stellen und nichtöffentliche Stellen nach Maßgabe der §§ 18 bis 20.

§ 15 Automatisierter Abruf und automatisierte Speicherung durch zur Identitätsfeststellung berechtigte Behörden

(1) Zur Identitätsfeststellung berechtigte Behörden dürfen den Ausweis nicht zum automatisierten Abruf personenbezogener Daten verwenden. Abweichend von Satz 1 dürfen Polizeibehörden und -dienststellen des Bundes und der Länder, die Behörden der Zollverwaltung sowie die Steuerfahndungsstellen der Länder den Ausweis im Rahmen ihrer Aufgaben und Befugnisse zum automatisierten Abruf personenbezogener Daten verwenden, die zu folgenden Zwecken im polizeilichen Fahndungsbestand gespeichert sind:

1. Grenzkontrolle,
2. Fahndung oder Aufenthaltsfeststellung zum Zweck der Strafverfolgung, Strafvollstreckung oder der Abwehr von Gefahren für die öffentliche Sicherheit oder
3. der zollamtlichen Überwachung im Rahmen der polizeilichen Beobachtung.

Über Abrufe, die zu keiner Feststellung geführt haben, dürfen, vorbehaltlich gesetzlicher Regelungen, die gemäß Absatz 2 erlassen werden, keine personenbezogenen Aufzeichnungen gefertigt werden.

(2) In den Fällen des Absatzes 1 dürfen personenbezogene Daten, soweit gesetzlich nichts anderes bestimmt ist, beim automatisierten Lesen des Ausweises nicht in Dateien gespeichert werden; dies gilt auch für Abrufe aus dem polizeilichen Fahndungsbestand, die zu einer Feststellung geführt haben.

§ 16 Echtheitsprüfung und Identitätsprüfung; Verarbeitung von Personalausweisdaten

(1) Soweit die Polizeivollzugsbehörden, die Zollverwaltung, die Steuerfahndungsstellen der Länder sowie die Personalausweis-, Pass- und Meldebehörden die Echtheit des Personalausweises oder die Identität des Inhabers nach anderen Rechtsvorschriften überprüfen dürfen, sind sie befugt, zum Zweck der Überprüfung der Echtheit des Personalausweises oder der Identität des Ausweisinhabers

1. die auf dem elektronischen Speicher- und Verarbeitungsmedium des Personalausweises gespeicherten biometrischen und sonstigen Daten zu verarbeiten,
2. die benötigten biometrischen Daten beim Personalausweisinhaber zu erheben und
3. die biometrischen Daten miteinander zu vergleichen.

Echtheits- oder Identitätskontrollen über öffentliche Kommunikationswege sind unzulässig.

(2) Die in Absatz 1 Satz 1 genannten Behörden dürfen Daten, die sie im Rahmen einer Identitätsfeststellung aus dem elektronischen Speicher- und Verarbeitungsmedium des Personalausweises verarbeitet haben, mit Ausnahme der biometrischen Daten zur Verarbeitung in einem Datenverarbeitungssystem automatisiert speichern, sofern sie dazu durch ein Gesetz oder auf Grund eines Gesetzes berechtigt sind. Im Übrigen sind die nach Absatz 1 Satz 1 erhobenen Daten unverzüglich nach Beendigung der Prüfung der Echtheit des Personalausweises oder der Identität des Ausweisinhabers zu löschen.

§ 17 Verarbeitung der sichtbaren Daten des Personalausweises

(1) Die in § 16 Absatz 1 Satz 1 genannten Behörden dürfen die auf dem Personalausweis sichtbar aufgedruckten Daten durch nicht automatisierte Verfahren erheben und verwenden, sofern sie dazu durch ein Gesetz oder auf Grund eines Gesetzes berechtigt sind.

(2) Können die Daten aus dem elektronischen Speicher- und Verarbeitungsmedium des Personalausweises nach § 16 Absatz 1 Satz 1 nicht ausgelesen werden, dürfen die dort genannten Behörden die Daten der maschinenlesbaren Zone nach § 5 Absatz 2 Satz 2 automatisiert auslesen und unter den Voraussetzungen des § 16 Absatz 2 speichern. § 16 Absatz 1 Satz 2, Absatz 2 Satz 2 gilt entsprechend.

§ 18 Elektronischer Identitätsnachweis

(1) Der Personalausweisinhaber, der mindestens 16 Jahre alt ist, kann den elektronischen Identitätsnachweis dazu verwenden, seine Identität gegenüber öffentlichen und nichtöffentlichen Stellen elektronisch nachzuweisen. Dies gilt auch dann, wenn er für eine andere Person, ein Unternehmen oder eine Behörde handelt. Abweichend von Satz 1 ist der elektronische Identitätsnachweis ausgeschlossen, wenn die Voraussetzungen des § 3a Abs. 1 des Verwaltungsverfahrensgesetzes, des § 87a Abs. 1 Satz 1 der Abgabenordnung oder des § 36a Abs. 1 des Ersten Buches Sozialgesetzbuch nicht vorliegen.

(2) Der elektronische Identitätsnachweis erfolgt durch Übermittlung von Daten

1. aus dem elektronischen Speicher- und Verarbeitungsmedium des Personalausweises oder
2. aus einem elektronischen Speicher- und Verarbeitungsmedium in einem mobilen Endgerät.

Dabei sind dem jeweiligen Stand der Technik entsprechende Maßnahmen zur Sicherstellung von Datenschutz und Datensicherheit zu treffen, die insbesondere die Vertraulichkeit und Unversehrtheit der Daten gewährleisten. Im Falle der Nutzung allgemein zugänglicher Netze sind Verschlüsselungsverfahren anzuwenden. Die Nutzung des elektronischen Identitätsnachweises durch eine andere Person als den Personalausweisinhaber ist unzulässig.

(3) Das Sperrmerkmal und die Angabe, ob der elektronische Identitätsnachweis gültig ist, sind zur Überprüfung, ob ein gesperrter oder abgelaufener elektronischer Identitätsnachweis vorliegt, immer zu übermitteln. Folgende weitere Daten können übermittelt werden:

1. Familienname,

1a. Geburtsname,

2. Vornamen,

3. Doktorgrad,
4. Tag der Geburt,
5. Ort der Geburt,
6. Anschrift,
6a. im amtlichen Gemeindeverzeichnis verwendeter eindeutiger Gemeindeschlüssel,
6b. Abkürzung für die Staatsangehörigkeit,
7. Dokumentenart,
7a. letzter Tag der Gültigkeitsdauer,
8. dienste- und kartenspezifisches Kennzeichen,
9. Abkürzung „D“ für Bundesrepublik Deutschland,
10. Angabe, ob ein bestimmtes Alter über- oder unterschritten wird,
11. Angabe, ob ein Wohnort dem abgefragten Wohnort entspricht, und
12. Ordensname, Künstlername.

(4) Die Daten werden nur übermittelt, wenn der Diensteanbieter ein gültiges Berechtigungszertifikat an den Inhaber des elektronischen Identitätsnachweises übermittelt und dieser in der Folge seine Geheimnummer eingibt. Der Diensteanbieter muss dem Inhaber des elektronischen Identitätsnachweises vor dessen Eingabe der Geheimnummer die Gelegenheit bieten, die folgenden Daten einzusehen:

1. Name, Anschrift und E-Mail-Adresse des Diensteanbieters,
2. Kategorien der zu übermittelnden Daten nach Absatz 3 Satz 2,
3. (weggefallen)
4. Hinweis auf die für den Diensteanbieter zuständigen Stellen, die die Einhaltung der Vorschriften zum Datenschutz kontrollieren,
5. letzter Tag der Gültigkeitsdauer des Berechtigungszertifikats.

(5) Die Übermittlung ist auf die im Berechtigungszertifikat genannten Datenkategorien beschränkt.

(6) Personalausweisbehörden dürfen im Rahmen der Änderung der Anschrift auf dem elektronischen Speicher- und Verarbeitungsmedium nach einer elektronischen Anmeldung gemäß § 23a des Bundesmeldegesetzes einen elektronischen Identitätsnachweis durchführen und hierzu ein hoheitliches Berechtigungszertifikat verwenden.

§ 18a Vor-Ort-Auslesen von Ausweisdaten unter Anwesenden

(1) Der Ausweisinhaber kann seinen Personalausweis ferner dazu verwenden, die in § 18 Absatz 3 Satz 2 genannten Daten zum Zwecke der medienbruchfreien Übernahme von Formulardaten unter Anwesenden zu übermitteln.

(2) Vor dem Vor-Ort-Auslesen der Daten ist der Vor-Ort-Diensteanbieter verpflichtet, anhand des Personalausweises per Lichtbildabgleich zu prüfen, ob die den Personalausweis

vorlegende Person der Ausweisinhaber ist. Die Daten werden nur übermittelt, wenn der Vor-Ort-Anbieter mit Einverständnis des Ausweisinhabers die Zugangsnummer ausliest und diese zusammen mit einem gültigen Vor-Ort-Zertifikat an das Speicher- und Verarbeitungsmedium des Personalausweises übermittelt.

§ 19 Speicherung im Rahmen des elektronischen Identitätsnachweises

(1) Die Speicherung eines Sperrmerkmals ist ausschließlich zulässig

1. in der Sperrliste nach § 10 Abs. 4 Satz 1 oder
2. vorübergehend beim Diensteanbieter zur Prüfung, ob der Personalausweis in den Sperrlisten nach § 10 Abs. 4 Satz 1 aufgeführt ist; die Daten sind nach der Prüfung unverzüglich zu löschen. Zur Ermöglichung auch wiederholter Prüfungen, ob der Personalausweis in den Sperrlisten nach § 10 Absatz 4 Satz 1 aufgeführt ist, erfolgt bei einem Diensteanbieter, der eine Identifizierung nach dem Geldwäschegesetz, der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG (ABl. L 257 vom 28.8.2014, S. 73), dem Vertrauensdienstegesetz oder dem Telekommunikationsgesetz durchführt, abweichend hiervon die Löschung eines gespeicherten Sperrmerkmals erst nach Ablauf einer Frist von einer Woche ab dem Speicherbeginn.

(2) Der Ausweishersteller speichert zur Durchführung des Auskunftsanspruchs nach § 10a Absatz 5 Satz 1 zu jeder Übermittlung nach § 10a Absatz 1 Satz 1 das dienste- und kartenspezifische Kennzeichen jeweils für das elektronische Speicher- und Verarbeitungsmedium des Personalausweises und des mobilen Endgeräts sowie das Datum und die Uhrzeit der Einrichtung, den letzten Tag der Gültigkeitsdauer, die Sperrsumme, das Sperrkennwort und den Hersteller und die Modellbezeichnung des mobilen Endgeräts. Die in Satz 1 genannten Daten sind spätestens einen Monat nach Ablauf der Gültigkeitsdauer des elektronischen Identitätsnachweises mit einem mobilen Endgerät zu löschen. Im Übrigen ist eine Speicherung des Sperrkennworts und der Sperrsumme zum elektronischen Identitätsnachweis mit dem Personalausweis ausschließlich im Personalausweisregister nach § 23 Absatz 3 Nummer 12 und im Melderegister zulässig.

(3) Eine zentrale, alle Sperrkennwörter oder alle Sperrmerkmale umfassende Speicherung ist unzulässig.

(4) Daten, die im Rahmen der Durchführung des elektronischen Identitätsnachweises aus technischen Gründen oder zum Abgleich mit der Sperrliste an den Diensteanbieter übermittelt werden, dürfen nur für den Zeitraum der Übermittlung gespeichert werden. Die Verarbeitung der Daten nach § 18 Abs. 3 Satz 2 bleibt hiervon unberührt.

(5) Die Speicherung der nach § 18 Absatz 3 Satz 2 oder nach § 18a übermittelten Daten ist zulässig zum Zwecke der Anlegung oder Änderung eines elektronischen Benutzerkontos.

(6) Die Übernahme der nach § 18 Absatz 3 Satz 2 oder nach § 18a übermittelten Daten in ein elektronisches Formular und deren Speicherung sind zulässig, soweit und solange die Speicherung zur Wahrnehmung der Geschäftszwecke des Diensteanbieters erforderlich ist. Zulässig ist auch, das Formular mit einem dauerhaften elektronischen Vermerk des Inhalts zu versehen, dass sich der Ausweisinhaber beim Ausfüllen des Formulars nach § 18 oder nach § 18a identifiziert hat.

§ 19a Speicherung durch Identifizierungsdiensteanbieter

(1) Ein Identifizierungsdiensteanbieter darf die personenbezogenen Daten des Ausweisinhabers ausschließlich zum Zwecke der bei ihm in Auftrag gegebenen Identifizierung sowie nach § 19 Absatz 6 zum Ausfüllen eines elektronischen Formulars verwenden, das ihm hierfür von seinem Auftraggeber zur Verfügung gestellt wurde. Das Anbringen eines elektronischen Vermerks nach § 19 Absatz 6 Satz 2 ist zulässig. Gesetzliche Aufzeichnungspflichten bleiben unberührt.

(2) Der Identifizierungsdiensteanbieter hat die personenbezogenen Daten des Ausweisinhabers zu löschen, sobald die Identifizierung abgeschlossen und gegebenenfalls das elektronische Formular sowie die auf Grund gesetzlicher Aufzeichnungspflichten aufgezeichneten Daten an den Auftraggeber übermittelt wurden.

§ 20 Verwendung durch öffentliche und nichtöffentliche Stellen

(1) Der Inhaber kann den Ausweis bei öffentlichen und nichtöffentlichen Stellen als Identitätsnachweis und Legitimationspapier verwenden.

(2) Der Ausweis darf nur vom Ausweisinhaber oder von anderen Personen mit Zustimmung des Ausweisinhabers in der Weise abgelichtet werden, dass die Ablichtung eindeutig und dauerhaft als Kopie erkennbar ist. Andere Personen als der Ausweisinhaber dürfen die Kopie nicht an Dritte weitergeben. Werden durch Ablichtung personenbezogene Daten aus dem Personalausweis erhoben oder verarbeitet, so darf die datenerhebende oder -verarbeitende Stelle dies nur mit Einwilligung des Ausweisinhabers tun. Die Vorschriften des allgemeinen Datenschutzrechts über die Erhebung und Verwendung personenbezogener Daten bleiben unberührt.

(3) Die Seriennummern dürfen nicht mit Hilfe automatisierter Verfahren zum Abruf oder zur Verknüpfung personenbezogener Daten verwendet werden. Abweichend hiervon dürfen die Seriennummern mit Hilfe automatisierter Verfahren zum Abruf verwenden

1. die Personalausweisbehörden zur Erfüllung ihrer Aufgaben,
2. die Polizeibehörden des Bundes und der Länder, der Militärische Abschirmdienst, der Bundesnachrichtendienst, die Verfassungsschutzbehörden des Bundes und der Länder, die Steuerfahndungsdienststellen der Länder, der Zollfahndungsdienst und die Hauptzollämter zur Klärung,
    a) wer Inhaber des Personalausweises ist für den Fall, dass eine ausländische öffentliche Stelle die Seriennummer des Personalausweises übermittelt hat und anhand der übrigen von der ausländischen Stelle übermittelten Daten eine Feststellung des Ausweisinhabers nicht möglich ist,
    b) ob der Personalausweis durch einen Nichtberechtigten genutzt wird oder
    c) ob der Personalausweis für ungültig erklärt oder abhandengekommen ist.

Der Ausweishersteller hat öffentlichen Stellen auf deren Verlangen die ausstellende Behörde mitzuteilen. Nichtöffentliche Stellen dürfen die Seriennummern, die Sperrkennwörter und die Sperrmerkmale nicht so verwenden, dass mit ihrer Hilfe ein automatisierter Abruf personenbezogener Daten oder eine Verknüpfung von Dateien möglich ist. Dies gilt nicht für den Abgleich von Sperrmerkmalen durch Diensteanbieter zum Zweck der Überprüfung, ob ein elektronischer Identitätsnachweis gesperrt ist.

(3a) Öffentliche Stellen dürfen, wenn dies durch ein Gesetz oder auf Grund eines Gesetzes bestimmt ist, mit Zustimmung des Personalausweisinhabers zur Prüfung der Identität des Personalausweisinhabers

1. die auf dem elektronischen Speicher- und Verarbeitungsmedium gespeicherten Daten nach § 5 Absatz 4 Satz 2 und die Daten, die zur Überprüfung der Echtheit des Personalausweises erforderlich sind, sowie das auf dem elektronischen Speicher- und Verarbeitungsmedium gespeicherte Lichtbild auslesen und
2. von den ausgelesenen Daten ausschließlich das Lichtbild, die Daten nach § 5 Absatz 4 Satz 2 Nummer 1 bis 3, 6, 7 sowie die Daten, die zur Überprüfung der Echtheit des Personalausweises erforderlich sind, verwenden.

Anlässlich der Datenverarbeitung nach Satz 1 überprüft die verarbeitende öffentliche Stelle die Echtheit des Personalausweises. Von den nach Satz 1 Nummer 1 ausgelesenen Daten sind die Daten nach Satz 1 Nummer 2 von der verarbeitenden öffentlichen Stelle unverzüglich nach Beendigung der Prüfung der Identität des Inhabers, die übrigen Daten unverzüglich nach dem Auslesen zu löschen, soweit dies nicht durch Gesetz oder auf Grund eines Gesetzes abweichend geregelt ist.

(4) Beförderungsunternehmen dürfen personenbezogene Daten aus der maschinenlesbaren Zone des Personalausweises elektronisch nur auslesen und verarbeiten, soweit sie auf Grund internationaler Abkommen oder Einreisebestimmungen zur Mitwirkung an Kontrolltätigkeiten im internationalen Reiseverkehr und zur Übermittlung personenbezogener Daten verpflichtet sind. Biometrische Daten dürfen nicht ausgelesen werden. Die Daten sind unverzüglich zu löschen, wenn sie für die Erfüllung dieser Pflichten nicht mehr erforderlich sind.

(5) Zum Zwecke des Jugendschutzes und mit Einwilligung des Ausweisinhabers dürfen die in § 5 Absatz 4 Satz 2 Nummer 6 und 7 genannten Daten aus der maschinenlesbaren Zone des Personalausweises erhoben werden, um das Alter des Ausweisinhabers und die Gültigkeit des Ausweises zu überprüfen. Eine Speicherung der Daten ist unzulässig.

Abschnitt 4
Hoheitliche Berechtigungszertifikate; Berechtigungen; elektronische Signaturen

§ 20a Hoheitliche Berechtigungszertifikate

(1) Zur Identitätsfeststellung berechtigte Behörden erhalten hoheitliche Berechtigungszertifikate, die ausschließlich für die hoheitliche Tätigkeit der Identitätsfeststellung zu verwenden sind.

(2) Personalausweisbehörden und der Ausweishersteller erhalten hoheitliche Berechtigungszertifikate. Umfang und Inhalt der in Satz 1 genannten hoheitlichen Berechtigungszertifikate bestimmen sich durch die auf Grund dieses Gesetzes den Personalausweisbehörden und dem Ausweishersteller jeweils zugewiesenen Zuständigkeiten.

(3) Das Bundesamt für Sicherheit in der Informationstechnik erhält hoheitliche Berechtigungszertifikate zur Qualitätssicherung anhand von Testausweisen.

§ 21 Berechtigungen für Diensteanbieter

(1) Um Daten im Wege des elektronischen Identitätsnachweises anzufragen, benötigen Diensteanbieter eine Berechtigung. Die Berechtigung lässt datenschutzrechtliche Vorschriften unberührt. Das Vorliegen einer Berechtigung ist durch die Vergabe von Berechtigungszertifikaten technisch abzusichern.

(2) Die Berechtigung wird auf Antrag erteilt. Die antragstellende Person muss die Daten nach § 18 Absatz 4 Satz 2 Nummer 1, 2 und 4 angeben. Die Berechtigung ist zu erteilen, wenn

1. der Diensteanbieter seine Identität gegenüber der Vergabestelle für Berechtigungszertifikate nachweist,
2. der Diensteanbieter das dem Antrag zu Grunde liegende Interesse an einer Berechtigung, insbesondere zur geplanten organisationsbezogenen Nutzung, darlegt,
3. der Diensteanbieter die Einhaltung des betrieblichen Datenschutzes versichert und
4. der Vergabestelle für Berechtigungszertifikate keine Anhaltspunkte für eine missbräuchliche Verwendung der Daten vorliegen.

(3) Die Berechtigung ist zu befristen. Die Gültigkeitsdauer darf einen Zeitraum von drei Jahren nicht überschreiten. Die Berechtigung darf nur von dem im Berechtigungszertifikat angegebenen Diensteanbieter verwendet werden. Sie wird auf Antrag wiederholt erteilt.

(4) Die Berechtigung ist zurückzunehmen, wenn der Diensteanbieter diese durch Angaben erwirkt hat, die in wesentlicher Beziehung unrichtig oder unvollständig waren. Sie ist zu widerrufen, wenn sie nicht oder nicht im gleichen Umfang hätte erteilt werden dürfen. Die Berechtigung soll zurückgenommen oder widerrufen werden, wenn die für den Diensteanbieter zuständige Datenschutzaufsichtsbehörde die Rücknahme oder den Widerruf verlangt, weil Tatsachen die Annahme rechtfertigen, dass der Diensteanbieter die auf Grund der Nutzung des Berechtigungszertifikates erhaltenen personenbezogenen Daten in unzulässiger Weise verarbeitet oder nutzt.

(5) Mit Bekanntgabe der Rücknahme oder des Widerrufs der Berechtigung darf der Diensteanbieter vorhandene Berechtigungszertifikate nicht mehr verwenden. Dies gilt nicht, solange und soweit die sofortige Vollziehung (§ 30) ausgesetzt worden ist.

(6) Der Diensteanbieter hat Änderungen der Angaben nach § 18 Absatz 4 Satz 2 Nummer 1 und 4 der Vergabestelle für Berechtigungszertifikate unverzüglich mitzuteilen.

(7) Öffentliche Stellen anderer Mitgliedstaaten der Europäischen Union sind berechtigt, Daten im Wege des elektronischen Identitätsnachweises anzufragen.

(8) Die Vergabestelle für Berechtigungszertifikate führt ein Register über die erteilten Berechtigungen.

§ 21a Vor-Ort-Berechtigung für Vor-Ort-Diensteanbieter

Um Ausweisdaten nach § 18a unter Anwesenden vor Ort auslesen zu dürfen, benötigen Vor-Ort-Diensteanbieter eine Vor-Ort-Berechtigung einschließlich eines Vor-Ort-Zertifikats. § 21 gilt hierfür entsprechend.

§ 21b Berechtigung für Identifizierungsdiensteanbieter

(1) Wer als Identifizierungsdiensteanbieter die Funktion des elektronischen Identitätsnachweises nach § 18 Absatz 2 Satz 1 in Verbindung mit § 19 Absatz 6 nutzen möchte, um Identifizierungsdienstleistungen für Dritte zu erbringen, bedarf einer Berechtigung.

(2) Die Berechtigung ist zu erteilen, wenn der Identifizierungsdiensteanbieter

1. durch technisch-organisatorische Maßnahmen die Einhaltung der in § 19a enthaltenen Vorgaben gewährleistet und
2. die weiteren Anforderungen an Datenschutz und Datensicherheit nach der Rechtsverordnung nach § 34 Satz 1 Nummer 7 erfüllt.

Im Übrigen gilt § 21 entsprechend.

§ 22 Elektronische Signatur

Der Personalausweis kann als qualifizierte elektronische Signaturerstellungseinheit im Sinne des Artikels 3 Nummer 23 der Verordnung (EU) Nr. 910/2014 ausgestaltet werden. Die Zertifizierung nach Artikel 30 der Verordnung (EU) Nr. 910/2014 erfolgt durch das Bundesamt für Sicherheit in der Informationstechnik. Die Vorschriften des Vertrauensdienstegesetzes bleiben unberührt.

Abschnitt 5
Personalausweisregister; Speicherungsvorschriften

§ 23 Personalausweisregister

(1) Die Personalausweisbehörden führen Personalausweisregister.

(2) Das Personalausweisregister dient der Durchführung dieses Gesetzes, insbesondere

1. der Ausstellung der Ausweise und der Feststellung ihrer Echtheit und
2. der Identitätsfeststellung der Person, die den Ausweis besitzt oder für die er ausgestellt ist.

(3) Das Personalausweisregister darf neben dem Lichtbild, der Unterschrift des Ausweisinhabers und verfahrensbedingten Bearbeitungsvermerken ausschließlich folgende Daten enthalten:

1. Familienname und Geburtsname,
2. Vornamen,
3. Doktorgrad,
4. Tag der Geburt,
5. Ort der Geburt,
6. Größe,
7. Farbe der Augen,
8. Anschrift,

9. Staatsangehörigkeit,
10. Familienname, Vornamen, Tag der Geburt und Unterschrift des gesetzlichen Vertreters,
11. Seriennummer,
12. Sperrkennwort und Sperrsumme,
13. letzter Tag der Gültigkeitsdauer,
14. ausstellende Behörde,
14a. die örtlich zuständige Personalausweisbehörde, wenn diese nicht mit der ausstellenden Personalausweisbehörde identisch ist,
15. Vermerke über Anordnungen nach § 6 Absatz 7 und Maßnahmen nach § 6a Absatz 1 bis 3,
16. (weggefallen)
17. E-Mail-Adresse, sofern der Personalausweisinhaber in die Speicherung einwilligt,
18. Ordensname, Künstlername und
19. den Nachweis über eine erteilte Ermächtigung nach § 8 Abs. 4 Satz 2.

(4) Personenbezogene Daten im Personalausweisregister sind mindestens bis zur Ausstellung eines neuen Ausweises, höchstens jedoch bis zu fünf Jahre nach dem Ablauf der Gültigkeit des Ausweises, auf den sie sich beziehen, zu speichern und dann zu löschen. Für die Personalausweisbehörde nach § 7 Abs. 2 bei der Wahrnehmung konsularischer Aufgaben beträgt die Frist 30 Jahre.

(5) Die zuständige Personalausweisbehörde führt den Nachweis über Personalausweise, für die sie eine Ermächtigung nach § 8 Abs. 4 Satz 2 erteilt hat.

(6) Wird eine andere als die ausstellende Personalausweisbehörde örtlich zuständig, darf sie die in Absatz 3 genannten und zur Wahrnehmung ihrer Aufgaben erforderlichen Daten mit Ausnahme der biometrischen Daten speichern. Absatz 4 gilt entsprechend.

§ 24 Verwendung im Personalausweisregister gespeicherter Daten

(1) Die Personalausweisbehörden dürfen personenbezogene Daten nur nach Maßgabe dieses Gesetzes, anderer Gesetze oder Rechtsverordnungen erheben oder verwenden.

(1a) Personalausweisbehörden dürfen anderen Personalausweisbehörden im automatisierten Verfahren Daten des Personalausweisregisters übermitteln oder Daten aus Personalausweisregistern, die in Zuständigkeit anderer Personalausweisbehörden geführt werden, abrufen, sofern dies zur Wahrnehmung ihrer Pflichten erforderlich ist. Dies gilt nicht für biometrische Daten.

(2) Die Personalausweisbehörden dürfen anderen Behörden auf deren Ersuchen Daten aus dem Personalausweisregister übermitteln, wenn

1. die ersuchende Behörde auf Grund von Gesetzen oder Rechtsverordnungen berechtigt ist, solche Daten zu erhalten,

2. die ersuchende Behörde ohne Kenntnis der Daten nicht in der Lage wäre, eine ihr obliegende Aufgabe zu erfüllen, und
3. die ersuchende Behörde die Daten bei dem Betroffenen nicht oder nur mit unverhältnismäßig hohem Aufwand erheben kann oder wenn nach der Art der Aufgabe, zu deren Erfüllung die Daten erforderlich sind, von einer solchen Datenerhebung abgesehen werden muss.

Hinsichtlich der Daten, die auch im Melderegister gespeichert sind, müssen die im Bundesmeldegesetz enthaltenen Beschränkungen beachtet werden.

(3) Die ersuchende Behörde trägt die Verantwortung dafür, dass die Voraussetzungen des Absatzes 2 vorliegen. Ein Ersuchen nach Absatz 2 darf nur von Bediensteten gestellt werden, die vom Behördenleiter dazu besonders ermächtigt sind. Die ersuchende Behörde hat den Anlass des Ersuchens und die Herkunft der übermittelten Daten und Unterlagen zu dokumentieren. Wird die Personalausweisbehörde vom Bundesamt für Verfassungsschutz, den Landesbehörden für Verfassungsschutz, dem Militärischen Abschirmdienst, dem Bundesnachrichtendienst, dem Bundeskriminalamt oder dem Generalbundesanwalt oder der Generalbundesanwältin um die Übermittlung von Daten ersucht, so hat die ersuchende Behörde den Familiennamen, die Vornamen und die Anschrift des Betroffenen unter Hinweis auf den Anlass der Übermittlung aufzuzeichnen. Die Aufzeichnungen sind gesondert aufzubewahren, durch technische und organisatorische Maßnahmen zu sichern und am Ende des Kalenderjahres, das dem Jahr der Übermittlung folgt, zu vernichten.

(4) Die Daten des Personalausweisregisters und des Melderegisters dürfen zur Berichtigung des jeweils anderen Registers verwendet werden.

§ 25 Datenübertragung und automatisierter Abruf von Lichtbildern

(1) In den Fällen des § 24 Abs. 2 dürfen personenbezogene Daten auch durch Datenübertragung übermittelt werden. § 12 Abs. 1 Satz 3 gilt entsprechend.

(2) Die Ordnungsbehörden dürfen das Lichtbild zum Zweck der Verfolgung von Verkehrsordnungswidrigkeiten im automatisierten Verfahren abrufen, wenn die Personalausweisbehörde auf andere Weise nicht erreichbar ist und ein weiteres Abwarten den Ermittlungszweck gefährden würde. Zuständig für den Abruf sind die Polizeivollzugsbehörden auf Ebene der Landkreise und kreisfreien Städte, die durch Landesrecht bestimmt werden. Die abrufende Behörde trägt die Verantwortung dafür, dass die Voraussetzungen der Absätze 1 und 2 Satz 1 vorliegen. Die Polizeibehörden des Bundes und der Länder, der Militärische Abschirmdienst, der Bundesnachrichtendienst, die Verfassungsschutzbehörden des Bundes und der Länder, Steuerfahndungsdienststellen der Länder, der Zollfahndungsdienst und die Hauptzollämter dürfen das Lichtbild zur Erfüllung ihrer Aufgaben im automatisierten Verfahren abrufen. Ferner dürfen die zur Ausstellung

1. des Führerscheins,
2. des Fahrerqualifizierungsnachweises oder
3. der Fahrerkarte

zuständigen Behörden das Lichtbild sowie die Unterschrift der antragstellenden Person im automatisierten Verfahren abrufen, wenn die antragstellende Person zuvor im Rahmen der Online-Beantragung in die elektronische Übermittlung eingewilligt hat. Die abrufende Behörde trägt die Verantwortung dafür, dass die Voraussetzungen des Absatzes 1 vorliegen. Al-

le Abrufe sind von den beteiligten Behörden so zu protokollieren, dass eine Kontrolle der Zulässigkeit der Abrufe möglich ist. Abrufe nach den Sätzen 4 und 5 werden nur von der abrufenden Behörde protokolliert. Die Protokolle enthalten:

1. die nach § 4 Absatz 1 der Pass- und Personalausweisdatenabrufverordnung verwendeten Auswahldaten bei Abrufen nach den Sätzen 4 und 5, in anderen Fällen den Familiennamen, Vornamen sowie den Tag und den Ort der Geburt der Person, deren Lichtbild abgerufen wurde,
2. Tag und Uhrzeit des Abrufs,
3. die Bezeichnung der am Abruf beteiligten Stellen,
4. die Angabe der abrufenden und der den Abruf anordnenden Person sowie
5. das Aktenzeichen.

§ 24 Abs. 3 Satz 5 gilt entsprechend.

§ 26 Sonstige Speicherung personenbezogener Daten

(1) Beantragung, Ausstellung und Aushändigung von Ausweisen dürfen nicht zum Anlass genommen werden, die dafür erforderlichen Angaben und biometrischen Merkmale außer bei den ausstellenden Personalausweisbehörden nach § 7 Abs. 1 und 2 nach den Vorgaben der §§ 23 bis 25 zu speichern. Entsprechendes gilt für die zur Ausstellung des Ausweises erforderlichen Antragsunterlagen sowie für personenbezogene Datenträger.

(2) Die bei der Personalausweisbehörde gespeicherten Fingerabdrücke sind spätestens nach Aushändigung des Personalausweises an die antragstellende Person zu löschen.

(3) Eine zentrale, alle Seriennummern umfassende Speicherung darf nur bei dem Ausweishersteller und ausschließlich zum Nachweis des Verbleibs der Ausweise erfolgen. Abgesehen von der Sperrsumme und dem letzten Tag der Gültigkeit der jeweiligen elektronischen Identitätsnachweise sowie den weiteren in § 19 Absatz 2 genannten Daten ist die Speicherung sonstiger personenbezogener Daten der antragstellenden Person bei dem Ausweishersteller unzulässig, soweit sie nicht ausschließlich und vorübergehend der Herstellung des Ausweises dient; die Angaben sind anschließend zu löschen.

(4) Eine bundesweite Datenbank der biometrischen Merkmale wird nicht errichtet.

Abschnitt 6
Pflichten des Ausweisinhabers; Ungültigkeit und Entziehung des Ausweises

§ 27 Pflichten des Ausweisinhabers

(1) Der Ausweisinhaber ist verpflichtet, der Personalausweisbehörde unverzüglich

1. den Ausweis vorzulegen, wenn eine Eintragung unrichtig ist,
2. auf Verlangen den alten Ausweis beim Empfang eines neuen Ausweises abzugeben,
3. den Verlust des Ausweises und sein Wiederauffinden anzuzeigen und im Falle des Wiederauffindens diesen vorzulegen,

4. anzuzeigen, wenn er auf Grund freiwilliger Verpflichtung in die Streitkräfte oder einen vergleichbaren bewaffneten Verband eines ausländischen Staates, dessen Staatsangehörigkeit er besitzt, eingetreten ist und
5. im Falle der Ausgabe des Personalausweiseses im Wege des Versands anzuzeigen, wenn die Sendung unbefugt geöffnet worden ist oder den Personalausweis nicht enthält oder wenn der Personalausweis beschädigt ist oder eine Angabe auf dem Personalausweis unrichtig ist.

(2) Der Personalausweisinhaber hat zumutbare Maßnahmen zu treffen, damit keine andere Person Kenntnis von der Geheimnummer erlangt. Die Geheimnummer darf insbesondere nicht auf dem Personalausweis vermerkt oder in anderer Weise zusammen mit diesem aufbewahrt sowie im Fall des elektronischen Identitätsnachweises mit einem mobilen Endgerät nicht auf diesem gespeichert werden. Ist dem Personalausweisinhaber bekannt, dass die Geheimnummer Dritten zur Kenntnis gelangt ist, soll er diese unverzüglich ändern oder die Funktion des elektronischen Identitätsnachweises sperren lassen. Satz 3 gilt entsprechend für den Fall, dass dem Personalausweisinhaber bekannt wird, dass die Geheimnummer eines elektronischen Identitätsnachweises mit einem mobilen Endgerät Dritten zur Kenntnis gelangt ist.

(3) Der Personalausweisinhaber soll durch technische und organisatorische Maßnahmen gewährleisten, dass der elektronische Identitätsnachweis gemäß § 18 nur in einer Umgebung eingesetzt wird, die nach dem jeweiligen Stand der Technik als sicher anzusehen ist. Dabei soll er insbesondere solche technischen Systeme und Bestandteile einsetzen, die vom Bundesamt für Sicherheit in der Informationstechnik als für diesen Einsatzzweck sicher bewertet werden.

§ 28 Ungültigkeit

(1) Ein Ausweis ist ungültig, wenn

1. er eine einwandfreie Feststellung der Identität des Ausweisinhabers nicht zulässt oder verändert worden ist,
2. Eintragungen nach diesem Gesetz fehlen oder – mit Ausnahme der Angaben über die Anschrift oder Größe – unzutreffend sind,
3. die Gültigkeitsdauer abgelaufen ist oder
4. gegen den Ausweisinhaber eine Anordnung im Sinne des § 6a Absatz 2 ergangen ist und er den Geltungsbereich dieses Gesetzes verlassen hat.

(2) Eine Personalausweisbehörde hat einen Ausweis für ungültig zu erklären, wenn die Voraussetzungen für seine Erteilung nicht vorgelegen haben oder nachträglich weggefallen sind.

(3) Störungen der Funktionsfähigkeit des elektronischen Speicher- und Verarbeitungsmediums berühren nicht die Gültigkeit des Personalausweises.

§ 29 Sicherstellung und Einziehung

(1) Ein nach § 28 Abs. 1 oder Abs. 2 ungültiger Ausweis kann eingezogen werden.

(2) Ein Ausweis kann sichergestellt werden, wenn

1. eine Person ihn unberechtigt besitzt oder

2. Tatsachen die Annahme rechtfertigen, dass die Voraussetzungen für eine Einziehung nach Absatz 1 vorliegen, oder
3. eine Entziehung im Sinne des § 6a Absatz 2 ergangen ist oder Tatsachen die Annahme rechtfertigen, dass ein Entziehungsgrund im Sinne des § 6a Absatz 2 vorliegt.

(3) Eine Sicherstellung oder Einziehung ist schriftlich zu bestätigen.

§ 30 Sofortige Vollziehung

Widerspruch und Anfechtungsklage gegen die Anordnung, dass der Ausweis nicht zum Verlassen Deutschlands berechtigt (§ 6 Abs. 7), gegen die Entziehung des Ausweises und die Ausstellung eines Ersatz-Personalausweises (§ 6a), gegen die Aufhebung der Berechtigung (§ 21 Abs. 5), gegen die Einziehung (§ 29 Abs. 1) und gegen die Sicherstellung des Ausweises (§ 29 Abs. 2) haben keine aufschiebende Wirkung.

Abschnitt 7
Gebühren und Auslagen; Bußgeldvorschriften

§ 31 Gebühren und Auslagen; Verordnungsermächtigung

(1) Für individuell zurechenbare öffentliche Leistungen nach diesem Gesetz und den auf diesem Gesetz beruhenden Rechtsverordnungen erheben die Personalausweisbehörden Gebühren und Auslagen nach den Absätzen 2 und 3.

(2) Die Gebühr soll die mit der individuell zurechenbaren öffentlichen Leistung verbundenen Kosten aller an der Leistung Beteiligten decken. In die Gebühr sind die mit der Leistung regelmäßig verbundenen Auslagen einzubeziehen. Zur Ermittlung der Gebühr sind die Kosten, die nach betriebswirtschaftlichen Grundsätzen als Einzel- und Gemeinkosten zurechenbar und ansatzfähig sind, insbesondere Personal- und Sachkosten sowie kalkulatorische Kosten, zu Grunde zu legen. Zu den Gemeinkosten zählen auch die Kosten der Rechts- und Fachaufsicht. Grundlage der Gebührenermittlung nach den Sätzen 1 bis 4 sind Kosten, die in der Gesamtheit der Länder mit der jeweiligen Leistung verbundenen sind. § 3 Absatz 1 und 2, die §§ 5 bis 7, 9 Absatz 3 bis 6 und die §§ 10 bis 12 des Bundesgebührengesetzes gelten entsprechend.

(3) Das Bundesministerium des Innern und für Heimat wird ermächtigt, für den Bereich der Landesverwaltung durch Rechtsverordnung mit Zustimmung des Bundesrates die gebührenpflichtigen Tatbestände, die Gebührenhöhe und die Auslagenerstattung näher zu bestimmen.

(4) Durch Besondere Gebührenverordnung des Auswärtigen Amts nach § 22 Absatz 4 des Bundesgebührengesetzes kann bestimmt werden, dass von den Auslandsvertretungen der Bundesrepublik Deutschland für individuell zurechenbare öffentliche Leistungen nach diesem Gesetz und den auf diesem Gesetz beruhenden Rechtsverordnungen zum Ausgleich von Kaufkraftunterschieden ein Zuschlag erhoben wird. Der Zuschlag kann bis zu 300 Prozent der Gebühren betragen.

§ 32 Bußgeldvorschriften

(1) Ordnungswidrig handelt, wer

1. entgegen § 1 Abs. 1 Satz 1, auch in Verbindung mit Abs. 2 Satz 1, einen Ausweis nicht besitzt,
2. entgegen § 1 Abs. 1 Satz 2, auch in Verbindung mit Abs. 2 Satz 1, einen Ausweis nicht oder nicht rechtzeitig vorlegt oder einen Abgleich mit dem Lichtbild nicht oder nicht rechtzeitig ermöglicht,
3. entgegen § 9 Abs. 2 Satz 2 einen dort genannten Antrag nicht oder nicht rechtzeitig stellt,
4. entgegen § 9 Abs. 3 Satz 1, auch in Verbindung mit Absatz 6 Satz 2, eine Angabe nicht richtig macht,
5. entgegen § 18 Abs. 2 Satz 4 einen elektronischen Identitätsnachweis nutzt,
6. entgegen § 20 Absatz 2 Satz 2 eine Kopie weitergibt oder
7. entgegen § 27 Absatz 1 Nummer 3 oder 4 eine Anzeige nicht oder nicht rechtzeitig erstattet.

(2) Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig

1. ohne Berechtigung nach § 21 Absatz 1 Satz 1 Daten anfragt,
2. entgegen § 21 Absatz 2 Satz 2, auch in Verbindung mit § 21a Satz 2 oder § 21b Absatz 2 Satz 2, eine Angabe nicht richtig macht,
3. entgegen § 21 Absatz 3 Satz 3 oder Absatz 5 Satz 1, jeweils auch in Verbindung mit § 21a Satz 2 oder § 21b Absatz 2 Satz 2, eine Berechtigung oder ein Berechtigungszertifikat verwendet,
4. entgegen § 21 Absatz 6, auch in Verbindung mit § 21a Satz 2 oder § 21b Absatz 2 Satz 2, eine Mitteilung nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig macht oder
5. ohne Berechtigung nach § 21b Absatz 1 eine dort genannte Funktion nutzt.

(3) Die Ordnungswidrigkeit kann in den Fällen des Absatzes 1 Nummer 5 sowie des Absatzes 2 Nummer 1, 2, 3 und 5 mit einer Geldbuße bis zu dreißigtausend Euro und in den übrigen Fällen mit einer Geldbuße bis zu dreitausend Euro geahndet werden.

§ 33 Bußgeldbehörden

Verwaltungsbehörden im Sinne des § 36 Abs. 1 Nr. 1 des Gesetzes über Ordnungswidrigkeiten sind, soweit dieses Gesetz von Bundesbehörden ausgeführt wird,

1. in den Fällen des § 32 Absatz 1 Nummer 2 und 5 die Bundespolizeibehörden jeweils für ihren Geschäftsbereich,
2. in den Fällen des § 32 Abs. 1 Nr. 4 das Auswärtige Amt für Ausweisangelegenheiten im Ausland,
3. in den Fällen des § 32 Abs. 2 Nr. 1 bis 4 die Vergabestelle für Berechtigungszertifikate nach § 7 Abs. 4 Satz 1.

Abschnitt 8
Verordnungsermächtigung; Übergangsvorschrift

§ 34 Verordnungsermächtigung

Das Bundesministerium des Innern und für Heimat wird ermächtigt, mit Zustimmung des Bundesrates durch Rechtsverordnung

1. die Muster der Ausweise zu bestimmen,
2. die Einzelheiten der technischen Anforderungen an die Speicherung des Lichtbildes und der Fingerabdrücke sowie den Zugriffsschutz auf die im elektronischen Speicher- und Verarbeitungsmedium abgelegten Daten zu regeln,
3. die Einzelheiten zu regeln
   a) über das Verfahren und die technischen Anforderungen für die Aufnahme, die elektronische Erfassung, die Echtheitsbewertung und die Qualitätssicherung des Lichtbilds,
   b) zur sicheren Übermittlung des Lichtbilds an die Personalausweisbehörde sowie zu einer Registrierung und Zertifizierung von Dienstleistern, welche Lichtbilder für die Personalausweisproduktion an die Personalausweisbehörde übermitteln,
   c) über das Verfahren und die technischen Anforderungen für die Aufnahme, die elektronische Erfassung, die Echtheitsbewertung und Qualitätssicherung der Fingerabdrücke, die Reihenfolge der zu speichernden Fingerabdrücke bei Fehlen eines Zeigefingers, ungenügender Qualität des Fingerabdrucks oder Verletzungen der Fingerkuppe und
   d) über die Form und die Einzelheiten für das Verfahren der Übermittlung sämtlicher Ausweisantragsdaten von den Personalausweisbehörden an den Ausweishersteller,
4. die Einzelheiten des Prüfverfahrens nach § 12 Absatz 2 Satz 2 zu regeln,
5. die Herstellung des Personalausweises und die Übermittlung und Übergabe von Geheimnummer, Entsperrnummer und Sperrkennwort zu regeln,
6. die Einzelheiten der Aushändigung und den Versand des Personalausweises zu regeln,

6a. die Einzelheiten zum Einschalten der Funktion zum elektronischen Identitätsnachweis, einschließlich des Verfahrens des nachträglichen Einschaltens der Funktion zum elektronischen Identitätsnachweis durch den Ausweishersteller nach elektronisch gestellter Beantragung, zu regeln,

7. die Änderung von Daten des Personalausweises wie den Namen oder die Anschrift, einschließlich des Verfahrens der Änderung der Anschrift auf dem elektronischen Speicher- und Verarbeitungsmedium nach einer elektronischen Anmeldung gemäß § 23a des Bundesmeldegesetzes, zu regeln,
8. die Einzelheiten zur Nutzung des elektronischen Identitätsnachweises und des Vor-Ort-Auslesens zu regeln,

8a. die Einzelheiten zur Einrichtung und zur Nutzung des elektronischen Identitätsnachweises mit einem mobilen Endgerät, sowie zu den technischen Anforderungen an mobile Endgeräte nach § 2 Absatz 13 zu regeln,

9. die Einzelheiten

   a) der Geheimnummer, einschließlich des Verfahrens des Neusetzens der Geheimnummer durch den Ausweishersteller nach elektronisch gestelltem Antrag,

   b) der Sperrung und Entsperrung des elektronischen Identitätsnachweises durch den Ausweisinhaber sowie

   c) der Speicherung und Löschung der Sperrmerkmale und des Sperrkennworts

   festzulegen,

10. die sicherheitstechnischen Rahmenbedingungen festzulegen, die vorliegen müssen, damit öffentliche und private Stellen ein Benutzerkonto nach § 19 Absatz 5 anlegen und betreiben dürfen,

11. die Einzelheiten der Vergabe der Berechtigungen und Berechtigungszertifikate festzulegen und

12. die Einzelheiten zur Durchführung von automatisierten Mitteilungen oder von automatisierten Abrufen nach § 25 sowie zur Form und zum Inhalt der zu übermittelnden Daten zu regeln.

Rechtsverordnungen nach Satz 1 ergehen im Benehmen mit dem Auswärtigen Amt, Rechtsverordnungen nach Satz 1 Nummer 3 Buchstabe b zusätzlich im Benehmen mit dem Bundesministerium für Wirtschaft und Klimaschutz. In einer Rechtsverordnung nach Satz 1 Nummer 8a sind Regelungen zu Maßnahmen gegen eine missbräuchliche Verwendung bei der Einrichtung eines elektronischen Identitätsnachweises mit einem mobilen Endgerät vorzusehen.

§ 34a Regelungsbefugnisse der Länder

Durch Landesrecht können zentrale Personalausweisregisterdatenbestände zur Speicherung des Lichtbilds und der Unterschrift für die Durchführung eines automatisierten Abrufs des Lichtbilds nach § 25 Absatz 2 Satz 1 und 4 sowie eines automatisierten Abrufs des Lichtbilds und der Unterschrift nach § 25 Absatz 2 Satz 5 eingerichtet werden. In diesem Fall gelten § 23 Absatz 4, § 25 Absatz 2 Satz 5 bis 8 und § 26 Absatz 4 entsprechend. Macht ein Land von der Regelungsbefugnis Gebrauch, hat es technisch sicherzustellen, dass die Lichtbilder und Unterschriften vor unbefugtem Zugriff geschützt sind. Die Lichtbilder und Unterschriften dürfen nur so gespeichert werden, dass keine Verknüpfung mit anderen als für den automatisierten Abruf benötigten Daten ermöglicht wird.

§ 35 Übergangsvorschrift

Abweichend von § 7 Abs. 2, § 8 Abs. 2, § 10 Abs. 1 Satz 4 und Abs. 2 Satz 2, § 23 Abs. 4 Satz 2 sowie § 31 Abs. 2 ist bis zum 31. Dezember 2012 für Deutsche mit Hauptwohnung im Ausland die Personalausweisbehörde nach § 7 Abs. 1 zuständig, in deren Bezirk er oder sie sich vorübergehend aufhält.

Gesetz über eine Karte für Unionsbürger und Angehörige des Europäischen Wirtschaftsraums mit Funktion zum elektronischen Identitätsnachweis (eID-Karte-Gesetz - eIDKG)

Inhaltsübersicht

Abschnitt 1
Allgemeine Vorschriften

§ 1 eID-Karte

(1) Für Staatsangehörige eines Mitgliedstaats der Europäischen Union oder eines Vertragsstaats des Abkommens über den Europäischen Wirtschaftsraum, die nicht Deutsche im Sinne des Artikels 116 Absatz 1 des Grundgesetzes sind, wird auf Antrag eine Karte mit Funktion zum elektronischen Identitätsnachweis (eID-Karte) ausgestellt.

(2) Die eID-Karte ermöglicht den elektronischen Identitätsnachweis und das Vor-Ort-Auslesen nach den §§ 12 und 13.

§ 2 Begriffsbestimmungen

(1) Diensteanbieter sind natürliche und juristische Personen, die zur Wahrnehmung von Aufgaben der öffentlichen Verwaltung oder zur Erfüllung eigener Geschäftszwecke den Nachweis der Identität oder einzelner Identitätsmerkmale des Karteninhabers benötigen und ihren Wohn-, Geschäfts- oder Dienstsitz innerhalb der Europäischen Union sowie in Staaten, in denen ein vergleichbarer Datenschutzstandard besteht, haben.

(2) Ein Berechtigungszertifikat ist eine elektronische Bescheinigung, die es einem Diensteanbieter ermöglicht,

1. seine Identität dem Karteninhaber nachzuweisen und

2. die Übermittlung personen- und kartenbezogener Daten aus der eID-Karte anzufragen.

(3) Das Sperrkennwort ist eine Zeichenfolge, die ausschließlich der Sperrung des elektronischen Identitätsnachweises mit einer eID-Karte oder mit einem mobilen Endgerät dient.

(4) Die Sperrsumme ist ein eindeutiges Merkmal, das aus dem Sperrkennwort, dem Familiennamen, den Vornamen und dem Tag der Geburt eines Karteninhabers errechnet wird. Es dient der Übermittlung einer Sperrung vom Sperrnotruf oder einer eID-Karte-Behörde an den Sperrlistenbetreiber. Mithilfe der Sperrsumme ermittelt der Sperrlistenbetreiber anhand der Referenzliste den Sperrschlüssel eines zu sperrenden elektronischen Identitätsnachweises.

(5) Sperrmerkmale eines elektronischen Identitätsnachweises mit einer eID-Karte oder mit einem mobilen Endgerät sind dienste- und kartenspezifische Zeichenfolgen, die ausschließlich der Erkennung abhandengekommener eID-Karten oder mobiler Endgeräte durch den Diensteanbieter dienen, für den sie errechnet wurden.

(6) Die Seriennummer einer eID-Karte setzt sich aus einer vierstelligen Behördenkennzahl und einer fünfstelligen, zufällig vergebenen Nummer zusammen und kann Ziffern und Buchstaben enthalten.

(7) Die Geheimnummer besteht aus einer sechsstelligen Ziffernfolge und dient der Freigabe der Datenübermittlung aus der eID-Karte oder aus einem mobilen Endgerät im Rahmen des elektronischen Identitätsnachweises.

(8) Die Zugangsnummer ist eine zufällig erzeugte, ausschließlich auf der Karte sichtbar aufgebrachte sechsstellige Ziffernfolge, die zur Absicherung gegen unberechtigten Zugriff auf die Kommunikation zwischen eID-Karte und Lesegeräten dient.

(9) Die Entsperrnummer ist eine zufällig erzeugte Ziffernfolge, die die Freischaltung der Geheimnummer ermöglicht, wenn diese nach dreimaliger Fehleingabe gesperrt worden ist.

(10) Karteninhaber ist die Person, für die die eID-Karte ausgestellt wurde.

(11) Im Sinne dieses Gesetzes ist ein mobiles Endgerät ein solches Gerät, das dem Stand der Technik entspricht, um einen elektronischen Identitätsnachweis nach § 12 Absatz 3 Satz 1 Nummer 2 durchführen zu können.

§ 3 Besitz und Eigentum; Hersteller, Vergabestelle und Sperrlistenbetreiber

(1) Niemand darf mehr als eine auf seine Person ausgestellte gültige eID-Karte besitzen.

(2) Die eID-Karte ist Eigentum der Bundesrepublik Deutschland.

(3) Das Bundesministerium des Innern und für Heimat bestimmt

1. den Kartenhersteller,
2. die Vergabestelle für Berechtigungszertifikate,
3. den Sperrlistenbetreiber

und macht deren Namen im Bundesanzeiger bekannt.

§ 4 Kartenmuster; Seriennummer; Chip

(1) Die eID-Karte wird nach einem einheitlichen Muster ausgestellt.

(2) Jede eID-Karte erhält eine neue Seriennummer. Die Seriennummer, das Sperrkennwort und Sperrmerkmale dürfen keine Daten über die Person des Karteninhabers oder Hinweise auf solche Daten enthalten.

(3) Die eID-Karte enthält neben der Seriennummer, der Angabe der ausstellenden Behörde, dem letzten Tag der Gültigkeitsdauer und der Zugangsnummer folgende sichtbar aufgebrachte Angaben über den Karteninhaber:

1. Familienname und Vornamen und
2. Tag und Ort der Geburt.

(4) Die eID-Karte besitzt ein elektronisches Speicher- und Verarbeitungsmedium (Chip), auf dem folgende Daten gespeichert werden:

1. Familienname und Geburtsname,
2. Vornamen,
3. Doktorgrad,
4. Tag und Ort der Geburt,
5. Anschrift; hat der Karteninhaber keine Wohnung in Deutschland, kann die Angabe „keine Wohnung in Deutschland“ eingetragen werden,
6. Staatsangehörigkeit,
7. Ordensname, Künstlername,
8. Dokumentenart und
9. letzter Tag der Gültigkeitsdauer.

Zur Einrichtung eines elektronischen Identitätsnachweises nach § 8a Absatz 1 Satz 1 dürfen auf einem elektronischen Speicher- und Verarbeitungsmedium in einem mobilen Endgerät die Daten nach Satz 1 gespeichert werden.

(5) Die gespeicherten Daten sind gegen unbefugtes Verändern, Löschen und Auslesen zu sichern.

§ 5 Gültigkeitsdauer

(1) Die eID-Karte wird für eine Gültigkeitsdauer von zehn Jahren ausgestellt.

(2) Eine Verlängerung der Gültigkeitsdauer ist nicht zulässig.

(3) Vor Ablauf der Gültigkeit einer eID-Karte kann eine neue eID-Karte beantragt werden, wenn ein berechtigtes Interesse an der Neuausstellung dargelegt wird.

§ 6 Sachliche Zuständigkeit

(1) Zuständig für Angelegenheiten, die die eID-Karte betreffen, sind:

1. in Deutschland die von den Ländern bestimmten Behörden,

2. im Ausland das Auswärtige Amt mit den von ihm bestimmten Auslandsvertretungen

(eID-Karte-Behörden).

(2) Für die Einziehung und Sicherstellung der eID-Karte sind neben den eID-Karte-Behörden auch die zur Identitätsfeststellung berechtigten Behörden (§ 2 Absatz 2 des Personalausweisgesetzes) zuständig.

(3) Zuständig

1. für die Erteilung und Aufhebung von Berechtigungen nach den §§ 15 bis 17 ist die Vergabestelle für Berechtigungszertifikate nach § 3 Absatz 3 Nummer 2,
2. für das Führen einer Sperrliste nach § 9 Absatz 3 ist der Sperrlistenbetreiber nach § 3 Absatz 3 Nummer 3.

(4) Für das elektronisch beantragte Neusetzen der Geheimnummer ist der Kartenhersteller zuständig.

(5) Für die Übermittlung von Daten nach § 4 Absatz 4 Satz 2 aus dem Chip der eID-Karte auf ein elektronisches Speicher- und Verarbeitungsmedium in einem mobilen Endgerät nach § 8a Absatz 1 Satz 1 sowie für die Auskunft nach § 8a Absatz 5 ist der Kartenhersteller zuständig.

§ 7 Örtliche Zuständigkeit

(1) Örtlich zuständig ist diejenige eID-Karte-Behörde, in deren Bezirk die antragstellende Person oder der Karteninhaber für seine Wohnung, bei mehreren Wohnungen für seine Hauptwohnung, meldepflichtig ist. Ist die Person nicht meldepflichtig, ist die eID-Karte-Behörde zuständig, in deren Bezirk die Person im Zeitpunkt der Antragstellung oder des die behördliche Tätigkeit auslösenden Ereignisses wohnt.

(1a) Für das Führen des eID-Karte-Registers nach § 19 ist die eID-Karte-Behörde zuständig, welche die eID-Karte ausgestellt hat.

(2) Im Ausland sind die vom Auswärtigen Amt bestimmten Auslandsvertretungen zuständig, in deren Bezirk sich die antragstellende Person oder der Karteninhaber gewöhnlich aufhält. Die antragstellende Person oder der Karteninhaber haben den Nachweis über ihren gewöhnlichen Aufenthaltsort zu erbringen.

Abschnitt 2
Ausstellung und Sperrung der eID-Karte; elektronischer Identitätsnachweis mit einem mobilen Endgerät

§ 8 Ausstellung der eID-Karte

(1) Die eID-Karte wird auf Antrag für die antragstellende Person ausgestellt, wenn sie

1. dem in § 1 Absatz 1 genannten Personenkreis unterfällt und
2. mindestens 13 Jahre alt ist.

Jugendliche, die mindestens 13 Jahre alt sind, dürfen Verfahrenshandlungen nach diesem Gesetz vornehmen.

(2) In dem Antrag sind alle Tatsachen anzugeben, die zur Feststellung der antragstellenden Person notwendig sind. Die Angaben zu dem Doktorgrad und zu den Ordens- und Künstlernamen sind freigestellt. Die antragstellende Person hat die erforderlichen Nachweise zu erbringen und sich unter Vorlage eines anerkannten und gültigen ausländischen Passes oder Personalausweises vor der ausgebenden Stelle persönlich zu identifizieren.

(3) Bestehen Zweifel über die Identität der antragstellenden Person, so ist die Ausstellung einer eID-Karte abzulehnen.

§ 8a Einrichtung des elektronischen Identitätsnachweises mit einem mobilen Endgerät

(1) Auf elektronische Veranlassung durch den Karteninhaber übermittelt der Kartenhersteller die Daten nach § 4 Absatz 4 Satz 2 aus dem Chip der eID-Karte in einem sicheren Verfahren auf ein elektronisches Speicher- und Verarbeitungsmedium in einem mobilen Endgerät. Der Karteninhaber weist seine Identität gegenüber dem Kartenhersteller mit einem elektronischen Identitätsnachweis nach § 12 nach. Ferner hat der Kartenhersteller Maßnahmen gegen eine missbräuchliche Verwendung der Daten im Anschluss an die Übermittlung der Daten auf das elektronische Speicher- und Verarbeitungsmedium in dem mobilen Endgerät vorzusehen. Der Karteninhaber ist auf seine Pflichten nach § 20 Absatz 2 sowie darauf hinzuweisen, dass das mobile Endgerät hinsichtlich der in seinem elektronischen Speicher- und Verarbeitungsmedium nach Absatz 1 gespeicherten Daten mit besonderer Sorgfalt zu behandeln ist.

(2) Die Gültigkeitsdauer eines elektronischen Identitätsnachweises nach § 12 Absatz 3 Satz 1 Nummer 2 auf Grundlage einer Übermittlung der Daten nach Absatz 1 beträgt fünf Jahre. Eine Verlängerung der Gültigkeitsdauer ist nicht zulässig. Durch Rechtsverordnung nach § 25 Nummer 8a kann eine kürzere Gültigkeitsdauer festgelegt werden. Eine Übermittlung nach Absatz 1 Satz 1 kann mehrfach durchgeführt werden.

(3) Im Zuge der Übermittlung nach Absatz 1 Satz 1 erzeugt der Kartenhersteller einen neuen Sperrschlüssel und eine neue Sperrsumme und übermittelt diese an den Sperrlistenbetreiber. § 9 Absatz 2 Satz 1 gilt entsprechend. Der Karteninhaber kann die Daten auf dem mobilen Endgerät selbst löschen.

(4) Werden die auf das elektronische Speicher- und Verarbeitungsmedium des mobilen Endgeräts übermittelten Daten nach Absatz 1 Satz 1 unrichtig, darf ein elektronischer Identitätsnachweis nach § 12 Absatz 3 Satz 1 Nummer 2 nicht durchgeführt werden. Zur weiteren Nutzung ist erneut eine Übermittlung nach Absatz 1 Satz 1 unter Verwendung des Chips der eID-Karte mit richtigen Angaben durchzuführen.

(5) Auf elektronischen Antrag des Karteninhabers hat der Kartenhersteller diesem Auskunft zu erteilen darüber, jeweils zu welchem Datum und zu welcher Uhrzeit eine Übermittlung nach Absatz 1 Satz 1 der Daten der eID-Karte des Karteninhabers auf ein elektronisches Speicher- und Verarbeitungsmedium in einem mobilen Endgerät durchgeführt wurde, sowie über jeweils den letzten Tag der Gültigkeitsdauer, das Sperrkennwort und den Hersteller und die Modellbezeichnung des mobilen Endgeräts. Zur Identifizierung der antragstellenden Person hat der Kartenhersteller zur Person des Karteninhabers einen elektronischen Identitätsnachweis nach § 12 durchzuführen.

§ 9 Sperrung und Entsperrung

(1) Die ausstellende eID-Karte-Behörde hat unverzüglich zur Aktualisierung der Sperrliste die Sperrsumme der eID-Karte an den Sperrlistenbetreiber zu übermitteln, wenn sie Kenntnis erlangt von

1. dem Abhandenkommen einer eID-Karte,
2. dem Versterben eines Karteninhabers oder
3. der Ungültigkeit einer nicht im Besitz der Behörde befindlichen eID-Karte nach § 21.

(2) Der Karteninhaber kann durch Mitteilung des Sperrkennworts an den Sperrlistenbetreiber eine sofortige Sperrung des elektronischen Identitätsnachweises veranlassen. Davon unberührt bleibt die Pflicht, den Verlust oder das Abhandenkommen der eID-Karte nach § 20 Absatz 1 Nummer 3 der eID-Karte-Behörde anzuzeigen.

(3) Der Sperrlistenbetreiber stellt den eID-Karte-Behörden für die Fälle nach Absatz 1 und den Karteninhabern für die Fälle nach Absatz 2 einen Sperrdienst über jederzeit öffentlich erreichbare Kommunikationsverbindungen zur Verfügung. § 10 Absatz 4 des Personalausweisgesetzes gilt entsprechend.

(4) Teilt nach erfolgter Sperrung nach Absatz 1 der Karteninhaber das Wiederauffinden seiner eID-Karte unter den Voraussetzungen des § 8 Absatz 2 Satz 3 mit oder bittet er nach einer Sperrung nach Absatz 2 unter den Voraussetzungen des § 8 Absatz 2 Satz 3 um Entsperrung, so ersucht die eID-Karte-Behörde den Sperrlistenbetreiber um Löschung des Sperreintrags zu dieser eID-Karte.

(5) Der Zeitpunkt der Meldung des Abhandenkommens eines Ausweises ist von der eID-Karte-Behörde oder Polizeibehörde zu dokumentieren und der ausstellenden eID-Karte-Behörde mitzuteilen.

§ 10 Informationspflichten

(1) Auf Verlangen des Karteninhabers hat die eID-Karte-Behörde ihm Einsicht in die im Chip der eID-Karte gespeicherten auslesbaren Daten zu gewähren.

(2) Die eID-Karte-Behörde hat die antragstellende Person bei Antragstellung über den elektronischen Identitätsnachweis nach § 12, einschließlich des elektronischen Identitätsnachweises mit einem mobilen Endgerät, und das Vor-Ort-Auslesen nach § 13 sowie über Maßnahmen zu unterrichten, die erforderlich sind, um die Sicherheit der Nutzung des elektronischen Identitätsnachweises zu gewährleisten. Sie hat Informationsmaterial bereitzustellen, in dem auch auf die Möglichkeit einer Sperrung hingewiesen wird. Die antragstellende Person ist auf das vorhandene Informationsmaterial hinzuweisen.

(3) Eine eID-Karte-Behörde, die Kenntnis von dem Abhandenkommen einer eID-Karte erlangt, hat die zuständige eID-Karte-Behörde, die ausstellende eID-Karte-Behörde und eine Polizeibehörde unverzüglich in Kenntnis zu setzen; eine Polizeibehörde, die anderweitig Kenntnis vom Abhandenkommen einer eID-Karte erlangt, hat die zuständige und die ausstellende eID-Karte-Behörde unverzüglich zu unterrichten. Dabei sollen Angaben zum Familiennamen, den Vornamen, zur Seriennummer, zur ausstellenden eID-Karte-Behörde, zum Ausstellungsdatum und zur Gültigkeitsdauer der eID-Karte übermittelt werden. Die Polizeibehörde hat die Einstellung in die polizeiliche Sachfahndung vorzunehmen.

§ 11 Datenerfassung, -prüfung und -übermittlung

Für die Form und das Verfahren der Datenerfassung, -prüfung und -übermittlung und für die Übermittlung von Geheimnummer, Entsperrnummer und Sperrkennwort gelten die §§ 12 und 13 des Personalausweisgesetzes entsprechend.

Abschnitt 3
Nutzung der eID-Karte

§ 12 Elektronischer Identitätsnachweis

(1) Der Karteninhaber kann seine eID-Karte dazu nutzen, seine Identität gegenüber öffentlichen und nichtöffentlichen Stellen elektronisch nachzuweisen. Dies gilt auch dann, wenn er für eine andere Person, ein Unternehmen oder eine Behörde handelt. Abweichend von Satz 1 ist der elektronische Identitätsnachweis ausgeschlossen, wenn die Voraussetzungen des § 3a Absatz 1 des Verwaltungsverfahrensgesetzes, des § 87a Absatz 1 Satz 1 der Abgabenordnung oder des § 36a Absatz 1 des Ersten Buches Sozialgesetzbuch nicht vorliegen.

(2) Die Nutzung des elektronischen Identitätsnachweises durch eine andere Person als den Karteninhaber ist unzulässig.

(3) Der elektronische Identitätsnachweis erfolgt durch Übermittlung von Daten

1. aus dem Chip der eID-Karte oder
2. aus einem elektronischen Speicher- und Verarbeitungsmedium in einem mobilen Endgerät.

Für die Einzelheiten der Datenübermittlung gilt § 18 Absatz 2 Satz 2, Absatz 3, 4 und 5 des Personalausweisgesetzes entsprechend.

(4) eID-Karte-Behörden dürfen im Rahmen der Änderung der Anschrift auf dem elektronischen Speicher- und Verarbeitungsmedium nach einer elektronischen Anmeldung gemäß § 23a des Bundesmeldegesetzes einen elektronischen Identitätsnachweis durchführen und hierzu ein hoheitliches Berechtigungszertifikat verwenden.

§ 13 Vor-Ort-Auslesen

(1) Der Karteninhaber kann seine eID-Karte ferner dazu verwenden, die im Chip gespeicherten Daten zum Zwecke der medienbruchfreien Übernahme von Formulardaten unter Anwesenden zu übermitteln.

(2) Vor dem Vor-Ort-Auslesen der Daten ist der Vor-Ort-Diensteanbieter verpflichtet, anhand eines gültigen Passes oder amtlichen Ausweises per Lichtbildabgleich zu prüfen, ob die die eID-Karte vorlegende Person der Karteninhaber ist. Die Daten werden nur übermittelt, wenn der Vor-Ort-Anbieter mit Einverständnis des Karteninhabers die Zugangsnummer ausliest und diese zusammen mit einem gültigen Vor-Ort-Zertifikat an den Chip der eID-Karte übermittelt.

§ 14 Speicherung im Rahmen des elektronischen Identitätsnachweises

Für die Speicherung von Daten im Rahmen des elektronischen Identitätsnachweises, auch durch Identifizierungsdiensteanbieter, gelten die §§ 19 und 19a des Personalausweisgesetzes entsprechend.

Abschnitt 4
Hoheitliche Berechtigungszertifikate; Berechtigungen; elektronische Signaturen

§ 14a Hoheitliche Berechtigungszertifikate

(1) eID-Karte-Behörden und der Kartenhersteller erhalten hoheitliche Berechtigungszertifikate. Umfang und Inhalt der in Satz 1 genannten hoheitlichen Berechtigungszertifikate bestimmen sich durch die aufgrund dieses Gesetzes den eID-Karte-Behörden und dem Kartenhersteller jeweils zugewiesenen Zuständigkeiten.

(2) Das Bundesamt für Sicherheit in der Informationstechnik erhält hoheitliche Berechtigungszertifikate zur Qualitätssicherung anhand von Testausweisen.

§ 15 Berechtigungen für Diensteanbieter

(1) Um Daten im Wege des elektronischen Identitätsnachweises anzufragen, benötigen Diensteanbieter eine Berechtigung. Die Berechtigung lässt datenschutzrechtliche Vorschriften unberührt. Das Vorliegen einer Berechtigung ist durch die Vergabe von Berechtigungszertifikaten technisch abzusichern.

(2) Für die Voraussetzungen und das Verfahren gelten die Vorschriften des § 21 Absatz 2 bis 8 des Personalausweisgesetzes entsprechend.

§ 16 Vor-Ort-Berechtigung für Vor-Ort-Diensteanbieter

Um Daten nach § 13 unter Anwesenden vor Ort auslesen zu dürfen, benötigen Vor-Ort-Diensteanbieter eine Vor-Ort-Berechtigung einschließlich eines Vor-Ort-Zertifikats. § 21 des Personalausweisgesetzes gilt hierfür entsprechend.

§ 17 Berechtigung für Identifizierungsdiensteanbieter

Wer als Identifizierungsdiensteanbieter die Funktion des elektronischen Identitätsnachweises nach § 12 nutzen möchte, um Identifizierungsdienstleistungen für Dritte zu erbringen, bedarf einer Berechtigung. § 21b des Personalausweisgesetzes gilt hierfür entsprechend.

§ 18 Elektronische Signatur

Die eID-Karte kann als qualifizierte elektronische Signaturerstellungseinheit im Sinne des Artikels 3 Nummer 23 der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG (ABl. L 257 vom 28.8.2014, S. 73; L 23 vom 29.1.2015, S. 19; L 155 vom 14.6.2016, S. 44) ausgestaltet werden. Die Zertifizierung nach Artikel 30 der Verordnung (EU) Nr. 910/2014 erfolgt durch das Bundesamt für Sicherheit in der Informationstechnik. Die Vorschriften des Vertrauensdienstegesetzes bleiben unberührt.

Abschnitt 5
eID-Karte-Register

§ 19 eID-Karte-Register

(1) Zur Durchführung dieses Gesetzes führen die eID-Karte-Behörden Register über die beantragten und ausgegebenen eID-Karten (eID-Karte-Register).

(2) Die Daten des eID-Karte-Registers und des Melderegisters dürfen zur Berichtigung des jeweils anderen Registers verwendet werden. Zu diesem Zweck dürfen eID-Karte-Behörden untereinander die im Register enthaltenen Daten übermitteln.

(3) Das eID-Karte-Register darf neben verfahrensbedingten Bearbeitungsvermerken ausschließlich folgende Daten enthalten:

1. Familienname und Geburtsname,
2. Vornamen,
3. Doktorgrad,
4. Tag der Geburt,
5. Ort der Geburt,
6. Anschrift,

6a. E-Mail-Adresse, sofern der Inhaber der eID-Karte in die Speicherung einwilligt,

7. Staatsangehörigkeit,
8. Seriennummer,
9. Sperrkennwort und Sperrsumme,
10. letzter Tag der Gültigkeitsdauer,
11. ausstellende Behörde,
12. die örtlich zuständige eID-Karte-Behörde, wenn diese nicht mit der ausstellenden eID-Karte-Behörde identisch ist, und
13. Ordensname, Künstlername.

(4) Personenbezogene Daten im eID-Karte-Register sind mindestens bis zur Ausstellung einer neuen eID-Karte, höchstens jedoch bis zum Ablauf der Gültigkeitsdauer der eID-Karte, auf die sie sich beziehen, zu speichern und dann zu löschen.

(5) Wird eine andere als die ausstellende eID-Karte-Behörde örtlich zuständig, darf sie die in Absatz 3 genannten und zur Wahrnehmung ihrer Aufgaben erforderlichen Daten speichern. Absatz 4 gilt entsprechend.

§ 19a Verwendung von im eID-Karte-Register gespeicherten Daten

eID-Karte-Behörden dürfen anderen eID-Karte-Behörden im automatisierten Verfahren Daten des eID-Karte-Registers übermitteln oder Daten aus eID-Karte-Registern, die in Zuständigkeit anderer eID-Karte-Behörden geführt werden, abrufen, sofern dies zur Wahrnehmung ihrer Pflichten erforderlich ist.

Abschnitt 6
Pflichten des Karteninhabers; Ungültigkeit und Einziehung

§ 20 Pflichten des Karteninhabers

(1) Der Karteninhaber ist verpflichtet, der eID-Karte-Behörde unverzüglich

1. die eID-Karte vorzulegen, wenn eine Eintragung unrichtig ist,
2. die alte eID-Karte beim Empfang einer neuen eID-Karte abzugeben,
3. den Verlust der eID-Karte und ihr Wiederauffinden anzuzeigen sowie
4. im Falle der Ausgabe der eID-Karte im Wege des postalischen Versands anzuzeigen, wenn die Sendung unbefugt geöffnet worden ist oder die eID-Karte nicht enthält oder wenn die eID-Karte beschädigt ist oder eine Angabe auf der eID-Karte unrichtig ist.

(2) Der Karteninhaber hat zumutbare Maßnahmen zu treffen, damit keine andere Person Kenntnis von der Geheimnummer erlangt. Die Geheimnummer darf insbesondere nicht auf der eID-Karte vermerkt oder in anderer Weise zusammen mit dieser aufbewahrt sowie im Fall des elektronischen Identitätsnachweises mit einem mobilen Endgerät nicht auf diesem gespeichert werden. Ist dem Karteninhaber bekannt, dass die Geheimnummer Dritten zur Kenntnis gelangt ist, soll er diese unverzüglich ändern oder die Funktion des elektronischen Identitätsnachweises sperren lassen. Satz 3 gilt entsprechend für den Fall, dass dem Karteninhaber bekannt wird, dass die Geheimnummer eines elektronischen Identitätsnachweises mit einem mobilen Endgerät Dritten zur Kenntnis gelangt ist.

(3) Der Karteninhaber soll durch technische und organisatorische Maßnahmen gewährleisten, dass der elektronische Identitätsnachweis nach § 12 nur in einer Umgebung eingesetzt wird, die nach dem jeweiligen Stand der Technik als sicher anzusehen ist. Dabei soll er insbesondere solche technischen Systeme und Bestandteile einsetzen, die vom Bundesamt für Sicherheit in der Informationstechnik als für diesen Einsatzzweck sicher bewertet werden.

§ 21 Ungültigkeit

(1) Eine eID-Karte ist ungültig, wenn

1. Eintragungen nach diesem Gesetz fehlen oder mit Ausnahme der Angabe über die Anschrift unzutreffend sind oder
2. die Gültigkeitsdauer abgelaufen ist.

(2) Die eID-Karte-Behörde hat eine eID-Karte für ungültig zu erklären, wenn die Voraussetzungen für ihre Erteilung im Zeitpunkt der Ausstellung nicht vorgelegen haben oder nachträglich weggefallen sind.

§ 22 Einziehung und Sicherstellung

(1) Eine ungültige eID-Karte kann eingezogen werden.

(2) Eine eID-Karte kann sichergestellt werden, wenn

1. eine Person sie unberechtigt besitzt oder
2. Tatsachen die Annahme rechtfertigen, dass die eID-Karte ungültig ist.

(3) Eine Sicherstellung oder Einziehung ist schriftlich zu bestätigen.

(4) Widerspruch und Anfechtungsklage haben in den Fällen der Absätze 1 und 2 keine aufschiebende Wirkung.

Abschnitt 7
Gebühren und Auslagen; Bußgeldvorschriften

§ 23 Gebühren und Auslagen; Verordnungsermächtigung

(1) Für individuell zurechenbare öffentliche Leistungen nach diesem Gesetz erheben die eID-Karte-Behörden Gebühren und Auslagen nach den Absätzen 2 und 3.

(2) Die Gebühr soll die mit der individuell zurechenbaren öffentlichen Leistung verbundenen Kosten aller an der Leistung Beteiligten decken. In die Gebühr sind die mit der Leistung regelmäßig verbundenen Auslagen einzubeziehen. Zur Ermittlung der Gebühr sind die Kosten, die nach betriebswirtschaftlichen Grundsätzen als Einzel- und Gemeinkosten zurechenbar und ansatzfähig sind, insbesondere Personal- und Sachkosten sowie kalkulatorische Kosten, zu Grunde zu legen. Zu den Gemeinkosten zählen auch die Kosten der Rechts- und Fachaufsicht. Grundlage der Gebührenermittlung nach den Sätzen 1 bis 4 sind Kosten, die in der Gesamtheit der Länder mit der jeweiligen Leistung verbunden sind. § 3 Absatz 1 und 2, die §§ 5 bis 7, 9 Absatz 3 bis 6 und die §§ 10 bis 12 des Bundesgebührengesetzes gelten entsprechend.

(3) Das Bundesministerium des Innern und für Heimat wird ermächtigt, für den Bereich der Landesverwaltung durch Rechtsverordnung mit Zustimmung des Bundesrates die gebührenpflichtigen Tatbestände, die Gebührenhöhe und die Auslagenerstattung näher zu bestimmen.

(4) Das Auswärtige Amt kann durch Besondere Gebührenverordnung nach § 22 Absatz 4 des Bundesgebührengesetzes bestimmen, dass von den Auslandsvertretungen der Bundesrepublik Deutschland für individuell zurechenbare öffentliche Leistungen nach diesem Gesetz und den auf diesem Gesetz beruhenden Rechtsverordnungen zum Ausgleich von Kaufkraftunterschieden ein Zuschlag erhoben wird. Der Zuschlag kann bis zu 300 Prozent betragen.

§ 24 Bußgeldvorschriften

(1) Ordnungswidrig handelt, wer

1. entgegen § 8 Absatz 2 Satz 1 eine Angabe nicht richtig macht,
2. entgegen § 12 Absatz 2 einen elektronischen Identitätsnachweis nutzt oder
3. entgegen § 20 Absatz 1 Nummer 3 eine Anzeige nicht oder nicht rechtzeitig erstattet.

(2) Die Ordnungswidrigkeit kann in den Fällen des Absatzes 1 Nummer 2 mit einer Geldbuße bis zu dreißigtausend Euro und in den übrigen Fällen mit einer Geldbuße bis zu dreitausend Euro geahndet werden.

§ 25 Verordnungsermächtigung

Das Bundesministerium des Innern und für Heimat wird ermächtigt, im Benehmen mit dem Auswärtigen Amt und mit Zustimmung des Bundesrates durch Rechtsverordnung

1. das Muster der eID-Karte zu bestimmen,
2. den Zugriffsschutz auf die im Chip abgelegten Daten zu regeln,
3. die Einzelheiten des Antragsverfahrens zu regeln,
4. die Einzelheiten über das Verfahren der Übermittlung sämtlicher Antragsdaten von den eID-Karte-Behörden an den Kartenhersteller zu regeln,
5. die Herstellung der eID-Karte und die Übermittlung und Übergabe von Geheimnummer, Entsperrnummer und Sperrkennwort zu regeln,
6. Einzelheiten der Aushändigung und den Versand der eID-Karte zu regeln,
7. die Änderung von Daten der eID-Karte wie den Namen oder die Anschrift, einschließlich des Verfahrens der Änderung der Anschrift auf dem elektronischen Speicher- und Verarbeitungsmedium nach einer elektronischen Anmeldung gemäß § 23a des Bundesmeldegesetzes, zu regeln,
8. die Einzelheiten zur Nutzung des elektronischen Identitätsnachweises und des Vor-Ort-Auslesens zu regeln,

8a. die Einzelheiten zur Einrichtung und zur Nutzung des elektronischen Identitätsnachweises mit einem mobilen Endgerät, sowie zu den technischen Anforderungen an mobile Endgeräte nach § 2 Absatz 11 zu regeln,

9. die Einzelheiten
   a) der Geheimnummer, einschließlich des Verfahrens des Neusetzens der Geheimnummer durch den Kartenhersteller nach elektronisch gestelltem Antrag,
   b) der Sperrung und Entsperrung sowie
   c) der Speicherung und Löschung der Sperrmerkmale und des Sperrkennworts

   festzulegen,
10. die sicherheitstechnischen Rahmenbedingungen festzulegen, die vorliegen müssen, damit öffentliche und private Stellen ein Benutzerkonto nach § 14 in Verbindung mit § 19 Absatz 5 des Personalausweisgesetzes anlegen und betreiben dürfen,
11. die Einzelheiten der Vergabe der Berechtigungen und der Berechtigungszertifikate festzulegen,
12. die Einzelheiten zur Durchführung von automatisierten Mitteilungen oder automatisierten Abrufen nach § 19a sowie zur Form und zum Inhalt der zu übermittelnden Daten festzulegen.

In einer Rechtsverordnung nach Satz 1 Nummer 8a sind Regelungen zu Maßnahmen gegen eine missbräuchliche Verwendung bei der Einrichtung eines elektronischen Identitätsnachweises mit einem mobilen Endgerät vorzusehen.

§ 26 Übergangsvorschrift

Abweichend von § 6 Absatz 1 Nummer 2 und § 7 Absatz 2 ist bis zum 31. Oktober 2021 für Antragsberechtigte mit gewöhnlichem Aufenthalt im Ausland diejenige Behörde nach § 6 Absatz 1 Nummer 1 zuständig, in deren Bezirk sich der Antragsberechtigte vorübergehend aufhält.

VERORDNUNG (EU) Nr. 910/2014 DES EUROPÄISCHEN PARLAMENTS UND DES RATES

vom 23. Juli 2014

über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG

KAPITEL I
ALLGEMEINE BESTIMMUNGEN

KAPITEL II
ELEKTRONISCHE IDENTIFIZIERUNG

ABSCHNITT 1
europäische brieftasche für die digitale identität

ABSCHNITT 2
elektronische identifizierungssysteme

[Vom Abdruck der Erwägungsgründe wurde abgesehen.]

KAPITEL I
ALLGEMEINE BESTIMMUNGEN

Artikel 1
Gegenstand

Diese Verordnung dient dem ordnungsgemäßen Funktionieren des Binnenmarkts und der Gewährleistung eines angemessenen Sicherheitsniveaus bei unionsweit genutzten elektronischen Identifizierungsmitteln und Vertrauensdiensten, um natürlichen und juristischen Personen die Ausübung des Rechts auf sichere Teilhabe an der digitalen Gesellschaft und auf Zugang zu öffentlichen und privaten Online-Diensten in der gesamten Union zu ermöglichen und zu erleichtern. Dazu wird in dieser Verordnung Folgendes festgelegt:

a) die Bedingungen, unter denen die Mitgliedstaaten elektronische Identifizierungsmittel für natürliche und juristische Personen, die einem notifizierten elektronischen Identifizierungssystem eines anderen Mitgliedstaats unterliegen anerkennen, sowie europäische Brieftaschen für die Digitale Identität bereitstellen und anerkennen müssen;

b) Vorschriften für Vertrauensdienste und insbesondere für elektronische Transaktionen;

c) ein Rechtsrahmen für elektronische Signaturen, elektronische Siegel, elektronische Zeitstempel, elektronische Dokumente, Dienste für die Zustellung elektronischer Einschreiben, Zertifizierungsdienste für die Website-Authentifizierung, die elektronische Archivierung, die elektronische Attributsbescheinigung, elektronische Signaturerstellungseinheiten, elektronische Siegelerstellungseinheiten und elektronische Journale.

Artikel 2
Anwendungsbereich

(1) Diese Verordnung gilt für von einem Mitgliedstaat notifizierte elektronische Identifizierungssysteme, für von einem Mitgliedstaat bereitgestellte europäische Brieftaschen für die Digitale Identität und für in der Union niedergelassene Vertrauensdiensteanbieter.

(2) Diese Verordnung findet keine Anwendung auf die Erbringung von Vertrauensdiensten, die ausschließlich innerhalb geschlossener Systeme aufgrund von nationalem Recht oder von Vereinbarungen zwischen einem bestimmten Kreis von Beteiligten verwendet werden.

(3) Diese Verordnung berührt nicht das Unionsrecht oder das nationale Recht in Bezug auf den Abschluss und die Gültigkeit von Verträgen oder andere rechtliche oder verfahrensmäßige Formvorschriften oder sektorspezifische Formvorschriften.

(4) Die vorliegende Verordnung gilt unbeschadet der Verordnung (EG) 2016/679 des Europäischen Parlaments und des Rates.

Artikel 3
Begriffsbestimmungen

Für die Zwecke dieser Verordnung gelten die folgenden Begriffsbestimmungen:

1. „Elektronische Identifizierung" ist der Prozess der Verwendung von Personenidentifizierungsdaten in elektronischer Form, die eine natürliche oder juristische Person oder eine natürliche Person, die eine andere natürliche Person oder eine juristische Person vertritt, eindeutig repräsentieren.

2. „Elektronisches Identifizierungsmittel" ist eine materielle und/oder immaterielle Einheit, die Personenidentifizierungsdaten enthält und zur Authentifizierung bei Online-Diensten oder gegebenenfalls bei Offline-Diensten verwendet wird.

3. „Personenidentifizierungsdaten" sind ein Datensatz, der im Einklang mit dem Unionsrecht oder dem nationalen Recht ausgestellt wird und es ermöglicht, die Identität einer natürlichen oder juristischen Person oder einer natürlichen Person, die eine andere natürliche Person oder eine juristische Person vertritt, festzustellen.

4. „Elektronisches Identifizierungssystem" ist ein System für die elektronische Identifizierung, in dessen Rahmen natürlichen oder juristischen Personen oder natürlichen Personen, die andere natürliche Personen oder juristische Personen vertreten, elektronische Identifizierungsmittel ausgestellt werden.

5. „Authentifizierung" ist ein elektronischer Prozess, der die Bestätigung der elektronischen Identifizierung einer natürlichen oder juristischen Person oder die Bestätigung des Ursprungs und der Unversehrtheit von Daten in elektronischer Form ermöglicht.

5a. „Nutzer" ist eine natürliche oder juristische Person oder eine natürliche Person, die eine andere natürliche Person oder eine juristische Person vertritt, die gemäß dieser Verordnung bereitgestellte Vertrauensdienste oder elektronische Identifizierungsmittel verwendet.

6. „Vertrauender Beteiligter“ ist eine natürliche oder juristische Person, die auf eine elektronische Identifizierung, europäische Brieftaschen für die Digitale Identität oder andere Mittel zur elektronischen Identifizierung oder einen Vertrauensdienst vertraut.

7. „Öffentliche Stelle“ bezeichnet einen Staat, eine Gebietskörperschaft, eine Einrichtung des öffentlichen Rechts oder einen Verband, der aus einer oder mehreren dieser Körperschaften oder Einrichtungen des öffentlichen Rechts besteht, oder eine private Einrichtung, die von mindestens einer dieser Körperschaften, Einrichtungen oder Verbände mit der Erbringung von öffentlichen Dienstleistungen beauftragt wurde, wenn sie im Rahmen dieses Auftrags handelt.

8. „Einrichtung des öffentlichen Rechts“ ist eine Einrichtung nach Artikel 2 Absatz 1 Nummer 4 der Richtlinie 2014/24/EU des Europäischen Parlaments und des Rates.

9. „Unterzeichner“ ist eine natürliche Person, die eine elektronische Signatur erstellt.

10. „Elektronische Signatur“ sind Daten in elektronischer Form, die anderen elektronischen Daten beigefügt oder logisch mit ihnen verbunden werden und die der Unterzeichner zum Unterzeichnen verwendet.

11. „Fortgeschrittene elektronische Signatur“ ist eine elektronische Signatur, die die Anforderungen des Artikels 26 erfüllt.

12. „Qualifizierte elektronische Signatur“ ist eine fortgeschrittene elektronische Signatur, die von einer qualifizierten elektronischen Signaturerstellungseinheit erstellt wurde und auf einem qualifizierten Zertifikat für elektronische Signaturen beruht.

13. „Elektronische Signaturerstellungsdaten“ sind eindeutige Daten, die vom Unterzeichner zum Erstellen einer elektronischen Signatur verwendet werden.

14. „Zertifikat für elektronische Signaturen“ ist eine elektronische Bescheinigung, die elektronische Signaturvalidierungsdaten mit einer natürlichen Person verknüpft und die mindestens den Namen oder das Pseudonym dieser Person bestätigt.

15. „Qualifiziertes Zertifikat für elektronische Signaturen“ ist ein von einem qualifizierten Vertrauensdiensteanbieter ausgestelltes Zertifikat für elektronische Signaturen, das die Anforderungen des Anhangs I erfüllt.

16. „Vertrauensdienst“ ist ein elektronischer Dienst, der in der Regel gegen Entgelt erbracht wird und aus irgendeiner der folgenden Tätigkeiten besteht:

    a) Ausstellung von Zertifikaten für elektronische Signaturen, von Zertifikaten für elektronische Siegel, von Zertifikaten für die Website-Authentifizierung oder von Zertifikaten für die Erbringung anderer Vertrauensdienste;

    b) Validierung von Zertifikaten für elektronische Signaturen, Zertifikaten für elektronische Siegel, Zertifikaten für die Website-Authentifizierung oder Zertifikaten für die Erbringung anderer Vertrauensdienste;

    c) Erstellung elektronischer Signaturen oder elektronischer Siegel;

    d) Validierung elektronischer Signaturen oder elektronischer Siegel;

e) Bewahrung von elektronischen Signaturen, elektronischen Siegeln, Zertifikaten für elektronische Signaturen oder Zertifikaten für elektronische Siegel;

f) Verwaltung elektronischer Fernsignaturerstellungseinheiten oder elektronischer Fernsiegelerstellungseinheiten;

g) Ausstellung elektronischer Attributsbescheinigungen;

h) Validierung elektronischer Attributsbescheinigungen;

i) Erstellung elektronischer Zeitstempel;

j) Validierung elektronischer Zeitstempel;

k) Erbringung von Diensten für die Zustellung elektronischer Einschreiben;

l) Validierung von durch Dienste für die Zustellung elektronischer Einschreiben übermittelten Daten und damit zusammenhängenden Nachweisen;

m) elektronische Archivierung elektronischer Daten und elektronischer Dokumente;

n) Aufzeichnung elektronischer Daten in einem elektronischen Journal.

17. „Qualifizierter Vertrauensdienst“ ist ein Vertrauensdienst, der die einschlägigen Anforderungen dieser Verordnung erfüllt.

18. „Konformitätsbewertungsstelle“ ist eine Konformitätsbewertungsstelle im Sinne der Begriffsbestimmung in Artikel 2 Nummer 13 der Verordnung (EG) Nr. 765/2008, die gemäß jener Verordnung als zur Durchführung der Konformitätsbewertung qualifizierter Vertrauensdiensteanbieter und der von ihnen erbrachten qualifizierten Vertrauensdienste oder zur Durchführung der Zertifizierung von europäischen Brieftaschen für die Digitale Identität oder elektronischen Identifizierungsmitteln befähigte Stelle akkreditiert worden ist.

19. „Vertrauensdiensteanbieter“ ist eine natürliche oder juristische Person, die einen oder mehrere Vertrauensdienste als qualifizierter oder nichtqualifizierter Vertrauensdiensteanbieter erbringt.

20. „Qualifizierter Vertrauensdiensteanbieter“ ist ein Vertrauensdiensteanbieter, der einen oder mehrere qualifizierte Vertrauensdienste erbringt und dem von der Aufsichtsstelle der Status eines qualifizierten Anbieters verliehen wurde.

21. „Produkt“ bezeichnet Hardware, Software oder spezifische Komponenten von Hard- oder Software, die zur Erbringung von elektronischen Identifizierungsdiensten und Vertrauensdiensten bestimmt sind.

22. „Elektronische Signaturerstellungseinheit“ ist eine konfigurierte Software oder Hardware, die zum Erstellen einer elektronischen Signatur verwendet wird.

23. „Qualifizierte elektronische Signaturerstellungseinheit“ ist eine elektronische Signaturerstellungseinheit, die die Anforderungen des Anhangs II erfüllt.

23a. „Qualifizierte elektronische Fernsignaturerstellungseinheit“ ist eine qualifizierte elektronische Signaturerstellungseinheit, die von einem qualifizierten Vertrauensdiensteanbieter gemäß Artikel 29a im Namen eines Unterzeichners verwaltet wird.

23b. „Qualifizierte elektronische Fernsiegelerstellungseinheit“ ist eine qualifizierte elektronische Siegelerstellungseinheit, die von einem qualifizierten Vertrauensdiensteanbieter gemäß Artikel 39a im Namen eines Siegelerstellers verwaltet wird.

24. „Siegelersteller“ ist eine juristische Person, die ein elektronisches Siegel erstellt.

25. „Elektronisches Siegel“ sind Daten in elektronischer Form, die anderen Daten in elektronischer Form beigefügt oder logisch mit ihnen verbunden werden, um deren Ursprung und Unversehrtheit sicherzustellen.

26. „Fortgeschrittenes elektronisches Siegel“ ist ein elektronisches Siegel, das die Anforderungen des Artikels 36 erfüllt.

27. „Qualifiziertes elektronisches Siegel“ ist ein fortgeschrittenes elektronisches Siegel, das von einer qualifizierten elektronischen Siegelerstellungseinheit erstellt wird und auf einem qualifizierten Zertifikat für elektronische Siegel beruht.

28. „Elektronische Siegelerstellungsdaten“ sind eindeutige Daten, die vom Siegelersteller zum Erstellen eines elektronischen Siegels verwendet werden.

29. „Zertifikat für elektronische Siegel“ ist eine elektronische Bescheinigung, die elektronische Siegelvalidierungsdaten mit einer juristischen Person verknüpft und den Namen dieser Person bestätigt.

30. „Qualifiziertes Zertifikat für elektronische Siegel“ ist ein von einem qualifizierten Vertrauensdiensteanbieter ausgestelltes Zertifikat für elektronische Siegel, das die Anforderungen des Anhangs III erfüllt.

31. „Elektronische Siegelerstellungseinheit“ ist eine konfigurierte Software oder Hardware, die zum Erstellen eines elektronischen Siegels verwendet wird.

32. „Qualifizierte elektronische Siegelerstellungseinheit“ ist eine elektronische Siegelerstellungseinheit, die die Anforderungen des Anhangs II sinngemäß erfüllt.

33. „Elektronischer Zeitstempel“ bezeichnet Daten in elektronischer Form, die andere Daten in elektronischer Form mit einem bestimmten Zeitpunkt verknüpfen und dadurch den Nachweis erbringen, dass diese anderen Daten zu diesem Zeitpunkt vorhanden waren.

34. „Qualifizierter elektronischer Zeitstempel“ ist ein elektronischer Zeitstempel, der die Anforderungen des Artikels 42 erfüllt.

35. „Elektronisches Dokument“ ist jeder in elektronischer Form, insbesondere als Text-, Ton-, Bild- oder audiovisuelle Aufzeichnung gespeicherte Inhalt.

36. „Dienst für die Zustellung elektronischer Einschreiben“ ist ein Dienst, der die Übermittlung von Daten zwischen Dritten mit elektronischen Mitteln ermöglicht und einen Nachweis der Handhabung der übermittelten Daten erbringt, darunter den Nachweis der Absendung und des Empfangs der Daten, und der die übertragenen Daten vor Verlust, Diebstahl, Beschädigung oder unbefugter Veränderung schützt.

37. „Qualifizierter Dienst für die Zustellung elektronischer Einschreiben“ ist ein Dienst für die Zustellung elektronischer Einschreiben, der die Anforderungen des Artikels 44 erfüllt.

38. „Zertifikat für die Website-Authentifizierung“ ist eine elektronische Bescheinigung, die die Authentifizierung einer Website ermöglicht und die Website mit der natürlichen oder juristischen Person verknüpft, der das Zertifikat ausgestellt wurde.

39. „Qualifiziertes Zertifikat für die Website-Authentifizierung“ ist ein von einem qualifizierten Vertrauensdiensteanbieter ausgestelltes Zertifikat für Website-Authentifizierung, das die Anforderungen des Anhangs IV erfüllt.

40. „Validierungsdaten“ sind Daten, die zur Validierung einer elektronischen Signatur oder eines elektronischen Siegels verwendet werden.

41. „Validierung“ ist der Prozess der Überprüfung und Bestätigung der Gültigkeit von Daten in elektronischer Form gemäß den Anforderungen dieser Verordnung.

42. „Europäische Brieftasche für die Digitale Identität“ ist ein elektronisches Identifizierungsmittel, das es dem Nutzer ermöglicht, Personenidentifizierungsdaten und elektronische Attributsbescheinigungen sicher zu speichern, zu verwalten und zu validieren, um sie vertrauenden Beteiligten und anderen Nutzern von europäischen Brieftaschen für die Digitale Identität zu präsentieren und mittels qualifizierter elektronischer Signaturen zu unterzeichnen oder mittels qualifizierter elektronischer Siegel zu besiegeln.

43. „Attribut“ ist ein Merkmal, eine Qualität, ein Recht oder die Erlaubnis einer natürlichen oder juristischen Person oder eines Objekts.

44. „Elektronische Attributsbescheinigung“ ist eine in elektronischer Form vorliegende Bescheinigung, die die Authentifizierung von Attributen ermöglicht.

45. „Qualifizierte elektronische Attributsbescheinigung“ ist eine von einem qualifizierten Vertrauensdiensteanbieter ausgestellte elektronische Attributsbescheinigung, die die Anforderungen des Anhangs V erfüllt.

46. „Von oder im Namen einer für eine authentische Quelle zuständigen öffentlichen Stelle ausgestellte elektronische Attributsbescheinigung“ ist eine elektronische Attributsbescheinigung, die gemäß Artikel 45f und Anhang VII von einer öffentlichen Stelle, die für eine authentische Quelle zuständig ist, oder von einer öffentlichen Stelle, die von dem Mitgliedstaat dafür benannt wurde, solche Attributsbescheinigungen im Namen der öffentlichen Stellen, die für authentische Quellen zuständig sind, auszustellen, ausgestellt wurde.

47. „Authentische Quelle“ ist ein Datenspeicher oder ein System, der bzw. das unter der Verantwortung einer öffentlichen Stelle oder privaten Einrichtung betrieben wird, Attribute zu einer natürlichen oder juristischen Person oder zu einem Objekt enthält und bereitstellt und als eine primäre Quelle für diese Informationen gilt oder im Einklang mit Unionsrecht oder nationalem Recht — einschließlich der Verwaltungspraxis — als authentisch anerkannt wird.

48. „Elektronische Archivierung“ ist ein Dienst für die Entgegennahme, die Speicherung, den Abruf und die Löschung elektronischer Daten und elektronischer Dokumente, der ihre Dauerhaftigkeit und Lesbarkeit gewährleistet sowie ihre Unversehrtheit, Vertraulichkeit und den Nachweis ihrer Herkunft während des gesamten Bewahrungszeitraums erhält.

49. „Qualifizierter elektronischer Archivierungsdienst“ ist ein elektronischer Archivierungsdienst, der von einem qualifizierten Vertrauensdiensteanbieter erbracht wird und der die Anforderungen des Artikels 45j erfüllt.

50. „Vertrauenssiegel der europäischen Brieftasche für die Digitale Identität“ ist eine nachprüfbare, einfache und erkennbare sowie eindeutig kommunizierte Angabe, dass eine europäische Brieftasche für die Digitale Identität gemäß dieser Verordnung bereitgestellt wurde.

51. „Starke Nutzerauthentifizierung“ ist eine Authentifizierung unter Heranziehung von mindestens zwei Authentifizierungsfaktoren aus verschiedenen Kategorien entweder von Wissen — etwas, das nur der Nutzer weiß –, Besitz — etwas, das nur der Nutzer besitzt — oder Inhärenz — etwas, das der Nutzer ist –, die insofern voneinander unabhängig sind, als die Nichterfüllung eines Kriteriums die Zuverlässigkeit der anderen nicht in Frage stellt, und die so konzipiert ist, dass die Vertraulichkeit der Authentifizierungsdaten geschützt ist.

52. „Elektronisches Journal“ ist eine Abfolge von Aufzeichnungen elektronischer Daten, die die Unversehrtheit dieser Aufzeichnungen und die Richtigkeit ihrer chronologischen Reihenfolge gewährleistet.

53. „Qualifiziertes elektronisches Journal“ ist ein elektronisches Journal, das von einem qualifizierten Vertrauensdiensteanbieter geführt wird und die Anforderungen des Artikels 45l erfüllt.

54. „Personenbezogene Daten“ sind alle Informationen im Sinne des Artikels 4 Nummer 1 der Verordnung (EU) 2016/679.

55. „Identitätsabgleich“ ist ein Verfahren, bei dem Personenidentifizierungsdaten oder elektronische Identifizierungsmittel mit einem bestehenden Konto, das derselben Person gehört, abgeglichen oder verknüpft werden.

56. „Datensatz“ sind elektronische Daten, die mit zugehörigen Metadaten zur Unterstützung der Verarbeitung der Daten erfasst werden.

57. „Offline-Modus“ — im Hinblick auf die Nutzung von europäischen Brieftaschen für die Digitale Identität — ist eine Interaktion zwischen einem Nutzer und einem Dritten an einem physischen Ort unter Nutzung von Technologien für kurze Distanzen (Proximity-Technologien), bei der für die Zwecke dieser Interaktion die europäische Brieftasche für die Digitale Identität nicht über elektronische Kommunikationsnetze auf internetbasierte Systeme zugreifen muss.

Artikel 4
Binnenmarktgrundsatz

(1) Die Erbringung von Vertrauensdiensten im Gebiet eines Mitgliedstaats durch einen in einem anderen Mitgliedstaat niedergelassenen Vertrauensdiensteanbieter unterliegt keinen Beschränkungen aus Gründen, die in den Anwendungsbereich dieser Verordnung fallen.

(2) Produkte und Vertrauensdienste, die dieser Verordnung entsprechen, dürfen im Binnenmarkt frei verkehren.

Artikel 5
Pseudonyme bei elektronischen Transaktionen

Unbeschadet spezifischer Vorschriften des Unionsrechts oder des nationalen Rechts, wonach die Nutzer sich identifizieren müssen, oder der Rechtswirkungen, die Pseudonyme nach nationalem Recht haben, darf die Benutzung von vom Nutzer gewählten Pseudonymen nicht untersagt werden.

KAPITEL II
ELEKTRONISCHE IDENTIFIZIERUNG

ABSCHNITT 1
europäische brieftasche für die digitale identität

Artikel 5a
Europäische Brieftaschen für die Digitale Identität

(1) Damit alle natürlichen und juristischen Personen in der Union einen sicheren, vertrauenswürdigen und nahtlosen grenzüberschreitenden Zugang zu öffentlichen und privaten Diensten erhalten –unter Wahrung der vollständigen Kontrolle über ihre Daten –, stellt jeder Mitgliedstaat innerhalb von 24 Monaten nach dem Tag des Inkrafttretens der in Absatz 23 und Artikel 5c Absatz 6 genannten Durchführungsrechtsakte mindestens eine europäische Brieftasche für die Digitale Identität bereit.

(2) Europäische Brieftaschen für die Digitale Identität werden auf eine der folgenden Art und Weisen bereitgestellt:

a) unmittelbar von einem Mitgliedstaat,

b) im Auftrag eines Mitgliedstaats,

c) unabhängig von einem Mitgliedstaat, aber von diesem Mitgliedstaat anerkannt.

(3) Für den Quellcode der Anwendungssoftwarekomponenten von europäischen Brieftaschen für die Digitale Identität muss eine Open-Source-Lizenz gelten. Die Mitgliedstaaten können vorsehen, dass in hinreichend begründeten Fällen der Quellcode bestimmter Komponenten, die nicht auf den Geräten des Nutzers installiert sind, nicht offengelegt wird.

(4) Europäische Brieftaschen für die Digitale Identität müssen dem Nutzer Folgendes auf eine nutzerfreundliche und für ihn transparente und nachvollziehbare Weise ermöglichen:

a) das sichere Anfordern, Erhalten, Auswählen, Kombinieren, Speichern, Löschen, Weitergeben und Vorweisen — unter alleiniger Kontrolle durch den Nutzer — elektronischer Attributsbescheinigungen und von Personenidentifizierungsdaten und, falls anwendbar, in Kombination mit elektronischen Attributsbescheinigungen, gegenüber vertrauenden Beteiligten, um sich online und, gegebenenfalls, offline für den Zugang zu öffentlichen und privaten Diensten zu authentifizieren, bei gleichzeitiger Sicherstellung, dass eine selektive Offenlegung von Daten möglich ist;

b) das Generieren von Pseudonymen und deren verschlüsselte und lokale Speicherung in der europäischen Brieftasche für die Digitale Identität;

c) die sichere Authentifizierung der europäischen Brieftasche für die Digitale Identität einer anderen Person und das Empfangen und Austauschen — zwischen den beiden europäischen Brieftaschen für die Digitale Identität — von Personenidentifizierungsdaten und elektronischen Attributsbescheinigungen;

d) den Zugang zur Protokollierung aller über die europäische Brieftasche für die Digitale Identität vorgenommenen Transaktionen über ein gemeinsames Dashboard, sodass der Nutzer in der Lage ist,

   i) eine aktuelle Auflistung der vertrauenden Beteiligten, mit denen der Nutzer eine Verbindung aufgebaut hat, und, falls anwendbar, alle weitergegebenen Daten einzusehen;

   ii) einen vertrauenden Beteiligten auf einfache Weise um die Löschung personenbezogener Daten gemäß Artikel 17 der Verordnung (EU) 2016/679 durch einen vertrauenden Beteiligten zu ersuchen;

   iii) eine Meldung auf einfache Weise an die zuständige nationale Datenschutzbehörde, wenn ein mutmaßlich unrechtmäßiges oder verdächtiges Ersuchen um Daten eingegangen ist;

e) das Unterzeichnen mit qualifizierten elektronischen Signaturen oder das Siegeln mit qualifizierten elektronischen Siegeln;

f) – soweit technisch möglich — das Herunterladen von Nutzerdaten, elektronischen Attributsbescheinigungen und Konfigurationen;

g) die Ausübung der Rechte des Nutzers auf Datenübertragbarkeit.

(5) Europäische Brieftaschen für die Digitale Identität müssen insbesondere

a) gemeinsame Protokolle und Schnittstellen für Folgendes unterstützen:

   i) die Ausstellung von Personenidentifizierungsdaten, qualifizierten und nicht qualifizierten elektronischen Attributsbescheinigungen oder qualifizierten und nicht qualifizierten Zertifikaten für die europäische Brieftasche für die Digitale Identität;

   ii) – bei vertrauenden Beteiligten — das Anfordern und Validieren von Personenidentifizierungsdaten und elektronische Attributsbescheinigungen;

   iii) das Weitergeben und Vorweisen von Personenidentifizierungsdaten oder elektronischen Attributsbescheinigungen oder selektiv offengelegten zugehörigen Daten online und, gegebenenfalls, offline — bei vertrauenden Beteiligten;

   iv) die Interaktion mit der europäischen Brieftasche für die Digitale Identität durch den Nutzer und die Anzeige eines ‚EU-Vertrauenssiegels der europäischen Brieftasche für die Digitale Identität';

   v) die sichere Einbindung des Nutzers durch die Verwendung eines elektronischen Identifizierungsmittels im Einklang mit Artikel 5a Absatz 24;

   vi) die Interaktion zwischen den europäischen Brieftaschen für die Digitale Identität zweier Personen für die Zwecke des sicheren Empfangens, Validierens und Austauschens — zwischen den beiden europäischen Brieftа-

schen für die Digitale Identität — von Personenidentifizierungsdaten und elektronischen Attributsbescheinigungen;

vii) die Authentifizierung und Identifizierung vertrauender Beteiligter durch Einführung von Authentifizierungsmechanismen gemäß Artikel 5b;

viii) – für vertrauende Beteiligte — die Überprüfung der Echtheit und Gültigkeit von europäischen Brieftaschen für die Digitale Identität;

ix) das Ersuchen an einen vertrauenden Beteiligten um die Löschung personenbezogener Daten gemäß Artikel 17 der Verordnung (EU) 2016/679;

x) die Meldung — durch einen vertrauenden Beteiligten — an die zuständige nationale Datenschutzbehörde, wenn eine mutmaßlich rechtswidrige oder verdächtige Anforderung von Daten eingegangen ist;

xi) die Erstellung qualifizierter elektronischer Signaturen oder elektronischer Siegel durch qualifizierte elektronische Signatur- oder Siegelerstellungseinheiten;

b) bewirken, dass Vertrauensdiensteanbietern, die elektronische Attributsbescheinigungen ausstellen, nach der Ausstellung dieser Attribute keinerlei Informationen über die Verwendung dieser elektronischen Bescheinigungen zur Verfügung gestellt werden;

c) sicherstellen, dass die vertrauenden Beteiligten durch die Einführung von Authentifizierungsmechanismen im Einklang mit Artikel 5b authentifiziert und identifiziert werden können;

d) die Anforderungen des Artikels 8 in Bezug auf die Sicherheitsstufe ‚hoch' erfüllen, insbesondere bezüglich der Anforderungen an Identitätsnachweis und Identitätsüberprüfung und an die Verwaltung und Authentifizierung elektronischer Identifizierungsmittel;

e) im Falle der elektronischen Attributsbescheinigung mit eingebetteten Offenlegungsregelungen den geeigneten Mechanismus einführen, um den Nutzer darüber zu unterrichten, dass der vertrauende Beteiligte oder der Nutzer der europäischen Brieftasche für die Digitale Identität, der um diese elektronische Attributsbescheinigung ersucht, über die Erlaubnis verfügt, auf diese Bescheinigung zuzugreifen;

f) gewährleisten, dass Personenidentifizierungsdaten, die über das elektronische Identifizierungssystem, in dessen Rahmen die europäische Brieftasche für die Digitale Identität bereitgestellt wird, eindeutig die mit der betreffenden europäischen Brieftasche für die Digitale Identität verknüpfte natürliche Person, juristische Person oder die die natürliche oder juristische Person vertretende Person repräsentieren;

g) allen natürlichen Personen die Möglichkeit bieten, mittels qualifizierter elektronischer Signaturen kostenlos zu unterzeichnen.

Ungeachtet des Unterabsatzes 1 Buchstabe g können die Mitgliedstaaten verhältnismäßige Maßnahmen vorsehen, um sicherzustellen, dass die kostenlose Verwendung qualifizierter elektronischer Signaturen durch natürliche Personen auf nichtgewerbliche Zwecke beschränkt wird.

(6) Die Mitgliedstaaten setzen die Nutzer unverzüglich von Sicherheitsverletzungen in Kenntnis, die ihre europäische Brieftasche für die Digitale Identität oder deren Inhalt möglicherweise vollständig oder teilweise kompromittiert haben könnten, und zwar insbesondere dann, wenn ihre europäische Brieftasche für die Digitale Identität gemäß Artikel 5e ausgesetzt oder widerrufen wurde;

(7) Unbeschadet des Artikels 5f können die Mitgliedstaaten im Einklang mit dem nationalen Recht zusätzliche Funktionen von europäischen Brieftaschen für die Digitale Identität vorsehen, einschließlich der Interoperabilität mit bestehenden nationalen elektronischen Identifikationsmitteln. Diese zusätzlichen Funktionen müssen dem vorliegenden Artikel entsprechen.

(8) Die Mitgliedstaaten stellen kostenlose Validierungsmechanismen bereit, um

a) sicherzustellen, dass die Echtheit und Gültigkeit der europäischen Brieftaschen für die Digitale Identität überprüft werden kann,

b) es Nutzern zu ermöglichen, die Echtheit und Gültigkeit der Identität von gemäß Artikel 5b registrierten vertrauenden Beteiligten zu überprüfen.

(9) Die Mitgliedstaaten tragen dafür Sorge, dass die Gültigkeit der europäischen Brieftasche für die Digitale Identität unter den folgenden Umständen widerrufen werden kann:

a) auf ausdrückliches Ersuchen des Nutzers,

b) wenn die Sicherheit der europäischen Brieftasche für die Digitale Identität kompromittiert worden ist,

c) nach dem Tod des Nutzers oder der Einstellung der Tätigkeit der juristischen Person.

(10) Anbieter von europäischen Brieftaschen für die Digitale Identität tragen dafür Sorge, dass Nutzer auf einfache Weise technische Unterstützung anfordern und technische Probleme oder andere Vorfälle, die negative Auswirkungen auf die Nutzung von europäischen Brieftaschen für die Digitale Identität haben, melden können.

(11) Europäische Brieftaschen für die Digitale Identität werden im Rahmen eines notifizierten elektronischen Identifizierungssystems mit der Sicherheitsstufe ‚hoch' bereitgestellt.

(12) Europäische Brieftaschen für die Digitale Identität sind mit ‚konzeptintegrierter Sicherheit' auszustatten.

(13) Die Ausstellung, die Verwendung und der Widerruf von europäischen Brieftaschen für die Digitale Identität erfolgt für alle natürlichen Personen kostenlos.

(14) Die Nutzer haben die uneingeschränkte Kontrolle über die Nutzung ihrer europäischen Brieftasche für die Digitale Identität und über die darin enthaltenen Daten. Der Anbieter der europäischen Brieftasche für die Digitale Identität sammelt weder Informationen über die Nutzung der europäischen Brieftasche für die Digitale Identität, die für die Erbringung der mit der europäischen Brieftasche für die Digitale Identität verbundenen Dienste nicht erforderlich sind, noch kombiniert er Personenidentifizierungsdaten oder andere gespeicherte oder im Zusammenhang mit der Verwendung der europäischen Brieftasche für die Digitale Identität stehende personenbezogene Daten mit personenbezogenen Daten aus anderen vom Anbieter angebotenen Diensten oder aus Diensten Dritter, die für die Bereitstellung der mit der europäischen Brieftasche für die Digitale Identität verbundenen Dienste nicht

erforderlich sind, es sei denn, der Nutzer hat dies ausdrücklich anders verlangt. Personenbezogene Daten in Bezug auf die Bereitstellung der europäischen Brieftasche für die Digitale Identität werden vom Anbieter der europäischen Brieftasche für die Digitale Identität von allen anderen gespeicherten Daten logisch getrennt gehalten. Wird die europäischen Brieftasche für die Digitale Identität von privaten Beteiligten gemäß Absatz 2 Buchstaben b und c des vorliegenden Artikels bereitgestellt, so gelten sinngemäß die Bestimmungen von Artikel 45h Absatz 3.

(15) Die Nutzung von europäischen Brieftaschen für die Digitale Identität ist freiwillig. Natürliche oder juristische Personen, die die europäische Brieftasche für die Digitale Identität nicht nutzen, dürfen in ihrem Zugang zu öffentlichen und privaten Diensten und zum Arbeitsmarkt sowie in ihrer unternehmerischen Freiheit in keiner Weise eingeschränkt oder benachteiligt werden. Der Zugang zu öffentlichen und privaten Diensten muss weiterhin über andere bestehende Identifizierungs- und Authentifizierungsmittel möglich sein.

(16) Der technische Rahmen der europäischen Brieftasche für die Digitale Identität

a) darf es Anbietern elektronischer Attributsbescheinigungen oder anderen Parteien nach Ausstellung der Attributsbescheinigung nicht erlauben, Daten zu erhalten, die es ermöglichen, Transaktionen oder Nutzerverhalten zu verfolgen, zu verknüpfen, zu korrelieren oder Kenntnisse über Transaktionen oder das Nutzerverhalten anderweitig zu erlangen, es sei denn, der Nutzer hat dies ausdrücklich genehmigt;

b) muss technische Verfahren zum Schutz der Privatsphäre ermöglichen, die die Unverknüpfbarkeit gewährleisten, wenn die Attributsbescheinigung keine Identifizierung des Nutzers erfordert.

(17) Jede Verarbeitung personenbezogener Daten durch die Mitgliedstaaten oder in deren Namen durch Stellen oder Parteien, die für die Bereitstellung von europäischen Brieftaschen für die Digitale Identität als elektronisches Identifizierungsmittel verantwortlich sind, erfolgt im Einklang mit geeigneten und wirksamen Datenschutzmaßnahmen. Es ist nachzuweisen, dass diese Verarbeitungstätigkeiten mit der Verordnung (EU) 2016/679 im Einklang stehen. Die Mitgliedstaaten können nationale Bestimmungen erlassen, um die Anwendung dieser Maßnahmen zu präzisieren.

(18) Die Mitgliedstaaten übermitteln der Kommission unverzüglich Informationen über

a) die Stelle, die für die Erstellung und Führung dieser Liste der registrierten vertrauenden Parteien, die im Einklang mit Artikel 5b Absatz 5 auf europäische Brieftaschen für die Digitale Identität vertrauen, zuständig ist, und der Ort, an dem die Liste aufzufinden ist;

b) die Stellen, die für die Bereitstellung europäischer Brieftaschen für die Digitale Identität im Einklang mit Artikel 5a Absatz 1 zuständig sind;

c) die Stellen, die dafür zuständig sind, sicherzustellen, dass die Personenidentifizierungsdaten im Einklang mit Artikel 5a Absatz 5 Buchstabe f mit der europäischen Brieftasche für die Digitale Identität verknüpft werden.

d) den Mechanismus, der die Validierung der Personenidentifizierungsdaten gemäß Artikel 5a Absatz 5 Buchstabe f und der Identität der vertrauenden Beteiligten ermöglicht;

e) die Mechanismen zur Validierung der Echtheit und Gültigkeit von europäischen Brieftaschen für die Digitale Identität.

Die Kommission macht die gemäß dem ersten Unterabsatz übermittelten Informationen der Öffentlichkeit über einen gesicherten Kanal in elektronisch signierter oder besiegelter Form zugänglich, die für eine automatisierte Verarbeitung geeignet ist.

(19) Unbeschadet des Absatzes 22 des vorliegenden Artikels gilt Artikel 11 entsprechend für die europäische Brieftasche für die Digitale Identität.

(20) Artikel 24 Absatz 2 Buchstabe b und Buchstaben d bis h gilt entsprechend für Anbieter von europäischen Brieftaschen für die Digitale Identität.

(21) Europäische Brieftaschen für die Digitale Identität werden gemäß der Richtlinie (EU) 2019/882 des Europäischen Parlaments und des Rates für Menschen mit Behinderungen zur gleichberechtigen Nutzung zugänglich gemacht.

(22) Für die Zwecke der Bereitstellung von europäischen Brieftaschen für die Digitale Identität und der elektronischen Identifizierungssysteme, in deren Rahmen sie bereitgestellt werden, unterliegen sie nicht den Anforderungen der Artikel 7, 9, 10, 12 und 12a.

(23) Bis zum 21. November 2024 erstellt die Kommission im Wege von Durchführungsrechtsakten eine Liste von Referenzstandards und legt, sofern erforderlich, die Spezifikationen und Verfahren für die in den Absätzen 4, 5, 8 und 18 des vorliegenden Artikels genannten Anforderungen in Bezug auf die europäische Brieftasche für die Digitale Identität fest. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 48 Absatz 2 genannten Prüfverfahren erlassen.

(24) Die Kommission erstellt im Wege von Durchführungsrechtsakten eine Liste von Referenzstandards und legt erforderlichenfalls Spezifikationen und Verfahren fest, um die Einbindung von Nutzern in die europäische Brieftasche für die Digitale Identität unter Nutzung entweder von elektronischen Identifizierungsmitteln der Sicherheitsstufe ‚hoch' oder von elektronischen Identifizierungsmitteln der Sicherheitsstufe ‚substanziell'– in Verbindung mit zusätzlichen Verfahren der Ferneinbindung, die zusammen den Anforderungen der Sicherheitsstufe ‚hoch' entsprechen — zu erleichtern. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 48 Absatz 2 genannten Prüfverfahren erlassen.

Artikel 5b
Vertrauende Beteiligte der europäischen Brieftaschen für die Digitale Identität

(1) Wenn ein vertrauender Beteiligter beabsichtigt, für die Bereitstellung öffentlicher oder privater Dienste auf europäische Brieftaschen für die Digitale Identität zurückzugreifen, registriert sich der vertrauende Beteiligte in dem Mitgliedstaat, in dem er niedergelassen ist.

(2) Das Registrierungsverfahren muss kosteneffizient und dem Risiko angemessen sein. Der vertrauende Beteiligte stellt mindestens Folgendes bereit:

a) die für die Authentifizierung von europäischen Brieftaschen für die Digitale Identität erforderlichen Informationen, die mindestens Folgendes umfassen:

   i) den Mitgliedstaat, in dem der vertrauende Beteiligte niedergelassen ist, und

   ii) den Namen des vertrauenden Beteiligten und gegebenenfalls seine Registrierungsnummer, wie in einem amtlichen Verzeichnis angegeben, zusammen mit den Identifikationsdaten dieses amtlichen Registers;

b) die Kontaktangaben des vertrauenden Beteiligten;

c) die beabsichtigte Verwendung von europäischen Brieftaschen für die Digitale Identität, einschließlich einer Angabe der Daten, die der vertrauende Beteiligte von den Nutzern anfordern muss.

(3) Vertrauende Beteiligte dürfen von Nutzern keine anderen Daten als die Daten verlangen, die gemäß Absatz 2 Buchstabe c angegeben wurden.

(4) Die Absätze 1 und 2 lassen das Unionsrecht oder das nationale Recht, das auf die Erbringung bestimmter Dienste anwendbar ist, unberührt.

(5) Die Mitgliedstaaten machen die in Absatz 2 genannten Informationen der Öffentlichkeit online in elektronisch signierter oder besiegelter Form zugänglich, die für eine automatisierte Verarbeitung geeignet ist.

(6) Vertrauende Beteiligte, die gemäß diesem Artikel registriert wurden, unterrichten die Mitgliedstaaten unverzüglich über jede Änderung der gemäß Absatz 2 in der Registrierung bereitgestellten Informationen.

(7) Die Mitgliedstaaten stellen einen gemeinsamen Mechanismus zur Ermöglichung der Identifizierung und Authentifizierung der vertrauenden Beteiligten entsprechend Artikel 5a Absatz 5 Buchstabe c bereit.

(8) Beabsichtigen vertrauende Beteiligte, auf europäische Brieftaschen für die Digitale Identität zurückzugreifen, so müssen sie sich gegenüber dem Nutzer identifizieren.

(9) Die vertrauenden Beteiligten sind für die Durchführung des Verfahrens zur Authentifizierung und Validierung von Personenidentifizierungsdaten und elektronischen Attributsbescheinigungen, die über europäische Brieftaschen für die Digitale Identität verlangt werden, verantwortlich. Vertrauende Beteiligte dürfen die Verwendung von Pseudonymen nicht verweigern, wenn die Identifizierung des Nutzers nicht im Unionsrecht oder im nationalen Recht vorgeschrieben ist.

(10) Vermittler, die im Namen vertrauender Beteiligter handeln, sind als vertrauende Beteiligte zu betrachten und dürfen keine Daten über den Inhalt der Transaktion speichern.

(11) Bis zum 21. November 2024 legt die Kommission technische und betriebliche Spezifikationen und Verfahren für die Anforderungen der Absätze 2, 5 und 6 bis 9 dieses Artikels im Wege von Durchführungsrechtsakten zur Umsetzung der europäischen Brieftasche für die Digitale Identität gemäß Artikel 5a Absatz 23 fest. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 48 Absatz 2 genannten Prüfverfahren erlassen.

Artikel 5c
Zertifizierung der europäischen Brieftaschen für die Digitale Identität

(1) Die Konformität der europäischen Brieftaschen für die Digitale Identität und des elektronischen Identifizierungssystems, in dessen Rahmen sie bereitgestellt werden, mit den Anforderungen gemäß Artikel 5a Absätze 4, 5 und 8, der Anforderung der logischen Trennung gemäß Artikel 5a Absatz 14 und, falls anwendbar, mit den in Artikel 5a Absatz 24 genannten Standards und technischen Spezifikationen werden von den von den Mitgliedstaaten benannten Konformitätsbewertungsstellen zertifiziert.

(2) Die Zertifizierung der Konformität von europäischen Brieftaschen für die Digitale Identität mit den in Absatz 1 dieses Artikels genannten Anforderungen oder Teilen davon, die

für die Cybersicherheit relevant sind, erfolgt im Einklang mit den gemäß der Verordnung (EU) 2019/881 des Europäischen Parlaments und des Rates erlassenen und in den gemäß Absatz 6 des vorliegenden Artikels erlassenen Durchführungsrechtsakten genannten europäischen Schemata für die Cybersicherheitszertifizierung.

(3) Für Anforderungen in Absatz 1 des vorliegenden Artikels genannte Anforderungen, die nicht für die Cybersicherheit relevant sind, und auch für in Absatz 1 vorliegenden Artikels genannte Anforderungen, die für die Cybersicherheit relevant sind, soweit die in Absatz 2 vorliegenden Artikels genannten Schemata für die Cybersicherheitszertifizierung diese Cybersicherheitsanforderungen nicht oder nur teilweise abdecken, richten die Mitgliedstaaten für diese Anforderungen nationale Zertifizierungssysteme ein, die den Anforderungen entsprechen, die in den in Absatz 6 des vorliegenden Artikels genannten Durchführungsrechtsakten festgelegt sind. Die Mitgliedstaaten übermitteln die Entwürfe ihrer nationalen Schemata für die Zertifizierung der gemäß Artikel 46e Absatz 1 eingesetzten europäische Kooperationsgruppe für die digitale Identität (im Folgenden ‚Kooperationsgruppe'). Die Kooperationsgruppe kann Stellungnahmen und Empfehlungen abgeben.

(4) Die Zertifizierung gemäß Absatz 1 gilt für einen Zeitraum von bis zu fünf Jahren, sofern alle zwei Jahre eine Schwachstellenbeurteilung durchgeführt wird. Wird eine Schwachstelle festgestellt und nicht zeitnah behoben, so wird die Zertifizierung aufgehoben.

(5) Die Erfüllung der Anforderungen nach Artikel 5a der vorliegenden Verordnung in Bezug auf die Verarbeitung personenbezogener Daten kann gemäß der Verordnung (EU) 2016/679 zertifiziert werden.

(6) Bis zum 21. November 2024 erstellt die Kommission im Wege von Durchführungsrechtsakten eine Liste von Referenzstandards und legt erforderlichenfalls die Spezifikationen und Verfahren für die Zertifizierung von in den Absätzen 1, 2 und 3 des vorliegenden Artikels genannten europäischen Brieftaschen für die Digitale Identität fest. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 48 Absatz 2 genannten Prüfverfahren erlassen.

(7) Die Mitgliedstaaten teilen der Kommission die Namen und Anschriften der in Absatz 1 genannten Konformitätsbewertungsstellen mit. Die Kommission stellt diese Informationen allen Mitgliedstaaten zur Verfügung.

(8) Der Kommission wird die Befugnis übertragen, gemäß Artikel 47 delegierte Rechtsakte zur Festlegung besonderer Kriterien, die von den in Absatz 1 dieses Artikels aufgeführten benannten Konformitätsbewertungsstellen zu erfüllen sind, zu erlassen.

Artikel 5d
Veröffentlichung einer Liste der zertifizierten europäischen Brieftaschen für die Digitale Identität

(1) Die Mitgliedstaaten unterrichten die Kommission und die gemäß Artikel 46e Absatz 1 eingesetzte Kooperationsgruppe unverzüglich über europäische Brieftaschen für die Digitale Identität, die gemäß Artikel 5a bereitgestellt und von den in Artikel 5c Absatz 1 genannten Konformitätsbewertungsstellen zertifiziert worden sind. Sie unterrichten die Kommission und die gemäß Artikel 46e Absatz 1 eingesetzte Kooperationsgruppe unverzüglich über jede Aufhebung der Zertifizierung und geben die Gründe für die Aufhebung an.

(2) Unbeschadet des Artikels 5a Absatz 18 umfassen die von den Mitgliedstaaten gemäß Absatz 1 des vorliegenden Artikels übermittelten Informationen mindestens Folgendes:

a) den Bericht über die Bewertung des Zertifikats und der Zertifizierung der zertifizierten europäischen Brieftasche für die Digitale Identität;

b) eine Beschreibung des elektronischen Identifizierungssystems, in dessen Rahmen die europäische Brieftasche für die Digitale Identität bereitgestellt wird;

c) das geltende Aufsichtssystem und Informationen über die Haftungsregelung in Bezug auf die Beteiligten, die die europäische Brieftasche für die Digitale Identität bereitstellen;

d) die für das elektronische Identifizierungssystem zuständige(n) Behörde(n);

e) Regelungen für die Aussetzung oder den Widerruf des elektronischen Identifizierungssystems oder der Authentifizierung oder der betroffenen beeinträchtigten Teile.

(3) Auf der Grundlage der gemäß Absatz 1 erhaltenen Informationen sorgt die Kommission für die Aufstellung, die Veröffentlichung im Amtsblatt der Europäischen Union und die Führung einer maschinenlesbaren Liste der zertifizierten europäischen Brieftaschen für die Digitale Identität.

(4) Ein Mitgliedstaat kann bei der Kommission die Streichung einer europäischen Brieftasche für die Digitale Identität und des elektronischen Identifizierungssystems, in dessen Rahmen sie bereitgestellt wird, aus der in Absatz 3 genannten Liste beantragen.

(5) Bei Änderungen an den gemäß Absatz 1 übermittelten Informationen übermittelt der Mitgliedstaat der Kommission aktualisierte Informationen.

(6) Die Kommission hält die in Absatz 3 genannte Liste auf dem neuesten Stand, indem sie die entsprechenden Änderungen an der Liste innerhalb eines Monats nach Eingang eines Antrags gemäß Absatz 4 oder an den aktualisierten Informationen gemäß Absatz 5 im Amtsblatt der Europäischen Union veröffentlicht.

(7) Bis zum 21. November 2024 legt die Kommission die Formate und Verfahren für die Zwecke der Absätze 1, 4 und 5 des vorliegenden Artikels im Wege eines Durchführungsrechtsakts zur Umsetzung von europäischen Brieftaschen für die Digitale Identität gemäß Artikel 5a Absatz 23 fest. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 48 Absatz 2 genannten Prüfverfahren erlassen.

Artikel 5e
Sicherheitsverletzung bei europäischen Brieftaschen für die Digitale Identität

(1) Im Falle einer Verletzung oder partiellen Beeinträchtigung der nach Artikel 5a bereitgestellten europäischen Brieftaschen für die Digitale Identität, der in Artikel 5a Absatz 8 genannten Validierungsmechanismen oder des elektronischen Identifizierungssystems, in dessen Rahmen die europäischen Brieftaschen für die Digitale Identität bereitgestellt werden, in einer Weise, die sich auf ihre Verlässlichkeit oder die Verlässlichkeit anderer europäischer Brieftaschen für die Digitale Identität auswirkt, setzt der Mitgliedstaat, der die europäische Brieftasche für die Digitale Identität bereitgestellt hat, unverzüglich die Bereitstellung und Nutzung von europäischen Brieftaschen für die Digitale Identität aus.

Wenn dies durch die Schwere der in Unterabsatz 1 genannten Sicherheitsverletzung oder -beeinträchtigung gerechtfertigt ist, entzieht der Mitgliedstaat europäische Brieftaschen für die Digitale Identität unverzüglich.

Der Mitgliedstaat unterrichtet die betroffenen Nutzer, die gemäß Artikel 46c Absatz 1 benannten einheitlichen Anlaufstellen, die vertrauenden Beteiligten und die Kommission entsprechend.

(2) Wird die in Absatz 1 Unterabsatz 1 dieses Artikels genannte Sicherheitsverletzung oder -beeinträchtigung nicht innerhalb von drei Monaten nach der Aussetzung behoben, so entzieht der Mitgliedstaat, der die europäischen Brieftaschen für die Digitale Identität bereitgestellt hat, europäische Brieftaschen für die Digitale Identität und widerruft deren Gültigkeit. Der Mitgliedstaat unterrichtet die betroffenen Nutzer, die gemäß Artikel 46c Absatz 1 benannten einheitlichen Anlaufstellen, die vertrauenden Beteiligten und die Kommission entsprechend von dem Entzug.

(3) Wurde hinsichtlich der in Absatz 1 Unterabsatz 1 des vorliegenden Artikels genannten Sicherheitsverletzung oder -beeinträchtigung Abhilfe geschaffen, so stellt der bereitstellende Mitgliedstaat die Bereitstellung und Nutzung von europäischen Brieftaschen für die Digitale Identität wieder her und unterrichtet hiervon unverzüglich die betroffenen Nutzer und die vertrauenden Beteiligten, die einheitliche Anlaufstelle gemäß Artikel 46c Absatz 1 und die Kommission.

(4) Die Kommission veröffentlicht die entsprechenden Änderungen an der in Artikel 5d genannten Liste unverzüglich im Amtsblatt der Europäischen Union.

(5) Bis zum 21. November 2024 erstellt die Kommission im Wege von Durchführungsrechtsakten eine Liste von Referenzstandards und legt, sofern erforderlich, die Spezifikationen und Verfahren für die in den Absätzen 1, 2 und 3 dieses Artikels genannten Maßnahmen fest. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 48 Absatz 2 genannten Prüfverfahren erlassen.

Artikel 5f
Grenzüberschreitende Verwendung auf europäische Brieftaschen für die Digitale Identität

(1) Verlangen Mitgliedstaaten für den Zugang zu einem von einer öffentlichen Stelle erbrachten Online-Dienst eine elektronische Identifizierung und Authentifizierung, so akzeptieren sie auch europäische Brieftaschen für die Digitale Identität, die gemäß dieser Verordnung bereitgestellt werden.

(2) Sind private vertrauende Beteiligte, die Dienste erbringen — mit Ausnahme von Kleinst- und kleinen Unternehmen im Sinne von Artikel 2 des Anhangs der Empfehlung 2003/361/EG der Kommission –, nach Unionsrecht oder nationalem Recht verpflichtet, eine Online-Identifizierung mit starker Nutzerauthentifizierung vorzunehmen, oder ist eine Online-Identifizierung mit starker Nutzerauthentifizierung vertraglich vorgeschrieben, auch in den Bereichen Verkehr, Energie, Bankenwesen, Finanzdienstleistungen, soziale Sicherheit, Gesundheit, Trinkwasser, Postdienste, digitale Infrastrukturen, Bildung oder Telekommunikation, so akzeptieren diese privaten vertrauenden Beteiligten hierfür spätestens 36 Monate nach dem Tag des Inkrafttretens der Durchführungsrechtsakte gemäß Artikel 5a Absatz 23 und Artikel 5c Absatz 6 und nur auf das freiwilliges Verlangen des Nutzers auch europäische Brieftaschen für die Digitale Identität, die gemäß dieser Verordnung bereitgestellt werden.

(3) Verlangen Anbieter sehr großer Online-Plattformen gemäß Artikel 33 der Verordnung (EU) 2022/2065 des Europäischen Parlaments und des Rates für den Zugang zu Online-Diensten eine Nutzerauthentifizierung, so akzeptieren und erleichtern sie hierfür auch die Verwendung von europäischen Brieftaschen für die Digitale Identität, die gemäß dieser Ver-

ordnung zur Nutzerauthentifizierung bereitgestellt werden, und zwar nur auf freiwilliges Verlangen des Nutzers und nur mit den Mindestdaten, die für den spezifischen Online-Dienst, für den die Authentifizierung verlangt wird, erforderlich sind.

(4) In Zusammenarbeit mit den Mitgliedstaaten erleichtert die Kommission die Aufstellung von Verhaltenskodizes in enger Zusammenarbeit mit allen einschlägigen Interessenträgern, einschließlich der Zivilgesellschaft, um zu der breiten Verfügbarkeit und Nutzbarkeit von europäischen Brieftaschen für die Digitale Identität im Anwendungsbereich dieser Verordnung beizutragen und Diensteanbieter dazu anzuhalten, die Entwicklung von Verhaltenskodizes abzuschließen.

(5) Innerhalb von 24 Monaten nach Einführung von europäischen Brieftaschen für die Digitale Identität bewertet die Kommission die Nachfrage, Verfügbarkeit und Nutzbarkeit von europäischen Brieftaschen für die Digitale Identität durch, wobei sie Kriterien wie die Inanspruchnahme durch Nutzer, die grenzüberschreitende Präsenz von Diensteanbietern, die technische Entwicklung, die Entwicklung der Verwendungsmuster und die Verbrauchernachfrage berücksichtigt.

ABSCHNITT 2
elektronische identifizierungssysteme

Artikel 6
Gegenseitige Anerkennung

(1) Ist für den Zugang zu einem von einer öffentlichen Stelle in einem Mitgliedstaat erbrachten Online-Dienst nach nationalem Recht oder aufgrund der Verwaltungspraxis eine elektronische Identifizierung mit einem elektronischen Identifizierungsmittel und mit einer Authentifizierung erforderlich, so wird ein in einem anderen Mitgliedstaat ausgestelltes elektronisches Identifizierungsmittel im ersten Mitgliedstaat für die Zwecke der grenzüberschreitenden Authentifizierung für diesen Online-Dienst anerkannt, sofern folgende Bedingungen erfüllt sind:

a) Das betreffende elektronische Identifizierungsmittel wird im Rahmen eines elektronischen Identifizierungssystems ausgestellt, das in der von der Kommission gemäß Artikel 9 veröffentlichten Liste aufgeführt ist.

b) Das Sicherheitsniveau des betreffenden elektronischen Identifizierungsmittels entspricht einem Sicherheitsniveau, das so hoch wie oder höher als das von der einschlägigen öffentlichen Stelle für den Zugang zu diesem Online-Dienst geforderte Sicherheitsniveau ist, sofern das Sicherheitsniveau dieses elektronischen Identifizierungsmittels dem Sicherheitsniveau „substanziell" oder „hoch" entspricht.

c) Die betreffende öffentliche Stelle verwendet für den Zugang zu diesem Online-Dienst das Sicherheitsniveau „substanziell" oder „hoch".

Diese Anerkennung muss spätestens 12 Monate nach Veröffentlichung der in Unterabsatz 1 Buchstabe a genannten Liste durch die Kommission erfolgen.

(2) Ein elektronisches Identifizierungsmittel, das über ein in der von der Kommission gemäß Artikel 9 veröffentlichten Liste enthaltenes elektronisches Identifizierungssystem ausgestellt wird und dem Sicherheitsniveau „niedrig" entspricht, kann von öffentlichen Stellen für die

Zwecke der grenzüberschreitenden Authentifizierung der von diesen Stellen erbrachten Online-Dienste anerkannt werden.

Artikel 7
Voraussetzungen für die Notifizierung elektronischer Identifizierungssysteme

Ein elektronisches Identifizierungssystem kann nach Artikel 9 Absatz 1 notifiziert werden, wenn sämtliche folgenden Bedingungen erfüllt sind:

a) Die elektronischen Identifizierungsmittel im Rahmen des betreffenden Systems werden

   i) vom notifizierenden Mitgliedstaat ausgestellt,

   ii) im Auftrag des notifizierenden Mitgliedstaats ausgestellt oder

   iii) unabhängig vom notifizierenden Mitgliedstaat ausgestellt und von diesem anerkannt.

b) Die elektronischen Identifizierungsmittel im Rahmen des elektronischen Identifizierungssystems können im notifizierenden Mitgliedstaat für den Zugang zu mindestens einem Dienst verwendet werden, der von einer öffentlichen Stelle bereitgestellt wird und für den eine elektronische Identifizierung erforderlich ist.

c) Das elektronische Identifizierungssystem und die im Rahmen dieses Systems ausgestellten elektronischen Identifizierungsmittel erfüllen die Anforderungen zumindest eines der Sicherheitsniveaus, die in dem in Artikel 8 Absatz 3 genannten Durchführungsrechtsakt aufgeführt sind.

d) Der notifizierende Mitgliedstaat stellt sicher, dass zum Zeitpunkt der Ausstellung des elektronischen Identifizierungsmittels im Rahmen des betreffenden Systems die Personenidentifizierungsdaten, die die betreffende Person eindeutig repräsentieren, der in Artikel 3 Nummer 1 genannten natürlichen oder juristischen Person entsprechend den technischen Spezifikationen, Normen und Verfahren für das einschlägige Sicherheitsniveau, die in dem in Artikel 8 Absatz 3 genannten Durchführungsrechtsakt aufgeführt sind, zugeordnet sind.

e) Der Beteiligte, der das elektronische Identifizierungsmittel im Rahmen des betreffenden Systems ausstellt, stellt sicher, dass das elektronische Identifizierungsmittel der in Buchstabe d dieses Artikels genannten Person entsprechend den technischen Spezifikationen, Normen und Verfahren für das betreffende Sicherheitsniveau, die in dem in Artikel 8 Absatz 3 genannten Durchführungsrechtsakt aufgeführt sind, zugewiesen wird.

f) Der notifizierende Mitgliedstaat stellt sicher, dass eine Online-Authentifizierung zur Verfügung steht, so dass jeder im Hoheitsgebiet eines anderen Mitgliedstaats niedergelassene vertrauende Beteiligte die in elektronischer Form empfangenen Personenidentifizierungsdaten bestätigen kann.

   Für vertrauende Beteiligte, die keine öffentlichen Stellen sind, kann der notifizierende Mitgliedstaat Bedingungen für den Zugang zu dieser Authentifizierung festlegen. Die grenzüberschreitende Authentifizierung ist gebührenfrei, wenn sie in Bezug auf einen Online-Dienst erfolgt, der von einer öffentlichen Stelle erbracht wird.

Die Mitgliedstaaten machen vertrauenden Beteiligten, die eine solche Authentifizierung durchführen möchten, keine spezifischen unverhältnismäßigen technischen Vorgaben, wenn derartige Vorgaben die Interoperabilität der notifizierten elektronischen Identifizierungssysteme verhindern oder erheblich beeinträchtigen.

g) Der notifizierende Mitgliedstaat stellt den anderen Mitgliedstaaten für die Zwecke des Artikels 12 Absatz 5 mindestens sechs Monate vor einer Notifizierung gemäß Artikel 9 Absatz 1 nach den Verfahrensmodalitäten, die in den gemäß Artikel 12 Absatz 6 erlassenen Durchführungsrechtsakten festgelegt sind, eine Beschreibung dieses Systems zur Verfügung.

h) Das elektronische Identifizierungssystem erfüllt die Anforderungen des in Artikel 12 Absatz 8 genannten Durchführungsrechtsakts.

Artikel 8
Sicherheitsniveaus elektronischer Identifizierungssysteme

(1) Ein gemäß Artikel 9 Absatz 1 notifiziertes elektronisches Identifizierungssystem gibt die Sicherheitsniveaus „niedrig", „substanziell" und/oder „hoch" an, die den nach diesem System ausgestellten elektronischen Identifizierungsmitteln zuerkannt wurden.

(2) Die Sicherheitsniveaus „niedrig", „substanziell" bzw. „hoch" erfüllen folgende Kriterien:

a) Das Sicherheitsniveau „niedrig" bezieht sich auf ein elektronisches Identifizierungmittel im Rahmen eines elektronischen Identifizierungssystems, das ein begrenztes Maß an Vertrauen in die beanspruchte oder behauptete Identität einer Person vermittelt und durch die Bezugnahme auf die diesbezüglichen technischen Spezifikationen, Normen und Verfahren einschließlich technischer Überprüfungen — deren Zweck in der Minderung der Gefahr des Identitätsmissbrauchs oder der Identitätsveränderung besteht — gekennzeichnet ist.

b) Das Sicherheitsniveau „substanziell" bezieht sich auf ein elektronisches Identifizierungsmittel im Rahmen eines elektronischen Identifizierungssystems, das ein substanzielles Maß an Vertrauen in die beanspruchte oder behauptete Identität einer Person vermittelt und durch die Bezugnahme auf die diesbezüglichen technischen Spezifikationen, Normen und Verfahren einschließlich entsprechender technischer Überprüfungen — deren Zweck in der substanziellen Minderung der Gefahr des Identitätsmissbrauchs oder der Identitätsveränderung besteht — gekennzeichnet ist.

c) Das Sicherheitsniveau „hoch" bezieht sich auf ein elektronisches Identifizierungsmittel im Rahmen eines elektronischen Identifizierungssystems, das ein höheres Maß an Vertrauen in die beanspruchte oder behauptete Identität einer Person als ein Identifizierungsmittel mit dem Sicherheitsniveau „substanziell" vermittelt und durch die Bezugnahme auf die diesbezüglichen technischen Spezifikationen, Normen und Verfahren einschließlich technischer Überprüfungen — deren Zweck in der Verhinderung des Identitätsmissbrauchs oder der Identitätsveränderung besteht — gekennzeichnet ist.

(3) Bis zum 18. September 2015 legt die Kommission unter Berücksichtigung der einschlägigen internationalen Normen vorbehaltlich des Absatzes 2 im Wege von Durchführungsrechtsakten technische Spezifikationen, Standards und Verfahren mit Mindestanforderun-

gen fest, auf die sich die Festlegung der Sicherheitsniveaus niedrig, „substanziell“ und „hoch“ für elektronische Identifizierungsmittel bezieht.

Diese technischen Spezifikationen, Normen und Verfahren mit Mindestanforderungen werden unter Bezugnahme auf die Zuverlässigkeit und Qualität folgender Elemente festgelegt:

a) des Verfahrens zum Nachweis und zur Überprüfung der Identität natürlicher oder juristischer Personen, die die Ausstellung elektronischer Identifizierungsmittel beantragen;

b) des Verfahrens zur Ausstellung der beantragten elektronischen Identifizierungsmittel;

c) des Authentifizierungsmechanismus, bei dem die natürliche oder juristische Person die elektronischen Identifizierungsmittel verwendet, um einem vertrauenden Beteiligten ihre Identität zu bestätigen;

d) der Einrichtung, die die Identifizierungsmittel ausstellt;

e) jeder anderen Stelle, die mit dem Antrag für die Ausstellung elektronischer Identifizierungsmittel befasst ist;

f) technischer und sicherheitsbezogener Spezifikationen der ausgestellten elektronischen Identifizierungsmittel.

Diese Durchführungsrechtsakte werden nach dem in Artikel 48 Absatz 2 genannten Prüfverfahren erlassen.

Artikel 9
Notifizierung

(1) Der notifizierende Mitgliedstaat notifiziert der Kommission folgende Informationen und unverzüglich alle späteren Änderungen dieser Informationen:

a) eine Beschreibung des elektronischen Identifizierungssystems einschließlich seiner Sicherheitsniveaus und des Ausstellers bzw. der Aussteller elektronischer Identifizierungsmittel im Rahmen des Systems;

b) das geltende Aufsichtssystem und Informationen über die Haftungsregelung in Bezug auf Folgendes:

   i) den das elektronische Identifizierungsmittel ausstellenden Beteiligten;

   ii) den das Authentifizierungsverfahren durchführenden Beteiligten;

c) die für das elektronische Identifizierungssystem zuständige(n) Behörde(n);

d) Informationen über die Einrichtung bzw. Einrichtungen, die die Registrierung der eindeutigen Personenidentifizierungsdaten verwaltet bzw. verwalten;

e) eine Beschreibung, inwieweit die Anforderungen des in Artikel 12 Absatz 8 genannten Durchführungsrechtsakts erfüllt werden;

f) eine Beschreibung der Authentifizierung gemäß Artikel 7 Buchstabe f;

g) Regelungen für die Aussetzung oder den Widerruf des notifizierten elektronischen Identifizierungssystems oder der Authentifizierung oder von den betroffenen beeinträchtigten Teilen.

(2) Die Kommission veröffentlicht im Amtsblatt der Europäischen Union unverzüglich eine Liste der gemäß Absatz 1 notifizierten elektronischen Identifizierungssysteme zusammen mit grundlegenden Informationen über diese Systeme.

(3) Die Kommission veröffentlicht im Amtsblatt der Europäischen Union die Änderungen an der in Absatz 2 genannten Liste innerhalb eines Monats ab dem Tag des Eingangs der Notifizierung des Mitgliedstaats.

(4) Ein Mitgliedstaat kann bei der Kommission die Streichung eines von diesem Mitgliedstaat notifizierten Identifizierungssystems aus der in Absatz 2 genannten Liste beantragen. Die Kommission veröffentlicht im Amtsblatt der Europäischen Union die entsprechenden Änderungen der Liste innerhalb eines Monats ab dem Zeitpunkt, zu dem das Ersuchen des Mitgliedstaats eingegangen ist.

(5) Die Kommission kann im Wege von Durchführungsrechtsakten Einzelheiten, Form und Verfahren für die Notifizierung nach Absatz 1 festlegen. Diese Durchführungsrechtsakte werden nach dem in Artikel 48 Absatz 2 genannten Prüfverfahren erlassen.

Artikel 10
Sicherheitsverletzung bei elektronischen Identifizierungssystemen

(1) Im Falle einer Verletzung oder partiellen Beeinträchtigung des nach Artikel 9 Absatz 1 notifizierten elektronischen Identifizierungssystems oder der in Artikel 7 Buchstabe f genannten Authentifizierung in einer Weise, die sich auf die Verlässlichkeit der grenzüberschreitenden Authentifizierung dieses Systems auswirkt, setzt der notifizierende Mitgliedstaat diese grenzüberschreitende Authentifizierung oder die entsprechenden beeinträchtigten Teile umgehend aus oder widerruft sie und unterrichtet hiervon die anderen Mitgliedstaaten und die Kommission.

(2) Wurde hinsichtlich der in Absatz 1 genannten Verletzung oder Beeinträchtigung Abhilfe geschaffen, so stellt der notifizierende Mitgliedstaat die grenzüberschreitende Authentifizierung wieder her und unterrichtet unverzüglich die anderen Mitgliedstaaten und die Kommission.

(3) Wird hinsichtlich der in Absatz 1 genannten Verletzung oder Beeinträchtigung nicht innerhalb von drei Monaten nach der Aussetzung oder dem Widerruf Abhilfe geschaffen, so meldet der notifizierende Mitgliedstaat den anderen Mitgliedstaaten und der Kommission die Zurücknahme des elektronischen Identifizierungssystems.

Die Kommission veröffentlicht die entsprechenden Änderungen an der in Artikel 9 Absatz 2 genannten Liste unverzüglich im Amtsblatt der Europäischen Union.

Artikel 11
Haftung

(1) Der notifizierende Mitgliedstaat haftet für die Schäden, die natürlichen oder juristischen Personen vorsätzlich oder fahrlässig zugefügt werden und die auf eine Verletzung der in Artikel 7 Buchstaben d und f festgelegten Pflichten bei einer grenzüberschreitenden Transaktion zurückzuführen sind.

(2) Der das elektronische Identifizierungsmittel ausstellende Beteiligte haftet für die Schäden, die natürlichen oder juristischen Personen vorsätzlich oder fahrlässig zugefügt werden und die auf eine Verletzung der in Artikel 7 Buchstabe e festgelegten Pflichten bei einer grenzüberschreitenden Transaktion zurückzuführen sind.

(3) Der das Authentifizierungsverfahren durchführende Beteiligte haftet für die Schäden, die natürlichen oder juristischen Personen vorsätzlich oder fahrlässig zugefügt werden und die auf die inkorrekte Durchführung der Authentifizierung nach Artikel 7 Buchstabe f bei einer grenzüberschreitenden Transaktion zurückzuführen sind.

(4) Die Absätze 1, 2 und 3 werden im Einklang mit den nationalen Vorschriften über die Haftung angewendet.

(5) Die Absätze 1, 2 und 3 berühren nicht die unter das nationale Recht fallende Haftung der Beteiligten an einer Transaktion, bei der dem gemäß Artikel 9 Absatz 1 notifizierten elektronischen Identifizierungssystem unterliegende elektronische Identifizierungsmittel verwendet wurden.

Artikel 11a
Grenzüberschreitender Identitätsabgleich

(1) Sind Mitgliedstaaten im Rahmen von grenzüberschreitenden Diensten vertrauende Beteiligte, so stellen sie einen Identitätsabgleich in Bezug auf natürliche Personen, die notifizierte elektronische Identifizierungsmittel oder europäischen Brieftaschen für die Digitale Identität verwenden, sicher.

(2) Die Mitgliedstaaten sehen technische und organisatorische Maßnahmen vor, um ein hohes Schutzniveau für personenbezogene Daten, die für den Identitätsabgleich verwendet werden, sicherzustellen und die Erstellung von Nutzerprofilen zu verhindern.

(3) Bis zum 21. November 2024 erstellt die Kommission eine Liste der Referenzstandards und legt, sofern notwendig, die Spezifikationen und Verfahren für die in Absatz 1 des vorliegenden Artikels genannten Anforderungen im Wege von Durchführungsrechtsakten fest. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 48 Absatz 2 genannten Prüfverfahren erlassen.

Artikel 12
Interoperabilität

(1) Die gemäß Artikel 9 Absatz 1 notifizierten nationalen elektronischen Identifizierungssysteme müssen interoperabel sein.

(2) Für die Zwecke des Absatzes 1 wird ein Interoperabilitätsrahmen geschaffen.

(3) Der Interoperabilitätsrahmen muss folgende Kriterien erfüllen:

a) Er ist auf Technologieneutralität angelegt und unterscheidet nicht zwischen spezifischen nationalen technischen Lösungen für die elektronische Identifizierung in dem betreffenden Mitgliedstaat,

b) er entspricht nach Möglichkeit den europäischen und internationalen Normen,

c) er fördert die Umsetzung des eingebauten Datenschutzes und der eingebauten Sicherheit.

(4) Der Interoperabilitätsrahmen besteht aus Folgendem:

a) einer Bezugnahme auf die mit den Sicherheitsniveaus nach Artikel 8 technischen Mindestanforderungen;

b) Angaben zur Entsprechung zwischen den nationalen Sicherheitsniveaus der notifizierten Identifizierungssysteme und den Sicherheitsniveaus nach Artikel 8;

c) einer Bezugnahme auf die technischen Mindestanforderungen für die Interoperabilität;

d) einer Bezugnahme auf einen über elektronische Identifizierungssysteme bereitgestellten Mindestsatz von Personenidentifizierungsdaten, die eine natürliche oder juristische Person eindeutig repräsentieren;

e) Verfahrensregelungen;

f) Regelungen zur Streitbeilegung und

g) gemeinsamen Sicherheitsnormen für den Betrieb.

(5) Die Mitgliedstaaten führen gegenseitige Begutachtungen der elektronischen Identifizierungssysteme, die in den Anwendungsbereich dieser Verordnung fallenden und die gemäß Artikel 9 Absatz 1 Buchstabe a zu notifizieren sind, durch.

(6) Bis zum 18. März 2025 legt die Kommission im Wege von Durchführungsrechtsakten die nötigen Verfahrensmodalitäten für die in Absatz 5 dieses Artikels genannten gegenseitigen Begutachtungen fest, um ein hohes Maß an Vertrauen und Sicherheit, das der Höhe des Risikos angemessen ist, zu fördern. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 48 Absatz 2 genannten Prüfverfahren erlassen.

(8) Bis zum 18. September 2025 erlässt die Kommission unter Zugrundelegung der in Absatz 3 des vorliegenden Artikels aufgeführten Kriterien und unter Berücksichtigung der Ergebnisse der Zusammenarbeit zwischen den Mitgliedstaaten Durchführungsrechtsakte zum Interoperabilitätsrahmen gemäß Absatz 4 des vorliegenden Artikels, um einheitliche Voraussetzungen für die Umsetzung der Verpflichtung gemäß Absatz 1 dieses Artikels vorzugeben. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 48 Absatz 2 genannten Prüfverfahren erlassen.

(9) Die in den Absätzen 7 und 8 genannten Durchführungsrechtsakte werden nach dem in Artikel 48 Absatz 2 genannten Prüfverfahren erlassen.

Artikel 12a
Zertifizierung elektronischer Identifizierungssysteme

(1) Die Konformität der zu notifizierenden elektronischen Identifizierungssysteme mit den in dieser Verordnung festgelegten Cybersicherheitsanforderungen, einschließlich der Konformität mit den für die Cybersicherheit relevanten Anforderungen, die in Artikel 8 Absatz 2 zu den Sicherheitsniveaus elektronischer Identifizierungssysteme festgelegt sind, wird von Konformitätsbewertungsstellen zertifiziert, die von den Mitgliedstaaten benannt werden.

(2) Die Zertifizierung gemäß Absatz 1 dieses Artikels wird im Rahmen eines einschlägigen Schemas für die Cybersicherheitszertifizierung gemäß der Verordnung (EU) 2019/881 oder Teilen davon durchgeführt, sofern das Cybersicherheitszertifikat oder Teile davon die Cybersicherheitsanforderungen abdecken.

(3) Die Zertifizierung gemäß Absatz 1 gilt für einen Zeitraum von bis zu fünf Jahren, sofern alle zwei Jahre eine Schwachstellenbeurteilung durchgeführt wird. Wird eine Schwachstelle festgestellt und nicht innerhalb von drei Monaten, nachdem dies festgestellt wurde, behoben, so wird die Zertifizierung aufgehoben.

(4) Ungeachtet des Absatzes 2 können die Mitgliedstaaten gemäß dem genannten Absatz von einem notifizierenden Mitgliedstaat zusätzliche Informationen über zertifizierte elektronische Identifizierungssysteme oder Teile davon anfordern.

(5) Die gegenseitige Begutachtung elektronischer Identifizierungssysteme gemäß Artikel 12 Absatz 5 erfolgt nicht bei elektronischen Identifizierungssystemen oder Teilen davon, die im Einklang mit Absatz 1 dieses Artikels zertifiziert wurden. Die Mitgliedstaaten können ein Zertifikat oder eine Erklärung der Konformität mit den in Artikel 8 Absatz 2 in Bezug auf das Sicherheitsniveau elektronischer Identifizierungssysteme festgelegten, nicht die Cybersicherheit betreffenden Anforderungen verwenden, das bzw. die nach einem einschlägigen Zertifizierungsschema oder Teilen solcher Schemata ausgestellt wurde.

(6) Die Mitgliedstaaten teilen der Kommission die Namen und Anschriften der in Absatz 1 genannten Konformitätsbewertungsstellen mit. Die Kommission stellt diese Informationen allen Mitgliedstaaten zur Verfügung.

Artikel 12b
Zugang zu Hardware- und Software-Funktionen

Wenn Anbieter von europäischen Brieftaschen für die Digitale Identität und Aussteller notifizierter elektronischer Identifizierungsmittel, die in gewerblicher oder beruflicher Eigenschaft handeln und dazu zentrale Plattformdienste im Sinne von Artikel 2 Nummer 2 der Verordnung (EU) 2022/1925 des Europäischen Parlaments und des Rates zum Zwecke oder im Zuge der Bereitstellung von Diensten im Zusammenhang mit der europäischen Brieftasche für die Digitale Identität und elektronischen Identifizierungsmitteln an Endnutzer verwenden, gewerbliche Nutzer im Sinne des Artikels 2 Nummer 21 der genannten Verordnung sind, so ermöglichen Torwächter ihnen insbesondere wirksame Interoperabilität mit — und Zugang für Zwecke der Interoperabilität zu — denselben Betriebssystem-, Hardware- oder Software-Funktionen. Im Sinne von Artikel 6 Absatz 7 der Verordnung (EU) 2022/1925 werden diese wirksame Interoperabilität und der Zugang kostenlos und unabhängig davon, ob die Hardware- oder Software-Funktionen, die der Torwächter bei der Erbringung solcher Dienste zur Verfügung hat oder verwendet, Teil des Betriebssystems sind, ermöglicht. Der vorliegende Artikel gilt unbeschadet des Artikels 5a Absatz 14 der vorliegenden Verordnung.

KAPITEL III
VERTRAUENSDIENSTE

ABSCHNITT 1
Allgemeine Bestimmungen

Artikel 13
Haftung und Beweislast

(1) Ungeachtet des Absatzes 2 dieses Artikels und unbeschadet der Verordnung (EU) 2016/679 haften Vertrauensdiensteanbieter für alle natürlichen oder juristischen Personen vorsätzlich oder fahrlässig zugefügten Schäden, die auf eine Verletzung der in dieser Verordnung festgelegten Pflichten zurückzuführen sind. Jede natürliche oder juristische Person, der infolge eines Verstoßes gegen diese Verordnung durch einen Vertrauensdiensteanbieter ein materieller oder immaterieller Schaden entstanden ist, hat das Recht, im Einklang mit dem Unionsrecht und dem nationalen Recht einen Anspruch auf Schadensersatz geltend zu machen.

Die Beweislast für den Nachweis des Vorsatzes oder der Fahrlässigkeit seitens eines nichtqualifizierten Vertrauensdiensteanbieters liegt bei der natürlichen oder juristischen Person, die den in Unterabsatz 1 genannten Schaden geltend macht.

Bei einem qualifizierten Vertrauensdiensteanbieter wird von Vorsatz oder Fahrlässigkeit ausgegangen, es sei denn, der qualifizierte Vertrauensdiensteanbieter weist nach, dass der in Unterabsatz 1 genannte Schaden entstanden ist, ohne dass er vorsätzlich oder fahrlässig gehandelt hat.

(2) Unterrichten Vertrauensdiensteanbieter ihre Kunden im Voraus hinreichend über Beschränkungen der Verwendung der von ihnen erbrachten Dienste und sind diese Beschränkungen für dritte Beteiligte ersichtlich, so haften die Vertrauensdiensteanbieter nicht für Schäden, die bei einer über diese Beschränkungen hinausgehenden Verwendung der Dienste entstanden sind.

(3) Die Absätze 1 und 2 werden im Einklang mit den nationalen Vorschriften über die Haftung angewendet.

Artikel 14
Internationale Aspekte

(1)Vertrauensdienste, die von in einem Drittland niedergelassenen Vertrauensdiensteanbietern oder von einer internationalen Organisation bereitgestellt werden, werden als rechtlich gleichwertig mit den Vertrauensdiensten anerkannt, die von in der Union niedergelassenen qualifizierten Vertrauensdiensteanbietern bereitgestellt werden, sofern die aus dem Drittland oder von einer internationalen Organisation stammenden Vertrauensdienste im Wege von Durchführungsrechtsakten oder einer gemäß Artikel 218 AEUV geschlossenen Vereinbarung zwischen der Union und dem betreffenden Drittland oder der internationalen Organisation anerkannt sind.

Die in Unterabsatz 1 genannten Durchführungsrechtsakte werden gemäß dem in Artikel 48 Absatz 2 genannten Prüfverfahren erlassen.

(2) Mit den in Absatz 1 genannten Durchführungsrechtsakten und der dort genannten Vereinbarung wird dafür gesorgt, dass die Anforderungen, die für die in der Union niedergelassenen qualifizierten Vertrauensdiensteanbieter und für die von ihnen erbrachten qualifizierten Vertrauensdienste gelten, von den Vertrauensdiensteanbietern in dem betroffenen Drittland oder von den internationalen Organisationen und von den von diesen erbrachten Vertrauensdiensten eingehalten werden. Drittländer und internationale Organisation erstellen, führen und veröffentlichen insbesondere eine Vertrauensliste anerkannter Vertrauensdiensteanbieter.

(3) Mit den Vereinbarungen gemäß Absatz 1 wird dafür gesorgt, dass die qualifizierten Vertrauensdienste, die von in der Union niedergelassenen qualifizierten Vertrauensdiensteanbietern erbracht werden, als rechtlich gleichwertig mit den Vertrauensdiensten anerkannt werden, die von Vertrauensdiensteanbietern in den Drittländern oder von internationalen Organisationen, mit denen die Vereinbarungen geschlossen wurden, erbracht werden.

Artikel 15
Barrierefreie Zugänglichkeit für Personen mit Behinderungen und besonderen Bedürfnissen

Elektronische Identifizierungsmittel, Vertrauensdienste und zur Erbringung solcher Dienste verwendete Endnutzerprodukte werden in einfacher und verständlicher Sprache gemäß dem Übereinkommen über die Rechte von Menschen mit Behinderungen und den Barrierefreiheitsanforderungen der Richtlinie (EU) 2019/882 zugänglich gemacht, wodurch sie auch Personen mit funktionellen Einschränkungen, wie z. B. ältere Personen, und Personen mit eingeschränktem Zugang zu digitalen Technologien zugutekommen.

Artikel 16
Sanktionen

(1) Unbeschadet des Artikels 31 der Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates legen die Mitgliedstaaten Regeln für Sanktionen bei Verstößen gegen diese Verordnung fest. Diese Sanktionen müssen wirksam, verhältnismäßig und abschreckend sein.

(2) Die Mitgliedstaaten stellen sicher, dass für Verstöße gegen diese Verordnung von qualifizierten und nichtqualifizierten Vertrauensdiensteanbietern Geldbußen verhängt werden mit einem Höchstmaß von mindestens:

a) 5 000 000 EUR, wenn es sich bei dem Vertrauensdiensteanbieter um eine natürliche Person handelt; oder

b) wenn es sich bei dem Vertrauensdiensteanbieter um eine juristische Person handelt, 5 000 000 EUR oder 1 % des gesamten weltweiten in dem Geschäftsjahr, das dem Jahr, in dem der Verstoß stattfand, vorausging, getätigten Umsatzes des Unternehmens, dem der Vertrauensdiensteanbieter angehörte, je nachdem, welcher Betrag höher ist.

(3) In Abhängigkeit vom Rechtssystem des betreffenden Mitgliedstaats können die Vorschriften über Geldbußen je nach den dort geltenden Regeln so angewandt werden, dass die Geldbuße von der zuständigen Aufsichtsstelle in die Wege geleitet und von den zuständigen nationalen Gerichten verhängt wird. Durch die Anwendung solcher Vorschriften in diesen Mitgliedstaaten wird sichergestellt, dass diese Rechtsmittel wirksam sind und die gleiche Wirkung wie direkt von zuständigen Aufsichtsbehörden verhängte Geldbußen haben.

ABSCHNITT 2
Nichtqualifizierte Vertrauensdienste

Artikel 19a
Anforderungen an nichtqualifizierte Vertrauensdiensteanbieter

(1) Für nichtqualifizierte Vertrauensdiensteanbieter, die nichtqualifizierte Vertrauensdienste erbringen, gilt Folgendes:

a) Sie haben angemessene Konzepte und treffen entsprechende Maßnahmen zur Beherrschung rechtlicher, geschäftlicher, betrieblicher und sonstiger direkter oder indirekter Risiken bei der Erbringung des nichtqualifizierten Vertrauensdienstes, diese umfassen unbeschadet des Artikels 21 der Richtlinie (EU) 2022/2555 zumindest jene in Bezug auf:

   i) Registrierungs- und Einbindungsverfahren für einen Vertrauensdienst;

   ii) Verfahrens- oder Verwaltungskontrollen, die für die Erbringung von Vertrauensdiensten erforderlich sind;

   iii) die Verwaltung und Durchführung von Vertrauensdiensten.

b) Sie teilen der Aufsichtsstelle, den identifizierbaren betroffenen Personen, der Öffentlichkeit, wenn es von öffentlichem Interesse ist, und gegebenenfalls anderen einschlägigen zuständigen Stellen unverzüglich, spätestens jedoch 24 Stunden, nachdem sie von etwaigen Sicherheitsverletzungen oder Störungen Kenntnis erlangt haben, alle Sicherheitsverletzungen oder Störungen bei der Erbringung des Dienstes oder der Durchführung der in Buchstabe a Ziffern i, ii oder iii genannten Maßnahmen, die erhebliche Auswirkungen auf den erbrachten Vertrauensdienst oder die darin gespeicherten personenbezogenen Daten haben, mit.

(2) Bis zum 21. Mai 2025 erstellt die Kommission im Wege von Durchführungsrechtsakten eine Liste von Referenzstandards und legt, sofern erforderlich, die Spezifikationen und Verfahren für Absatz 1 Buchstabe a des vorliegenden Artikels fest. Werden diese Standards, Spezifikationen und Verfahren eingehalten, so wird davon ausgegangen, dass die Anforderungen dieses Artikels erfüllt sind. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 48 Absatz 2 genannten Prüfverfahren erlassen.

ABSCHNITT 3
Qualifizierte Vertrauensdienste

Artikel 20
Beaufsichtigung qualifizierter Vertrauensdiensteanbieter

(1) Qualifizierte Vertrauensdiensteanbieter werden mindestens alle 24 Monate auf eigene Kosten von einer Konformitätsbewertungsstelle geprüft. Mit der Prüfung soll bestätigt werden, dass die qualifizierten Vertrauensdiensteanbieter und die von ihnen erbrachten qualifizierten Vertrauensdienste die Anforderungen dieser Verordnung und des Artikels 21 der Richtlinie (EU) 2022/2555 erfüllen. Die qualifizierten Vertrauensdiensteanbieter legen der

Aufsichtsstelle den entsprechenden Konformitätsbewertungsbericht innerhalb von drei Arbeitstagen nach dessen Eingang vor.

(1a) Qualifizierte Vertrauensdiensteanbieter unterrichten die Aufsichtsstelle mindestens einen Monat vor geplanten Prüfungen und gestatten der Aufsichtsstelle auf Anfrage die Teilnahme als Beobachter.

(1b) Die Mitgliedstaaten teilen der Kommission unverzüglich die Namen, Adressen und Angaben zur Akkreditierung der in Absatz 1 genannten Konformitätsbewertungsstellen sowie alle nachfolgenden Änderungen daran mit. Die Kommission stellt diese Informationen allen Mitgliedstaaten zur Verfügung.

(2) Unbeschadet des Absatzes 1 kann die Aufsichtsstelle jederzeit eine Überprüfung vornehmen oder eine Konformitätsbewertungsstelle um eine Konformitätsbewertung der qualifizierten Vertrauensdiensteanbieter — auf Kosten dieser Vertrauensdiensteanbieter — ersuchen, um nachzuweisen, dass sie und die von ihnen erbrachten qualifizierten Vertrauensdienste die in dieser Verordnung festgelegten Anforderungen erfüllen. Ist dem Anschein nach gegen Vorschriften zum Schutz personenbezogener Daten verstoßen worden, so unterrichtet die betreffende Aufsichtsstelle unverzüglich die gemäß Artikel 51 der Verordnung (EU) 2016/679 eingerichteten zuständigen Aufsichtsbehörden.

(3) Verstößt der qualifizierte Vertrauensdiensteanbieter gegen eine in dieser Verordnung festgelegte Anforderung, so fordert die Aufsichtsstelle ihn auf, gegebenenfalls innerhalb einer bestimmten Frist Abhilfe zu schaffen.

Schafft dieser Anbieter keine Abhilfe bzw. innerhalb der von der Aufsichtsstelle gegebenenfalls gesetzten Frist keine Abhilfe, so entzieht die Aufsichtsstelle, soweit dies insbesondere durch die Tragweite, die Dauer und die Auswirkungen dieses Verstoßes gerechtfertigt ist, dem betreffenden Anbieter oder dem von ihm erbrachten betroffenen Dienst den Qualifikationsstatus.

(3a) Wenn die gemäß Artikel 8 Absatz 1 der Richtlinie (EU) 2022/2555 benannten oder eingerichteten zuständigen Behörden die Aufsichtsstelle davon in Kenntnis setzen, dass der qualifizierte Vertrauensdiensteanbieter gegen eine der in Artikel 21 der genannten Richtlinie festgelegten Anforderungen verstößt, so entzieht die Aufsichtsstelle, soweit dies insbesondere durch die Tragweite, die Dauer und die Auswirkungen dieses Verstoßes gerechtfertigt ist, dem betreffenden Anbieter oder dem von ihm erbrachten betroffenen Dienst den Qualifikationsstatus.

(3b) Wenn die gemäß Artikel 51 der Verordnung (EU) 2016/679 eingerichteten Aufsichtsbehörden die Aufsichtsstelle davon in Kenntnis setzen, dass der qualifizierte Vertrauensdiensteanbieter gegen eine der in der genannten Verordnung festgelegten Anforderungen verstößt, entzieht die Aufsichtsstelle, soweit dies insbesondere durch die Tragweite, die Dauer und die Auswirkungen dieses Verstoßes gerechtfertigt ist, dem betreffenden Anbieter oder dem von ihm erbrachten betroffenen Dienst den Qualifikationsstatus.

(3c) Die Aufsichtsstelle unterrichtet den qualifizierten Vertrauensdiensteanbieter darüber, dass ihm oder dem betreffenden Dienst der Qualifikationsstatus entzogen wurde. Die Aufsichtsstelle unterrichtet die gemäß Artikel 22 Absatz 3 der vorliegenden Verordnung notifizierte Stelle, damit die in Absatz 1 jenes Artikels genannten Vertrauenslisten aktualisiert werden, und die gemäß Artikel 8 Absatz 1 der Richtlinie (EU) 2022/2555 benannte oder eingerichtete zuständige Behörde.

(4) Bis zum 21. Mai 2025 erstellt die Kommission im Wege von Durchführungsrechtsakten eine Liste von Referenzstandards und legt, sofern erforderlich, Spezifikationen und Verfahren für Folgendes fest:

a) die Akkreditierung der Konformitätsbewertungsstellen und den in Absatz 1 genannten Konformitätsbewertungsbericht;

b) die Prüfvorschriften, nach denen die Konformitätsbewertungsstellen ihre Konformitätsbewertung, einschließlich einer Kombinationsbewertung, der in Absatz 1 genannten qualifizierten Vertrauensdiensteanbieter durchführen;

c) die Konformitätsbewertungssysteme für die Durchführung der Konformitätsbewertung der qualifizierten Vertrauensdiensteanbieter durch die Konformitätsbewertungsstellen und für die Vorlage des in Absatz 1 genannten Berichts.

Diese Durchführungsrechtsakte werden gemäß dem in Artikel 48 Absatz 2 genannten Prüfverfahren erlassen.

Artikel 21
Beginn der Erbringung qualifizierter Vertrauensdienste

(1) Beabsichtigen Vertrauensdiensteanbieter, mit der Erbringung eines qualifizierten Vertrauensdienstes zu beginnen, so teilen sie der Aufsichtsstelle ihre Absicht mit und legen einen von einer Konformitätsbewertungsstelle ausgestellten Konformitätsbewertungsbericht bei, in dem die Erfüllung der in dieser Verordnung und in Artikel 21 der Richtlinie (EU) 2022/2555 festgelegten Anforderungen bestätigt wird.

(2) Die Aufsichtsstelle überprüft, ob der Vertrauensdiensteanbieter und die von ihm erbrachten Vertrauensdienste die in dieser Verordnung festgelegten Anforderungen erfüllen, insbesondere hinsichtlich der Anforderungen an qualifizierte Vertrauensdiensteanbieter und an die von ihnen erbrachten qualifizierten Vertrauensdienste.

Zur Überprüfung, ob der Vertrauensdiensteanbieter die Anforderungen des Artikels 21 der Richtlinie (EU) 2022/2555 erfüllt, fordert die Aufsichtsstelle die gemäß Artikel 8 Absatz 1 der genannten Richtlinie benannten oder eingerichteten zuständigen Behörden auf, diesbezügliche Aufsichtsmaßnahmen durchzuführen und sie unverzüglich und in jedem Fall innerhalb von zwei Monaten nach Erhalt des Ersuchens über das Ergebnis zu unterrichten. Wird die Überprüfung nicht innerhalb von zwei Monaten nach der Mitteilung abgeschlossen, so unterrichten diese zuständigen Behörden die Aufsichtsstelle hierüber unter Angabe der Gründe für die Verzögerung und der Frist, innerhalb deren die Überprüfung abzuschließen ist.

Gelangt die Aufsichtsstelle zu dem Schluss, dass der Vertrauensdiensteanbieter und die von ihm erbrachten Vertrauensdienste die in dieser Verordnung festgelegten Anforderungen erfüllen, so verleiht sie dem Vertrauensdiensteanbieter und den von ihm erbrachten Vertrauensdiensten den Qualifikationsstatus und unterrichtet die in Artikel 22 Absatz 3 genannte Stelle, damit die in Artikel 22 Absatz 1 genannten Vertrauenslisten entsprechend aktualisiert werden; dies erfolgt spätestens drei Monate nach der Mitteilung gemäß Absatz 1 dieses Artikels.

Wird die Überprüfung nicht innerhalb von drei Monaten nach der Mitteilung abgeschlossen, so unterrichtet die Aufsichtsstelle den Vertrauensdiensteanbieter hierüber unter Angabe der Gründe für die Verzögerung und der Frist, innerhalb deren die Überprüfung abzuschließen ist.

(3) Qualifizierte Vertrauensdiensteanbieter können mit der Erbringung des qualifizierten Vertrauensdienstes beginnen, nachdem der qualifizierte Status in den in Artikel 22 Absatz 1 genannten Vertrauenslisten ausgewiesen wurde.

(4) Bis zum 21. Mai 2025 legt die Kommission im Wege von Durchführungsrechtsakten Form und Verfahren der Mitteilung und Überprüfung für die Zwecke der Absätze 1 und 2 des vorliegenden Artikels fest. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 48 Absatz 2 genannten Prüfverfahren erlassen.

Artikel 22
Vertrauenslisten

(1) Jeder Mitgliedstaat sorgt für die Aufstellung, Führung und Veröffentlichung von Vertrauenslisten, die Angaben zu den qualifizierten Vertrauensdiensteanbietern, für die er verantwortlich ist, und den von ihnen erbrachten qualifizierten Vertrauensdiensten, umfassen.

(2) Die Mitgliedstaaten erstellen, führen und veröffentlichen auf gesicherte Weise elektronisch unterzeichnete oder besiegelte Vertrauenslisten gemäß Absatz 1 in einer für eine automatisierte Verarbeitung geeigneten Form.

(3) Die Mitgliedstaaten übermitteln der Kommission unverzüglich Informationen über die für die Erstellung, Führung und Veröffentlichung der nationalen Vertrauenslisten verantwortlichen Stellen, den Ort der Veröffentlichung der Listen, die zur Unterzeichnung oder Besiegelung der Vertrauenslisten verwendeten Zertifikate und alle etwaigen Änderungen dieser Informationen.

(4) Die Kommission macht die Informationen nach Absatz 3 auf sichere Weise und elektronisch unterzeichnet oder besiegelt in einer für eine automatisierte Verarbeitung geeigneten Form öffentlich zugänglich.

(5) Bis 18. September 2015 präzisiert die Kommission im Wege von Durchführungsrechtsakten die Angaben gemäß Absatz 1 und legt die technischen Spezifikationen und die Form der Vertrauenslisten für die Zwecke der Absätze 1 bis 4 fest. Diese Durchführungsrechtsakte werden nach dem in Artikel 48 Absatz 2 genannten Prüfverfahren erlassen.

Artikel 23
EU-Vertrauenssiegel für qualifizierte Vertrauensdiensteanbieter

(1) Nachdem der Qualifikationsstatus nach Artikel 21 Absatz 2 Unterabsatz 2 in der Vertrauensliste nach Artikel 22 Absatz 1 ausgewiesen wurde, können qualifizierte Vertrauensdiensteanbieter das EU-Vertrauenssiegel verwenden, um in einfacher, wiedererkennbarer und klarer Weise die von ihnen erbrachten qualifizierten Vertrauensdienste zu kennzeichnen.

(2) Qualifizierte Vertrauensdienstanbieter, die für die qualifizierten Vertrauensdienste das EU-Vertrauenssiegel nach Absatz 1 verwenden, sorgen dafür, dass auf ihrer Website ein Link zur einschlägigen Vertrauensliste zur Verfügung steht.

(3) Die Kommission legt bis 1. Juli 2015 im Wege von Durchführungsrechtsakten Spezifikationen zur Form und insbesondere zur Aufmachung, Zusammensetzung, Größe und Gestaltung des EU-Vertrauenssiegels für qualifizierte Vertrauensdienste fest. Diese Durchführungsrechtsakte werden nach dem in Artikel 48 Absatz 2 genannten Prüfverfahren erlassen.

Artikel 24
Anforderungen an qualifizierte Vertrauensdiensteanbieter

(1) Bei der Ausstellung eines qualifizierten Zertifikats oder einer qualifizierten elektronischen Attributsbescheinigung überprüft der qualifizierte Vertrauensdiensteanbieter die Identität und gegebenenfalls spezifische Attribute der natürlichen oder juristischen Person, der das qualifizierte Zertifikat oder die qualifizierte elektronische Attributsbescheinigung ausgestellt werden soll.

(1a) Die Überprüfung der Identität nach Absatz 1 wird anhand geeigneter Mittel vom qualifizierten Vertrauensdiensteanbieter entweder unmittelbar oder über einen Dritten auf der Grundlage einer der folgenden Methoden oder — sofern erforderlich — einer Kombination davon im Einklang mit den in Absatz 1c genannten Durchführungsrechtsakten durchgeführt:

a) mit der europäischen Brieftasche für die Digitale Identität oder einem notifizierten elektronischen Identifizierungsmittel, das die Anforderungen des Artikels 8 in Bezug auf das Sicherheitsniveau hoch erfüllt;

b) mit einem Zertifikat einer qualifizierten elektronischen Signatur oder eines qualifizierten elektronischen Siegels, das gemäß Buchstabe a, c oder d ausgestellt wurde;

c) mit anderen Identifizierungsmethoden, die die Identifizierung der Person mit einem hohen Maß an Vertrauen gewährleisten und deren Konformität von einer Konformitätsbewertungsstelle bestätigt wird;

d) durch die physische Anwesenheit der natürlichen Person oder eines bevollmächtigten Vertreters der juristischen Person nach geeigneten Nachweisen und Verfahren im Einklang mit dem nationalen Recht.

(1b) Die Überprüfung der Attribute gemäß Absatz 1 wird anhand geeigneter Mittel vom qualifizierten Vertrauensdiensteanbieter entweder unmittelbar oder über einen Dritten auf der Grundlage einer der folgenden Methoden oder — sofern erforderlich — einer Kombination davon im Einklang mit den in Absatz 1c genannten Durchführungsrechtsakten durchgeführt:

a) mit der europäischen Brieftasche für die Digitale Identität oder einem notifizierten elektronischen Identifizierungsmittel, das die Anforderungen des Artikels 8 in Bezug auf das Sicherheitsniveau hoch erfüllt;

b) mit einem Zertifikat einer qualifizierten elektronischen Signatur oder eines qualifizierten elektronischen Siegels, das gemäß Absatz 1a Buchstabe a, c oder d ausgestellt wurde;

c) mit einer qualifizierten elektronischen Attributsbescheinigung;

d) mit anderen Methoden, die die Überprüfung von Attributen mit einem hohen Maß an Vertrauen gewährleisten und deren Konformität von einer Konformitätsbewertungsstelle bestätigt wird;

e) über die physische Anwesenheit der natürlichen Person oder eines bevollmächtigten Vertreters der juristischen Person nach geeigneten Nachweisen und Verfahren im Einklang mit dem nationalen Recht.

(1c) Bis zum 21. Mai 2025 erstellt die Kommission im Wege von Durchführungsrechtsakten eine Liste von Referenzstandards und legt, sofern erforderlich, Spezifikationen und Verfahren für die Überprüfung der Identität und der Attribute im Einklang mit Absätzen 1, 1a und 1b dieses Artikels fest. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 48 Absatz 2 genannten Prüfverfahren erlassen.

(2) Für qualifizierte Vertrauensdiensteanbieter, die qualifizierte Vertrauensdienste erbringen, gilt Folgendes:

a) Sie unterrichten die Aufsichtsstelle mindestens einen Monat vor der Vornahme von Änderungen bei der Erbringung ihrer qualifizierten Vertrauensdienste bzw. mindestens drei Monate vorher im Fall einer beabsichtigten Einstellung dieser Tätigkeiten.

b) Sie beschäftigen Personal und gegebenenfalls Unterauftragnehmer, das bzw. die über das erforderliche Fachwissen, die erforderliche Zuverlässigkeit, die erforderliche Erfahrung und die erforderlichen Qualifikationen verfügt bzw. verfügen, in Bezug auf die Vorschriften für die Sicherheit und den Schutz personenbezogener Daten angemessen geschult worden ist und Verwaltungs- und Managementverfahren anwendet, die den anerkannten europäischen oder internationalen Normen entsprechen.

c) Sie verfügen in Bezug auf das Haftungsrisiko für Schäden gemäß Artikel 13 über ausreichende Finanzmittel und/oder schließen eine angemessene Haftpflichtversicherung nach nationalem Recht ab.

d) Sie informieren Personen, die einen qualifizierten Vertrauensdienst nutzen wollen, in klarer, umfassender und leicht zugänglicher Weise in einem öffentlich zugänglichen Raum und individuell über die genauen Bedingungen für die Nutzung des Dienstes, einschließlich Nutzungsbeschränkungen, bevor sie vertragliche Beziehungen zu dieser Person eingehen.

e) Sie verwenden vertrauenswürdige Systeme und Produkte, die vor Veränderungen geschützt sind und die technische Sicherheit und Zuverlässigkeit der von ihnen unterstützten Prozesse sicherstellen, einschließlich der Verwendung geeigneter kryptografischer Verfahren.

f) Sie verwenden vertrauenswürdige Systeme für die Speicherung der ihnen übermittelten Daten in einer überprüfbaren Form, so dass

   i) diese nur mit Zustimmung der Person, auf die sich die Daten beziehen, öffentlich abrufbar sind,

   ii) nur befugte Personen Daten eingeben und gespeicherte Daten ändern können,

   iii) die Daten auf ihre Echtheit hin überprüft werden können.

fa) Unbeschadet des Artikels 21 der Richtlinie (EU) 2022/2555 haben sie angemessene Strategien und treffen entsprechende Maßnahmen zur Beherrschung rechtlicher, geschäftlicher, betrieblicher und sonstiger direkter oder indirekter Risiken bei der Erbringung des qualifizierten Vertrauensdienstes, einschließlich zumindest Maßnahmen in Bezug auf Folgendes:

   i) Registrierungs- und Einbindungsverfahren für einen Dienst;

ii) Verfahrens- oder Verwaltungskontrollen;

iii) die Verwaltung und Durchführung von Diensten.

fb) Sie teilen der Aufsichtsstelle, den identifizierbaren betroffenen Personen, gegebenenfalls anderen einschlägigen zuständigen Stellen und — auf Ersuchen der Aufsichtsstelle — der Öffentlichkeit, wenn es von öffentlichem Interesse ist, unverzüglich, in jedem Fall innerhalb von 24 Stunden nach dem Vorfall, alle Sicherheitsverstöße oder Störungen bei der Erbringung des Dienstes oder der Durchführung der in Buchstabe fa Ziffern i, ii oder iii genannten Maßnahmen, die erhebliche Auswirkungen auf den erbrachten Vertrauensdienst oder die darin gespeicherten personenbezogenen Daten haben, mit.

g) Sie ergreifen geeignete Maßnahmen gegen Fälschung, Diebstahl oder missbräuchliche Verwendung von Daten oder gegen unberechtigte Löschung, Änderung oder Unzugänglichmachung von Daten;

h) Sie zeichnen alle einschlägigen Informationen über die von dem qualifizierten Vertrauensdiensteanbieter ausgegebenen und empfangenen Daten auf und bewahren sie auch nach der Einstellung der Tätigkeit des qualifizierten Vertrauensdiensteanbieters so lange wie nötig auf, um bei Gerichtsverfahren entsprechende Beweismittel liefern zu können und die Kontinuität des Dienstes sicherzustellen. Die Aufzeichnung kann in elektronischer Form erfolgen.

i) Sie verfügen über einen fortlaufend aktualisierten Beendigungsplan, um die Kontinuität des Dienstes nach den von der Aufsichtsstelle gemäß Artikel 46b Absatz 4 Buchstabe i geprüften Vorgaben sicherzustellen.

k) Sie erstellen im Falle qualifizierter Vertrauensdiensteanbieter, die qualifizierte Zertifikate ausstellen, eine Zertifikatsdatenbank und halten sie auf dem neuesten Stand.

Die Aufsichtsstelle kann ergänzende Informationen zu den gemäß Unterabsatz 1 Buchstabe a übermittelten Angaben oder das Ergebnis einer Konformitätsbewertung anfordern und kann die Erteilung der Erlaubnis, die beabsichtigten Änderungen an den qualifizierten Vertrauensdiensten vorzunehmen, an Bedingungen knüpfen. Wird die Überprüfung nicht innerhalb von drei Monaten nach der Mitteilung abgeschlossen, so unterrichtet die Aufsichtsstelle den Vertrauensdiensteanbieter hierüber unter Angabe der Gründe für die Verzögerung und der Frist, innerhalb deren die Überprüfung abzuschließen ist.

(3) Beschließt ein qualifizierter Vertrauensdiensteanbieter, der qualifizierte Zertifikate ausstellt, ein Zertifikat zu widerrufen, so registriert er den Widerruf in seiner Zertifikatsdatenbank und veröffentlicht den Widerrufsstatus des Zertifikats zeitnah und in jedem Fall innerhalb von 24 Stunden nach Erhalt des Ersuchens. Der Widerruf wird sofort nach seiner Veröffentlichung wirksam.

(4) Im Zusammenhang mit Absatz 3 stellen qualifizierte Vertrauensdiensteanbieter, die qualifizierte Zertifikate ausstellen, den vertrauenden Beteiligten Informationen über den Gültigkeits- oder Widerrufsstatus der von ihnen ausgestellten qualifizierten Zertifikate zur Verfügung. Diese Informationen werden zumindest auf Zertifikatsbasis jederzeit und über die Gültigkeitsdauer des Zertifikats hinaus automatisch auf zuverlässige, kostenlose und effiziente Weise bereitgestellt.

(4a) Die Absätze 3 und 4 gelten für den Widerruf qualifizierter elektronischer Attributsbescheinigungen entsprechend.

(4b) Der Kommission wird die Befugnis übertragen, gemäß Artikel 47 delegierte Rechtsakte zur Einführung von zusätzlichen Maßnahmen im Sinne von Absatz 2 Buchstabe fa dieses Artikels zu erlassen.

(5) Bis zum 21. Mai 2025 erstellt die Kommission im Wege von Durchführungsrechtsakten eine Liste von Referenzstandards und legt, sofern erforderlich, die Spezifikationen und Verfahren für die in Absatz 2 des vorliegenden Artikels genannten Anforderungen fest. Werden diese Standards, Spezifikationen und Verfahren eingehalten, so wird davon ausgegangen, dass die Anforderungen dieses Absatzes erfüllt sind. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 48 Absatz 2 genannten Prüfverfahren erlassen.

Artikel 24a
Anerkennung qualifizierter Vertrauensdienste

(1) Qualifizierte elektronische Signaturen, die auf einem von einem Mitgliedstaat ausgestellten qualifizierten Zertifikat beruhen, und qualifizierte elektronische Siegel, die auf einem in einem Mitgliedstaat ausgestellten qualifizierten Zertifikat beruhen, werden in allen anderen Mitgliedstaaten als qualifizierte elektronische Signaturen bzw. qualifizierte elektronische Siegel anerkannt.

(2) In einem Mitgliedstaat zertifizierte qualifizierte elektronische Signaturerstellungseinheiten und qualifizierte elektronische Siegelerstellungseinheiten werden in allen anderen Mitgliedstaaten als qualifizierte elektronische Signaturerstellungseinheiten bzw. qualifizierte elektronische Siegelerstellungseinheiten anerkannt.

(3) Ein qualifiziertes Zertifikat für elektronische Signaturen, ein qualifiziertes Zertifikat für elektronische Siegel, ein qualifizierter Vertrauensdienst zur Verwaltung qualifizierter elektronischer Fernsignaturerstellungseinheiten und ein qualifizierter Vertrauensdienst zur Verwaltung qualifizierter elektronischer Fernsiegelerstellungseinheiten, das bzw. der in einem Mitgliedstaat bereitgestellt wird, wird in alle anderen Mitgliedstaaten als qualifiziertes Zertifikat für elektronische Signaturen, qualifiziertes Zertifikat für elektronische Siegel, qualifizierter Vertrauensdienst zur Verwaltung qualifizierter elektronischer Fernsignaturerstellungseinheiten und qualifizierter Vertrauensdienst zur Verwaltung qualifizierter elektronischer Fernsiegelerstellungseinheiten anerkannt.

(4) Ein qualifizierter Validierungsdienst für qualifizierte elektronische Signaturen und ein qualifizierter Validierungsdienst für qualifizierte elektronische Siegel, die in einem Mitgliedstaat bereitgestellt werden, werden in allen anderen Mitgliedstaaten als qualifizierter Validierungsdienst für qualifizierte elektronische Signaturen bzw. qualifizierter Validierungsdienst für qualifizierte elektronische Siegel anerkannt.

(5) Ein qualifizierter Bewahrungsdienst für qualifizierte elektronische Signaturen und ein qualifizierter Bewahrungsdienst für qualifizierte elektronische Siegel, die in einem Mitgliedstaat bereitgestellt werden, werden in allen anderen Mitgliedstaaten als qualifizierter Bewahrungsdienst für qualifizierte elektronische Signaturen bzw. qualifizierter Bewahrungsdienst für qualifizierte elektronische Siegel anerkannt.

(6) Ein in einem Mitgliedstaat bereitgestellter qualifizierter elektronischer Zeitstempel wird in allen anderen Mitgliedstaaten als qualifizierter elektronischer Zeitstempel anerkannt.

(7) Ein in einem Mitgliedstaat ausgestelltes qualifiziertes Zertifikat für die Website-Authentifizierung wird in allen anderen Mitgliedstaaten als qualifiziertes Zertifikat für die Website-Authentifizierung anerkannt.

(8) Ein in einem Mitgliedstaat bereitgestellter qualifizierter Dienst für die Zustellung elektronischer Einschreiben wird in allen anderen Mitgliedstaaten als qualifizierter Dienst für die Zustellung elektronischer Einschreiben anerkannt.

(9) Eine in einem Mitgliedstaat ausgestellte qualifizierte elektronische Attributsbescheinigung wird in allen anderen Mitgliedstaaten als qualifizierte elektronische Attributsbescheinigung anerkannt.

(10) Ein qualifizierter elektronischer Archivierungsdienst, der in einem Mitgliedstaat bereitgestellt wird, wird in allen anderen Mitgliedstaaten als qualifizierter elektronischer Archivierungsdienst anerkannt.

(11) Ein qualifiziertes elektronisches Journal, das in einem Mitgliedstaat bereitgestellt wird, wird in allen anderen Mitgliedstaaten als qualifiziertes elektronisches Journal anerkannt.

ABSCHNITT 4
Elektronische Signaturen

Artikel 25
Rechtswirkung elektronischer Signaturen

(1) Einer elektronischen Signatur darf die Rechtswirkung und die Zulässigkeit als Beweismittel in Gerichtsverfahren nicht allein deshalb abgesprochen werden, weil sie in elektronischer Form vorliegt oder weil sie die Anforderungen an qualifizierte elektronische Signaturen nicht erfüllt.

(2) Eine qualifizierte elektronische Signatur hat die gleiche Rechtswirkung wie eine handschriftliche Unterschrift.

Artikel 26
Anforderungen an fortgeschrittene elektronische Signaturen

Eine fortgeschrittene elektronische Signatur erfüllt alle folgenden Anforderungen:

a) Sie ist eindeutig dem Unterzeichner zugeordnet.

b) Sie ermöglicht die Identifizierung des Unterzeichners.

c) Sie wird unter Verwendung elektronischer Signaturerstellungsdaten erstellt, die der Unterzeichner mit einem hohen Maß an Vertrauen unter seiner alleinigen Kontrolle verwenden kann.

d) Sie ist so mit den auf diese Weise unterzeichneten Daten verbunden, dass eine nachträgliche Veränderung der Daten erkannt werden kann.

(2) Bis zum 21. Mai 2026 bewertet die Kommission, ob es erforderlich ist, Durchführungsrechtsakte zu erlassen, mit denen eine Liste von Referenzstandards erstellt wird und gegebenenfalls Spezifikationen und Verfahren für fortgeschrittene elektronische Signaturen festgelegt werden. Auf der Grundlage dieser Bewertung kann die Kommission solche Durchführungsrechtsakte erlassen. Bei fortgeschrittenen elektronischen Signaturen, die diese Stan-

dards, Spezifikationen und Verfahren erfüllen, wird davon ausgegangen, dass sie die Anforderungen an fortgeschrittene elektronische Signaturen erfüllen. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 48 Absatz 2 genannten Prüfverfahren erlassen.

Artikel 27
Elektronische Signaturen in öffentlichen Diensten

(1) Verlangt ein Mitgliedstaat für die Verwendung in einem Online-Dienst, der von einer öffentlichen Stelle oder im Namen einer öffentlichen Stelle angeboten wird, eine fortgeschrittene elektronische Signatur, so erkennt dieser Mitgliedstaat fortgeschrittene elektronische Signaturen, fortgeschrittene elektronische Signaturen, die auf einem qualifizierten Zertifikat für elektronische Signaturen beruhen, und qualifizierte elektronische Signaturen zumindest in den Formaten oder unter Verwendung der Verfahren an, die in den Durchführungsrechtsakten nach Absatz 5 festgelegt sind.

(2) Verlangt ein Mitgliedstaat für die Verwendung in einem Online-Dienst, der von einer öffentlichen Stelle oder im Namen einer öffentlichen Stelle angeboten wird, eine fortgeschrittene elektronische Signatur, die auf einem qualifizierten Zertifikat beruht, so erkennt dieser Mitgliedstaat fortgeschrittene elektronische Signaturen, die auf einem qualifizierten Zertifikat beruhen, und qualifizierte elektronische Signaturen zumindest in den Formaten oder unter Verwendung der Verfahren an, die in den Durchführungsrechtsakten nach Absatz 5 festgelegt sind.

(3) Die Mitgliedstaaten verlangen für die grenzüberschreitende Verwendung in einem Online-Dienst, der von einer öffentlichen Stelle angeboten wird, keine elektronische Signatur mit einem höheren Sicherheitsniveau als dem der qualifizierten elektronischen Signatur.

(5) Die Kommission legt bis zum 18. September 2015 im Wege von Durchführungsrechtsakten und unter Berücksichtigung der bestehenden Praxis sowie bestehender Normen und Unionsrechtsvorschriften Referenzformate für fortgeschrittene elektronische Signaturen oder Referenzverfahren fest, wenn alternative Formate verwendet werden. Diese Durchführungsrechtsakte werden nach dem in Artikel 48 Absatz 2 genannten Prüfverfahren erlassen.

Artikel 28
Qualifizierte Zertifikate für elektronische Signaturen

(1) Qualifizierte Zertifikate für elektronische Signaturen müssen die Anforderungen des Anhangs I erfüllen.

(2) Für qualifizierte Zertifikate für elektronische Signaturen dürfen keine obligatorischen Anforderungen gelten, die über die in Anhang I festgelegten hinausgehen.

(3) Qualifizierte Zertifikate für elektronische Signaturen können zusätzliche fakultative spezifische Attribute enthalten. Diese Attribute dürfen die Interoperabilität und Anerkennung qualifizierter elektronischer Signaturen nicht berühren.

(4) Wird ein qualifiziertes Zertifikat für elektronische Signaturen nach der anfänglichen Aktivierung widerrufen, ist es ab dem Zeitpunkt des Widerrufs nicht mehr gültig und sein Status darf unter keinen Umständen rückgängig gemacht werden.

(5) Die Mitgliedstaaten können vorbehaltlich der folgenden Bedingungen nationale Vorschriften zur vorläufigen Aussetzung eines qualifizierten Zertifikats für eine elektronische Signatur erlassen:

a) Ist ein qualifiziertes Zertifikat für elektronische Signaturen vorläufig ausgesetzt worden, so verliert dieses Zertifikat für die Dauer der Aussetzung seine Gültigkeit.

b) Die Dauer der Aussetzung wird in der Zertifikatsdatenbank deutlich angegeben und der Status der Aussetzung ist während der Dauer der Aussetzung im Rahmen des Dienstes, der die Informationen über den Status des Zertifikats bereitstellt, ersichtlich.

(6) Bis zum 21. Mai 2025 erstellt die Kommission im Wege von Durchführungsrechtsakten eine Liste von Referenzstandards und legt, sofern erforderlich, Spezifikationen und Verfahren für qualifizierte Zertifikate für elektronische Signaturen fest. Bei qualifizierten Zertifikaten für elektronische Signaturen, die diese Standards, Spezifikationen und Verfahren erfüllen, wird davon ausgegangen, dass sie die Anforderungen des Anhangs I erfüllen. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 48 Absatz 2 genannten Prüfverfahren erlassen.

Artikel 29
Anforderungen an qualifizierte elektronische Signaturerstellungseinheiten

(1) Qualifizierte elektronische Signaturerstellungseinheiten müssen die Anforderungen des Anhangs II erfüllen.

(1a) Das Erzeugen oder Verwalten elektronischer Signaturerstellungsdaten oder das Vervielfältigen solcher Signaturerstellungsdaten zu Sicherungszwecken wird nur im Namen des Unterzeichners, auf dessen Verlangen, und von einem qualifizierten Vertrauensdiensteanbieter durchgeführt, der einen qualifizierten Vertrauensdienst zur Verwaltung einer qualifizierten elektronischen Fernsignaturerstellungseinheit erbringt.

(2) Die Kommission kann im Wege von Durchführungsrechtsakten Kennnummern für Normen für qualifizierte elektronische Signaturerstellungseinheiten festlegen. Bei qualifizierten elektronischen Signaturerstellungseinheiten, die diesen Normen entsprechen, wird davon ausgegangen, dass sie die Anforderungen des Anhangs II erfüllen. Diese Durchführungsrechtsakte werden nach dem in Artikel 48 Absatz 2 genannten Prüfverfahren erlassen.

Artikel 29a
Anforderungen an einen qualifizierten Dienst zur Verwaltung qualifizierter elektronischer Fernsignaturerstellungseinheiten

(1) Die Verwaltung qualifizierter Fernsignaturerstellungseinheiten als qualifizierter Dienst wird nur von einem qualifizierten Vertrauensdiensteanbieter durchgeführt, der

a) elektronische Signaturerstellungsdaten im Namen des Unterzeichners erzeugt oder verwaltet;

b) unbeschadet Anhang II Nummer 1 Buchstabe d die elektronischen Signaturerstellungsdaten nur zu Sicherungszwecken vervielfältiget, sofern die folgenden Anforderungen erfüllt sind:

   i) die vervielfältigten Datensätze müssen das gleiche Sicherheitsniveau wie die Original-Datensätze aufweisen;

   ii) es dürfen nicht mehr vervielfältigte Datensätze vorhanden sein als zur Gewährleistung der Kontinuität des Dienstes unbedingt nötig;

c) alle Anforderungen erfüllt, die in dem gemäß Artikel 30 ausgestellten Zertifizierungsbericht für die spezifische qualifizierte elektronische Fernsignaturerstellungseinheit angegeben sind.

(2) Bis zum 21. Mai 2025 erstellt die Kommission im Wege von Durchführungsrechtsakten eine Liste von Referenzstandards und legt, sofern erforderlich, Spezifikationen und Verfahren für die Zwecke des Absatzes 1 des vorliegenden Artikels fest. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 48 Absatz 2 genannten Prüfverfahren erlassen.

Artikel 30
Zertifizierung qualifizierter elektronischer Signaturerstellungseinheiten

(1) Die Konformität qualifizierter elektronischer Signaturerstellungseinheiten mit den Anforderungen des Anhangs II wird von geeigneten, von den Mitgliedstaaten benannten öffentlichen oder privaten Stellen zertifiziert.

(2) Die Mitgliedstaaten teilen der Kommission die Namen und Anschriften der öffentlichen oder privaten Stellen gemäß Absatz 1 mit. Die Kommission stellt diese Informationen den Mitgliedstaaten zur Verfügung.

(3) Die Zertifizierung nach Absatz 1 beruht auf einem der folgenden Verfahren:

a) einem Sicherheitsbewertungsverfahren, das entsprechend einer der Normen für die Sicherheitsbewertung informationstechnischer Produkte durchgeführt wurde, die auf der gemäß Unterabsatz 2 aufzustellenden Liste stehen;

b) einem anderen als dem unter Buchstabe a genannten Verfahren, sofern dabei gleichwertige Sicherheitsniveaus angewendet werden und die öffentliche oder private Stelle gemäß Absatz 1 der Kommission dieses Verfahren mitteilt. Dieses Verfahren darf nur angewendet werden, wenn Normen im Sinne des Buchstaben a nicht vorliegen oder ein Sicherheitsbewertungsverfahren im Sinne des Buchstaben a im Gange ist.

Die Kommission stellt im Wege von Durchführungsrechtsakten eine Liste mit Normen für die Sicherheitsbewertung informationstechnischer Produkte nach Buchstabe a auf. Diese Durchführungsrechtsakte werden nach dem in Artikel 48 Absatz 2 genannten Prüfverfahren erlassen.

(3a) Die Gültigkeitsdauer einer Zertifizierung nach Absatz 1 darf einen Zeitraum von fünf Jahren nicht überschreiten, sofern Schwachstellenbeurteilungen alle zwei Jahre durchgeführt werden. Werden Schwachstellen festgestellt und nicht behoben, so wird die Zertifizierung aufgehoben.

(4) Der Kommission wird die Befugnis übertragen, gemäß Artikel 47 delegierte Rechtsakte in Bezug auf die Festlegung besonderer Kriterien, die von den in Absatz 1 dieses Artikels aufgeführten benannten Stellen zu erfüllen sind, zu erlassen.

Artikel 31
Veröffentlichung einer Liste zertifizierter qualifizierter elektronischer Signaturerstellungseinheiten

(1) Die Mitgliedstaaten notifizieren der Kommission unverzüglich, spätestens aber innerhalb eines Monats nach Abschluss der Zertifizierung, Informationen über qualifizierte elektroni-

sche Signaturerstellungseinheiten, die von den in Artikel 30 Absatz 1 genannten Stellen zertifiziert worden sind. Sie notifizieren der Kommission ferner unverzüglich, spätestens aber innerhalb eines Monats nach Annullierung der Zertifizierung, Informationen über nicht mehr zertifizierte elektronische Signaturerstellungseinheiten.

(2) Auf der Grundlage der erhaltenen Informationen sorgt die Kommission für die Aufstellung, Veröffentlichung und Führung einer Liste zertifizierter qualifizierter elektronischer Signaturerstellungseinheiten.

(3) Bis zum 21. Mai 2025 legt die Kommission im Wege von Durchführungsrechtsakten Form und Verfahren, die für die Zwecke des Absatzes 1 dieses Artikels anwendbar sind, fest. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 48 Absatz 2 genannten Prüfverfahren erlassen.

Artikel 32
Anforderungen an die Validierung qualifizierter elektronischer Signaturen

(1) Mit dem Verfahren für die Validierung einer qualifizierten elektronischen Signatur wird die Gültigkeit einer qualifizierten elektronischen Signatur bestätigt, wenn

a) das der Signatur zugrunde liegende Zertifikat zum Zeitpunkt des Signierens ein qualifiziertes Zertifikat für elektronische Signaturen war, das die Anforderungen des Anhangs I erfüllt,

b) das qualifizierte Zertifikat von einem qualifizierten Vertrauensdiensteanbieter ausgestellt wurde und zum Zeitpunkt des Signierens gültig war,

c) die Signaturvalidierungsdaten den Daten entsprechen, die dem vertrauenden Beteiligten bereitgestellt werden,

d) der eindeutige Datensatz, der den Unterzeichner im Zertifikat repräsentiert, dem vertrauenden Beteiligten korrekt bereitgestellt wird,

e) die etwaige Benutzung eines Pseudonyms dem vertrauenden Beteiligten eindeutig angegeben wird, wenn zum Zeitpunkt des Signierens ein Pseudonym benutzt wurde,

f) die elektronische Signatur von einer qualifizierten elektronischen Signaturerstellungseinheit erstellt wurde,

g) die Unversehrtheit der unterzeichneten Daten nicht beeinträchtigt ist,

h) die Anforderungen des Artikels 26 zum Zeitpunkt des Signierens erfüllt waren.

Bei einer Validierung qualifizierter elektronischer Signaturen, die den in Absatz 3 genannten Standards, Spezifikationen und Verfahren entspricht, wird davon ausgegangen, dass sie die Anforderungen des Unterabsatzes 1 erfüllt.

(2) Das zur Validierung der qualifizierten elektronischen Signatur verwendete System stellt dem vertrauenden Beteiligten das korrekte Ergebnis des Validierungsprozesses bereit und ermöglicht es ihm, etwaige Sicherheitsprobleme zu erkennen.

(3) Bis zum 21. Mai 2025 erstellt die Kommission im Wege von Durchführungsrechtsakten eine Liste von Referenzstandards und legt, sofern erforderlich, Spezifikationen und Verfahren für die Validierung qualifizierter elektronischer Signaturen fest. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 48 Absatz 2 genannten Prüfverfahren erlassen.

Artikel 32a
Anforderungen an die Validierung fortgeschrittener elektronischer Signaturen, die auf qualifizierten Zertifikaten beruhen

(1) Mit dem Verfahren für die Validierung einer fortgeschrittenen elektronischen Signatur, die auf einem qualifizierten Zertifikat beruht, wird die Gültigkeit einer fortgeschrittenen elektronischen Signatur, die auf einem qualifizierten Zertifikat beruht, bestätigt, wenn

a) das der Signatur zugrunde liegende Zertifikat zum Zeitpunkt des Signierens ein qualifiziertes Zertifikat für elektronische Signaturen war, das die Anforderungen des Anhangs I erfüllt,

b) das qualifizierte Zertifikat von einem qualifizierten Vertrauensdiensteanbieter ausgestellt wurde und zum Zeitpunkt des Signierens gültig war,

c) die Signaturvalidierungsdaten den Daten entsprechen, die dem vertrauenden Beteiligten bereitgestellt werden,

d) der eindeutige Datensatz, der den Unterzeichner im Zertifikat repräsentiert, dem vertrauenden Beteiligten korrekt bereitgestellt wird,

e) die etwaige Benutzung eines Pseudonyms dem vertrauenden Beteiligten eindeutig angegeben wird, wenn zum Zeitpunkt des Signierens ein Pseudonym benutzt wurde,

f) die Unversehrtheit der unterzeichneten Daten nicht beeinträchtigt ist,

g) die Anforderungen des Artikels 26 zum Zeitpunkt des Signierens erfüllt waren.

(2) Das zur Validierung der auf einem qualifizierten Zertifikat beruhenden fortgeschrittenen elektronischen Signatur verwendete System stellt dem vertrauenden Beteiligten das korrekte Ergebnis des Validierungsprozesses bereit und ermöglicht es ihm, etwaige Sicherheitsprobleme zu erkennen.

(3) Bis zum 21. Mai 2025 erstellt die Kommission im Wege von Durchführungsrechtsakten eine Liste von Referenzstandards und legt, sofern erforderlich, Spezifikationen und Verfahren für die Validierung fortgeschrittener elektronischer Signaturen, die auf qualifizierten Zertifikaten beruhen, fest. Bei einer Validierung fortgeschrittener elektronischer Signaturen, die auf qualifizierten Zertifikaten beruhen, die diesen Standards, Spezifikationen und Verfahren entspricht, wird davon ausgegangen, dass sie die Anforderungen des Absatzes 1 des vorliegenden Artikels erfüllt. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 48 Absatz 2 genannten Prüfverfahren erlassen.

Artikel 33
Qualifizierter Validierungsdienst für qualifizierte elektronische Signaturen

(1) Qualifizierte Validierungsdienste für qualifizierte elektronische Signaturen können nur von qualifizierten Vertrauensdiensteanbietern erbracht werden, die

a) eine Validierung gemäß Artikel 32 Absatz 1 durchführen und

b) es vertrauenden Beteiligten ermöglichen, das Ergebnis des Validierungsprozesses automatisch in zuverlässiger und effizienter Weise mit Bestätigung durch die fortgeschrittene elektronische Signatur oder das fortgeschrittene elektronische Siegel des Anbieters des qualifizierten Validierungsdienstes zu erhalten.

(2) Bis zum 21. Mai 2025 erstellt die Kommission im Wege von Durchführungsrechtsakten eine Liste von Referenzstandards und legt, sofern erforderlich, die Spezifikationen und Verfahren für qualifizierte Validierungsdienste nach Absatz 1 dieses Artikels fest. Bei einer Validierung qualifizierter Validierungsdienste für qualifizierte elektronische Signaturen, die diesen Standards, Spezifikationen und Verfahren entspricht, wird davon ausgegangen, dass sie die Anforderungen des Absatzes 1 des vorliegenden Artikels erfüllt. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 48 Absatz 2 genannten Prüfverfahren erlassen.

Artikel 34
Qualifizierter Bewahrungsdienst für qualifizierte elektronische Signaturen

(1) Ein qualifizierter Bewahrungsdienst für qualifizierte elektronische Signaturen kann nur von qualifizierten Vertrauensdiensteanbietern erbracht werden, die Verfahren und Technologien verwenden, die es ermöglichen, die Vertrauenswürdigkeit der qualifizierten elektronischen Signatur über den Zeitraum ihrer technologischen Geltung hinaus zu verlängern.

(1a) Bei Regelungen für qualifizierte Bewahrungsdienste für qualifizierte elektronische Signaturen, die den in Absatz 2 genannten Standards, Spezifikationen und Verfahren entsprechen, wird davon ausgegangen, dass sie die Anforderungen des Absatzes 1 erfüllen.

(2) Bis zum 21. Mai 2025 erstellt die Kommission im Wege von Durchführungsrechtsakten eine Liste von Referenzstandards und legt, sofern erforderlich, Spezifikationen und Verfahren für qualifizierte Bewahrungsdienste für qualifizierte elektronische Signaturen fest. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 48 Absatz 2 genannten Prüfverfahren erlassen.

ABSCHNITT 5
Elektronische Siegel

Artikel 35
Rechtswirkung elektronischer Siegel

(1) Einem elektronischen Siegel darf die Rechtswirkung und die Zulässigkeit als Beweismittel in Gerichtsverfahren nicht allein deshalb abgesprochen werden, weil es in einer elektronischen Form vorliegt oder nicht die Anforderungen an qualifizierte elektronische Siegel erfüllt.

(2) Für ein qualifiziertes elektronisches Siegel gilt die Vermutung der Unversehrtheit der Daten und der Richtigkeit der Herkunftsangabe der Daten, mit denen das qualifizierte elektronische Siegel verbunden ist.

Artikel 36
Anforderungen an fortgeschrittene elektronische Siegel

Ein fortgeschrittenes elektronisches Siegel erfüllt alle folgenden Anforderungen:

a) Es ist eindeutig dem Siegelersteller zugeordnet.

b) Es ermöglicht die Identifizierung des Siegelerstellers.

c) Es wird unter Verwendung von elektronischen Siegelerstellungsdaten erstellt, die der Siegelersteller mit einem hohen Maß an Vertrauen unter seiner Kontrolle zum Erstellen elektronischer Siegel verwenden kann.

d) Es ist so mit den Daten, auf die es sich bezieht, verbunden, dass eine nachträgliche Veränderung der Daten erkannt werden kann.

(2) Bis zum 21. Mai 2026 führt die Kommission eine Bewertung durch, ob es erforderlich ist, Durchführungsrechtsakte zu erlassen, mit denen eine Liste von Referenzstandards erstellt wird und gegebenenfalls Spezifikationen und Verfahren für fortgeschrittene elektronische Signaturen festgelegt werden. Auf der Grundlage der Ergebnisse dieser Bewertung kann die Kommission solche Durchführungsrechtsakte erlassen. Bei fortgeschrittenen elektronischen Siegeln, die diesen Standards, Spezifikationen und Verfahren entsprechen, wird davon ausgegangen, dass sie die Anforderungen an fortgeschrittene elektronische Siegel erfüllen. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 48 Absatz 2 genannten Prüfverfahren erlassen.

Artikel 37
Elektronische Siegel in öffentlichen Diensten

(1) Verlangt ein Mitgliedstaat ein fortgeschrittenes elektronisches Siegel für die Verwendung in einem Online-Dienst, der von einer öffentlichen Stelle oder im Namen einer öffentlichen Stelle angeboten wird, so erkennt dieser Mitgliedstaat fortgeschrittene elektronische Siegel, fortgeschrittene elektronische Siegel, die auf einem qualifizierten Zertifikat für elektronische Siegel beruhen, und qualifizierte elektronische Siegel zumindest in den Formaten oder unter Verwendung der Verfahren, die in den Durchführungsrechtsakten nach Absatz 5 festgelegt sind, an.

(2) Verlangt ein Mitgliedstaat für die Verwendung in einem Online-Dienst, der von einer öffentlichen Stelle oder im Namen einer öffentlichen Stelle angeboten wird, ein fortgeschrittenes elektronisches Siegel, das auf einem qualifizierten Zertifikat beruht, so erkennt dieser Mitgliedstaat fortgeschrittene elektronische Siegel, die auf einem qualifizierten Zertifikat beruhen, und qualifizierte elektronische Siegel zumindest in den Formaten oder unter Verwendung der Verfahren, die in den Durchführungsrechtsakten nach Absatz 5 festgelegt sind, an.

(3) Die Mitgliedstaaten verlangen für die grenzüberschreitende Verwendung in einem Online-Dienst, der von einer öffentlichen Stelle angeboten wird, kein elektronisches Siegel mit einem höheren Sicherheitsniveau als dem des qualifizierten elektronischen Siegels.

(5) Die Kommission legt bis zum 18. September 2015 im Wege von Durchführungsrechtsakten und unter Berücksichtigung der bestehenden Praxis sowie der bestehenden Normen und Unionsrechtsakte Durchführungsrechtsakte Referenzformate für fortgeschrittene elektronische Siegel oder Referenzverfahren fest, wenn alternative Formate verwendet werden. Diese Durchführungsrechtsakte werden nach dem in Artikel 48 Absatz 2 genannten Prüfverfahren erlassen.

Artikel 38
Qualifizierte Zertifikate für elektronische Siegel

(1) Qualifizierte Zertifikate für elektronische Siegel müssen die Anforderungen des Anhangs III erfüllen.

(2) Für qualifizierte Zertifikate für elektronische Siegel dürfen keine verbindlichen Anforderungen gelten, die über die in Anhang III festgelegten hinausgehen.

(3) Qualifizierte Zertifikate für elektronische Siegel können zusätzliche fakultative spezifische Attribute enthalten. Diese Attribute berühren nicht die Interoperabilität und Anerkennung qualifizierter elektronischer Siegel.

(4) Wird ein qualifiziertes Zertifikat für elektronische Siegel nach der anfänglichen Aktivierung widerrufen, ist es ab dem Zeitpunkt des Widerrufs nicht mehr gültig und sein Status darf unter keinen Umständen rückgängig gemacht werden.

(5) Die Mitgliedstaaten können vorbehaltlich der folgenden Bedingungen nationale Vorschriften zur vorläufigen Aussetzung qualifizierter Zertifikate für elektronische Siegel erlassen:

a) Ist ein qualifiziertes Zertifikat für elektronische Siegel vorläufig ausgesetzt worden, so verliert dieses Zertifikat für die Dauer der Aussetzung seine Gültigkeit.

b) Die Dauer der Aussetzung wird in der Zertifikatsdatenbank deutlich angegeben und der Status der Aussetzung ist während der Dauer der Aussetzung im Rahmen des Dienstes, der die Informationen über den Status des Zertifikats bereitstellt, ersichtlich.

(6) Bis zum 21. Mai 2025 erstellt die Kommission im Wege von Durchführungsrechtsakten eine Liste von Referenzstandards und legt, sofern erforderlich, Spezifikationen und Verfahren für qualifizierte Zertifikate für elektronische Siegel fest. Bei qualifizierten Zertifikaten für elektronische Siegel, die diesen Standards, Spezifikationen und Verfahren entsprechen, wird davon ausgegangen, dass sie die Anforderungen des Anhangs III erfüllen. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 48 Absatz 2 genannten Prüfverfahren erlassen.

Artikel 39
Qualifizierte elektronische Siegelerstellungseinheiten

(1) Artikel 29 gilt sinngemäß für die Anforderungen an qualifizierte elektronische Siegelerstellungseinheiten.

(2) Artikel 30 gilt sinngemäß für die Zertifizierung qualifizierter elektronischer Siegelerstellungseinheiten.

(3) Artikel 31 gilt sinngemäß für die Veröffentlichung einer Liste qualifizierter elektronischer Siegelerstellungseinheiten.

Artikel 39a
Anforderungen an einen qualifizierten Dienst zur Verwaltung qualifizierter elektronischer Fernsiegelerstellungseinheiten

Artikel 29a gilt sinngemäß für einen qualifizierten Dienst zur Verwaltung qualifizierter elektronischer Fernsiegelerstellungseinheiten.

Artikel 40
Validierung und Bewahrung qualifizierter elektronischer Siegel

Die Artikel 32, 33 und 34 gelten sinngemäß für die Validierung und Bewahrung qualifizierter elektronischer Siegel.

Artikel 40a
Anforderungen an die Validierung fortgeschrittener elektronischer Siegel, die auf qualifizierten Zertifikaten beruhen

Artikel 32a gilt sinngemäß für die Validierung fortgeschrittener elektronischer Siegel, die auf qualifizierten Zertifikaten beruhen.

ABSCHNITT 6
Elektronische Zeitstempel

Artikel 41
Rechtswirkung elektronischer Zeitstempel

(1) Einem elektronischen Zeitstempel darf die Rechtswirkung und die Zulässigkeit als Beweismittel in Gerichtsverfahren nicht allein deshalb abgesprochen werden, weil er in elektronischer Form vorliegt oder nicht die Anforderungen an qualifizierte elektronische Zeitstempel erfüllt.

(2) Für qualifizierte elektronische Zeitstempel gilt die Vermutung der Richtigkeit des Datums und der Zeit, die darin angegeben sind, sowie der Unversehrtheit der mit dem Datum und der Zeit verbundenen Daten.

Artikel 42
Anforderungen an qualifizierte elektronische Zeitstempel

(1) Der qualifizierte elektronische Zeitstempel muss die folgenden Anforderungen erfüllen:

a) Er verknüpft Datum und Zeit so mit Daten, dass die Möglichkeit der unbemerkten Veränderung der Daten nach vernünftigem Ermessen ausgeschlossen ist.

b) Er beruht auf einer korrekten Zeitquelle, die mit der koordinierten Weltzeit verknüpft ist.

c) Er wird mit einer fortgeschrittenen elektronischen Signatur unterzeichnet oder einem fortgeschrittenen elektronischen Siegel des qualifizierten Vertrauensdienstanbieters versiegelt oder es wird ein gleichwertiges Verfahren verwendet.

(1a) Bei der Verknüpfung von Datums- und Zeitangaben mit Daten und einer Richtigkeit der Zeitquellen, die den in Absatz 2 genannten Standards, Spezifikationen und Verfahren entsprechen, wird davon ausgegangen, dass die Anforderungen des Absatzes 1 erfüllt sind.

(2) Bis zum 21. Mai 2025 erstellt die Kommission im Wege von Durchführungsrechtsakten eine Liste von Referenzstandards und legt, sofern erforderlich, Spezifikationen und Verfahren für die Verknüpfung von Datums- und Zeitangaben mit Daten und für die Bestimmung der Richtigkeit von Zeitquellen fest. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 48 Absatz 2 genannten Prüfverfahren erlassen.

ABSCHNITT 7
Dienste für die Zustellung elektronischer Einschreiben

Artikel 43
Rechtswirkung eines Dienstes für die Zustellung elektronischer Einschreiben

(1) Daten, die mittels eines Dienstes für die Zustellung elektronischer Einschreiben abgesendet und empfangen werden, darf die Rechtswirkung und die Zulässigkeit als Beweismittel in Gerichtsverfahren nicht allein deshalb abgesprochen werden, weil sie in elektronischer Form vorliegen oder weil die Anforderungen an qualifizierte Dienste für die Zustellung elektronischer Einschreiben nicht erfüllt sind.

(2) Für Daten, die mittels eines qualifizierten Dienstes für die Zustellung elektronischer Einschreiben abgesendet und empfangen werden, gilt die Vermutung der Unversehrtheit der Daten, der Absendung dieser Daten durch den identifizierten Absender und des Empfangs der Daten durch den identifizierten Empfänger und der Korrektheit des Datums und der Uhrzeit der Absendung und des Empfangs, wie sie von dem qualifizierten Dienst für die Zustellung elektronischer Einschreiben angegeben werden.

Artikel 44
Anforderungen an qualifizierte Dienste für die Zustellung elektronischer Einschreiben

(1) Qualifizierte Dienste für die Zustellung elektronischer Einschreiben müssen folgende Anforderungen erfüllen:

a) Sie werden von einem oder mehreren qualifizierten Vertrauensdiensteanbietern erbracht.

b) Sie stellen die Identifizierung des Absenders mit einem hohen Maß an Vertrauenswürdigkeit sicher.

c) Sie stellen die Identifizierung des Empfängers vor der Zustellung der Daten sicher.

d) Das Absenden und Empfangen der Daten ist durch eine fortgeschrittene elektronische Signatur oder ein fortgeschrittenes elektronisches Siegel eines qualifizierten Vertrauensdiensteanbieters auf eine Weise gesichert, die die Möglichkeit einer unbemerkten Veränderung der Daten ausschließt.

e) Jede Veränderung der Daten, die zum Absenden oder Empfangen der Daten nötig ist, wird dem Absender und dem Empfänger der Daten deutlich angezeigt.

f) Das Datum und die Zeit des Absendens, Empfangens oder einer Änderung der Daten werden durch einen qualifizierten elektronischen Zeitstempel angezeigt.

Im Fall der Weiterleitung der Daten zwischen zwei oder mehreren qualifizierten Vertrauensdiensteanbietern gelten die Anforderungen der Buchstaben a bis f für alle beteiligten qualifizierten Vertrauensdiensteanbieter.

(1a) Bei Prozessen des Absendens und Empfangens von Daten, die den in Absatz 2 genannten Standards, Spezifikationen und Verfahren entsprechen, wird davon ausgegangen, dass sie die Anforderungen des Absatzes 1 erfüllen.

(2) Bis zum 21. Mai 2025 erstellt die Kommission im Wege von Durchführungsrechtsakten eine Liste von Referenzstandards und legt, sofern erforderlich, Spezifikationen und Verfahren für Prozesse des Absendens und Empfangens von Daten fest. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 48 Absatz 2 genannten Prüfverfahren erlassen.

(2a) Anbieter qualifizierter Dienste für die Zustellung elektronischer Einschreiben können sich auf Interoperabilität zwischen von ihnen erbrachten qualifizierten Diensten für die Zustellung elektronischer Einschreiben einigen. Ein solcher Interoperabilitätsrahmen muss die Anforderungen des Absatzes 1 erfüllen und diese Erfüllung wird von einer Konformitätsbewertungsstelle bestätigt.

(2b) Die Kommission kann im Wege von Durchführungsrechtsakten eine Liste von Referenzstandards erstellen und, sofern erforderlich, Spezifikationen und Verfahren für den Interoperabilitätsrahmen nach Absatz 2a des vorliegenden Artikels festlegen. Die technischen Spezifikationen und der Inhalt der Standards müssen kosteneffizient und verhältnismäßig sein. Die Durchführungsrechtsakte werden gemäß dem in Artikel 48 Absatz 2 genannten Prüfverfahren erlassen.

ABSCHNITT 8
Website-Authentifizierung

Artikel 45
Anforderungen an qualifizierte Zertifikate für die Website-Authentifizierung

(1) Qualifizierte Zertifikate für die Website-Authentifizierung müssen die Anforderungen des Anhangs IV erfüllen. Die Bewertung der Erfüllung dieser Anforderungen erfolgt entsprechend den Standards, Spezifikationen und Verfahren nach Absatz 2 dieses Artikels.

(1a) Die gemäß Absatz 1 des vorliegenden Artikels ausgestellten qualifizierten Zertifikate für die Website-Authentifizierung werden von Anbietern von Webbrowsern anerkannt. Anbieter von Webbrowsern stellen sicher, dass in dem Zertifikat bescheinigte Identitätsdaten und zusätzliche bescheinigte Attribute benutzerfreundlich dargestellt werden. Anbieter von Webbrowsern gewährleisten die Unterstützung der in Absatz 1 des vorliegenden Artikels genannten qualifizierten Zertifikate für die Website-Authentifizierung und die Interoperabilität mit diesen; davon ausgenommen sind Kleinstunternehmen und Kleinunternehmen, wie in Artikel 2 des Anhangs der Empfehlung 2003/361/EG der Kommission definiert, während der ersten fünf Jahre ihrer Tätigkeit als Anbieter von Webbrowserdiensten.

(1b) Für qualifizierte Zertifikate für die Website-Authentifizierung dürfen keine verbindlichen Anforderungen gelten, die über die in Absatz1 festgelegten hinausgehen.

(2) Bis zum 21. Mai 2025 erstellt die Kommission im Wege von Durchführungsrechtsakten eine Liste von Referenzstandards und legt, sofern erforderlich, die Spezifikationen und Verfahren für qualifizierte Zertifikate für die Website-Authentifizierung nach Absatz 1 des vorliegenden Artikels fest. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 48 Absatz 2 genannten Prüfverfahren erlassen.

Artikel 45a
Cybersicherheits-Vorsorgemaßnahmen

(1) Anbieter von Webbrowsern ergreifen keine Maßnahmen, die ihren Verpflichtungen nach Artikel 45 entgegenstehen, insbesondere den Anforderungen, qualifizierte Zertifikate für die Website-Authentifizierung anzuerkennen und die bereitgestellten Identitätsdaten benutzerfreundlich darzustellen.

(2) Abweichend von Absatz 1, und nur in Fällen begründeter Bedenken hinsichtlich Sicherheitsverletzungen oder eines Integritätsverlusts eines bestimmten Zertifikats oder eines Satzes von Zertifikaten, können Anbieter von Webbrowsern Vorsorgemaßnahmen in Bezug auf dieses Zertifikat oder diesen Satz von Zertifikaten ergreifen.

(3) Wenn ein Anbieter eines Webbrowsers Maßnahmen gemäß Absatz 2 ergreift, teilt der Anbieter des Webbrowsers der Kommission, der zuständigen Aufsichtsstelle, der Einrichtung, der das Zertifikat ausgestellt wurde und dem qualifizierten Vertrauensdiensteanbieter, der das Zertifikat oder den Satz von Zertifikaten ausgestellt hat, ihre Bedenken unverzüglich schriftlich zusammen mit einer Beschreibung der Maßnahmen, die aufgrund dieser Bedenken ergriffen worden sind, mit. Bei Erhalt einer solchen Meldung stellt die zuständige Aufsichtsstelle dem betreffenden Anbieter des Webbrowsers eine Empfangsbestätigung aus.

(4) Die zuständige Aufsichtsstelle untersucht die in der Meldung vorgebrachten Themen gemäß Artikel 46b Absatz 4 Buchstabe k. Wenn das Ergebnis der Untersuchung nicht zum Widerruf des Qualifikationsstatus des Zertifikats führt, informiert die Aufsichtsstelle den Anbieter des Webbrowsers entsprechend und fordert diesen Anbieter auf, die Vorsorgemaßnahmen nach Absatz 2 dieses Artikels zu beenden.

ABSCHNITT 9
elektronische attributsbescheinigung

Artikel 45b
Rechtswirkungen der elektronischen Attributsbescheinigung

(1) Einer elektronischen Attributsbescheinigung darf die Rechtswirkung oder die Zulässigkeit als Beweismittel in Gerichtsverfahren nicht allein deshalb abgesprochen werden, weil sie in elektronischer Form vorliegt oder nicht die Anforderungen an qualifizierte elektronische Attributsbescheinigungen erfüllt.

(2) Eine qualifizierte elektronische Attributsbescheinigung und Attributsbescheinigungen, die von oder im Namen einer für eine authentische Quelle zuständigen öffentlichen Stelle ausgestellt werden, haben dieselbe Rechtswirkung wie rechtmäßig ausgestellte Bescheinigungen in Papierform.

(3) Eine Attributsbescheinigung, die von oder im Namen einer für eine authentische Quelle zuständigen öffentlichen Stelle in einem Mitgliedstaat ausgestellt wurde, wird in allen Mitgliedstaaten als Attributsbescheinigung, die von oder im Namen einer für eine authentische Quelle zuständigen öffentlichen Stelle ausgestellt wurde, anerkannt.

Artikel 45c
Elektronische Attributsbescheinigung in öffentlichen Diensten

Wird eine elektronische Identifizierung mit einem elektronischen Identifizierungsmittel und einer Authentifizierung nach nationalem Recht für den Zugang zu einem von einer öffentlichen Stelle erbrachten Online-Dienst verlangt, so dürfen Personenidentifizierungsdaten, die in der elektronischen Attributsbescheinigung enthalten sind, eine elektronische Identifizierung mit einem elektronischen Identifizierungsmittel und eine Authentifizierung der elektronischen Identifizierung nicht ersetzen, es sei denn, der Mitgliedstaat hat dies ausdrücklich gestattet. In diesem Fall werden auch qualifizierte elektronische Attributsbescheinigungen aus anderen Mitgliedstaaten akzeptiert.

Artikel 45d
Anforderungen an die qualifizierte elektronische Attributsbescheinigung

(1) Qualifizierte elektronische Attributsbescheinigungen müssen die Anforderungen des Anhangs V erfüllen.

(2) Die Bewertung der Erfüllung der Anforderungen des Anhangs V erfolgt gemäß den in Absatz 5 dieses Artikels genannten Standards, Spezifikationen und Verfahren.

(3) Für qualifizierte elektronische Attributsbescheinigungen dürfen keine verbindlichen Anforderungen gelten, die über die in Anhang V festgelegten hinausgehen.

(4) Wird eine qualifizierte elektronische Attributsbescheinigung nach der anfänglichen Ausstellung widerrufen, so ist sie ab dem Zeitpunkt des Widerrufs nicht mehr gültig und darf unter keinen Umständen erneut Gültigkeit erlangen.

(5) Bis zum 21. November 2024 erstellt die Kommission im Wege von Durchführungsrechtsakten eine Liste von Referenzstandards und legt, sofern erforderlich, Spezifikationen und Verfahren für qualifizierte elektronische Attributsbescheinigungen fest. Diese Durchführungsrechtsakte stehen im Einklang mit den Durchführungsrechtsakten zur Umsetzung der europäischen Brieftasche für die Digitale Identität nach Artikel 5a Absatz 23. Sie werden gemäß dem in Artikel 48 Absatz 2 genannten Prüfverfahren erlassen.

Artikel 45e
Überprüfung der Attribute anhand authentischer Quellen

(1) Die Mitgliedstaaten sorgen innerhalb von 24 Monaten nach dem Tag des Inkrafttretens der Durchführungsrechtsakte nach Artikel 5a Absatz 23 und Artikel 5c Absatz 6 dafür, dass zumindest für die in Anhang VI aufgeführten Attribute, soweit diese Attribute auf authentischen Quellen des öffentlichen Sektors beruhen, Maßnahmen getroffen werden, die es qualifizierten Vertrauensdiensteanbietern elektronischer Attributsbescheinigungen ermöglichen, diese Attribute auf Verlangen des Nutzers gemäß Unionsrecht oder nationalem Recht mit elektronischen Mitteln zu überprüfen.

(2) Bis zum 21. November 2024 erstellt die Kommission unter Berücksichtigung einschlägiger internationaler Normen im Wege von Durchführungsrechtsakten eine Liste von Referenzstandards und legt, sofern erforderlich, Spezifikationen und Verfahren für den Katalog der Attribute sowie die Systeme für die Attributsbescheinigung und die Überprüfungsverfahren für qualifizierte elektronische Attribute für die Zwecke von Absatz 1 des vorliegenden Artikels fest. Diese Durchführungsrechtsakte stehen im Einklang mit den Durchführungsrechtsakten zur Umsetzung der europäischen Brieftasche für die Digitale Identität

nach Artikel 5a Absatz 23. Sie werden gemäß dem in Artikel 48 Absatz 2 genannten Prüfverfahren erlassen.

Artikel 45f
Anforderungen an elektronische Attributsbescheinigungen, die von oder im Namen einer für eine authentische Quelle zuständigen öffentlichen Stelle ausgestellt werden

(1) Eine elektronische Attributsbescheinigung, die von oder im Namen einer für eine authentische Quelle zuständigen öffentlichen Stelle ausgestellt wird, muss folgende Anforderungen erfüllen:

a) die in Anhang VII festgelegten Anforderungen;

b) das qualifizierte Zertifikat, das der qualifizierten elektronischen Signatur oder dem qualifizierten elektronischen Siegel der öffentlichen Stelle nach Artikel 3 Nummer 46, die als Aussteller nach Anhang VII Buchstabe b identifiziert wurde, zugrunde liegt, enthält einen spezifischen Satz zertifizierter Attribute in einer für eine automatisierte Verarbeitung geeigneten Form und

   i) aus dem hervorgeht, dass die ausstellende Stelle gemäß Vorschriften des Unionsrechts oder des nationalen Rechts als für die authentische Quelle, auf deren Grundlage die elektronische Attributsbescheinigung ausgestellt wird, zuständige Stelle oder als die in deren Namen handlungsbefugte Stelle eingerichtet wurde,

   ii) der einen Datensatz enthält, der die unter Ziffer i genannte authentische Quelle eindeutig repräsentiert, und

   iii) in dem die unter Ziffer i genannten Vorschriften des Unionsrechts und des nationalen Rechts angegeben sind.

(2) Der Mitgliedstaat, in dem die öffentlichen Stellen nach Artikel 3 Nummer 46 niedergelassen sind, stellt sicher, dass die öffentlichen Stellen, die elektronische Attributsbescheinigungen ausstellen, ein Maß an Verlässlichkeit und Vertrauenswürdigkeit aufweisen, die den qualifizierten Vertrauensdiensteanbietern gemäß Artikel 24 entsprechen.

(3) Die Mitgliedstaaten teilen der Kommission die öffentlichen Stellen nach Artikel 3 Nummer 46 mit. Diese Mitteilung umfasst einen von einer Konformitätsbewertungsstelle ausgestellten Konformitätsbewertungsbericht, in dem bestätigt wird, dass die Anforderungen der Absätze 1, 2 und 6 des vorliegenden Artikels erfüllt sind. Die Kommission macht die Liste der öffentlichen Stellen nach Artikel 3 Nummer 46 auf sichere Weise und elektronisch unterzeichnet oder besiegelt in einer für eine automatisierte Verarbeitung geeigneten Form öffentlich zugänglich.

(4) Wurde eine elektronische Attributsbescheinigung, die von oder im Namen einer für eine authentische Quelle zuständigen öffentlichen Stelle ausgestellt wurde, nach der ursprünglichen Ausstellung widerrufen, so verliert sie ab dem Zeitpunkt ihres Widerrufs ihre Gültigkeit und ihr Status wird nicht wiederhergestellt.

(5) Bei elektronischen Attributsbescheinigungen, die von oder im Namen einer für eine authentische Quelle zuständigen öffentlichen Stelle ausgestellt wurden, wird davon ausgegangenen, dass sie die Anforderungen des Absatzes 1 erfüllen, sofern sie den in Standards, Spezifikationen und Verfahren nach Absatz 6 entsprechen.

(6) Bis zum 21. November 2024 erstellt die Kommission im Wege von Durchführungsrechtsakten eine Liste von Referenzstandards und legt, sofern erforderlich, Spezifikationen und Verfahren für elektronische Attributsbescheinigungen, die von oder im Namen einer für eine authentische Quelle zuständigen öffentlichen Stelle ausgestellt werden, fest. Diese Durchführungsrechtsakte stehen im Einklang mit den Durchführungsrechtsakten zur Umsetzung der europäischen Brieftasche für die Digitale Identität nach Artikel 5a Absatz 23. Sie werden gemäß dem in Artikel 48 Absatz 2 genannten Prüfverfahren erlassen.

(7) Bis zum 21. November 2024 erstellt die Kommission im Wege von Durchführungsrechtsakten eine Liste von Referenzstandards und legt, sofern erforderlich, die Spezifikationen und Verfahren für die Zwecke des Absatzes 3 dieses Artikels fest. Diese Durchführungsrechtsakte stehen im Einklang mit den Durchführungsrechtsakten zur Umsetzung der europäischen Brieftasche für die Digitale Identität nach Artikel 5a Absatz 23. Sie werden gemäß dem in Artikel 48 Absatz 2 genannten Prüfverfahren erlassen.

(8) Öffentliche Stellen nach Artikel 3 Nummer 46, die elektronische Attributsbescheinigungen ausstellen, stellen eine Schnittstelle zu den nach Artikel 5a bereitgestellten europäischen Brieftaschen für die Digitale Identität bereit.

Artikel 45g
Ausstellung elektronischer Attributsbescheinigungen für europäische Brieftaschen für die Digitale Identität

(1) Anbieter elektronischer Attributsbescheinigungen bieten Nutzern der europäischen Brieftasche für die Digitale Identität die Möglichkeit, die elektronische Attributsbescheinigung unabhängig von dem Mitgliedstaat, in dem die europäische Brieftasche für die Digitale Identität bereitgestellt wird, anzufordern, zu erhalten, zu speichern und zu verwalten.

(2) Anbieter qualifizierter elektronischer Attributsbescheinigungen stellen eine Schnittstelle zu den nach Artikel 5a bereitgestellten europäischen Brieftaschen für die Digitale Identität bereit.

Artikel 45h
Zusätzliche Vorschriften für die Erbringung von Diensten für elektronische Attributsbescheinigungen

(1) Anbieter qualifizierter und nichtqualifizierter Dienste für elektronische Attributsbescheinigungen dürfen personenbezogene Daten in Bezug auf die Erbringung dieser Dienste nicht mit personenbezogenen Daten aus anderen von ihnen oder ihren Geschäftspartnern angebotenen Diensten kombinieren.

(2) Personenbezogene Daten in Bezug auf die Erbringung von Diensten für elektronische Attributsbescheinigungen werden von allen anderen vom Anbieter elektronischer Attributsbescheinigungen gespeicherten Daten logisch getrennt gehalten.

(3) Anbieter elektronischer Attributsbescheinigungen setzen die Bereitstellung solcher qualifizierter Vertrauensdienste auf eine Weise um, dass sie von anderen von ihnen bereitgestellten Diensten funktional getrennt ist.

ABSCHNITT 10
elektronische archivierungsdienste

Artikel 45i
Rechtswirkung elektronischer Archivierungsdienste

(1) Elektronischen Daten und elektronischen Dokumenten, die mittels eines elektronischen Archivierungsdienstes aufbewahrt werden, darf die Rechtswirkung oder die Zulässigkeit als Beweismittel in Gerichtsverfahren nicht allein deshalb abgesprochen werden, weil sie in elektronischer Form vorliegen oder weil sie nicht mittels eines qualifizierten elektronischen Archivierungsdienstes aufbewahrt werden.

(2) Für elektronische Daten und elektronische Dokumente, die mittels eines qualifizierten elektronischen Archivierungsdienstes aufbewahrt werden, gilt die Vermutung der Unversehrtheit und der Richtigkeit der Herkunftsangabe für den Zeitraum der Bewahrung durch den qualifizierten Vertrauensdiensteanbieter.

Artikel 45j
Anforderungen an qualifizierte elektronische Archivierungsdienste

(1) Qualifizierte elektronische Archivierungsdienste müssen folgende Anforderungen erfüllen:

a) sie werden von qualifizierten Vertrauensdiensteanbietern erbracht;

b) sie verwenden Verfahren und Technologien, mit denen die Dauerhaftigkeit und Lesbarkeit der elektronischen Daten und elektronischen Dokumente über den Zeitraum ihrer technologischen Geltung hinaus und mindestens während des gesamten rechtlichen oder vertraglichen Bewahrungszeitraums gewährleistet werden können, wobei ihre Unversehrtheit und die Richtigkeit ihrer Herkunftsangaben gewahrt werden;

c) sie stellen sicher, dass diese elektronischen Daten und diese elektronischen Dokumente so aufbewahrt werden, dass sie vor Verlust und Veränderung geschützt sind, mit Ausnahme von Änderungen in Bezug auf das Medium oder das elektronische Format;

d) sie ermöglichen es autorisierten vertrauenden Beteiligten, einen Bericht auf automatisierte Weise zu erhalten, mit dem bestätigt wird, dass für aus einem qualifizierten elektronischen Archiv abgerufene elektronische Daten und elektronische Dokumente die Vermutung der Unversehrtheit der Daten ab dem Beginn des Bewahrungszeitraums bis zum Zeitpunkt des Abrufs gilt;

Der in Unterabsatz 1 Buchstabe d genannte Bericht wird in zuverlässiger und effizienter Weise bereitgestellt und trägt die qualifizierte elektronische Signatur oder das qualifizierte elektronische Siegel des Anbieters des qualifizierten elektronischen Archivierungsdienstes.

(2) Bis zum 21. Mai 2025 erstellt die Kommission im Wege von Durchführungsrechtsakten eine Liste von Referenzstandards und legt, sofern erforderlich, Spezifikationen und Verfahren für qualifizierte elektronische Archivierungsdienste fest. Bei qualifizierten elektronischen Archivierungsdiensten, die diesen Standards, Spezifikationen und Verfahren entsprechen, wird davon ausgegangen, dass sie die Anforderungen für qualifizierte elektronische

Archivierungsdienste erfüllen. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 48 Absatz 2 genannten Prüfverfahren erlassen.

ABSCHNITT 11
elektronische journale

Artikel 45k
Rechtswirkungen elektronischer Journale

(1) Einem elektronischen Journal darf die Rechtswirkung oder die Zulässigkeit als Beweismittel in Gerichtsverfahren nicht allein deshalb abgesprochen werden, weil es in elektronischer Form vorliegt oder die Anforderungen an qualifizierte elektronische Journale nicht erfüllt.

(2) Für Datensätze in einem qualifizierten elektronischen Journal gilt die Vermutung der eindeutigen und genauen fortlaufenden chronologischen Reihenfolge und der Unversehrtheit.

Artikel 45l
Anforderungen an qualifizierte elektronische Journale

(1) Qualifizierte elektronische Journale müssen folgende Anforderungen erfüllen:

a) sie werden von einem oder mehreren qualifizierten Vertrauensdiensteanbietern erstellt und verwaltet;

b) sie stellen die Herkunft der Datensätze im Journal fest;

c) sie gewährleisten die eindeutige fortlaufende chronologische Reihenfolge der Datensätze im Journal;

d) sie zeichnen die Daten so auf, dass jede spätere Änderung an den Daten sofort erkennbar ist, und gewährleisten somit ihre Unversehrtheit im Zeitverlauf.

(2) Bei einem elektronischen Journal, das den in Absatz 3 genannten Standards, Spezifikationen und Verfahren entspricht, wird davon ausgegangen, dass es die Anforderungen des Absatzes 1 erfüllt.

(3) Bis zum 21. Mai 2025 erstellt die Kommission im Wege von Durchführungsrechtsakten eine Liste von Referenzstandards und legt, sofern erforderlich, die Spezifikationen und Verfahren für qualifizierte Validierungsdienste nach Absatz 1 des vorliegenden Artikels fest. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 48 Absatz 2 genannten Prüfverfahren erlassen.

KAPITEL IV
ELEKTRONISCHE DOKUMENTE

Artikel 46
Rechtswirkung elektronischer Dokumente

Einem elektronischen Dokument darf die Rechtswirkung und die Zulässigkeit als Beweismittel in Gerichtsverfahren nicht allein deshalb abgesprochen werden, weil es in elektronischer Form vorliegt.

KAPITEL IVa
RAHMEN FÜR DIE GOVERNANCE

Artikel 46a
Aufsicht über den Rahmen für die europäischen Brieftasche für die Digitale Identität

(1) Die Mitgliedsstaaten benennen eine oder mehrere in ihrem Hoheitsgebiet niedergelassene Aufsichtsstellen.

Die gemäß Unterabsatz 1 benannten Aufsichtsstellen erhalten die erforderlichen Befugnisse und angemessene Ressourcen für die Wahrnehmung ihrer Aufgaben auf wirksame, effiziente und unabhängige Weise.

(2) Die Mitgliedstaaten teilen der Kommission die Namen und die Adressen ihrer nach Absatz 1 benannten Aufsichtsstellen sowie alle nachfolgenden Änderungen daran mit. Die Kommission veröffentlicht eine Liste der benannten Aufsichtsstellen.

(3) Die nach Absatz 1 benannten Aufsichtsstellen nehmen folgende Funktionen wahr:

a) Ausübung der Aufsicht über die im Hoheitsgebiet des benennenden Mitgliedstaats niedergelassenen Anbieter von europäischen Brieftaschen für die Digitale Identität, um, im Wege von Ex-ante- und Ex-post-Aufsichtstätigkeiten zu gewährleisten, dass diese Anbieter und von diesen bereitgestellte europäische Brieftaschen für die Digitale Identität den Anforderungen dieser Verordnung entsprechen;

b) erforderlichenfalls Ergreifen von Maßnahmen in Bezug auf die im Hoheitsgebiet des benennenden Mitgliedstaats niedergelassenen Anbieter von europäischen Brieftaschen für die Digitale Identität im Wege von Ex-post-Aufsichtstätigkeiten, wenn sie Informationen darüber erhalten, dass Anbieter oder von diesen bereitgestellte europäische Brieftaschen für die Digitale Identität gegen diese Verordnung verstoßen.

(4) Die nach Absatz 1 benannten Aufsichtsstellen nehmen unter anderem insbesondere folgende Aufgaben wahr:

a) Zusammenarbeit mit anderen Aufsichtsstellen und Unterstützung dieser Stellen gemäß den Artikeln 46c und 46e;

b) Anforderung der für die Überwachung der Einhaltung der vorliegenden Verordnung erforderlichen Informationen;

c) Unterrichtung der nach Artikel 8 Absatz 1 der Richtlinie (EU) 2022/2555 benannten oder eingerichteten zuständigen Behörden der betroffenen Mitgliedstaaten

über alle erheblichen Sicherheitsverletzungen oder Fälle von Integritätsverlust, von denen sie bei der Wahrnehmung ihrer Aufgaben Kenntnis erlangen, und in Fällen, in denen weitere Mitgliedstaaten von einer erheblichen Sicherheitsverletzung oder einem erheblichen Integritätsverlust betroffen sind, Unterrichtung der benannten oder eingerichteten einheitlichen Anlaufstelle nach Artikel 8 Absatz 3 der Richtlinie (EU) 2022/2555 des betroffenen Mitgliedstaats und der benannten einheitlichen Anlaufstellen nach Artikel 46c Absatz 1 der vorliegenden Verordnung in den anderen betroffenen Mitgliedstaaten sowie Information der Öffentlichkeit oder Verpflichtung von Anbietern der europäischen Brieftasche für die Digitale Identität, dies zu tun, wenn die Aufsichtsstelle feststellt, dass eine Offenlegung der Sicherheitsverletzung oder des Integritätsverlusts im öffentlichen Interesse wäre;

d) Überprüfungen vor Ort und Fernaufsicht;

e) Verpflichtung der Anbieter von europäischen Brieftaschen für die Digitale Identität, bei jedem Fall von Nichteinhaltung der Anforderungen dieser Verordnung Abhilfe zu schaffen;

f) Aussetzen oder Widerrufen der Registrierung und der Einbeziehung der vertrauenden Beteiligten in den Mechanismus nach Artikel 5b Absatz 7 im Falle rechtswidriger oder betrügerischer Verwendung der europäischen Brieftaschen für die Digitale Identität;

g) Zusammenarbeit mit den gemäß Artikel 51 der Verordnung (EU) 2016/679 eingerichteten zuständigen Aufsichtsbehörden, insbesondere deren unverzügliche Unterrichtung, wenn anscheinend gegen Datenschutzvorschriften verstoßen wurde, sowie über Sicherheitsverletzungen, die anscheinend Verletzungen des Schutzes personenbezogener Daten darstellen.

(5) Verlangt die nach Absatz 1 benannte Aufsichtsstelle vom Anbieter einer europäischen Brieftasche für die Digitale Identität bei Nichteinhaltung der Anforderungen nach dieser Verordnung gemäß Absatz 4 Buchstabe e Abhilfe zu schaffen und kommt dieser Anbieter dieser Aufforderung — gegebenenfalls innerhalb einer von der Aufsichtsstelle gesetzten Frist — nicht nach, so kann die nach Absatz 1 benannte Aufsichtsstelle unter Berücksichtigung insbesondere der Tragweite, der Dauer und der Auswirkungen der Nichteinhaltung anordnen, dass der Anbieter die Bereitstellung der europäischen Brieftasche für die Digitale Identität aussetzt oder beendet. Die Aufsichtsstelle setzt die Aufsichtsstellen anderer Mitgliedstaaten, die Kommission, vertrauende Beteiligte und Nutzer der europäischen Brieftasche für die Digitale Identität unverzüglich von der Entscheidung, die Aussetzung oder Beendigung der Bereitstellung der europäischen Brieftasche für die Digitale Identität zu verlangen, in Kenntnis.

(6) Bis zum 31. März jedes Jahres legt jede nach Absatz 1 benannte Aufsichtsstelle der Kommission einen Bericht über ihre hauptsächlichen Tätigkeiten während des vorangegangenen Kalenderjahres vor. Die Kommission stellt diese jährlichen Berichte dem Parlament und dem Rat zur Verfügung.

(7) Bis zum 21. Mai 2025 legt die Kommission im Wege von Durchführungsrechtsakten Form und Verfahren für die in Absatz 6 des vorliegenden Artikels genannten Berichte fest. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 48 Absatz 2 genannten Prüfverfahren erlassen.

Artikel 46b
Beaufsichtigung von Vertrauensdiensten

(1) Die Mitgliedstaaten benennen eine Aufsichtsstelle, die in ihrem Hoheitsgebiet niedergelassen ist, oder sie benennen, aufgrund einer gegenseitigen Vereinbarung mit einem anderen Mitgliedstaat, eine in diesem anderen Mitgliedstaat niedergelassene Aufsichtsstelle. Diese Aufsichtsstelle ist für die Wahrnehmung der Aufsichtsaufgaben im benennenden Mitgliedstaat im Hinblick auf Vertrauensdienste verantwortlich.

Die gemäß Unterabsatz 1 benannten Aufsichtsstellen erhalten die erforderlichen Befugnisse und angemessene Ressourcen für die Wahrnehmung ihrer Aufgaben.

(2) Die Mitgliedstaaten teilen der Kommission die Namen und die Adressen ihrer nach Absatz 1 benannten Aufsichtsstellen sowie alle nachfolgenden Änderungen daran mit. Die Kommission veröffentlicht eine Liste der benannten Aufsichtsstellen.

(3) Die nach Absatz 1 benannten Aufsichtsstellen nehmen folgende Funktionen wahr:

a) Ausübung der Aufsicht über die im Hoheitsgebiet des benennenden Mitgliedstaats niedergelassenen qualifizierten Vertrauensdiensteanbieter und Gewährleistung im Wege von Ex-ante- und Ex-post-Aufsichtstätigkeiten, dass diese qualifizierten Vertrauensdiensteanbieter und die von ihnen erbrachten qualifizierten Vertrauensdienste den Anforderungen dieser Verordnung entsprechen;

b) erforderlichenfalls Durchführung von Maßnahmen im Wege von Ex-post-Aufsichtstätigkeiten in Bezug auf die im Hoheitsgebiet des benennenden Mitgliedstaats niedergelassenen nichtqualifizierten Vertrauensdiensteanbieter, wenn sie Kenntnis davon erhalten, dass diese nichtqualifizierten Vertrauensdiensteanbieter oder die von ihnen erbrachten Vertrauensdienste die Anforderungen dieser Verordnung mutmaßlich nicht erfüllen;

(4) Die nach Absatz 1 benannten Aufsichtsstelle nimmt unter anderem insbesondere folgende Aufgaben wahr:

a) Unterrichtung der nach Artikel 8 Absatz 1 der Richtlinie (EU) 2022/2555 benannten oder eingerichteten zuständigen Behörden der betroffenen Mitgliedstaaten über alle erheblichen Sicherheitsverletzungen oder Fälle von Integritätsverlust, von denen sie bei der Wahrnehmung ihrer Aufgaben Kenntnis erlangt, und in Fällen, in denen weitere Mitgliedstaaten von einer erheblichen Sicherheitsverletzung oder einem Integritätsverlust betroffen sind, Unterrichtung der benannten oder eingerichteten einheitlichen Anlaufstelle nach Artikel 8 Absatz 3 der Richtlinie (EU) 2022/2555 des betroffenen Mitgliedstaats und der benannten einheitlichen Anlaufstellen nach Artikel 46c Absatz 1 der vorliegenden Verordnung in den anderen betroffenen Mitgliedstaaten sowie Information der Öffentlichkeit oder Verpflichtung des Vertrauensdiensteanbieters, dies zu tun, wenn die Aufsichtsstelle feststellt, dass eine Offenlegung der Sicherheitsverletzung oder des Integritätsverlusts im öffentlichen Interesse wäre;

b) Zusammenarbeit mit anderen Aufsichtsstellen und Unterstützung dieser Stellen gemäß den Artikeln 46c und 46e;

c) Analyse der Konformitätsbewertungsberichte gemäß Artikel 20 Absatz 1 und Artikel 21 Absatz 1;

d) Berichterstattung an die Kommission über ihre hauptsächlichen Tätigkeiten gemäß Absatz 6 dieses Artikels;

e) Durchführung von Überprüfungen oder Beauftragung einer Konformitätsbewertungsstelle mit der Durchführung einer Konformitätsbewertung der qualifizierten Vertrauensdiensteanbieter gemäß Artikel 20 Absatz 2;

f) Zusammenarbeit mit den gemäß Artikel 51 der Verordnung (EU) 2016/679 eingerichteten zuständigen Aufsichtsbehörden, insbesondere deren unverzügliche Unterrichtung, wenn scheinbar gegen Datenschutzvorschriften verstoßen wurde, sowie über Sicherheitsverletzungen, die mögliche Verletzungen des Schutzes personenbezogener Daten darstellen;

g) Verleihung des Qualifikationsstatus an Vertrauensdiensteanbieter und die von ihnen erbrachten Dienste sowie Entzug dieses Status gemäß den Artikeln 20 und 21;

h) Unterrichtung der in Artikel 22 Absatz 3 genannten, für die nationale Vertrauensliste verantwortlichen Stelle über ihre Entscheidung, den Qualifikationsstatus zu verleihen oder zu entziehen, soweit es sich dabei nicht um die nach Absatz 1 benannte Aufsichtsstelle selbst handelt;

i) Überprüfung des Vorliegens und der ordnungsgemäßen Anwendung von Vorschriften über Beendigungspläne für den Fall, dass der qualifizierte Vertrauensdiensteanbieter seine Tätigkeit einstellt, wobei auch die Frage, wie die Informationen gemäß Artikel 24 Absatz 2 Buchstabe h weiter zugänglich gehalten werden, geprüft wird;

j) Verpflichtung der Vertrauensdiensteanbieter, bei jedem Fall von Nichteinhaltung der Anforderungen dieser Verordnung Abhilfe zu schaffen;

k) Prüfung von Angaben von Anbietern von Webbrowsern nach Artikel 45a und erforderlichenfalls Ergreifen von Maßnahmen.

(5) Die Mitgliedstaaten können verlangen, dass die nach Absatz 1 benannte Aufsichtsstelle nach Maßgabe des nationalen Rechts eine Vertrauensinfrastruktur einrichtet, unterhält und aktualisiert.

(6) Bis zum 31. März jedes Jahres legt jede nach Absatz 1 benannte Aufsichtsstelle der Kommission einen Bericht über ihre hauptsächlichen Tätigkeiten während des vorangegangenen Kalenderjahres vor. Die Kommission stellt diese jährlichen Berichte dem Parlament und dem Rat zur Verfügung.

(7) Bis zum 21. Mai 2025 nimmt die Kommission Leitlinien über die Wahrnehmung der Aufgaben nach Absatz 4 dieses Artikels durch die nach Absatz 1 benannten Aufsichtsstellen an und legt im Wege von Durchführungsrechtsakten Form und Verfahren für die in Absatz 6 des vorliegenden Artikels genannten Berichte fest. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 48 Absatz 2 genannten Prüfverfahren erlassen.

Artikel 46c
Einheitliche Anlaufstellen

(1) Jeder Mitgliedstaat benennt eine einheitliche Anlaufstelle für Vertrauensdienste, europäische Brieftaschen für die Digitale Identität und notifizierte elektronische Identifizierungssysteme.

(2) Jede einheitliche Anlaufstelle fungiert als Verbindungsstelle, um die grenzüberschreitende Zusammenarbeit zwischen den Aufsichtsstellen für Vertrauensdiensteanbieter und zwischen den Aufsichtsstellen für die Anbieter von europäischen Brieftaschen für die Digitale Identität und gegebenenfalls der Kommission und der Agentur der Europäischen Union für Cybersicherheit (ENISA) sowie mit anderen nationalen zuständigen Behörden innerhalb des Mitgliedstaats zu gewährleisten.

(3) Jeder Mitgliedstaat veröffentlicht die Namen und die Adressen der nach Absatz 1 benannten einheitlichen Anlaufstellen sowie alle nachfolgenden Änderungen daran und teilt diese der Kommission unverzüglich mit.

(4) Die Kommission veröffentlicht eine Liste der nach Absatz 3 mitgeteilten einheitlichen Anlaufstellen.

Artikel 46d
Gegenseitige Amtshilfe

(1) Um die Beaufsichtigung und Durchsetzung von Verpflichtungen im Rahmen dieser Verordnung zu erleichtern, können nach Artikel 46a Absatz 1 und Artikel 46b Absatz 1 benannten Aufsichtsstellen unter anderem durch die gemäß Artikel 46e Absatz 1 eingerichtete Kooperationsgruppe, um Amtshilfe von den Aufsichtsstellen eines anderen Mitgliedstaats ersuchen, in dem der Anbieter der europäischen Brieftasche für die Digitale Identität oder der Vertrauensdienstanbieter ansässig ist, oder in dem sich sein Netz und seine Informationssysteme befinden, oder in dem seine Dienste angeboten werden.

(2) Gegenseitige Amtshilfe umfasst mindestens Folgendes:

a) Die Aufsichtsstelle, die Aufsichts- und Durchsetzungsmaßnahmen in einem Mitgliedstaat anwendet, informiert und konsultiert die Aufsichtsstelle des anderen betroffenen Mitgliedstaats.

b) Die Aufsichtsstelle kann die Aufsichtsstelle eines anderen betroffenen Mitgliedstaats ersuchen, Aufsichts- oder Durchsetzungsmaßnahmen zu ergreifen, einschließlich beispielsweise Ersuchen um Nachprüfungen im Zusammenhang mit den Konformitätsbewertungsberichten gemäß den Artikeln 20 und 21 in Bezug auf die Erbringung von Vertrauensdienten.

c) Gegebenenfalls können Aufsichtsstellen gemeinsame Untersuchungen mit den Aufsichtsstellen anderer Mitgliedstaaten durchführen.

Die Vorkehrungen und Verfahren für gemeinsame Tätigkeiten nach Unterabsatz 1 werden von den betreffenden Mitgliedstaaten nach Maßgabe ihres jeweiligen nationalen Rechts vereinbart und festgelegt.

(3) Die Aufsichtsstelle, an die ein Amtshilfeersuchen gerichtet wird, kann dieses Ersuchen aus einem der folgenden Gründe ablehnen:

a) Die erbetene Unterstützung steht in keinem angemessenen Verhältnis zu den nach Artikel 46a und 46b durchgeführten Aufsichtstätigkeiten der Aufsichtsstelle;

b) die Aufsichtsstelle ist für die Gewährung der erbetenen Unterstützung nicht zuständig;

c) die Gewährung der erbetenen Unterstützung wäre nicht vereinbar mit dieser Verordnung.

(4) Bis zum 21. Mai 2025 und danach alle zwei Jahre gibt die gemäß Artikel 46e Absatz 1 eingerichtete Kooperationsgruppe Leitlinien zu organisatorischen Aspekten und Verfahren für die gegenseitige Amtshilfe gemäß den Absätzen 1 und 2 dieses Artikels heraus.

Artikel 46e
Europäische Kooperationsgruppe für die digitale Identität

(1) Um die grenzübergreifende Zusammenarbeit und den Informationsaustausch unter den Mitgliedstaaten im Bereich der Vertrauensdienste, der europäischen Brieftaschen für die Digitale Identität und der notifizierten elektronischen Identifizierungssysteme zu erleichtern, richtet die Kommission die europäische Kooperationsgruppe für die digitale Identität (im Folgenden „Kooperationsgruppe") ein.

(2) Die Kooperationsgruppe setzt sich aus von den Mitgliedstaaten und der Kommission ernannten Vertretern zusammen. Den Vorsitz in der Kooperationsgruppe führt die Kommission. Die Kommission stellt das Sekretariat der Kooperationsgruppe bereit.

(3) Vertreter einschlägiger Interessenträger können ad hoc zur Teilnahme an Sitzungen der Kooperationsgruppe und an ihrer Tätigkeit als Beobachter eingeladen werden.

(4) Die ENISA wird als Beobachter zur Teilnahme an den Tätigkeiten der Kooperationsgruppe, zum Gedankenaustausch, zum Austausch von bewährten Verfahren und Informationen zu relevanten Aspekten der Cybersicherheit, wie beispielsweise das Melden von Sicherheitsverletzungen, und zur Verwendung von Cybersicherheitszertifikaten oder Cybersicherheitsnormen eingeladen.

(5) Die Kooperationsgruppe nimmt folgende Aufgaben wahr:

a) Beratungen und Zusammenarbeit mit der Kommission zu neuen politischen Initiativen im Bereich der europäischen Brieftaschen für die Digitale Identität, elektronischen Identifizierungsmittel und Vertrauensdienste;

b) Beratung der Kommission, sofern angemessen, während der frühen Phase der Vorbereitung von Entwürfen von Durchführungsrechtsakten und delegierten Rechtsakten, die gemäß dieser Verordnung angenommen werden sollen;

c) zur Unterstützung der Aufsichtsstellen bei der Umsetzung der Bestimmungen dieser Verordnung:

   i) Austausch von bewährten Verfahren und Informationen über die Anwendung der Bestimmungen dieser Verordnung;

   ii) Prüfung der einschlägigen Entwicklungen in den Bereichen europäische Brieftaschen für die Digitale Identität, elektronische Identifizierung und Vertrauensdienste;

   iii) Organisation regelmäßiger gemeinsame Sitzungen mit relevanten Interessenträgern aus der gesamten Union, um die Tätigkeiten der Kooperationsgruppe zu erörtern und Beiträge zu neuen politischen Herausforderungen einzuholen;

   iv) Gedankenaustausch und Austausch von bewährten Verfahren und Informationen in Bezug auf relevante Cybersicherheitsaspekte der europäi-

schen Brieftasche für die Digitale Identität, der elektronischen Identifizierungssysteme und der Vertrauensdienste mit Unterstützung der ENISA;

v) Austausch bewährter Verfahren für die Entwicklung und Umsetzung von Strategien für die Meldung von Sicherheitsverletzungen sowie gemeinsame Maßnahmen gemäß den Artikeln 5e und 10;

vi) Organisation gemeinsamer Sitzungen mit der NIS-Kooperationsgruppe gemäß Artikel 14 Absatz 1 der Richtlinie (EU) 2022/2555 zum Austausch relevanter Informationen in Bezug auf Vertrauensdienste und elektronische Identifizierung im Zusammenhang mit Cyberbedrohungen, Cybervorfällen, Schwachstellen, Sensibilisierungsinitiativen, Schulungen, Übungen und Kompetenzen, Kapazitätsaufbau, Kapazitäten im Bereich der Standards und technische Spezifikationen sowie Standards und technische Spezifikationen;

vii) Erörterung spezifischer Ersuchen und Amtshilfe nach Artikel 46d auf Ersuchen einer Aufsichtsbehörde;

viii) Erleichterung des Informationsaustauschs zwischen Aufsichtsstellen durch Bereitstellung von Leitlinien zu den organisatorischen Aspekten und Verfahren für die gegenseitige Amtshilfe gemäß Artikel 46d;

d) Organisation gegenseitiger Begutachtung der gemäß dieser Verordnung zu notifizierenden elektronischen Identifizierungssysteme.

(6) Die Mitgliedstaaten gewährleisten eine sichere, wirksame und effiziente Zusammenarbeit der benannten Vertreter in der Kooperationsgruppe.

(7) Bis zum 21. Mai 2025 legt die Kommission im Wege von Durchführungsrechtsakten die erforderlichen Verfahrensmodalitäten zur Erleichterung der Zusammenarbeit zwischen den Mitgliedstaaten nach Absatz 5 Buchstabe d dieses Artikels fest. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 48 Absatz 2 genannten Prüfverfahren erlassen.

KAPITEL V
BEFUGNISÜBERTRAGUNGEN UND DURCHFÜHRUNGSBESTIMMUNGEN

Artikel 47
Ausübung der Befugnisübertragung

(1) Die Befugnis zum Erlass delegierter Rechtsakte wird der Kommission unter den in diesem Artikel festgelegten Bedingungen übertragen.

(2) Die Befugnis zum Erlass delegierter Rechtsakte gemäß Artikel 5c Absatz 7, Artikel 24 Absatz 4b und Artikel 30 Absatz 4 wird der Kommission auf unbestimmte Zeit ab dem 17. September 2014 übertragen.

(3) Die Befugnisübertragung gemäß Artikel 5c Absatz 7, Artikel 24 Absatz 4b und Artikel 30 Absatz 4 kann vom Europäischen Parlament oder vom Rat jederzeit widerrufen werden. Der Beschluss über den Widerruf beendet die Übertragung der in diesem Beschluss angegebenen Befugnis. Er wird am Tag nach seiner Veröffentlichung im Amtsblatt der Europäischen Union oder zu einem im Beschluss über den Widerruf angegebenen späteren Zeit-

punkt wirksam. Die Gültigkeit von delegierten Rechtsakten, die bereits in Kraft sind, wird von dem Beschluss über den Widerruf nicht berührt.

(4) Sobald die Kommission einen delegierten Rechtsakt erlässt, übermittelt sie ihn gleichzeitig dem Europäischen Parlament und dem Rat.

(5) Ein delegierter Rechtsakt, der gemäß Artikel 5c Absatz 7, Artikel 24 Absatz 4b oder Artikel 30 Absatz 4 erlassen wurde, tritt nur in Kraft, wenn weder das Europäische Parlament noch der Rat innerhalb einer Frist von zwei Monaten nach Übermittlung dieses Rechtsakts an das Europäische Parlament und den Rat Einwände erhoben haben oder wenn vor Ablauf dieser Frist das Europäische Parlament und der Rat beide der Kommission mitgeteilt haben, dass sie keine Einwände erheben werden. Auf Initiative des Europäischen Parlaments oder des Rates wird diese Frist um zwei Monate verlängert.

Artikel 48
Ausschussverfahren

(1) Die Kommission wird von einem Ausschuss unterstützt. Dieser Ausschuss ist ein Ausschuss im Sinne der Verordnung (EU) Nr. 182/2011.

(2) Wird auf diesen Absatz Bezug genommen, so gilt Artikel 5 der Verordnung (EU) Nr. 182/2011.

KAPITEL VI
SCHLUSSBESTIMMUNGEN

Artikel 48a
Berichtspflichten

(1) Die Mitgliedstaaten sorgen für die Erhebung von Statistiken über das Funktionieren von europäischen Brieftaschen für die Digitale Identität und der qualifizierten Vertrauensdienste, die in ihrem Hoheitsgebiet angeboten werden.

(2) Die nach Absatz 1 erhobenen Statistiken umfassen Folgendes:

a) die Zahl der natürlichen und juristischen Personen, die eine gültige europäische Brieftasche für die Digitale Identität haben;

b) die Art und Anzahl der Dienste, die die Verwendung der europäischen Brieftasche für die Digitale Identität akzeptieren;

c) die Anzahl der Beschwerden von Nutzern und der Vorfälle in Bezug auf Verbraucherschutz oder Datenschutz betreffend vertrauende Beteiligte und qualifizierte Vertrauensdienste;

d) einen zusammenfassenden Bericht mit Daten zu Vorfällen, durch die die Verwendung der europäischen Brieftasche für die Digitale Identität verhindert wurde;

e) eine Zusammenfassung signifikanter Cybersicherheitsvorfälle, Verletzungen des Datenschutzes und der betroffenen Nutzer von europäischen Brieftaschen für die Digitale Identität oder qualifizierten Vertrauensdiensten.

(3) Die in Absatz 2 genannten Statistiken werden der Öffentlichkeit in einem offenen und weithin verwendeten maschinenlesbaren Format zur Verfügung gestellt.

(4) Bis zum 31. März jedes Jahres übermitteln die Mitgliedstaaten der Kommission einen Bericht über die nach Absatz 2 erhobenen Statistiken.

Artikel 49
Überprüfung

(1) Die Kommission überprüft die Anwendung dieser Verordnung und erstattet dem Europäischen Parlament und dem Rat bis zum 21. Mai 2026 darüber Bericht. In diesem Bericht bewertet die Kommission insbesondere, ob es angezeigt ist, den Anwendungsbereich dieser Verordnung oder ihrer spezifischen Bestimmungen, einschließlich insbesondere der Bestimmungen in Artikel 5c Absatz 5, zu ändern, wobei den bei der Anwendung dieser Verordnung gesammelten Erfahrungen sowie den Entwicklungen der Technologie, des Marktes und des Rechts Rechnung getragen wird. Diesem Bericht wird erforderlichenfalls ein Vorschlag zur Änderung dieser Verordnung beigefügt.

(2) Der in Absatz 1 genannte Bericht enthält eine Bewertung der Verfügbarkeit, Sicherheit und Nutzbarkeit der notifizierten elektronischen Identifizierungsmittel und der europäischen Brieftaschen für die Digitale Identität, die in den Anwendungsbereich dieser Verordnung fallen, und eine Bewertung, ob alle privaten Online-Diensteanbieter, die zur Authentifizierung der Nutzer auf elektronische Identifizierungsdienste Dritter zurückgreifen, dazu verpflichtet werden sollen, die Verwendung von notifizierten elektronischen Identifizierungsmitteln und europäischen Brieftaschen für die Digitale Identität zu akzeptieren.

(3) Bis zum 21. Mai 2030 und danach alle vier Jahre legt die Kommission dem Europäischen Parlament und dem Rat einen Bericht über die Fortschritte im Hinblick auf die Verwirklichung der mit dieser Verordnung verfolgten Ziele vor.

Artikel 50
Aufhebung

(1) Die Richtlinie 1999/93/EG wird mit Wirkung vom 1. Juli 2016 aufgehoben.

(2) Bezugnahmen auf die aufgehobene Richtlinie gelten als Bezugnahmen auf diese Verordnung.

Artikel 51
Übergangsbestimmungen

(1) Sichere Signaturerstellungseinheiten, deren Übereinstimmung mit den Anforderungen des Artikels 3 Absatz 4 der Richtlinie 1999/93/EG festgestellt wurde, gelten bis zum 21. Mai 2027 weiterhin als qualifizierte elektronische Signaturerstellungseinheiten gemäß dieser Verordnung.

(2) Qualifizierte Zertifikate, die natürlichen Personen gemäß der Richtlinie 1999/93/EG ausgestellt wurden, gelten bis zum 21. Mai 2026 weiterhin als qualifizierte Zertifikate für elektronische Signaturen gemäß dieser Verordnung.

(3) Die Verwaltung qualifizierter elektronischer Fernsignaturerstellungseinheiten und Fernsiegelerstellungseinheiten durch qualifizierte Vertrauensdiensteanbieter, die keine qualifizierten Vertrauensdiensteanbieter sind, die qualifizierte Vertrauensdienste für die Verwal-

tung qualifizierter elektronischer Fernsignaturerstellungseinheiten und Fernsiegelerstellungseinheiten gemäß den Artikeln 29a und 39a erbringen, darf bis zum 21. Mai 2026 fortgeführt werden, ohne dass die Pflicht besteht, für diese Verwaltungsdienste den Qualifikationsstatus zu erlangen.

(4) Qualifizierte Vertrauensdiensteanbieter, denen der Qualifikationsstatus gemäß dieser Verordnung vor dem 20. Mai 2024 zuerkannt wurde, legen der Aufsichtsstelle so bald wie möglich, jedenfalls bis zum 21. Mai 2026, einen Konformitätsbewertungsbericht vor, mit dem die Einhaltung des Artikels 24 Absätze 1, 1a und 1b nachgewiesen wird.

Artikel 52
Inkrafttreten

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

(2) Diese Verordnung gilt ab dem 1. Juli 2016 mit folgenden Ausnahmen:

a) Artikel 8 Absatz 3, Artikel 9 Absatz 5, Artikel 12 Absätze 2 bis 9, Artikel 17 Absatz 8, Artikel 19 Absatz 4, Artikel 20 Absatz 4, Artikel 21 Absatz 4, Artikel 22 Absatz 5, Artikel 23 Absatz 3, Artikel 24 Absatz 5, Artikel 27 Absätze 4 und 5, Artikel 28 Absatz 6, Artikel 29 Absatz 2, Artikel 30 Absätze 3 und 4, Artikel 31 Absatz 3, Artikel 32 Absatz 3, Artikel 33 Absatz 2, Artikel 34 Absatz 2, Artikel 37 Absätze 4 und 5, Artikel 38 Absatz 6, Artikel 42 Absatz 2, Artikel 44 Absatz 2, Artikel 45 Absatz 2 sowie Artikel 47 und 48 gelten ab dem 17. September 2014;

b) Artikel 7, Artikel 8 Absätze 1 und 2, Artikel 9, 10, 11 und Artikel 12 Absatz 1 gelten ab dem Datum des Beginns der Anwendung der in Artikel 8 Absatz 3 und Artikel 12 Absatz 8 genannten Durchführungsrechtsakte;

c) Artikel 6 findet drei Jahre nach dem Datum des Beginns der Anwendung der in Artikel 8 Absatz 3 und Artikel 12 Absatz 8 genannten Durchführungsrechtsakte Anwendung.

(3) Ist das notifizierte elektronische Identifizierungssystem vor dem in Absatz 2 Buchstabe c genannten Datum in der von der Kommission gemäß Artikel 9 veröffentlichten Liste aufgeführt, so erfolgt die Anerkennung der elektronischen Identifizierungsmittel dieses Systems gemäß Artikel 6 spätestens 12 Monate nach der Veröffentlichung dieses Systems, jedoch nicht vor dem in Absatz 2 Buchstabe c genannten Datum.

(4) Abweichend von Absatz 2 Buchstabe c kann ein Mitgliedstaat entscheiden, dass elektronische Identifizierungsmittel eines von einem anderen Mitgliedstaat gemäß Artikel 9 Absatz 1 notifizierten elektronischen Identifizierungssystems in dem ersten Mitgliedstaat ab dem Datum des Beginns der Anwendung der in Artikel 8 Absatz 3 und Artikel 12 Absatz 8 genannten Durchführungsrechtsakte anerkannt werden. Die betreffenden Mitgliedstaaten setzen die Kommission davon in Kenntnis. Die Kommission veröffentlicht diese Informationen.

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

ANHANG I
ANFORDERUNGEN AN QUALIFIZIERTE ZERTIFIKATE FÜR ELEKTRONISCHE SIGNATUREN

Qualifizierte Zertifikate für elektronische Signaturen enthalten Folgendes:

a) eine Angabe, dass das Zertifikat als qualifiziertes Zertifikat für elektronische Signaturen ausgestellt wurde, zumindest in einer zur automatischen Verarbeitung geeigneten Form;

b) einen Datensatz, der den qualifizierten Vertrauensdiensteanbieter, der die qualifizierten Zertifikate ausstellt, eindeutig repräsentiert und zumindest die Angabe des Mitgliedstaats enthält, in dem der Anbieter niedergelassen ist, sowie

   — bei einer juristischen Person: den Namen und gegebenenfalls die Registriernummer gemäß der amtlichen Eintragung;

   — bei einer natürlichen Person: den Namen der Person;

c) mindestens den Namen des Unterzeichners oder ein Pseudonym; wird ein Pseudonym verwendet, ist dies eindeutig anzugeben;

d) elektronische Signaturvalidierungsdaten, die den elektronischen Signaturerstellungsdaten entsprechen;

e) Angaben zu Beginn und Ende der Gültigkeitsdauer des Zertifikats;

f) den Identitätscode des Zertifikats, der für den qualifizierten Vertrauensdiensteanbieter eindeutig sein muss;

g) die fortgeschrittene elektronische Signatur oder das fortgeschrittene elektronische Siegel des ausstellenden qualifizierten Vertrauensdiensteanbieters;

h) den Ort, an dem das Zertifikat, das der fortgeschrittenen elektronischen Signatur oder dem fortgeschrittenen elektronischen Siegel gemäß Buchstabe g zugrunde liegt, kostenlos zur Verfügung steht;

i) die Angabe des Gültigkeitsstatus des qualifizierten Zertifikats oder den Ort der Dienste, die genutzt werden können, um den Status zu überprüfen;

j) falls sich die elektronischen Signaturerstellungsdaten, die den elektronischen Signaturvalidierungsdaten entsprechen, in einer qualifizierten elektronischen Signaturerstellungseinheit befinden — eine geeignete Angabe dieses Umstands, zumindest in einer zur automatischen Verarbeitung geeigneten Form.

ANHANG II
ANFORDERUNGEN AN QUALIFIZIERTE ELEKTRONISCHE SIGNATURERSTELLUNGSEINHEITEN

(1) Qualifizierte elektronische Signaturerstellungseinheiten müssen durch geeignete Technik und Verfahren zumindest gewährleisten, dass

a) die Vertraulichkeit der zum Erstellen der elektronischen Signatur verwendeten elektronischen Signaturerstellungsdaten angemessen sichergestellt ist,

b) die zum Erstellen der elektronischen Signatur verwendeten elektronischen Signaturerstellungsdaten praktisch nur einmal vorkommen können,

c) die zum Erstellen der elektronischen Signatur verwendeten elektronischen Signaturerstellungsdaten mit hinreichender Sicherheit nicht abgeleitet werden können und die elektroni-

sche Signatur bei Verwendung der jeweils verfügbaren Technik verlässlich gegen Fälschung geschützt ist,

d) die zum Erstellen der elektronischen Signatur verwendeten elektronischen Signaturerstellungsdaten vom rechtmäßigen Unterzeichner gegen eine Verwendung durch andere verlässlich geschützt werden können.

(2) Qualifizierte elektronische Signaturerstellungseinheiten dürfen die zu unterzeichnenden Daten nicht verändern und nicht verhindern, dass dem Unterzeichner diese Daten vor dem Unterzeichnen angezeigt werden.

ANHANG III
ANFORDERUNGEN AN QUALIFIZIERTE ZERTIFIKATE FÜR ELEKTRONISCHE SIEGEL

Qualifizierte Zertifikate für elektronische Siegel enthalten

a) eine Angabe, dass das Zertifikat als qualifiziertes Zertifikat für elektronische Siegel ausgestellt wurde, zumindest in einer zur automatischen Verarbeitung geeigneten Form,

b) einen Datensatz, der den qualifizierten Vertrauensdiensteanbieter, der die qualifizierten Zertifikate ausstellt, eindeutig repräsentiert und zumindest die Angabe des Mitgliedstaats enthält, in dem der Anbieter niedergelassen ist, sowie

   — bei einer juristischen Person: den Namen und gegebenenfalls die Registriernummer gemäß der amtlichen Eintragung,

   — bei einer natürlichen Person: den Namen der Person,

c) zumindest den Namen des Siegelerstellers und gegebenenfalls die Registriernummer gemäß der amtlichen Eintragung,

d) elektronische Siegelvalidierungsdaten, die den elektronischen Siegelerstellungsdaten entsprechen,

e) Angaben zu Beginn und Ende der Gültigkeitsdauer des Zertifikats,

f) den Identitätscode des Zertifikats, der für den qualifizierten Vertrauensdiensteanbieter eindeutig sein muss,

g) die fortgeschrittene elektronische Signatur oder das fortgeschrittene elektronische Siegel des ausstellenden qualifizierten Vertrauensdiensteanbieters,

h) den Ort, an dem das Zertifikat, das der fortgeschrittenen elektronischen Signatur oder dem fortgeschrittenen elektronischen Siegel gemäß Buchstabe g zugrunde liegt, kostenlos zur Verfügung steht,

i) die Angabe des Gültigkeitsstatus des qualifizierten Zertifikats oder den Ort der Dienste, die genutzt werden können, um den Status zu überprüfen;

j) falls sich die elektronischen Siegelerstellungsdaten, die den elektronischen Siegelvalidierungsdaten entsprechen, in einer qualifizierten elektronischen Siegelerstellungseinheit befinden — eine geeignete Angabe dieses Umstands, zumindest in einer zur automatischen Verarbeitung geeigneten Form.

ANHANG IV
ANFORDERUNGEN AN QUALIFIZIERTE ZERTIFIKATE FÜR DIE WEBSITE-AUTHENTIFIZIERUNG

Qualifizierte Zertifikate für die Website-Authentifizierung enthalten Folgendes:

a) eine Angabe, dass das Zertifikat als qualifiziertes Zertifikat für die Website-Authentifizierung ausgestellt wurde, zumindest in einer zur automatischen Verarbeitung geeigneten Form;

b) einen Datensatz, der den qualifizierten Vertrauensdiensteanbieter, der die qualifizierten Zertifikate ausstellt, eindeutig repräsentiert und zumindest die Angabe des Mitgliedstaats enthält, in dem der Anbieter niedergelassen ist, sowie

— bei einer juristischen Person: den Namen und gegebenenfalls die Registriernummer gemäß der amtlichen Eintragung;

— bei einer natürlichen Person: den Namen der Person;

c) bei natürlichen Personen: zumindest den Namen der Person, der das Zertifikat ausgestellt wurde, oder ein Pseudonym; wird ein Pseudonym verwendet, ist dies eindeutig anzugeben;

ca) bei juristischen Personen: einen eindeutigen Datensatz, der die juristische Person, der das Zertifikat ausgestellt wird, eindeutig repräsentiert und der zumindest den Nahmen der juristischen Person, der das Zertifikat ausgestellt wird, und sofern anwendbar, die Registernummer gemäß der amtlichen Eintragung enthält;

d) Bestandteile der Anschrift der natürlichen oder juristischen Person, der das Zertifikat ausgestellt wird, zumindest den Ort und den Staat, und gegebenenfalls gemäß der amtlichen Eintragung;

e) die Domänennamen, die von der natürlichen oder juristischen Person, der das Zertifikat ausgestellt wird, betrieben werden;

f) Angaben zu Beginn und Ende der Gültigkeitsdauer des Zertifikats;

g) den Identitätscode des Zertifikats, der für den qualifizierten Vertrauensdiensteanbieter eindeutig sein muss;

h) die fortgeschrittene elektronische Signatur oder das fortgeschrittene elektronische Siegel des ausstellenden qualifizierten Vertrauensdiensteanbieters;

i) den Ort, an dem das Zertifikat, das der fortgeschrittenen elektronischen Signatur oder dem fortgeschrittenen elektronischen Siegel gemäß Buchstabe h zugrunde liegt, kostenlos zur Verfügung steht;

j) die Angabe des Gültigkeitsstatus des qualifizierten Zertifikats oder den Ort der Dienste, die genutzt werden können, um den Status zu überprüfen.

ANHANG V
ANFORDERUNGEN AN QUALIFIZIERTE ELEKTRONISCHE ATTRIBUTSBESCHEINIGUNGEN

Qualifizierte elektronische Attributsbescheinigungen enthalten Folgendes:

a) eine Angabe, dass die Bescheinigung als qualifizierte elektronische Attributsbescheinigung ausgestellt wurde, zumindest in einer zur automatischen Verarbeitung geeigneten Form;

b) einen Datensatz, der den qualifizierten Vertrauensdiensteanbieter, der die qualifizierte elektronische Attributsbescheinigung ausstellt, eindeutig repräsentiert und zumindest die Angabe des Mitgliedstaats enthält, in dem der Anbieter niedergelassen ist, sowie

   i) bei einer juristischen Person: den Namen und gegebenenfalls die Registriernummer gemäß der amtlichen Eintragung,

   ii) bei einer natürlichen Person: den Namen der Person;

c) einen Datensatz, der die Stelle, auf die sich die bescheinigten Attribute beziehen, eindeutig repräsentiert; wird ein Pseudonym verwendet, ist dies eindeutig anzugeben;

d) die bescheinigten Attribute, gegebenenfalls mit den erforderlichen Angaben zur Feststellung des Geltungsbereichs dieser Attribute;

e) Angaben zu Beginn und Ende der Gültigkeitsdauer der Bescheinigung;

f) den Identitätscode der Bescheinigung, der für den qualifizierten Vertrauensdiensteanbieter eindeutig sein muss, und gegebenenfalls die Angabe des Bescheinigungssystems, zu dem die Attributsbescheinigung gehört;

g) die qualifizierte elektronische Signatur oder das qualifizierte elektronische Siegel des ausstellenden qualifizierten Vertrauensdiensteanbieters;

h) den Ort, an dem das Zertifikat, das der qualifizierten elektronischen Signatur oder dem qualifizierten elektronischen Siegel gemäß Buchstabe g zugrunde liegt, kostenlos zur Verfügung steht;

i) die Angabe des Gültigkeitsstatus der Bescheinigung oder den Ort der Dienste, die genutzt werden können, um den Status zu überprüfen.

ANHANG VI
MINDESTLISTE DER ATTRIBUTE

Gemäß Artikel 45e sorgen die Mitgliedstaaten dafür, dass Maßnahmen getroffen werden, die es qualifizierten Vertrauensdiensteanbietern elektronischer Attributsbescheinigungen ermöglichen, auf Verlangen des Nutzers mit elektronischen Mitteln anhand der betreffenden authentischen Quelle auf nationaler Ebene oder über benannte Vermittler, die auf nationaler Ebene anerkannt sind, nach Maßgabe des Unionsrechts oder des nationalen Rechts und sofern diese Attribute aus authentischen Quellen des öffentlichen Sektors stammen, die Echtheit der folgenden Attribute zu überprüfen:

1. Adresse,

2. Alter,

3. Geschlecht,

4. Personenstand,

5. Familienzusammensetzung,

6. Staatsangehörigkeit oder Staatsbürgerschaft,

7. Bildungsabschlüsse, Titel und Erlaubnisse,

8. Berufsqualifikationen, Titel und Berechtigungen,

9. Vollmachten und Mandate, eine natürliche oder juristische Person zu vertreten,

10. behördliche Genehmigungen und Lizenzen,

11. Für juristische Personen Finanzdaten und Unternehmensdaten.

ANHANG VII
ANFORDERUNGEN AN ELEKTRONISCHE ATTRIBUTSBESCHEINIGUNGEN, DIE VON ODER IM NAMEN EINER FÜR EINE AUTHENTISCHE QUELLE ZUSTÄNDIGEN ÖFFENTLICHEN STELLE AUSGESTELLT WERDEN

Eine elektronische Attributsbescheinigung, die von oder im Namen einer für eine authentische Quelle zuständigen öffentlichen Stelle ausgestellt wird, enthält Folgendes:

a) eine Angabe — zumindest in einer für die automatische Verarbeitung geeigneten Form –, dass die Bescheinigung als elektronische Bescheinigung, die von oder im Namen einer für eine authentische Quelle zuständigen öffentlichen Stelle ausgestellt wird, ausgestellt wurde;

b) einen Datensatz, der die öffentliche Stelle, die die elektronische Attributsbescheinigung ausstellt, eindeutig repräsentiert und zumindest die Angabe des Mitgliedstaats, in dem diese öffentliche Stelle niedergelassen ist, und ihres Namens sowie gegebenenfalls ihrer Registriernummer gemäß der amtlichen Eintragung enthält;

c) einen Datensatz, der die Stelle, auf die sich die bescheinigten Attribute beziehen, eindeutig repräsentiert; wird ein Pseudonym verwendet, ist dies eindeutig anzugeben;

d) die bescheinigten Attribute, gegebenenfalls mit den erforderlichen Angaben zur Feststellung des Geltungsbereichs dieser Attribute;

e) Angaben zu Beginn und Ende der Gültigkeitsdauer der Bescheinigung;

f) den Identitätscode der Bescheinigung, der für die ausstellende öffentliche Stelle eindeutig sein muss, und gegebenenfalls die Angabe des Bescheinigungssystems, zu dem die Attributsbescheinigung gehört;

g) die qualifizierte elektronische Signatur oder das qualifizierte elektronische Siegel der ausstellenden Stelle,

h) den Ort, an dem das Zertifikat, das der qualifizierten elektronischen Signatur oder dem qualifizierten elektronischen Siegel gemäß Buchstabe g zugrunde liegt, kostenlos zur Verfügung steht;

i) die Angabe des Gültigkeitsstatus der Bescheinigung oder den Ort der Dienste, die genutzt werden können, um den Status zu überprüfen.

Vertrauensdienstegesetz (VDG)

Inhaltsübersicht

Teil 1
Allgemeine Bestimmungen

§ 1 Anwendungsbereich

(1) Dieses Gesetz regelt die wirksame Durchführung der Vorschriften über Vertrauensdienste in der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG (ABl. L 257 vom 28.8.2014, S. 73) in der jeweils geltenden Fassung.

(2) Unberührt bleiben Rechtsvorschriften, die die Nutzung bestimmter Vertrauensdienste und die hierfür zu verwendenden Produkte regeln.

§ 2 Aufsichtsstelle; zuständige Stelle für die Informationssicherheit

(1) Die Aufgaben der Aufsichtsstelle nach Artikel 17 der Verordnung (EU) Nr. 910/2014 und nach diesem Gesetz sowie nach der Rechtsverordnung nach § 20 obliegen

1. der Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen (Bundesnetzagentur) für die Bereiche

   a) Erstellung, Überprüfung und Validierung elektronischer Signaturen, elektronischer Siegel oder elektronischer Zeitstempel und Dienste für die Zustellung elektronischer Einschreiben sowie von diese Dienste betreffenden Zertifikaten nach Artikel 3 Nummer 16 Buchstabe a der Verordnung (EU) Nr. 910/2014 und

   b) Bewahrung von diese Dienste betreffenden elektronischen Signaturen, Siegeln oder Zertifikaten nach Artikel 3 Nummer 16 Buchstabe c der Verordnung (EU) Nr. 910/2014 und

2. dem Bundesamt für Sicherheit in der Informationstechnik für den Bereich Erstellung, Überprüfung und Validierung von Zertifikaten für die Website-Authentifizierung nach Artikel 3 Nummer 16 Buchstabe b der Verordnung (EU) Nr. 910/2014.

(2) Von der Aufgabenzuweisung an die Bundesnetzagentur unberührt bleiben die Aufgaben des Bundesamtes für Sicherheit in der Informationstechnik nach dem BSI-Gesetz und nach weiteren Fachgesetzen, insbesondere

1. bei der Erstellung technischer Standards in nationalen, europäischen und internationalen Gremien in Abstimmung mit der Bundesnetzagentur,
2. die Bewertung von Algorithmen und zugehörigen Parametern sowie
3. die Erstellung technischer Vorgaben und die Bewertung technischer Standards für den Einsatz von Vertrauensdiensten in Digitalisierungsvorhaben nach Maßgabe der entsprechenden Fachgesetze.

(3) Das Bundesamt für Sicherheit in der Informationstechnik ist die für die Informationssicherheit zuständige nationale Stelle im Sinne von Artikel 19 Absatz 2 der Verordnung (EU) Nr. 910/2014.

§ 3 Verfahren über eine einheitliche Stelle

Verwaltungsverfahren nach diesem Gesetz oder nach der Rechtsverordnung nach § 20 können über eine einheitliche Stelle im Sinne des Verwaltungsverfahrensgesetzes abgewickelt werden.

§ 4 Aufsichtsmaßnahmen; Untersagung des Betriebs

(1) Ergänzend zu den Aufgaben aus der Verordnung (EU) Nr. 910/2014 obliegt der Aufsichtsstelle auch die Aufsicht über die Einhaltung dieses Gesetzes sowie der Rechtsverordnung nach § 20.

(2) Die Aufsichtsstelle kann gegenüber Vertrauensdiensteanbietern die erforderlichen Maßnahmen zur Einhaltung dieses Gesetzes sowie der Rechtsverordnung nach § 20 treffen. Zur Einhaltung dieses Gesetzes sowie der Rechtsverordnung nach § 20 kann sie von Vertrauensdiensteanbietern Nachweise anfordern und selbst Überprüfungen vornehmen. Im Übrigen stehen der Aufsichtsstelle die Maßnahmen nach der Verordnung (EU) Nr. 910/2014, insbesondere nach Artikel 17 Absatz 4, auch zur Durchsetzung dieses Gesetzes sowie der Rechtsverordnung nach § 20 zur Verfügung.

(3) Die Aufsichtsstelle kann einem Vertrauensdiensteanbieter den Betrieb vorübergehend, teilweise oder ganz untersagen, wenn

1. Maßnahmen nach Artikel 17 Absatz 4 Buchstabe j der Verordnung (EU) Nr. 910/2014 keinen Erfolg versprechen und
2. Tatsachen die Annahme rechtfertigen, dass der Anbieter die Voraussetzungen für den Betrieb eines Vertrauensdienstes nach der Verordnung (EU) Nr. 910/2014 sowie nach diesem Gesetz und nach der Rechtsverordnung nach § 20 nicht erfüllt.

§ 5 Mitwirkungspflichten der Vertrauensdiensteanbieter

(1) Zur Prüfung der Einhaltung ihrer Verpflichtungen haben der Vertrauensdiensteanbieter und die für ihn tätigen Dritten den Bediensteten und Beauftragten

1. der Aufsichtsstelle das Betreten der Geschäfts- und Betriebsräume während der üblichen Betriebszeiten zu gestatten,
2. der Aufsichtsstelle auf Verlangen die in Betracht kommenden Bücher, Aufzeichnungen, Belege, Schriftstücke und sonstigen Unterlagen zur Einsicht vorzulegen, auch soweit sie in elektronischer Form geführt werden,
3. der Aufsichtsstelle Auskunft zu erteilen und
4. der Aufsichtsstelle die erforderliche Unterstützung zu gewähren.

(2) Die zur Erteilung einer Auskunft verpflichtete natürliche Person kann die Auskunft auf solche Fragen verweigern, deren Beantwortung sie selbst oder einen der in § 52 Absatz 1 der Strafprozessordnung bezeichneten Angehörigen der Gefahr der Verfolgung wegen einer Straftat oder eines Verfahrens nach dem Gesetz über Ordnungswidrigkeiten aussetzen würde. Hierüber ist die Person zu belehren. Die Vorschriften über die Glaubhaftmachung des

Verweigerungsgrundes nach § 56 der Strafprozessordnung sind entsprechend anzuwenden. Die Sätze 1 und 2 gelten für die Vorlage von Unterlagen entsprechend.

§ 6 Haftung

Ein Vertrauensdiensteanbieter haftet für Dritte, die er mit Aufgaben nach der Verordnung (EU) Nr. 910/2014, nach diesem Gesetz und nach der Rechtsverordnung nach § 20 beauftragt hat, wie für eigenes Handeln. Die Vorschrift zum Nichteintritt der Ersatzpflicht nach § 831 Absatz 1 Satz 2 des Bürgerlichen Gesetzbuchs ist nicht anzuwenden.

§ 7 Barrierefreie Dienste

(1) Soweit möglich, haben Vertrauensdiensteanbieter die von ihnen angebotenen Vertrauensdienste für Menschen mit Behinderungen zugänglich und nutzbar zu machen. Soweit sie für die Nutzung der Vertrauensdienste erforderliche Endnutzerprodukte von Drittanbietern anbieten, haben sie, soweit möglich, auch mindestens ein marktübliches Endnutzerprodukt für Menschen mit Behinderungen anzubieten. Bei der Bewertung der Durchführbarkeit von Maßnahmen nach den Sätzen 1 und 2 sind auch technische und wirtschaftliche Belange zu berücksichtigen.

(2) Die Vertrauensdiensteanbieter haben auf ihrer Internetseite über die von ihnen vorgenommenen Maßnahmen zur Barrierefreiheit der Vertrauensdienste und der zur Erbringung solcher Dienste verwendeten Endnutzerprodukte zu informieren. Außerdem haben sie dort Hinweise zu geben, die die Nutzung der von ihnen angebotenen Vertrauensdienste und der hierbei verwendeten Endnutzerprodukte durch Menschen mit Behinderungen erleichtern. Diese Informationen und Hinweise sowie die Informationen, die sich an alle Verbraucher richten, müssen nach Maßgabe der Rechtsverordnung nach § 20 barrierefrei zugänglich und nutzbar sein.

(3) Barrieren können von jedermann der Aufsichtsstelle gemeldet werden.

§ 8 Datenschutz

(1) Unbeschadet anderer Rechtsgrundlagen dürfen Vertrauensdiensteanbieter auch bei Dritten personenbezogene Daten verarbeiten, soweit dies für die Erbringung, einschließlich der Prüfung und Sicherstellung der rechtlichen Gültigkeit, des jeweiligen Vertrauensdienstes erforderlich ist.

(2) Der Vertrauensdiensteanbieter darf personenbezogene Daten einer Person, die Vertrauensdienste nutzt, den zuständigen Stellen übermitteln,

1. soweit die zuständigen Stellen die Übermittlung nach Maßgabe der hierfür geltenden Bestimmungen verlangen, da die Übermittlung erforderlich ist
   a) für die Verfolgung von Straftaten oder Ordnungswidrigkeiten,
   b) zur Abwehr von Gefahren für die öffentliche Sicherheit oder Ordnung oder
   c) für die Erfüllung der gesetzlichen Aufgaben der Verfassungsschutzbehörden des Bundes und der Länder, des Bundesnachrichtendienstes, des Militärischen Abschirmdienstes oder der Finanzbehörden, oder
2. soweit Gerichte die Übermittlung im Rahmen anhängiger Verfahren nach Maßgabe der hierfür geltenden Bestimmungen anordnen.

Die Berechtigung zur Datenübermittlung nach Satz 1 Nummer 1 gilt nicht, soweit sie durch andere Gesetze ausdrücklich ausgeschlossen ist.

(3) Die Vertrauensdiensteanbieter haben die Übermittlung zu dokumentieren. Die Dokumentation ist zwölf Monate aufzubewahren.

(4) Hat die zuständige Stelle ein Verlangen nach Datenübermittlung nach Absatz 2 Nummer 1 gestellt, so unterrichtet sie die betroffene Person über die erfolgte Übermittlung der Daten. Von der Unterrichtung kann abgesehen werden, solange die Wahrnehmung der gesetzlichen Aufgaben gefährdet würde und solange das Interesse der betroffenen Person an der Unterrichtung nicht überwiegt. Fünf Jahre nach der Übermittlung kann endgültig von der Benachrichtigung abgesehen werden, wenn die Voraussetzungen für die Benachrichtigung mit an Sicherheit grenzender Wahrscheinlichkeit auch in Zukunft nicht eintreten werden.

(5) Die allgemeinen Datenschutzanforderungen bleiben unberührt.

Teil 2
Allgemeine Vorschriften für qualifizierte Vertrauensdienste

§ 9 Vertrauenslisten

Die Bundesetzagentur ist für die Aufstellung, Führung und Veröffentlichung von Vertrauenslisten nach Artikel 22 Absatz 1 der Verordnung (EU) Nr. 910/2014 zuständig.

§ 10 Deckungsvorsorge

Die Mindestsumme für die gemäß Artikel 24 Absatz 2 Buchstabe c der Verordnung (EU) Nr. 910/2014 erforderliche angemessene Deckungsvorsorge beträgt jeweils 250 000 Euro für einen Schaden, der durch ein haftungsauslösendes Ereignis gemäß Artikel 13 der Verordnung (EU) Nr. 910/2014 verursacht worden ist.

§ 11 Identitätsprüfung

(1) Die Bundesnetzagentur legt nach Anhörung der betroffenen Kreise und im Einvernehmen mit dem Bundesamt für Sicherheit in der Informationstechnik durch Verfügung im Amtsblatt fest, welche sonstigen Identifizierungsmethoden im Sinne des Artikels 24 Absatz 1 Unterabsatz 2 Buchstabe d Satz 1 der Verordnung (EU) Nr. 910/2014 anerkannt sind und welche Mindestanforderungen dafür jeweils gelten.

(2) Die Bundesnetzagentur überprüft die Verfügung nach Absatz 1 regelmäßig im Abstand von vier Jahren sowie

1. bei der begründeten Annahme, dass Methoden nicht mehr hinreichend sicher sind, oder
2. auf Ersuchen des Bundesamtes für Sicherheit in der Informationstechnik.

(3) Innovative Identifizierungsmethoden, die noch nicht durch Verfügung im Amtsblatt anerkannt sind, können von der Bundesnetzagentur im Einvernehmen mit dem Bundesamt für Sicherheit in der Informationstechnik und nach Anhörung der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit für einen Zeitraum von bis zu zwei Jahren vorläufig anerkannt werden, sofern eine Konformitätsbewertungsstelle die gleichwertige Si-

cherheit der Identifizierungsmethode im Sinne des Artikels 24 Absatz 1 Unterabsatz 2 Buchstabe d der Verordnung (EU) Nr. 910/2014 bestätigt hat. Die Bundesnetzagentur veröffentlicht die vorläufig anerkannten Identifizierungsmethoden auf ihrer Internetseite. Die Bundesnetzagentur und das Bundesamt für Sicherheit in der Informationstechnik überwachen die Eignung der vorläufig anerkannten Identifizierungsmethoden über den gesamten Zeitraum der vorläufigen Anerkennung. Werden durch die Überwachung sicherheitsrelevante Risiken bei der vorläufig anerkannten Identifizierungsmethode erkannt, so kann die Aufsichtsstelle im Einvernehmen mit dem Bundesamt für Sicherheit in der Informationstechnik dem qualifizierten Vertrauensdiensteanbieter die Behebung dieser Risiken durch ergänzende Maßnahmen auferlegen, sofern dies sicherheitstechnisch sinnvoll ist. Lässt sich durch ergänzende Maßnahmen keine hinreichende Sicherheit der vorläufig anerkannten Identifizierungsmethode gewährleisten, so soll die Aufsichtsstelle dem qualifizierten Vertrauensdiensteanbieter die Nutzung dieser Identifizierungsmethode untersagen.

(4) Der qualifizierte Vertrauensdiensteanbieter darf nach Maßgabe der datenschutzrechtlichen Bestimmungen personenbezogene Daten nutzen, die zu einem früheren Zeitpunkt im Rahmen einer ordnungsgemäßen Identitätsprüfung erhoben wurden, sofern und soweit diese Daten zum Zeitpunkt der Antragstellung die zuverlässige Identitätsfeststellung des Antragstellers gewährleisten.

§ 12 Attribute in qualifizierten Zertifikaten für elektronische Signaturen und Siegel

(1) Ein qualifiziertes Zertifikat für elektronische Signaturen kann auf Verlangen eines Antragstellers folgende Attribute enthalten:

1. Angaben über die Vertretungsmacht des Antragstellers für eine dritte Person,
2. amts- und berufsbezogene oder sonstige Angaben zur Person des Antragstellers und
3. weitere personenbezogene Angaben.

Angaben über die Vertretungsmacht dürfen nur dann in das qualifizierte Zertifikat aufgenommen werden, wenn dem qualifizierten Vertrauensdiensteanbieter die Einwilligung der dritten Person nachgewiesen wird. Amts- und berufsbezogene oder sonstige Angaben zur Person des Antragstellers dürfen nur dann in das qualifizierte Zertifikat aufgenommen werden, wenn die jeweils zuständige Stelle die Angaben bestätigt hat. Weitere personenbezogene Angaben dürfen in ein qualifiziertes Zertifikat nur mit Einwilligung des Betroffenen aufgenommen werden.

(2) Soll in das qualifizierte Zertifikat anstelle des Namens ein Pseudonym eingetragen werden, so sind Angaben über eine Vertretungsmacht für eine dritte Person oder amts- und berufsbezogene oder sonstige Angaben zur Person nur zulässig, wenn eine Einwilligung der dritten Person oder der jeweils zuständigen Stelle zur Verwendung des Pseudonyms vorliegt.

(3) Die Absätze 1 und 2 gelten entsprechend für qualifizierte Zertifikate für elektronische Siegel. Attribute in qualifizierten Zertifikaten für elektronische Siegel können auch die Vertretungsverhältnisse innerhalb der antragstellenden juristischen Person enthalten, sofern diese Vertretungsverhältnisse dem qualifizierten Vertrauensdiensteanbieter nachgewiesen werden.

§ 13 Unterrichtung über Sicherheitsmaßnahmen und Rechtswirkungen

(1) Der qualifizierte Vertrauensdiensteanbieter hat die Personen, die er nach Artikel 24 Absatz 2 Buchstabe d der Verordnung (EU) Nr. 910/2014 über die Nutzungsbedingungen zu unterrichten hat, weil sie einen qualifizierten Vertrauensdienst nutzen wollen, auch

1. über die Maßnahmen zu unterrichten, die erforderlich sind, um zur Sicherheit der angebotenen qualifizierten Vertrauensdienste und deren zuverlässiger Nutzung beizutragen, und dabei auf entsprechende Informationsmöglichkeiten hinzuweisen, insbesondere auf Informationsangebote der Hersteller von Produkten für qualifizierte Vertrauensdienste und auf Informationsangebote der Aufsichtsstellen,
2. darauf hinzuweisen, dass entsprechend § 15 qualifiziert elektronisch signierte, gesiegelte oder zeitgestempelte Daten bei Bedarf durch geeignete Maßnahmen neu zu schützen sind, bevor der Sicherheitswert der vorhandenen Signaturen, Siegel oder Zeitstempel durch Zeitablauf geringer wird, und
3. über die Rechtswirkungen der angebotenen qualifizierten Vertrauensdienste zu unterrichten.

(2) Soweit eine Person, die einen qualifizierten Vertrauensdienst nutzen will, bereits zu einem früheren Zeitpunkt nach Artikel 24 Absatz 2 Buchstabe d der Verordnung (EU) Nr. 910/2014 sowie nach Absatz 1 unterrichtet worden ist und sich keine Änderungen ergeben haben, kann eine erneute Unterrichtung unterbleiben.

§ 14 Widerruf qualifizierter Zertifikate

(1) Der qualifizierte Vertrauensdiensteanbieter hat ein noch gültiges qualifiziertes Zertifikat insbesondere dann unverzüglich zu widerrufen, wenn

1. die Person, der das qualifizierte Zertifikat ausgestellt wurde, es verlangt,
2. das qualifizierte Zertifikat auf Grund falscher Angaben zu den Anhängen I, III und IV der Verordnung (EU) Nr. 910/2014 ausgestellt wurde,
3. er seine Tätigkeit beendet und diese nicht von einem anderen qualifizierten Vertrauensdiensteanbieter fortgeführt wird oder
4. Tatsachen die Annahme rechtfertigen, dass
   a) das qualifizierte Zertifikat gefälscht oder nicht hinreichend fälschungssicher ist oder
   b) die verwendeten qualifizierten elektronischen Signaturerstellungseinheiten oder qualifizierten elektronischen Siegelerstellungseinheiten Sicherheitsmängel aufweisen.

Weitere Widerrufsgründe können vertraglich vereinbart werden. Wurde ein qualifiziertes Zertifikat mit falschen Angaben ausgestellt, so kann der qualifizierte Vertrauensdiensteanbieter dies zusätzlich kenntlich machen.

(2) Enthält ein qualifiziertes Zertifikat Attribute nach § 12 Absatz 1 oder § 12 Absatz 3 Satz 2, so kann auch die dritte Person oder die für die amts- und berufsbezogenen oder sonstigen Angaben zur Person zuständige Stelle einen Widerruf des Zertifikats verlangen, wenn

1. die Vertretungsmacht entfällt oder
2. die Voraussetzungen für die amts- und berufsbezogenen oder sonstigen Angaben zur Person nach Aufnahme in das qualifizierte Zertifikat entfallen.

(3) Liegen die in Absatz 1 Satz 1 Nummer 3 oder eine der in Absatz 1 Satz 1 Nummer 4 genannten Voraussetzungen vor, so kann die Aufsichtsstelle den Widerruf eines qualifizierten Zertifikats anordnen.

§ 15 Langfristige Beweiserhaltung

Sofern hierfür Bedarf besteht, sind qualifiziert elektronisch signierte, gesiegelte oder zeitgestempelte Daten durch geeignete Maßnahmen neu zu schützen, bevor der Sicherheitswert der vorhandenen Signaturen, Siegel oder Zeitstempel durch Zeitablauf geringer wird. Die neue Sicherung muss nach dem Stand der Technik erfolgen.

§ 16 Beendigungsplan; auf Dauer prüfbare Vertrauensdienste

(1) In dem Beendigungsplan nach Artikel 24 Absatz 2 Buchstabe i der Verordnung (EU) Nr. 910/2014 hat ein qualifizierter Vertrauensdiensteanbieter alle erforderlichen Maßnahmen vorzusehen, damit bei Einstellung der Tätigkeit, bei Entzug des Qualifikationsstatus oder wenn die Eröffnung eines Insolvenzverfahrens beantragt und die Tätigkeit nicht fortgesetzt wird, alle von ihm ausgegebenen qualifizierten Zertifikate im Zusammenhang mit elektronischen Signaturen und Siegeln sowie Zertifikate im Zusammenhang mit Anhang I Buchstabe g, Anhang III Buchstabe g und Artikel 42 Absatz 1 Buchstabe c der Verordnung (EU) Nr. 910/2014 einschließlich der Widerrufsinformationen

1. von einem anderen qualifizierten Vertrauensdiensteanbieter übernommen werden können oder
2. von der Bundesnetzagentur in die Vertrauensinfrastruktur nach Absatz 5 übernommen werden können.

Im Falle von Satz 1 Nummer 2 hat der qualifizierte Vertrauensdiensteanbieter die noch gültigen Zertifikate vor der Übermittlung an die Bundesnetzagentur zu widerrufen. Er hat in jedem Fall sicherzustellen, dass die dazugehörigen Aufzeichnungen nach Artikel 24 Absatz 2 Buchstabe h der Verordnung (EU) Nr. 910/2014 an den Übernehmenden übermittelt werden.

(2) Im Beendigungsplan hat der qualifizierte Vertrauensdiensteanbieter auch Vorkehrungen zu treffen, um die Inhaber der in Absatz 1 Satz 1 genannten Zertifikate, soweit möglich, mindestens zwei Monate im Voraus über die Einstellung seiner Tätigkeit und über die Übernahme seiner Zertifikate zu benachrichtigen.

(3) In den Fällen des Absatzes 1 Satz 1 Nummer 2 erteilt die Bundesnetzagentur bei Vorliegen eines berechtigten Interesses Auskunft zu den Aufzeichnungen, soweit dies technisch und ohne unverhältnismäßig großen Aufwand möglich ist. Ein darüber hinausgehendes Auskunftsrecht gemäß § 19 des Bundesdatenschutzgesetzes und nach Artikel 15 der Verordnung (EU) 2016/679 bleibt hiervon unberührt.

(4) Qualifizierte Vertrauensdiensteanbieter haben für die gesamte Zeit ihres Betriebs

1. die in Absatz 1 Satz 1 genannten Zertifikate auch über den Zeitraum ihrer Gültigkeit hinaus zusammen mit den dazugehörigen Widerrufsinformationen in einer

Zertifikatsdatenbank nach Artikel 24 Absatz 2 Buchstabe k und Absatz 4 der Verordnung (EU) Nr. 910/2014 zu führen und

2. die dazugehörigen Aufzeichnungen nach Artikel 24 Absatz 2 Buchstabe h der Verordnung (EU) Nr. 910/2014 aufzubewahren.

(5) Die Bundesnetzagentur hat eine Vertrauensinfrastruktur zur dauerhaften Prüfbarkeit qualifizierter elektronischer Zertifikate und qualifizierter elektronischer Zeitstempel einzurichten, zu unterhalten und laufend zu aktualisieren. Näheres regelt die Rechtsverordnung nach § 20 Absatz 2 Nummer 5.

Teil 3
Qualifizierte elektronische Signaturen und Siegel

§ 17 Benannte Stellen nach Artikel 30 Absatz 1 der Verordnung (EU) Nr. 910/2014

(1) Die Bundesnetzagentur benennt auf Antrag eine Organisation als private Stelle gemäß Artikel 30 Absatz 1 der Verordnung (EU) Nr. 910/2014 sowie gemäß Artikel 39 Absatz 2 in Verbindung mit Artikel 30 Absatz 1 der Verordnung (EU) Nr. 910/2014, sofern die Akkreditierungsstelle nach § 1 Absatz 1 des Akkreditierungsstellengesetzes durch Akkreditierung festgestellt hat, dass die private Stelle die erforderlichen Anforderungen erfüllt. Die Benennung kann

1. inhaltlich beschränkt werden, vorläufig erteilt werden oder mit einer Befristung versehen erteilt werden und

2. mit Auflagen verbunden sein.

(2) Solange die Europäische Kommission keine delegierten Rechtsakte nach Artikel 30 Absatz 4 der Verordnung (EU) Nr. 910/2014 erlassen hat, erstellt und veröffentlicht

1. die Akkreditierungsstelle die fachlichen Kriterien, die für die Akkreditierung zu erfüllen sind, und

2. die Bundesnetzagentur die fachlichen Kriterien, die für die Benennung als private Stelle nach Artikel 30 Absatz 1 der Verordnung (EU) Nr. 910/2014 zu erfüllen sind.

Die Erstellung der fachlichen Kriterien erfolgt unter maßgeblicher Berücksichtigung der Entscheidung der Kommission vom 6. November 2000 über die Mindestkriterien, die von den Mitgliedstaaten bei der Benennung der Stellen gemäß Artikel 3 Absatz 4 der Richtlinie 1999/93/EG des Europäischen Parlaments und des Rates über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen zu berücksichtigen sind (ABl. L 289 vom 16.11.2000, S. 42).

(3) Eine Stelle, die nach § 17 Absatz 4 Satz 1 des Signaturgesetzes in Verbindung mit § 18 des Signaturgesetzes anerkannt wurde, nimmt hinsichtlich der von ihr auf Grundlage des Signaturgesetzes bestätigten Produkte ihre hiermit zusammenhängenden Aufgaben bis zum Auslaufen der entsprechenden Produktbestätigungen wahr.

(4) Das Bundesamt für Sicherheit in der Informationstechnik ist die öffentliche Stelle gemäß Artikel 30 Absatz 1 der Verordnung (EU) Nr. 910/2014 sowie gemäß Artikel 39 Absatz 2 in Verbindung mit Artikel 30 Absatz 1 der Verordnung (EU) Nr. 910/2014.

Teil 4
Qualifizierte Dienste für die Zustellung elektronischer Einschreiben

§ 18 Dienste für die Zustellung elektronischer Einschreiben

Liegt der Konformitätsbewertungsstelle für einen qualifizierten Dienst für die Zustellung elektronischer Einschreiben eine Akkreditierung nach Abschnitt 4 des De-Mail-Gesetzes vor, so soll die Konformitätsbewertungsstelle die Konformitätsbewertung dieses qualifizierten Dienstes nach Möglichkeit auf die Prüfung der Nachweise beschränken, die im Rahmen der Akkreditierung nach § 18 Absatz 3 des De-Mail-Gesetzes erbracht worden sind.

Teil 5
Schlussvorschriften

§ 19 Bußgeldvorschriften

(1) Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig

1. entgegen § 12 Absatz 1 Satz 2, 3 oder 4 oder Absatz 2, jeweils auch in Verbindung mit Absatz 3 Satz 1 oder einer Rechtsverordnung nach § 20 Absatz 2 Nummer 1, eine Angabe in ein qualifiziertes Zertifikat aufnimmt,
2. entgegen § 14 Absatz 1 Satz 1 Nummer 1 bis 4 oder § 16 Absatz 1 Satz 2 ein Zertifikat nicht oder nicht rechtzeitig widerruft,
3. entgegen § 16 Absatz 1 Satz 3, auch in Verbindung mit der Rechtsverordnung nach § 20 Absatz 2 Nummer 1, nicht sicherstellt, dass eine Aufzeichnung übermittelt wird, oder
4. entgegen § 16 Absatz 2 in Verbindung mit der Rechtsverordnung nach § 20 Absatz 2 Nummer 1 eine dort genannte Vorkehrung nicht oder nicht rechtzeitig trifft.

(2) Ordnungswidrig handelt, wer gegen die Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG (ABl. L 257 vom 28.8.2014, S. 73; L 23 vom 29.1.2015, S. 19) verstößt, indem er vorsätzlich oder fahrlässig

1. entgegen Artikel 19 Absatz 2 Unterabsatz 1 eine Meldung nicht, nicht richtig oder nicht rechtzeitig macht,
2. entgegen Artikel 19 Absatz 2 Unterabsatz 2 eine Person nicht, nicht richtig oder nicht rechtzeitig unterrichtet,
3. entgegen Artikel 21 Absatz 1 eine Mitteilung nicht, nicht richtig oder nicht rechtzeitig vorlegt,
4. entgegen Artikel 24 Absatz 1 Unterabsatz 1 die Identität einer Person nicht oder nicht rechtzeitig überprüft,

5. entgegen Artikel 24 Absatz 2 Buchstabe c in Verbindung mit § 10 in Verbindung mit einer Rechtsverordnung nach § 20 Absatz 2 Nummer 3 eine Haftpflichtversicherung nicht oder nicht rechtzeitig abschließt,
6. entgegen Artikel 24 Absatz 2 Buchstabe e oder f, jeweils in Verbindung mit einer Rechtsverordnung nach § 20 Absatz 2 Nummer 1, ein vertrauenswürdiges System oder Produkt nicht verwendet,
7. entgegen Artikel 24 Absatz 2 Buchstabe g in Verbindung mit einer Rechtsverordnung nach § 20 Absatz 2 Nummer 1 eine dort genannte Maßnahme nicht oder nicht rechtzeitig trifft,
8. entgegen Artikel 24 Absatz 2 Buchstabe h Satz 1 eine Information nicht richtig aufzeichnet oder
9. entgegen Artikel 24 Absatz 3 Satz 1 einen Widerruf nicht oder nicht rechtzeitig veröffentlicht.

(3) Die Ordnungswidrigkeit kann in den Fällen des Absatzes 2 Nummer 5 bis 8 mit einer Geldbuße bis zu einhunderttausend Euro, in den übrigen Fällen mit einer Geldbuße bis zu zwanzigtausend Euro geahndet werden.

(4) Verwaltungsbehörden im Sinne des § 36 Absatz 1 Nummer 1 des Gesetzes über Ordnungswidrigkeiten sind die Bundesnetzagentur und das Bundesamt für Sicherheit in der Informationstechnik jeweils im Rahmen ihrer Zuständigkeit nach § 2 Absatz 1.

§ 20 Verordnungsermächtigung

(1) Die Bundesregierung legt durch Rechtsverordnung nähere Anforderungen an die Zugänglich- und Nutzbarmachung von Vertrauensdiensten nach Artikel 15 der Verordnung (EU) Nr. 910/2014 und nach § 7 fest. Sie hat dabei technische und wirtschaftliche Belange zu berücksichtigen. Die Rechtsverordnung kann auch Nachweis-, Mitwirkungs- und Informationspflichten der Vertrauensdiensteanbieter enthalten.

(2) Die Bundesregierung wird ermächtigt, in der Rechtsverordnung nach Absatz 1 auch die zur Durchführung der Verordnung (EU) Nr. 910/2014 und dieses Gesetzes erforderlichen Rechtsvorschriften zu erlassen über

1. die Ausgestaltung der Pflichten der Vertrauensdiensteanbieter bei der Betriebsaufnahme, während des Betriebs und bei der Einstellung des Betriebs nach den Artikeln 17 bis 24 der Verordnung (EU) Nr. 910/2014 und nach den §§ 4 und 5, 9 bis 18,
2. die Durchführung gemeinsamer Untersuchungen nach Artikel 18 Absatz 3 der Verordnung (EU) Nr. 910/2014,
3. die zur Erfüllung der Verpflichtung zur Deckungsvorsorge nach § 10 zulässigen Sicherheitsleistungen sowie über deren Umfang, Höhe und inhaltliche Ausgestaltung,
4. die Anforderungen im Zusammenhang mit einer Zertifikatsdatenbank nach § 16 Absatz 4 Nummer 1,
5. die Einrichtung einer Vertrauensinfrastruktur zur dauerhaften Prüfbarkeit qualifizierter elektronischer Zertifikate und qualifizierter elektronischer Zeitstempel nach § 16 Absatz 5 und

6. die Einzelheiten des Verfahrens der Anerkennung und der Tätigkeit von Zertifizierungsstellen nach § 17.

§ 21 Übergangsvorschrift

Zertifizierungsdiensteanbieter, die qualifizierte Zertifikate im Sinne von § 2 Nummer 3 des Signaturgesetzes ausgestellt haben, dürfen diese qualifizierten Zertifikate als qualifizierte Vertrauensdiensteanbieter für qualifizierte Zertifikate nach der Verordnung (EU) Nr. 910/2014 weiterhin in ihrem Zertifikatsverzeichnis führen. Sie dürfen weiter alle in diesem Zusammenhang mit ihren Kunden vereinbarten Dienste anbieten, insbesondere einen Widerrufsdienst. § 16 Absatz 1 gilt entsprechend. Die von der Bundesnetzagentur gemäß § 16 Absatz 1 des Signaturgesetzes ausgestellten Zertifikate werden mit Ablauf des 14. November 2018 gesperrt.

Gesetz zur Regelung des Zugangs zu Informationen des Bundes (Informationsfreiheitsgesetz - IFG)

§ 1 Grundsatz

(1) Jeder hat nach Maßgabe dieses Gesetzes gegenüber den Behörden des Bundes einen Anspruch auf Zugang zu amtlichen Informationen. Für sonstige Bundesorgane und -einrichtungen gilt dieses Gesetz, soweit sie öffentlich-rechtliche Verwaltungsaufgaben wahrnehmen. Einer Behörde im Sinne dieser Vorschrift steht eine natürliche Person oder juristische Person des Privatrechts gleich, soweit eine Behörde sich dieser Person zur Erfüllung ihrer öffentlich-rechtlichen Aufgaben bedient.

(2) Die Behörde kann Auskunft erteilen, Akteneinsicht gewähren oder Informationen in sonstiger Weise zur Verfügung stellen. Begehrt der Antragsteller eine bestimmte Art des Informationszugangs, so darf dieser nur aus wichtigem Grund auf andere Art gewährt werden. Als wichtiger Grund gilt insbesondere ein deutlich höherer Verwaltungsaufwand.

(3) Regelungen in anderen Rechtsvorschriften über den Zugang zu amtlichen Informationen gehen mit Ausnahme des § 29 des Verwaltungsverfahrensgesetzes und des § 25 des Zehnten Buches Sozialgesetzbuch vor.

§ 2 Begriffsbestimmungen

Im Sinne dieses Gesetzes ist

1. amtliche Information: jede amtlichen Zwecken dienende Aufzeichnung, unabhängig von der Art ihrer Speicherung. Entwürfe und Notizen, die nicht Bestandteil eines Vorgangs werden sollen, gehören nicht dazu;
2. Dritter: jeder, über den personenbezogene Daten oder sonstige Informationen vorliegen.

§ 3 Schutz von besonderen öffentlichen Belangen

Der Anspruch auf Informationszugang besteht nicht,

1. wenn das Bekanntwerden der Information nachteilige Auswirkungen haben kann auf
   a) internationale Beziehungen,
   b) militärische und sonstige sicherheitsempfindliche Belange der Bundeswehr,
   c) Belange der inneren oder äußeren Sicherheit,
   d) Kontroll- oder Aufsichtsaufgaben der Finanz-, Wettbewerbs- und Regulierungsbehörden,
   e) Angelegenheiten der externen Finanzkontrolle,
   f) Maßnahmen zum Schutz vor unerlaubtem Außenwirtschaftsverkehr,

g) die Durchführung eines laufenden Gerichtsverfahrens, den Anspruch einer Person auf ein faires Verfahren oder die Durchführung strafrechtlicher, ordnungswidrigkeitsrechtlicher oder disziplinarischer Ermittlungen,

2. wenn das Bekanntwerden der Information die öffentliche Sicherheit gefährden kann,

3. wenn und solange

   a) die notwendige Vertraulichkeit internationaler Verhandlungen oder

   b) die Beratungen von Behörden beeinträchtigt werden,

4. wenn die Information einer durch Rechtsvorschrift oder durch die Allgemeine Verwaltungsvorschrift zum materiellen und organisatorischen Schutz von Verschlusssachen geregelten Geheimhaltungs- oder Vertraulichkeitspflicht oder einem Berufs- oder besonderen Amtsgeheimnis unterliegt,

5. hinsichtlich vorübergehend beigezogener Information einer anderen öffentlichen Stelle, die nicht Bestandteil der eigenen Vorgänge werden soll,

6. wenn das Bekanntwerden der Information geeignet wäre, fiskalische Interessen des Bundes im Wirtschaftsverkehr oder wirtschaftliche Interessen der Sozialversicherungen zu beeinträchtigen,

7. bei vertraulich erhobener oder übermittelter Information, soweit das Interesse des Dritten an einer vertraulichen Behandlung im Zeitpunkt des Antrags auf Informationszugang noch fortbesteht,

8. gegenüber den Nachrichtendiensten sowie den Behörden und sonstigen öffentlichen Stellen des Bundes, soweit sie Aufgaben im Sinne des § 10 Nr. 3 des Sicherheitsüberprüfungsgesetzes wahrnehmen.

§ 4 Schutz des behördlichen Entscheidungsprozesses

(1) Der Antrag auf Informationszugang soll abgelehnt werden für Entwürfe zu Entscheidungen sowie Arbeiten und Beschlüsse zu ihrer unmittelbaren Vorbereitung, soweit und solange durch die vorzeitige Bekanntgabe der Informationen der Erfolg der Entscheidung oder bevorstehender behördlicher Maßnahmen vereitelt würde. Nicht der unmittelbaren Entscheidungsvorbereitung nach Satz 1 dienen regelmäßig Ergebnisse der Beweiserhebung und Gutachten oder Stellungnahmen Dritter.

(2) Der Antragsteller soll über den Abschluss des jeweiligen Verfahrens informiert werden.

§ 5 Schutz personenbezogener Daten

(1) Zugang zu personenbezogenen Daten darf nur gewährt werden, soweit das Informationsinteresse des Antragstellers das schutzwürdige Interesse des Dritten am Ausschluss des Informationszugangs überwiegt oder der Dritte eingewilligt hat. Besondere Kategorien personenbezogener Daten im Sinne des Artikels 9 Absatz 1 der 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; L 314 vom 22.11.2016, S. 72; L 127 vom 23.5.2018, S. 2) in der jeweils geltenden Fassung dürfen nur übermittelt werden, wenn der Dritte ausdrücklich eingewilligt hat.

(2) Das Informationsinteresse des Antragstellers überwiegt nicht bei Informationen aus Unterlagen, soweit sie mit dem Dienst- oder Amtsverhältnis oder einem Mandat des Dritten in Zusammenhang stehen und bei Informationen, die einem Berufs- oder Amtsgeheimnis unterliegen.

(3) Das Informationsinteresse des Antragstellers überwiegt das schutzwürdige Interesse des Dritten am Ausschluss des Informationszugangs in der Regel dann, wenn sich die Angabe auf Name, Titel, akademischen Grad, Berufs- und Funktionsbezeichnung, Büroanschrift und -telekommunikationsnummer beschränkt und der Dritte als Gutachter, Sachverständiger oder in vergleichbarer Weise eine Stellungnahme in einem Verfahren abgegeben hat.

(4) Name, Titel, akademischer Grad, Berufs- und Funktionsbezeichnung, Büroanschrift und -telekommunikationsnummer von Bearbeitern sind vom Informationszugang nicht ausgeschlossen, soweit sie Ausdruck und Folge der amtlichen Tätigkeit sind und kein Ausnahmetatbestand erfüllt ist.

§ 6 Schutz des geistigen Eigentums und von Betriebs- oder Geschäftsgeheimnissen

Der Anspruch auf Informationszugang besteht nicht, soweit der Schutz geistigen Eigentums entgegensteht. Zugang zu Betriebs- oder Geschäftsgeheimnissen darf nur gewährt werden, soweit der Betroffene eingewilligt hat.

§ 7 Antrag und Verfahren

(1) Über den Antrag auf Informationszugang entscheidet die Behörde, die zur Verfügung über die begehrten Informationen berechtigt ist. Im Fall des § 1 Abs. 1 Satz 3 ist der Antrag an die Behörde zu richten, die sich der natürlichen oder juristischen Person des Privatrechts zur Erfüllung ihrer öffentlich-rechtlichen Aufgaben bedient. Betrifft der Antrag Daten Dritter im Sinne von § 5 Abs. 1 und 2 oder § 6, muss er begründet werden. Bei gleichförmigen Anträgen von mehr als 50 Personen gelten die §§ 17 bis 19 des Verwaltungsverfahrensgesetzes entsprechend.

(2) Besteht ein Anspruch auf Informationszugang zum Teil, ist dem Antrag in dem Umfang stattzugeben, in dem der Informationszugang ohne Preisgabe der geheimhaltungsbedürftigen Informationen oder ohne unverhältnismäßigen Verwaltungsaufwand möglich ist. Entsprechendes gilt, wenn sich der Antragsteller in den Fällen, in denen Belange Dritter berührt sind, mit einer Unkenntlichmachung der diesbezüglichen Informationen einverstanden erklärt.

(3) Auskünfte können mündlich, schriftlich oder elektronisch erteilt werden. Die Behörde ist nicht verpflichtet, die inhaltliche Richtigkeit der Information zu prüfen.

(4) Im Fall der Einsichtnahme in amtliche Informationen kann sich der Antragsteller Notizen machen oder Ablichtungen und Ausdrucke fertigen lassen. § 6 Satz 1 bleibt unberührt.

(5) Die Information ist dem Antragsteller unter Berücksichtigung seiner Belange unverzüglich zugänglich zu machen. Der Informationszugang soll innerhalb eines Monats erfolgen. § 8 bleibt unberührt.

§ 8 Verfahren bei Beteiligung Dritter

(1) Die Behörde gibt einem Dritten, dessen Belange durch den Antrag auf Informationszugang berührt sind, schriftlich Gelegenheit zur Stellungnahme innerhalb eines Monats, so-

fern Anhaltspunkte dafür vorliegen, dass er ein schutzwürdiges Interesse am Ausschluss des Informationszugangs haben kann.

(2) Die Entscheidung nach § 7 Abs. 1 Satz 1 ergeht schriftlich und ist auch dem Dritten bekannt zu geben. Der Informationszugang darf erst erfolgen, wenn die Entscheidung dem Dritten gegenüber bestandskräftig ist oder die sofortige Vollziehung angeordnet worden ist und seit der Bekanntgabe der Anordnung an den Dritten zwei Wochen verstrichen sind. § 9 Abs. 4 gilt entsprechend.

§ 9 Ablehnung des Antrags; Rechtsweg

(1) Die Bekanntgabe einer Entscheidung, mit der der Antrag ganz oder teilweise abgelehnt wird, hat innerhalb der Frist nach § 7 Abs. 5 Satz 2 zu erfolgen.

(2) Soweit die Behörde den Antrag ganz oder teilweise ablehnt, hat sie mitzuteilen, ob und wann der Informationszugang ganz oder teilweise zu einem späteren Zeitpunkt voraussichtlich möglich ist.

(3) Der Antrag kann abgelehnt werden, wenn der Antragsteller bereits über die begehrten Informationen verfügt oder sich diese in zumutbarer Weise aus allgemein zugänglichen Quellen beschaffen kann.

(4) Gegen die ablehnende Entscheidung sind Widerspruch und Verpflichtungsklage zulässig. Ein Widerspruchsverfahren nach den Vorschriften des 8. Abschnitts der Verwaltungsgerichtsordnung ist auch dann durchzuführen, wenn die Entscheidung von einer obersten Bundesbehörde getroffen wurde.

§ 10 Gebühren und Auslagen

(1) Für individuell zurechenbare öffentliche Leistungen nach diesem Gesetz werden Gebühren und Auslagen erhoben. Dies gilt nicht für die Erteilung einfacher Auskünfte.

(2) Die Gebühren sind auch unter Berücksichtigung des Verwaltungsaufwandes so zu bemessen, dass der Informationszugang nach § 1 wirksam in Anspruch genommen werden kann.

(3) Das Bundesministerium des Innern, für Bau und Heimat wird ermächtigt, für individuell zurechenbare öffentliche Leistungen nach diesem Gesetz die Gebührentatbestände und Gebührensätze durch Rechtsverordnung ohne Zustimmung des Bundesrates zu bestimmen. § 10 des Bundesgebührengesetzes findet keine Anwendung.

§ 11 Veröffentlichungspflichten

(1) Die Behörden sollen Verzeichnisse führen, aus denen sich die vorhandenen Informationssammlungen und -zwecke erkennen lassen.

(2) Organisations- und Aktenpläne ohne Angabe personenbezogener Daten sind nach Maßgabe dieses Gesetzes allgemein zugänglich zu machen.

(3) Die Behörden sollen die in den Absätzen 1 und 2 genannten Pläne und Verzeichnisse sowie weitere geeignete Informationen in elektronischer Form allgemein zugänglich machen.

§ 12 Bundesbeauftragter für die Informationsfreiheit

(1) Jeder kann den Bundesbeauftragten für die Informationsfreiheit anrufen, wenn er sein Recht auf Informationszugang nach diesem Gesetz als verletzt ansieht.

(2) Die Aufgabe des Bundesbeauftragten für die Informationsfreiheit wird von dem Bundesbeauftragten für den Datenschutz wahrgenommen.

(3) Die Bestimmungen des Bundesdatenschutzgesetzes in der am 24. Mai 2018 geltenden Fassung über die Kontrollaufgaben des Bundesbeauftragten für den Datenschutz (§ 24 Abs. 1 und 3 bis 5), über Beanstandungen (§ 25 Abs. 1 Satz 1 Nr. 1 und 4, Satz 2 und Abs. 2 und 3) sowie über weitere Aufgaben gemäß § 26 Abs. 1 bis 3 gelten entsprechend.

§ 13 (weggefallen)

§ 14 Bericht und Evaluierung

Die Bundesregierung unterrichtet den Deutschen Bundestag zwei Jahre vor Außerkrafttreten über die Anwendung dieses Gesetzes. Der Deutsche Bundestag wird das Gesetz ein Jahr vor Außerkrafttreten auf wissenschaftlicher Grundlage evaluieren.

§ 15 Inkrafttreten

Dieses Gesetz tritt am 1. Januar 2006 in Kraft.

Umweltinformationsgesetz (UIG)

Abschnitt 1
Allgemeine Vorschriften

§ 1 Zweck des Gesetzes; Anwendungsbereich

(1) Zweck dieses Gesetzes ist es, den rechtlichen Rahmen für den freien Zugang zu Umweltinformationen bei informationspflichtigen Stellen sowie für die Verbreitung dieser Umweltinformationen zu schaffen.

(2) Dieses Gesetz gilt für informationspflichtige Stellen des Bundes und der bundesunmittelbaren juristischen Personen des öffentlichen Rechts.

§ 2 Begriffsbestimmungen

(1) Informationspflichtige Stellen sind

1. die Regierung und andere Stellen der öffentlichen Verwaltung. Gremien, die diese Stellen beraten, gelten als Teil der Stelle, die deren Mitglieder beruft. Zu den informationspflichtigen Stellen gehören nicht
   a) die obersten Bundesbehörden, soweit und solange sie im Rahmen der Gesetzgebung tätig werden, und
   b) Gerichte des Bundes, soweit sie nicht Aufgaben der öffentlichen Verwaltung wahrnehmen;
2. natürliche oder juristische Personen des Privatrechts, soweit sie öffentliche Aufgaben wahrnehmen oder öffentliche Dienstleistungen erbringen, die im Zusammenhang mit der Umwelt stehen, insbesondere solche der umweltbezogenen Daseinsvorsorge, und dabei der Kontrolle des Bundes oder einer unter der Aufsicht des Bundes stehenden juristischen Person des öffentlichen Rechts unterliegen.

(2) Kontrolle im Sinne des Absatzes 1 Nummer 2 liegt vor, wenn

1. die Person des Privatrechts bei der Wahrnehmung der öffentlichen Aufgabe oder bei der Erbringung der öffentlichen Dienstleistung gegenüber Dritten besonderen Pflichten unterliegt oder über besondere Rechte verfügt, insbesondere ein Kontrahierungszwang oder ein Anschluss- und Benutzungszwang besteht, oder
2. eine oder mehrere der in Absatz 1 Nummer 2 genannten juristischen Personen des öffentlichen Rechts allein oder zusammen, unmittelbar oder mittelbar
   a) die Mehrheit des gezeichneten Kapitals des Unternehmens besitzen,
   b) über die Mehrheit der mit den Anteilen des Unternehmens verbundenen Stimmrechte verfügen oder
   c) mehr als die Hälfte der Mitglieder des Verwaltungs-, Leitungs- oder Aufsichtsorgans des Unternehmens bestellen können, oder
3. mehrere juristische Personen des öffentlichen Rechts zusammen unmittelbar oder mittelbar über eine Mehrheit im Sinne der Nummer 2 Buchstabe a bis c verfügen

und der überwiegende Anteil an dieser Mehrheit den in Absatz 1 Nummer 2 genannten juristischen Personen des öffentlichen Rechts zuzuordnen ist.

(3) Umweltinformationen sind unabhängig von der Art ihrer Speicherung alle Daten über

1. den Zustand von Umweltbestandteilen wie Luft und Atmosphäre, Wasser, Boden, Landschaft und natürliche Lebensräume einschließlich Feuchtgebiete, Küsten- und Meeresgebiete, die Artenvielfalt und ihre Bestandteile, einschließlich gentechnisch veränderter Organismen, sowie die Wechselwirkungen zwischen diesen Bestandteilen;
2. Faktoren wie Stoffe, Energie, Lärm und Strahlung, Abfälle aller Art sowie Emissionen, Ableitungen und sonstige Freisetzungen von Stoffen in die Umwelt, die sich auf die Umweltbestandteile im Sinne der Nummer 1 auswirken oder wahrscheinlich auswirken;
3. Maßnahmen oder Tätigkeiten, die
   a) sich auf die Umweltbestandteile im Sinne der Nummer 1 oder auf Faktoren im Sinne der Nummer 2 auswirken oder wahrscheinlich auswirken oder
   b) den Schutz von Umweltbestandteilen im Sinne der Nummer 1 bezwecken; zu den Maßnahmen gehören auch politische Konzepte, Rechts- und Verwaltungsvorschriften, Abkommen, Umweltvereinbarungen, Pläne und Programme;
4. Berichte über die Umsetzung des Umweltrechts;
5. Kosten-Nutzen-Analysen oder sonstige wirtschaftliche Analysen und Annahmen, die zur Vorbereitung oder Durchführung von Maßnahmen oder Tätigkeiten im Sinne der Nummer 3 verwendet werden, und
6. den Zustand der menschlichen Gesundheit und Sicherheit, die Lebensbedingungen des Menschen sowie Kulturstätten und Bauwerke, soweit sie jeweils vom Zustand der Umweltbestandteile im Sinne der Nummer 1 oder von Faktoren, Maßnahmen oder Tätigkeiten im Sinne der Nummern 2 und 3 betroffen sind oder sein können; hierzu gehört auch die Kontamination der Lebensmittelkette.

(4) Eine informationspflichtige Stelle verfügt über Umweltinformationen, wenn diese bei ihr vorhanden sind oder für sie bereitgehalten werden. Ein Bereithalten liegt vor, wenn eine natürliche oder juristische Person, die selbst nicht informationspflichtige Stelle ist, Umweltinformationen für eine informationspflichtige Stelle im Sinne des Absatzes 1 aufbewahrt, auf die diese Stelle einen Übermittlungsanspruch hat.

Abschnitt 2
Informationszugang auf Antrag

§ 3 Anspruch auf Zugang zu Umweltinformationen

(1) Jede Person hat nach Maßgabe dieses Gesetzes Anspruch auf freien Zugang zu Umweltinformationen, über die eine informationspflichtige Stelle im Sinne des § 2 Absatz 1 verfügt, ohne ein rechtliches Interesse darlegen zu müssen. Daneben bleiben andere Ansprüche auf Zugang zu Informationen unberührt.

(2) Der Zugang kann durch Auskunftserteilung, Gewährung von Akteneinsicht oder in sonstiger Weise eröffnet werden. Wird eine bestimmte Art des Informationszugangs beantragt, so darf dieser nur aus gewichtigen Gründen auf andere Art eröffnet werden. Als gewichtiger Grund gilt insbesondere ein deutlich höherer Verwaltungsaufwand. Soweit Umweltinformationen der antragstellenden Person bereits auf andere, leicht zugängliche Art, insbesondere durch Verbreitung nach § 10, zur Verfügung stehen, kann die informationspflichtige Stelle die Person auf diese Art des Informationszugangs verweisen.

(3) Soweit ein Anspruch nach Absatz 1 besteht, sind die Umweltinformationen der antragstellenden Person unter Berücksichtigung etwaiger von ihr angegebener Zeitpunkte, spätestens jedoch mit Ablauf der Frist nach Satz 2 Nummer 1 oder Nummer 2 zugänglich zu machen. Die Frist beginnt mit Eingang des Antrags bei der informationspflichtigen Stelle, die über die Informationen verfügt, und endet

1. mit Ablauf eines Monats oder
2. soweit Umweltinformationen derart umfangreich und komplex sind, dass die in Nummer 1 genannte Frist nicht eingehalten werden kann, mit Ablauf von zwei Monaten.

§ 4 Antrag und Verfahren

(1) Umweltinformationen werden von einer informationspflichtigen Stelle auf Antrag zugänglich gemacht.

(2) Der Antrag muss erkennen lassen, zu welchen Umweltinformationen der Zugang gewünscht wird. Ist der Antrag zu unbestimmt, so ist der antragstellenden Person dies innerhalb eines Monats mitzuteilen und Gelegenheit zur Präzisierung des Antrags zu geben. Kommt die antragstellende Person der Aufforderung zur Präzisierung nach, beginnt der Lauf der Frist zur Beantwortung von Anträgen erneut. Die Informationssuchenden sind bei der Stellung und Präzisierung von Anträgen zu unterstützen.

(3) Wird der Antrag bei einer informationspflichtigen Stelle gestellt, die nicht über die Umweltinformationen verfügt, leitet sie den Antrag an die über die begehrten Informationen verfügende Stelle weiter, wenn ihr diese bekannt ist, und unterrichtet die antragstellende Person hierüber. Anstelle der Weiterleitung des Antrags kann sie die antragstellende Person auch auf andere ihr bekannte informationspflichtige Stellen hinweisen, die über die Informationen verfügen.

(4) Wird eine andere als die beantragte Art des Informationszugangs im Sinne von § 3 Absatz 2 eröffnet, ist dies innerhalb der Frist nach § 3 Absatz 3 Satz 2 Nummer 1 unter Angabe der Gründe mitzuteilen.

(5) Über die Geltung der längeren Frist nach § 3 Absatz 3 Satz 2 Nummer 2 ist die antragstellende Person spätestens mit Ablauf der Frist nach § 3 Absatz 3 Satz 2 Nummer 1 unter Angabe der Gründe zu unterrichten.

§ 5 Ablehnung des Antrags

(1) Wird der Antrag ganz oder teilweise nach den §§ 8 und 9 abgelehnt, ist die antragstellende Person innerhalb der Fristen nach § 3 Absatz 3 Satz 2 hierüber zu unterrichten. Eine Ablehnung liegt auch dann vor, wenn nach § 3 Absatz 2 der Informationszugang auf andere Art gewährt oder die antragstellende Person auf eine andere Art des Informationszugangs verwiesen wird. Der antragstellenden Person sind die Gründe für die Ablehnung mitzutei-

len; in den Fällen des § 8 Absatz 2 Nummer 4 ist darüber hinaus die Stelle, die das Material vorbereitet, sowie der voraussichtliche Zeitpunkt der Fertigstellung mitzuteilen. § 39 Absatz 2 des Verwaltungsverfahrensgesetzes findet keine Anwendung.

(2) Wenn der Antrag schriftlich gestellt wurde oder die antragstellende Person dies begehrt, erfolgt die Ablehnung in schriftlicher Form. Sie ist auf Verlangen der antragstellenden Person in elektronischer Form mitzuteilen, wenn der Zugang hierfür eröffnet ist.

(3) Liegt ein Ablehnungsgrund nach § 8 oder § 9 vor, sind die hiervon nicht betroffenen Informationen zugänglich zu machen, soweit es möglich ist, die betroffenen Informationen auszusondern.

(4) Die antragstellende Person ist im Falle der vollständigen oder teilweisen Ablehnung eines Antrags auch über die Rechtsschutzmöglichkeiten gegen die Entscheidung sowie darüber zu belehren, bei welcher Stelle und innerhalb welcher Frist um Rechtsschutz nachgesucht werden kann.

§ 6 Rechtsschutz

(1) Für Streitigkeiten nach diesem Gesetz ist der Verwaltungsrechtsweg gegeben.

(2) Gegen die Entscheidung durch eine Stelle der öffentlichen Verwaltung im Sinne des § 2 Absatz 1 Nummer 1 ist ein Widerspruchsverfahren nach den §§ 68 bis 73 der Verwaltungsgerichtsordnung auch dann durchzuführen, wenn die Entscheidung von einer obersten Bundesbehörde getroffen worden ist.

(3) Ist die antragstellende Person der Auffassung, dass eine informationspflichtige Stelle im Sinne des § 2 Absatz 1 Nummer 2 den Antrag nicht vollständig erfüllt hat, kann sie die Entscheidung der informationspflichtigen Stelle nach Absatz 4 überprüfen lassen. Die Überprüfung ist nicht Voraussetzung für die Erhebung der Klage nach Absatz 1. Eine Klage gegen die zuständige Stelle nach § 13 Absatz 1 ist ausgeschlossen.

(4) Der Anspruch auf nochmalige Prüfung ist gegenüber der informationspflichtigen Stelle im Sinne des § 2 Absatz 1 Nummer 2 innerhalb eines Monats, nachdem diese Stelle mitgeteilt hat, dass der Anspruch nicht oder nicht vollständig erfüllt werden kann, schriftlich geltend zu machen. Die informationspflichtige Stelle hat der antragstellenden Person das Ergebnis ihrer nochmaligen Prüfung innerhalb eines Monats zu übermitteln.

(5) Durch Landesgesetz kann für Streitigkeiten um Ansprüche gegen private informationspflichtige Stellen auf Grund von landesrechtlichen Vorschriften über den Zugang zu Umweltinformationen der Verwaltungsrechtsweg vorgesehen werden.

§ 7 Unterstützung des Zugangs zu Umweltinformationen

(1) Die informationspflichtigen Stellen ergreifen Maßnahmen, um den Zugang zu den bei ihnen verfügbaren Umweltinformationen zu erleichtern. Zu diesem Zweck wirken sie darauf hin, dass Umweltinformationen, über die sie verfügen, zunehmend in elektronischen Datenbanken oder in sonstigen Formaten gespeichert werden, die über Mittel der elektronischen Kommunikation abrufbar sind.

(2) Die informationspflichtigen Stellen treffen praktische Vorkehrungen zur Erleichterung des Informationszugangs, beispielsweise durch

1. die Benennung von Auskunftspersonen oder Informationsstellen,

2. die Veröffentlichung von Verzeichnissen über verfügbare Umweltinformationen,
3. die Einrichtung öffentlich zugänglicher Informationsnetze und Datenbanken oder
4. die Veröffentlichung von Informationen über behördliche Zuständigkeiten.

(3) Soweit möglich, gewährleisten die informationspflichtigen Stellen, dass alle Umweltinformationen, die von ihnen oder für sie zusammengestellt werden, auf dem gegenwärtigen Stand, exakt und vergleichbar sind.

§ 7a Bundesbeauftragte für die Informationsfreiheit

§ 12 des Informationsfreiheitsgesetzes findet auf Anträge auf Zugang zu Umweltinformationen nach § 3 entsprechende Anwendung.

Abschnitt 3
Ablehnungsgründe

§ 8 Schutz öffentlicher Belange

(1) Soweit das Bekanntgeben der Informationen nachteilige Auswirkungen hätte auf

1. die internationalen Beziehungen, die Verteidigung oder bedeutsame Schutzgüter der öffentlichen Sicherheit,
2. die Vertraulichkeit der Beratungen von informationspflichtigen Stellen im Sinne des § 2 Absatz 1,
3. die Durchführung eines laufenden Gerichtsverfahrens, den Anspruch einer Person auf ein faires Verfahren oder die Durchführung strafrechtlicher, ordnungswidrigkeitenrechtlicher oder disziplinarrechtlicher Ermittlungen oder
4. den Zustand der Umwelt und ihrer Bestandteile im Sinne des § 2 Absatz 3 Nummer 1 oder Schutzgüter im Sinne des § 2 Absatz 3 Nummer 6,

ist der Antrag abzulehnen, es sei denn, das öffentliche Interesse an der Bekanntgabe überwiegt. Der Zugang zu Umweltinformationen über Emissionen kann nicht unter Berufung auf die in den Nummern 2 und 4 genannten Gründe abgelehnt werden.

(2) Soweit ein Antrag

1. offensichtlich missbräuchlich gestellt wurde,
2. sich auf interne Mitteilungen der informationspflichtigen Stellen im Sinne des § 2 Absatz 1 bezieht,
3. bei einer Stelle, die nicht über die Umweltinformationen verfügt, gestellt wird, sofern er nicht nach § 4 Absatz 3 weitergeleitet werden kann,
4. sich auf die Zugänglichmachung von Material, das gerade vervollständigt wird, noch nicht abgeschlossener Schriftstücke oder noch nicht aufbereiteter Daten bezieht oder
5. zu unbestimmt ist und auf Aufforderung der informationspflichtigen Stelle nach § 4 Absatz 2 nicht innerhalb einer angemessenen Frist präzisiert wird,

ist er abzulehnen, es sei denn, das öffentliche Interesse an der Bekanntgabe überwiegt.

§ 9 Schutz sonstiger Belange

(1) Soweit

1. durch das Bekanntgeben der Informationen personenbezogene Daten offenbart und dadurch Interessen der Betroffenen erheblich beeinträchtigt würden,
2. Rechte am geistigen Eigentum, insbesondere Urheberrechte, durch das Zugänglichmachen von Umweltinformationen verletzt würden oder
3. durch das Bekanntgeben Betriebs- oder Geschäftsgeheimnisse zugänglich gemacht würden oder die Informationen dem Steuergeheimnis oder dem Statistikgeheimnis unterliegen,

ist der Antrag abzulehnen, es sei denn, die Betroffenen haben zugestimmt oder das öffentliche Interesse an der Bekanntgabe überwiegt. Der Zugang zu Umweltinformationen über Emissionen kann nicht unter Berufung auf die in den Nummern 1 und 3 genannten Gründe abgelehnt werden. Vor der Entscheidung über die Offenbarung der durch Satz 1 Nummer 1 bis 3 geschützten Informationen sind die Betroffenen anzuhören. Die informationspflichtige Stelle hat in der Regel von einer Betroffenheit im Sinne des Satzes 1 Nummer 3 auszugehen, soweit übermittelte Informationen als Betriebs- und Geschäftsgeheimnisse gekennzeichnet sind. Soweit die informationspflichtige Stelle dies verlangt, haben mögliche Betroffene im Einzelnen darzulegen, dass ein Betriebs- oder Geschäftsgeheimnis vorliegt.

(2) Umweltinformationen, die private Dritte einer informationspflichtigen Stelle übermittelt haben, ohne rechtlich dazu verpflichtet zu sein oder rechtlich verpflichtet werden zu können, und deren Offenbarung nachteilige Auswirkungen auf die Interessen der Dritten hätte, dürfen ohne deren Einwilligung anderen nicht zugänglich gemacht werden, es sei denn, das öffentliche Interesse an der Bekanntgabe überwiegt. Der Zugang zu Umweltinformationen über Emissionen kann nicht unter Berufung auf die in Satz 1 genannten Gründe abgelehnt werden.

Abschnitt 4
Verbreitung von Umweltinformationen

§ 10 Unterrichtung der Öffentlichkeit

(1) Die informationspflichtigen Stellen unterrichten die Öffentlichkeit in angemessenem Umfang aktiv und systematisch über die Umwelt. In diesem Rahmen verbreiten sie Umweltinformationen, die für ihre Aufgaben von Bedeutung sind und über die sie verfügen.

(2) Zu den zu verbreitenden Umweltinformationen gehören zumindest:

1. der Wortlaut von völkerrechtlichen Verträgen, das von den Organen der Europäischen Gemeinschaften erlassene Gemeinschaftsrecht sowie Rechtsvorschriften von Bund, Ländern oder Kommunen über die Umwelt oder mit Bezug zur Umwelt;
2. politische Konzepte sowie Pläne und Programme mit Bezug zur Umwelt;
3. Berichte über den Stand der Umsetzung von Rechtsvorschriften sowie Konzepten, Plänen und Programmen nach den Nummern 1 und 2, sofern solche Berichte von

den jeweiligen informationspflichtigen Stellen in elektronischer Form ausgearbeitet worden sind oder bereitgehalten werden;

4. Daten oder Zusammenfassungen von Daten aus der Überwachung von Tätigkeiten, die sich auf die Umwelt auswirken oder wahrscheinlich auswirken;

5. Zulassungsentscheidungen, die erhebliche Auswirkungen auf die Umwelt haben, und Umweltvereinbarungen sowie

6. zusammenfassende Darstellung und Bewertung der Umweltauswirkungen nach den §§ 24 und 25 des Gesetzes über die Umweltverträglichkeitsprüfung in der Fassung der Bekanntmachung vom 24. Februar 2010 (BGBl. I S. 94) in der jeweils geltenden Fassung und Risikobewertungen im Hinblick auf Umweltbestandteile nach § 2 Absatz 3 Nummer 1.

In Fällen des Satzes 1 Nummer 5 und 6 genügt zur Verbreitung die Angabe, wo solche Informationen zugänglich sind oder gefunden werden können. Die veröffentlichten Umweltinformationen werden in angemessenen Abständen aktualisiert.

(3) Die Verbreitung von Umweltinformationen soll in für die Öffentlichkeit verständlicher Darstellung und leicht zugänglichen Formaten erfolgen. Hierzu sollen, soweit vorhanden, elektronische Kommunikationsmittel verwendet werden. Zur Verbreitung von Umweltinformationen nach Absatz 2 Satz 1 Nummer 5 und 6 auch in Verbindung mit Satz 2 kann das zentrale Internetportal des Bundes nach § 20 Absatz 1 Satz 1 des Gesetzes über die Umweltverträglichkeitsprüfung genutzt werden. Satz 2 gilt nicht für Umweltinformationen, die vor Inkrafttreten dieses Gesetzes angefallen sind, es sei denn, sie liegen bereits in elektronischer Form vor.

(4) Die Anforderungen an die Unterrichtung der Öffentlichkeit nach den Absätzen 1 und 2 können auch dadurch erfüllt werden, dass Verknüpfungen zu Internet-Seiten eingerichtet werden, auf denen die zu verbreitenden Umweltinformationen zu finden sind.

(5) Im Falle einer unmittelbaren Bedrohung der menschlichen Gesundheit oder der Umwelt haben die informationspflichtigen Stellen sämtliche Informationen, über die sie verfügen und die es der eventuell betroffenen Öffentlichkeit ermöglichen könnten, Maßnahmen zur Abwendung oder Begrenzung von Schäden infolge dieser Bedrohung zu ergreifen, unmittelbar und unverzüglich zu verbreiten; dies gilt unabhängig davon, ob diese Folge menschlicher Tätigkeit oder einer natürlichen Ursache ist. Verfügen mehrere informationspflichtige Stellen über solche Informationen, sollen sie sich bei deren Verbreitung abstimmen.

(6) § 7 Absatz 1 und 3 sowie die §§ 8 und 9 finden entsprechende Anwendung.

(7) Die Wahrnehmung der Aufgaben des § 10 kann auf bestimmte Stellen der öffentlichen Verwaltung oder private Stellen übertragen werden.

(8) Die Bundesregierung wird ermächtigt, durch Rechtsverordnung ohne Zustimmung des Bundesrates zu regeln:

1. die Art und Weise der Verbreitung von Umweltinformationen nach Absatz 2 Satz 1 Nummer 5 und 6 auch in Verbindung mit Satz 2 über das zentrale Internetportal des Bundes nach § 20 Absatz 1 Satz 1 des Gesetzes über die Umweltverträglichkeitsprüfung oder über andere elektronische Kommunikationswege sowie

2. die Einzelheiten der Aktualisierung von veröffentlichten Umweltinformationen gemäß Absatz 2 Satz 3, einschließlich des nachträglichen Wegfalls der Unterrichtungspflicht nach Absatz 1.

§ 11 Umweltzustandsbericht

Die Bundesregierung veröffentlicht regelmäßig im Abstand von nicht mehr als vier Jahren einen Bericht über den Zustand der Umwelt im Bundesgebiet. Hierbei berücksichtigt sie § 10 Absatz 1, 3 und 6. Der Bericht enthält Informationen über die Umweltqualität und vorhandene Umweltbelastungen. Der erste Bericht nach Inkrafttreten dieses Gesetzes ist spätestens am 31. Dezember 2006 zu veröffentlichen.

Abschnitt 5
Schlussvorschriften

§ 12 Gebühren und Auslagen

(1) Für die Übermittlung von Informationen auf Grund dieses Gesetzes werden Gebühren und Auslagen erhoben. Dies gilt nicht für die Erteilung mündlicher und einfacher schriftlicher Auskünfte, die Einsichtnahme in Umweltinformationen vor Ort, Maßnahmen und Vorkehrungen nach § 7 Absatz 1 und 2 sowie die Unterrichtung der Öffentlichkeit nach den §§ 10 und 11.

(2) Die Gebühren sind auch unter Berücksichtigung des Verwaltungsaufwandes so zu bemessen, dass der Informationsanspruch nach § 3 Absatz 1 wirksam in Anspruch genommen werden kann.

(3) Die Bundesregierung wird ermächtigt, für individuell zurechenbare öffentliche Leistungen von informationspflichtigen Stellen die Höhe der Gebühren und Auslagen durch Rechtsverordnung, die nicht der Zustimmung des Bundesrates bedarf, zu bestimmen. § 9 Absatz 1 und 2 sowie die §§ 10 und 12 des Bundesgebührengesetzes finden keine Anwendung.

(4) Private informationspflichtige Stellen im Sinne des § 2 Absatz 1 Nummer 2 können für die Übermittlung von Informationen nach diesem Gesetz von der antragstellenden Person Gebühren- und Auslagenerstattung entsprechend den Grundsätzen nach den Absätzen 1 und 2 verlangen. Die Höhe der erstattungsfähigen Gebühren und Auslagen bemisst sich nach den in der Rechtsverordnung nach Absatz 3 festgelegten Sätzen für individuell zurechenbare öffentliche Leistungen von informationspflichtigen Stellen des Bundes und der bundesunmittelbaren juristischen Personen des öffentlichen Rechts.

§ 13 Überwachung

(1) Die zuständigen Stellen der öffentlichen Verwaltung, die die Kontrolle im Sinne des § 2 Absatz 2 für den Bund oder eine unter der Aufsicht des Bundes stehende juristische Person des öffentlichen Rechts ausüben, überwachen die Einhaltung dieses Gesetzes durch private informationspflichtige Stellen im Sinne des § 2 Absatz 1 Nummer 2.

(2) Die informationspflichtigen Stellen nach § 2 Absatz 1 Nummer 2 haben den zuständigen Stellen auf Verlangen alle Informationen herauszugeben, die die Stellen zur Wahrnehmung ihrer Aufgaben nach Absatz 1 benötigen.

(3) Die nach Absatz 1 zuständigen Stellen können gegenüber den informationspflichtigen Stellen nach § 2 Absatz 1 Nummer 2 die zur Einhaltung und Durchführung dieses Gesetzes erforderlichen Maßnahmen ergreifen oder Anordnungen treffen.

(4) Die Bundesregierung wird ermächtigt, durch Rechtsverordnung, die nicht der Zustimmung des Bundesrates bedarf, die Aufgaben nach den Absätzen 1 bis 3 abweichend von Absatz 1 auf andere Stellen der öffentlichen Verwaltung zu übertragen.

§ 14 Ordnungswidrigkeiten

(1) Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig einer vollziehbaren Anordnung nach § 13 Absatz 3 zuwiderhandelt.

(2) Die Ordnungswidrigkeit nach Absatz 1 kann mit einer Geldbuße bis zu zehntausend Euro geahndet werden.

Gesetz zur Verbesserung der gesundheitsbezogenen Verbraucherinformation (Verbraucherinformationsgesetz – VIG)

§ 1 Anwendungsbereich

Durch dieses Gesetz erhalten Verbraucherinnen und Verbraucher freien Zugang zu den bei informationspflichtigen Stellen vorliegenden Informationen über

1. Erzeugnisse im Sinne des Lebensmittel- und Futtermittelgesetzbuches (Erzeugnisse) sowie
2. Verbraucherprodukte, die dem § 2 Nummer 25 des Produktsicherheitsgesetzes unterfallen (Verbraucherprodukte),

damit der Markt transparenter gestaltet und hierdurch der Schutz der Verbraucherinnen und Verbraucher vor gesundheitsschädlichen oder sonst unsicheren Erzeugnissen und Verbraucherprodukten sowie vor Täuschung beim Verkehr mit Erzeugnissen und Verbraucherprodukten verbessert wird.

§ 2 Anspruch auf Zugang zu Informationen

(1) Jeder hat nach Maßgabe dieses Gesetzes Anspruch auf freien Zugang zu allen Daten über

1. von den nach Bundes- oder Landesrecht zuständigen Stellen festgestellte nicht zulässige Abweichungen von Anforderungen
   a) des Lebensmittel- und Futtermittelgesetzbuches und des Produktsicherheitsgesetzes,
   b) der auf Grund dieser Gesetze erlassenen Rechtsverordnungen,
   c) unmittelbar geltender Rechtsakte der Europäischen Gemeinschaft oder der Europäischen Union im Anwendungsbereich der genannten Gesetze

   sowie Maßnahmen und Entscheidungen, die im Zusammenhang mit den in den Buchstaben a bis c genannten Abweichungen getroffen worden sind,
2. von einem Erzeugnis oder einem Verbraucherprodukt ausgehende Gefahren oder Risiken für Gesundheit und Sicherheit von Verbraucherinnen und Verbrauchern,
3. die Zusammensetzung von Erzeugnissen und Verbraucherprodukten, ihre Beschaffenheit, die physikalischen, chemischen und biologischen Eigenschaften einschließlich ihres Zusammenwirkens und ihrer Einwirkung auf den Körper, auch unter Berücksichtigung der bestimmungsgemäßen Verwendung oder vorhersehbaren Fehlanwendung,
4. die Kennzeichnung, die Herkunft, die Verwendung, das Herstellen und das Behandeln von Erzeugnissen und Verbraucherprodukten,
5. zugelassene Abweichungen von den in Nummer 1 genannten Rechtsvorschriften über die in den Nummern 3 und 4 genannten Merkmale oder Tätigkeiten,
6. die Ausgangsstoffe und die bei der Gewinnung der Ausgangsstoffe angewendeten Verfahren,

7. Überwachungsmaßnahmen oder andere behördliche Tätigkeiten oder Maßnahmen zum Schutz von Verbraucherinnen und Verbrauchern, einschließlich der Auswertung dieser Tätigkeiten und Maßnahmen, sowie Statistiken über Verstöße gegen in § 39 Absatz 1 Satz 1 des Lebensmittel- und Futtermittelgesetzbuches und § 8 des Marktüberwachungsgesetzes genannte Rechtsvorschriften, soweit sich die Verstöße auf Erzeugnisse oder Verbraucherprodukte beziehen,

(Informationen), die bei einer Stelle im Sinne des Absatzes 2 unabhängig von der Art ihrer Speicherung vorhanden sind. Der Anspruch nach Satz 1 besteht insoweit, als kein Ausschluss- oder Beschränkungsgrund nach § 3 vorliegt.

(2) Stelle im Sinne des Absatzes 1 Satz 1 ist

1. jede Behörde im Sinne des § 1 Absatz 4 des Verwaltungsverfahrensgesetzes, die auf Grund

   a) anderer bundesrechtlicher oder

   b) landesrechtlicher

   Vorschriften öffentlich-rechtliche Aufgaben oder Tätigkeiten wahrnimmt, die der Erfüllung der in § 1 des Lebensmittel- und Futtermittelgesetzbuches genannten Zwecke oder bei Verbraucherprodukten der Gewährleistung von Sicherheit und Gesundheit nach den Vorschriften des Produktsicherheitsgesetzes sowie der auf Grund des Produktsicherheitsgesetzes erlassenen Rechtsverordnungen dienen,

2. jede natürliche oder juristische Person des Privatrechts, die auf Grund

a) anderer bundesrechtlicher oder

b) landesrechtlicher

   Vorschriften öffentlich-rechtliche Aufgaben oder Tätigkeiten wahrnimmt, die der Erfüllung der in § 1 des Lebensmittel- und Futtermittelgesetzbuches genannten Zwecke oder bei Verbraucherprodukten der Gewährleistung von Sicherheit und Gesundheit nach den Vorschriften des Produktsicherheitsgesetzes sowie der auf Grund des Produktsicherheitsgesetzes erlassenen Rechtsverordnungen dienen und der Aufsicht einer Behörde unterstellt ist.

Satz 1 gilt im Fall einer Gemeinde oder eines Gemeindeverbandes nur, wenn der Gemeinde oder dem Gemeindeverband die Aufgaben nach diesem Gesetz durch Landesrecht übertragen worden sind.

(3) Zu den Stellen im Sinne des Absatzes 2 Satz 1 gehören nicht die obersten Bundes- und Landesbehörden, soweit sie im Rahmen der Gesetzgebung oder beim Erlass von Rechtsverordnungen tätig werden, unabhängige Organe der Finanzkontrolle sowie Gerichte, Justizvollzugsbehörden, Strafverfolgungs- und Disziplinarbehörden und diesen vorgesetzte Dienststellen.

(4) Die Vorschriften dieses Gesetzes gelten nicht, soweit in anderen Rechtsvorschriften entsprechende oder weitergehende Vorschriften vorgesehen sind.

§ 3 Ausschluss- und Beschränkungsgründe

Der Anspruch nach § 2 besteht wegen

1. entgegenstehender öffentlicher Belange nicht,
   a) soweit das Bekanntwerden der Informationen
      aa) nachteilige Auswirkungen haben kann auf internationale Beziehungen oder militärische und sonstige sicherheitsempfindliche Belange der Bundeswehr oder
      bb) die Vertraulichkeit der Beratung von Behörden berührt oder eine erhebliche Gefahr für die öffentliche Sicherheit verursachen kann;
   b) während der Dauer eines Verwaltungsverfahrens, eines Gerichtsverfahrens, eines strafrechtlichen Ermittlungsverfahrens, eines Disziplinarverfahrens, eines Gnadenverfahrens oder eines ordnungswidrigkeitsrechtlichen Verfahrens hinsichtlich der Informationen, die Gegenstand des Verfahrens sind, es sei denn, es handelt sich um Informationen nach § 2 Absatz 1 Satz 1 Nummer 1 oder 2 oder das öffentliche Interesse an der Bekanntgabe überwiegt;
   c) soweit das Bekanntwerden der Information geeignet ist, fiskalische Interessen der um Auskunft ersuchten Stelle im Wirtschaftsverkehr zu beeinträchtigen, oder Dienstgeheimnisse verletzt werden könnten;
   d) soweit Informationen betroffen sind, die im Rahmen einer Dienstleistung entstanden sind, die die Stelle auf Grund einer privatrechtlichen Vereinbarung außerhalb des ihr gesetzlich zugewiesenen Aufgabenbereichs des Verbraucherschutzes erbracht hat;
   e) in der Regel bei Informationen nach § 2 Absatz 1 Satz 1 Nummer 1, die vor mehr als fünf Jahren seit der Antragstellung entstanden sind;
2. entgegenstehender privater Belange nicht, soweit
   b) Zugang zu personenbezogenen Daten beantragt wird,
   c) der Schutz des geistigen Eigentums, insbesondere Urheberrechte, dem Informationsanspruch entgegensteht,
   d) durch die begehrten Informationen Betriebs- oder Geschäftsgeheimnisse, insbesondere Rezepturen, Konstruktions- oder Produktionsunterlagen, Informationen über Fertigungsverfahren, Forschungs- und Entwicklungsvorhaben sowie sonstiges geheimnisgeschütztes technisches oder kaufmännisches Wissen, offenbart würden oder
   e) Zugang zu Informationen beantragt wird, die einer Stelle auf Grund einer durch Rechtsvorschrift angeordneten Pflicht zur Meldung oder Unterrichtung mitgeteilt worden sind; dies gilt auch, wenn das meldende oder unterrichtende Unternehmen irrig angenommen hat, zur Meldung oder Unterrichtung verpflichtet zu sein.

Satz 1 Nummer 2 Buchstabe a bis c gilt nicht, wenn die Betroffenen dem Informationszugang zugestimmt haben oder das öffentliche Interesse an der Bekanntgabe überwiegt. Im Fall des Satzes 1 Nummer 1 Buchstabe b zweiter Halbsatz dürfen Informationen nach § 2 Absatz 1 Satz 1 Nummer 1 während eines laufenden strafrechtlichen Ermittlungsverfahrens oder eines Verfahrens vor einem Strafgericht nur

1. soweit und solange hierdurch der mit dem Verfahren verfolgte Untersuchungszweck nicht gefährdet wird und
2. im Benehmen mit der zuständigen Staatsanwaltschaft oder dem zuständigen Gericht

herausgegeben werden. Im Fall des Satzes 1 Nummer 2 Buchstabe a gilt § 5 Absatz 1 Satz 2 und Absatz 3 und 4 des Informationsfreiheitsgesetzes entsprechend. Der Zugang zu folgenden Informationen kann nicht unter Berufung auf das Betriebs- und Geschäftsgeheimnis abgelehnt werden:

1. Informationen nach § 2 Absatz 1 Satz 1 Nummer 1 und 2,
2. Informationen nach § 2 Absatz 1 Satz 1 Nummer 3 und 4, soweit im Einzelfall hinreichende Anhaltspunkte dafür vorliegen, dass von dem jeweiligen Erzeugnis oder Verbraucherprodukt eine Gefährdung oder ein Risiko für Sicherheit und Gesundheit ausgeht und auf Grund unzureichender wissenschaftlicher Erkenntnis oder aus sonstigen Gründen die Ungewissheit nicht innerhalb der gebotenen Zeit behoben werden kann, und
3. Informationen nach § 2 Absatz 1 Satz 1 Nummer 3 bis 6, soweit sie im Rahmen der amtlichen Überwachungstätigkeit nach den in § 2 Absatz 1 Satz 1 Nummer 1 genannten Vorschriften gewonnen wurden und die Einhaltung der Grenzwerte, Höchstgehalte oder Höchstmengen betreffen, die in den in § 2 Absatz 1 Satz 1 Nummer 1 genannten Vorschriften enthalten sind.

Gleiches gilt für den Namen des Händlers, der das Erzeugnis oder Verbraucherprodukt an Verbraucher abgibt, sowie für die Handelsbezeichnung, eine aussagekräftige Beschreibung und bildliche Darstellung des Erzeugnisses oder Verbraucherproduktes und in den Fällen des § 2 Absatz 1 Satz 1 Nummer 1 zusätzlich für den Namen und die Anschrift des Herstellers, Bevollmächtigten, Einführers, Händlers sowie jedes Gliedes der Liefer- und Vertriebskette; Satz 1 Nummer 2 Buchstabe a ist nicht anzuwenden.

§ 4 Antrag

(1) Die Information wird auf Antrag erteilt. Der Antrag muss hinreichend bestimmt sein und insbesondere erkennen lassen, auf welche Informationen er gerichtet ist. Ferner soll der Antrag den Namen und die Anschrift des Antragstellers enthalten. Zuständig ist

1. soweit Zugang zu Informationen bei einer Stelle des Bundes beantragt wird, diese Stelle,
2. im Übrigen die nach Landesrecht zuständige Stelle.

Abweichend von Satz 4 Nummer 1 ist im Fall einer natürlichen oder juristischen Person des Privatrechts für die Bescheidung des Antrags die Aufsicht führende Behörde zuständig.

(2) Informationspflichtig ist jeweils die nach Maßgabe des Absatzes 1 Satz 4 auch in Verbindung mit Satz 5 zuständige Stelle. Diese ist nicht dazu verpflichtet, Informationen, die bei ihr nicht vorhanden sind oder auf Grund von Rechtsvorschriften nicht verfügbar gehalten werden müssen, zu beschaffen.

(3) Der Antrag soll abgelehnt werden,

1. soweit er sich auf Entwürfe zu Entscheidungen sowie Arbeiten und Beschlüsse zu ihrer unmittelbaren Vorbereitung bezieht, es sei denn, es handelt sich um die Ergebnisse einer Beweiserhebung, ein Gutachten oder eine Stellungnahme von Dritten,
2. bei vertraulich übermittelten oder erhobenen Informationen oder
3. wenn durch das vorzeitige Bekanntwerden der Erfolg bevorstehender behördlicher Maßnahmen gefährdet würde,
4. soweit durch die Bearbeitung des Antrags die ordnungsgemäße Erfüllung der Aufgaben der Behörde beeinträchtigt würde,
5. bei wissenschaftlichen Forschungsvorhaben einschließlich der im Rahmen eines Forschungsvorhabens erhobenen und noch nicht abschließend ausgewerteten Daten, bis diese Vorhaben wissenschaftlich publiziert werden.

(4) Ein missbräuchlich gestellter Antrag ist abzulehnen. Dies ist insbesondere der Fall, wenn der Antragsteller über die begehrten Informationen bereits verfügt.

(5) Wenn der Antragsteller sich die begehrten Informationen in zumutbarer Weise aus allgemein zugänglichen Quellen beschaffen kann, kann der Antrag abgelehnt und der Antragsteller auf diese Quellen hingewiesen werden. Die Voraussetzungen nach Satz 1 sind insbesondere dann erfüllt, wenn die Stelle den Informationszugang bereits nach § 6 Absatz 1 Satz 3 gewährt. Satz 1 gilt entsprechend, soweit sich in den Fällen des § 2 Absatz 1 Satz 1 Nummer 2 bis 6 eine der in § 3 Satz 6 genannten Personen im Rahmen einer nach den Vorschriften des Verwaltungsverfahrensgesetzes oder den entsprechenden Vorschriften der Verwaltungsverfahrensgesetze der Länder durchgeführten Anhörung verpflichtet, die begehrte Information selbst zu erteilen, es sei denn, der Antragsteller hat nach § 6 Absatz 1 Satz 2 ausdrücklich um eine behördliche Auskunftserteilung gebeten oder es bestehen Anhaltspunkte dafür, dass die Information durch die Person nicht, nicht rechtzeitig oder nicht vollständig erfolgen wird.

§ 5 Entscheidung über den Antrag

(1) Das Verfahren einschließlich der Beteiligung Dritter, deren rechtliche Interessen durch den Ausgang des Verfahrens berührt werden können, richtet sich nach dem Verwaltungsverfahrensgesetz oder den Verwaltungsverfahrensgesetzen der Länder. Für die Anhörung gelten § 28 des Verwaltungsverfahrensgesetzes oder die entsprechenden Vorschriften der Verwaltungsverfahrensgesetze der Länder mit der Maßgabe, dass von einer Anhörung auch abgesehen werden kann

1. bei der Weitergabe von Informationen im Sinne des § 2 Absatz 1 Satz 1 Nummer 1,
2. in Fällen, in denen dem oder der Dritten die Erhebung der Information durch die Stelle bekannt ist und er oder sie in der Vergangenheit bereits Gelegenheit hatte, zur Weitergabe derselben Information Stellung zu nehmen, insbesondere wenn bei gleichartigen Anträgen auf Informationszugang eine Anhörung zu derselben Information bereits durchgeführt worden ist.

Bei gleichförmigen Anträgen von mehr als 20 Personen gelten die §§ 17 und 19 des Verwaltungsverfahrensgesetzes entsprechend.

(2) Der Antrag ist in der Regel innerhalb von einem Monat zu bescheiden. Im Fall einer Beteiligung Dritter verlängert sich die Frist auf zwei Monate; der Antragsteller ist hierüber zu unterrichten. Die Entscheidung über den Antrag ist auch der oder dem Dritten bekannt zu geben. Auf Nachfrage des Dritten legt die Stelle diesem Namen und Anschrift des Antragstellers offen.

(3) Wird dem Antrag stattgegeben, sind Ort, Zeit und Art des Informationszugangs mitzuteilen. Wird der Antrag vollständig oder teilweise abgelehnt, ist mitzuteilen, ob und gegebenenfalls wann die Informationen ganz oder teilweise zu einem späteren Zeitpunkt zugänglich sind.

(4) Widerspruch und Anfechtungsklage haben in den in § 2 Absatz 1 Satz 1 Nummer 1 genannten Fällen keine aufschiebende Wirkung. Auch wenn von der Anhörung Dritter nach Absatz 1 abgesehen wird, darf der Informationszugang erst erfolgen, wenn die Entscheidung dem oder der Dritten bekannt gegeben worden ist und diesem ein ausreichender Zeitraum zur Einlegung von Rechtsbehelfen eingeräumt worden ist. Der Zeitraum nach Satz 2 soll 14 Tage nicht überschreiten.

(5) Ein Vorverfahren findet abweichend von § 68 der Verwaltungsgerichtsordnung auch dann statt, wenn die Entscheidung von einer obersten Bundesbehörde erlassen worden ist. Widerspruchsbehörde ist die oberste Bundesbehörde.

§ 6 Informationsgewährung

(1) Die informationspflichtige Stelle kann den Informationszugang durch Auskunftserteilung, Gewährung von Akteneinsicht oder in sonstiger Weise eröffnen. Wird eine bestimmte Art des Informationszugangs begehrt, so darf dieser nur aus wichtigem Grund auf andere Art gewährt werden. Die informationspflichtige Stelle kann Informationen, zu denen Zugang zu gewähren ist, auch unabhängig von einem Antrag nach § 4 Absatz 1 über das Internet oder in sonstiger öffentlich zugänglicher Weise zugänglich machen; § 5 Absatz 1 gilt entsprechend. Die Informationen sollen für die Verbraucherinnen und Verbraucher verständlich dargestellt werden.

(2) Soweit der informationspflichtigen Stelle keine Erkenntnisse über im Antrag nach § 4 Absatz 1 begehrte Informationen vorliegen, leitet sie den Antrag, soweit ihr dies bekannt und möglich ist, von Amts wegen an die Stelle weiter, der die Informationen vorliegen, und unterrichtet den Antragsteller über die Weiterleitung.

(3) Die informationspflichtige Stelle ist nicht verpflichtet, die inhaltliche Richtigkeit der Informationen zu überprüfen, soweit es sich nicht um personenbezogene Daten handelt. Der informationspflichtigen Stelle bekannte Hinweise auf Zweifel an der Richtigkeit sind mitzuteilen.

(4) Stellen sich die von der informationspflichtigen Stelle zugänglich gemachten Informationen im Nachhinein als falsch oder die zugrunde liegenden Umstände als unrichtig wiedergegeben heraus, so ist dies unverzüglich richtig zu stellen, sofern der oder die Dritte dies beantragt oder dies zur Wahrung erheblicher Belange des Gemeinwohls erforderlich ist. Die Richtigstellung soll in derselben Weise erfolgen, in der die Information zugänglich gemacht wurde.

§ 7 Gebühren und Auslagen

(1) Für individuell zurechenbare öffentliche Leistungen der Behörden nach diesem Gesetz werden vorbehaltlich des Satzes 2 kostendeckende Gebühren und Auslagen erhoben. Der Zugang zu Informationen nach § 2 Absatz 1 Satz 1 Nummer 1 ist bis zu einem Verwaltungsaufwand von 1 000 Euro gebühren- und auslagenfrei, der Zugang zu sonstigen Informationen bis zu einem Verwaltungsaufwand von 250 Euro. Sofern der Antrag nicht gebühren- und auslagenfrei bearbeitet wird, ist der Antragsteller über die voraussichtliche Höhe der Gebühren und Auslagen vorab zu informieren. Er ist auf die Möglichkeit hinzuweisen, seinen Antrag zurücknehmen oder einschränken zu können.

(2) Die Bundesregierung wird ermächtigt, durch Rechtsverordnung ohne Zustimmung des Bundesrates die gebührenpflichtigen Tatbestände und die Gebührenhöhe zu bestimmen, soweit dieses Gesetz durch Stellen des Bundes ausgeführt wird. § 15 Absatz 2 des Verwaltungskostengesetzes vom 23. Juni 1970 (BGBl. I S. 821) in der am 14. August 2013 geltenden Fassung findet keine Anwendung.

Gesetz über den Zugang zu digitalen Geodaten (Geodatenzugangsgesetz - GeoZG)

Abschnitt 1
Ziel und Anwendungsbereich

§ 1 Ziel des Gesetzes

Dieses Gesetz dient dem Aufbau einer nationalen Geodateninfrastruktur. Es schafft den rechtlichen Rahmen für

1. den Zugang zu Geodaten, Geodatendiensten und Metadaten von geodatenhaltenden Stellen sowie
2. die Nutzung dieser Daten und Dienste, insbesondere für Maßnahmen, die Auswirkungen auf die Umwelt haben können.

§ 2 Anwendungsbereich

(1) Dieses Gesetz gilt für geodatenhaltende Stellen des Bundes und der bundesunmittelbaren juristischen Personen des öffentlichen Rechts.

(2) Natürliche und juristische Personen des Privatrechts können Geodaten und Metadaten über das Geoportal nach § 9 Absatz 2 bereitstellen, wenn sie sich verpflichten, diese Daten nach den Bestimmungen dieses Gesetzes bereitzustellen und hierfür die technischen Voraussetzungen zu schaffen.

(3) Dieses Gesetz gilt auch für Geodatendienste, die sich auf Daten beziehen, die in den Geodaten enthalten sind, auf die dieses Gesetz Anwendung findet.

(4) Dieses Gesetz gilt nach Maßgabe des Seerechtsübereinkommens der Vereinten Nationen vom 10. Dezember 1982 (BGBl. 1994 II S. 1798; 1995 II S. 602) auch im Bereich der ausschließlichen Wirtschaftszone und des Festlandsockels.

Abschnitt 2
Begriffsbestimmungen

§ 3 Allgemeine Begriffe

(1) Geodaten sind alle Daten mit direktem oder indirektem Bezug zu einem bestimmten Standort oder geografischen Gebiet.

(2) Metadaten sind Informationen, die Geodaten oder Geodatendienste beschreiben und es ermöglichen, Geodaten und Geodatendienste zu ermitteln, in Verzeichnisse aufzunehmen und zu nutzen.

(3) Geodatendienste sind vernetzbare Anwendungen, welche Geodaten und Metadaten in strukturierter Form zugänglich machen. Dies sind im Einzelnen:

1. Suchdienste, die es ermöglichen, auf der Grundlage des Inhalts entsprechender Metadaten nach Geodaten und Geodatendiensten zu suchen und den Inhalt der Metadaten anzuzeigen,

2. Darstellungsdienste, die es zumindest ermöglichen, darstellbare Geodaten anzuzeigen, in ihnen zu navigieren, sie zu vergrößern oder zu verkleinern, zu verschieben, Daten zu überlagern sowie Informationen aus Legenden und sonstige relevante Inhalte von Metadaten anzuzeigen,
3. Dienste, die das Herunterladen und, wenn durchführbar, den direkten Zugriff auf Kopien von Geodaten ermöglichen (Downloaddienste),
4. Transformationsdienste zur geodätischen Umwandlung von Geodaten.

(4) Interoperabilität ist die Kombinierbarkeit von Daten beziehungsweise die Kombinierbarkeit und Interaktionsfähigkeit verschiedener Systeme und Techniken unter Einhaltung gemeinsamer Standards.

(5) Geodateninfrastruktur ist eine Infrastruktur bestehend aus Geodaten, Metadaten und Geodatendiensten, Netzdiensten und -technologien, Vereinbarungen über gemeinsame Nutzung, über Zugang und Verwendung sowie Koordinierungs- und Überwachungsmechanismen, -prozesse und -verfahren mit dem Ziel, Geodaten verschiedener Herkunft interoperabel verfügbar zu machen.

(6) Geoportal ist eine elektronische Kommunikations-, Transaktions- und Interaktionsplattform, die über Geodatendienste und weitere Netzdienste den Zugang zu den Geodaten ermöglicht.

(7) Netzdienste sind netzbasierte Anwendungen zur Kommunikation, Transaktion und Interaktion.

(8) Geodatenhaltende Stellen im Sinne dieses Gesetzes sind die informationspflichtigen Stellen im Sinne von § 2 Absatz 1 des Umweltinformationsgesetzes vom 22. Dezember 2004 (BGBl. I S. 3704).

§ 4 Betroffene Geodaten und Geodatendienste

(1) Dieses Gesetz gilt für Geodaten, die noch in Verwendung stehen und die folgenden Bedingungen erfüllen:

1. Sie beziehen sich auf das Hoheitsgebiet der Bundesrepublik Deutschland oder auf die ausschließliche Wirtschaftszone der Bundesrepublik Deutschland gemäß Seerechtsübereinkommen der Vereinten Nationen;
2. sie liegen in elektronischer Form vor;
3. sie sind vorhanden bei
   a) einer geodatenhaltenden Stelle, fallen unter ihren öffentlichen Auftrag und
      aa) wurden von einer geodatenhaltenden Stelle erstellt oder
      bb) sind bei einer solchen eingegangen oder
      cc) werden von dieser geodatenhaltenden Stelle verwaltet oder aktualisiert,
   b) Dritten, denen nach § 2 Absatz 2 Anschluss an die nationale Geodateninfrastruktur gewährt wird,

   oder werden für diese bereitgehalten;

4. sie betreffen eines oder mehrere der folgenden Themen:

   a) Koordinatenreferenzsysteme (Systeme zur eindeutigen räumlichen Referenzierung von Geodaten anhand eines Koordinatensatzes (x, y, z) oder Angaben zu Breite, Länge und Höhe auf der Grundlage eines geodätischen horizontalen und vertikalen Datums),

   b) geografische Gittersysteme (harmonisiertes Gittersystem mit Mehrfachauflösung, gemeinsamem Ursprungspunkt und standardisierter Lokalisierung und Größe der Gitterzellen),

   c) geografische Bezeichnungen (Namen von Gebieten, Regionen, Orten, Großstädten, Vororten, Städten oder Siedlungen sowie jedes geografische oder topografische Merkmal von öffentlichem oder historischem Interesse),

   d) Verwaltungseinheiten (lokale, regionale und nationale Verwaltungseinheiten, die die Gebiete abgrenzen, in denen die Bundesrepublik Deutschland Hoheitsbefugnisse hat oder ausübt und die durch Verwaltungsgrenzen voneinander getrennt sind),

   e) Adressen (Lokalisierung von Grundstücken anhand von Adressdaten, in der Regel Straßenname, Hausnummer und Postleitzahl),

   f) Flurstücke oder Grundstücke (Gebiete, die anhand des Grundbuchs oder gleichwertiger Verzeichnisse bestimmt werden),

   g) Verkehrsnetze (Verkehrsnetze und zugehörige Infrastruktureinrichtungen für Straßen-, Schienen- und Luftverkehr sowie Schifffahrt; dies umfasst auch die Verbindungen zwischen den verschiedenen Netzen und das transeuropäische Verkehrsnetz im Sinne der Entscheidung Nr. 1692/96/EG des Europäischen Parlaments und des Rates vom 23. Juli 1996 über gemeinschaftliche Leitlinien für den Aufbau eines transeuropäischen Verkehrsnetzes (ABl. L 228 vom 9.9.1996, S. 1), zuletzt geändert durch die Verordnung (EG) Nr. 1791/2006 des Rates (ABl. L 363 vom 20.12.2006, S. 1), und künftige Überarbeitungen dieser Entscheidung),

   h) Gewässernetz (Elemente des Gewässernetzes, einschließlich Meeresgebiete und aller sonstigen Wasserkörper und hiermit verbundener Teilsysteme, darunter Einzugsgebiete und Teileinzugsgebiete; gegebenenfalls gemäß den Definitionen der Richtlinie 2000/60/EG des Europäischen Parlaments und des Rates vom 23. Oktober 2000 zur Schaffung eines Ordnungsrahmens für Maßnahmen der Gemeinschaft im Bereich der Wasserpolitik (ABl. L 327 vom 22.12.2000, S. 1), die zuletzt durch die Richtlinie 2009/31/EG (ABl. L 140 vom 5.6.2009, S. 114) geändert worden ist, und in Form von Netzen),

   i) Schutzgebiete (Gebiete, die im Rahmen des internationalen und des gemeinschaftlichen Rechts der Mitgliedstaaten ausgewiesen sind oder verwaltet werden, um spezifische Erhaltungsziele zu erreichen),

   j) Höhe (digitale Höhenmodelle für Land-, Eis- und Wasserflächen inklusive Tiefenmessung bei Gewässern und Mächtigkeit bei Eisflächen, sowie Uferlinien; (Geländemodelle)),

k) Bodenbedeckung (physische und biologische Bedeckung der Erdoberfläche, einschließlich künstlicher Flächen, landwirtschaftlicher Flächen, Wälder, natürlicher (naturnaher) Gebiete, Feuchtgebiete und Wasserkörper),

l) Orthofotografie (georeferenzierte Bilddaten der Erdoberfläche von satelliten- oder luftfahrzeuggestützten Sensoren),

m) Geologie (geologische Beschreibung anhand von Zusammensetzung und Struktur des Untergrundes; dies umfasst auch Grundgebirgs- und Sedimentgesteine, Lockersedimente, Grundwasserleiter und -stauer, Störungen, Geomorphologie und anderes),

n) statistische Einheiten (Einheiten für die Verbreitung oder Verwendung statistischer Daten),

o) Gebäude (geografischer Standort von Gebäuden),

p) Boden (Beschreibung von Boden und Unterboden anhand von Tiefe, Textur, Struktur und Gehalt an Teilchen sowie organischem Material, Steinigkeit, Erosion, gegebenenfalls durchschnittliches Gefälle und erwartete Wasserspeicherkapazität),

q) Bodennutzung (Beschreibung von Gebieten anhand ihrer derzeitigen und geplanten künftigen Funktion oder ihres sozioökonomischen Zwecks wie zum Beispiel Wohn-, Industrie- oder Gewerbegebiete, land- oder forstwirtschaftliche Flächen, Freizeitgebiete),

r) Gesundheit und Sicherheit (geografische Verteilung verstärkt auftretender pathologischer Befunde (zum Beispiel Allergien, Krebserkrankungen, Erkrankungen der Atemwege), Informationen über Auswirkungen auf die Gesundheit (zum Beispiel Biomarker, Rückgang der Fruchtbarkeit, Epidemien) oder auf das Wohlbefinden (zum Beispiel Ermüdung, Stress) der Menschen in unmittelbarem Zusammenhang mit der Umweltqualität (zum Beispiel Luftverschmutzung, Chemikalien, Abbau der Ozonschicht, Lärm) oder in mittelbarem Zusammenhang mit der Umweltqualität (zum Beispiel Nahrung, genetisch veränderte Organismen)),

s) Versorgungswirtschaft und staatliche Dienste (Versorgungseinrichtungen wie Abwasser- und Abfallentsorgung, Energieversorgung und Wasserversorgung; staatliche Verwaltungs- und Sozialdienste wie öffentliche Verwaltung, Katastrophenschutz, Schulen und Krankenhäuser),

t) Umweltüberwachung (Standort und Betrieb von Umweltüberwachungseinrichtungen einschließlich Beobachtung und Messung von Schadstoffen, des Zustands von Umweltmedien und anderen Parametern des Ökosystems wie zum Beispiel Artenvielfalt, ökologischer Zustand der Vegetation durch oder im Auftrag von öffentlichen Behörden),

u) Produktions- und Industrieanlagen (Standorte für industrielle Produktion, einschließlich durch die Richtlinie 2010/75/EU des Europäischen Parlaments und des Rates vom 24. November 2010 über Industrieemissionen (integrierte Vermeidung und Verminderung der Umweltverschmutzung) (Neufassung) (ABl. L 334 vom 17.12.2010, S. 17) erfasste Anlagen und Einrichtungen zur Wasserentnahme sowie Bergbau- und Lagerstandorte),

v) landwirtschaftliche Anlagen und Aquakulturanlagen (landwirtschaftliche Anlagen und Produktionsstätten einschließlich Bewässerungssysteme, Gewächshäuser und Ställe),

w) Verteilung der Bevölkerung – Demografie (geografische Verteilung der Bevölkerung, einschließlich Bevölkerungsmerkmale und Tätigkeitsebenen, zusammengefasst nach Gitter, Region, Verwaltungseinheit oder sonstigen analytischen Einheiten),

x) Bewirtschaftungsgebiete, Schutzgebiete, geregelte Gebiete und Berichterstattungseinheiten (auf internationaler, europäischer, nationaler, regionaler und lokaler Ebene bewirtschaftete, geregelte oder zu Zwecken der Berichterstattung herangezogene Gebiete, dazu zählen Deponien, Trinkwasserschutzgebiete, nitratempfindliche Gebiete, geregelte Fahrwasser auf Binnen- und Seewasserstraßen, Gebiete für die Abfallverklappung, Lärmschutzgebiete, für Exploration und Bergbau ausgewiesene Gebiete, Flussgebietseinheiten, entsprechende Berichterstattungseinheiten und Gebiete des Küstenzonenmanagements),

y) Gebiete mit naturbedingten Risiken (gefährdete Gebiete, eingestuft nach naturbedingten Risiken (sämtliche atmosphärischen, hydrologischen, seismischen, vulkanischen Phänomene sowie Naturfeuer, die auf Grund ihres örtlichen Auftretens sowie ihrer Schwere und Häufigkeit signifikante Auswirkungen auf die Gesellschaft haben können), zum Beispiel Überschwemmungen, Erdrutsche und Bodensenkungen, Lawinen, Waldbrände, Erdbeben oder Vulkanausbrüche),

z) atmosphärische Bedingungen (physikalische Bedingungen in der Atmosphäre, dazu zählen Geodaten auf der Grundlage von Messungen, Modellen oder einer Kombination aus beiden sowie Angabe der Messstandorte),

z1) meteorologische Objekte (Witterungsbedingungen und deren Messung: Niederschlag, Temperatur, Gesamtverdunstung (Evapotranspiration), Windgeschwindigkeit und Windrichtung),

z2) ozeanografische Objekte (physikalische Bedingungen der Ozeane wie zum Beispiel Strömungsverhältnisse, Salinität, Wellenhöhe),

z3) Meeresregionen (physikalische Bedingungen von Meeren und salzhaltigen Gewässern, aufgeteilt nach Regionen und Teilregionen mit gemeinsamen Merkmalen),

z4) biogeografische Regionen (Gebiete mit relativ homogenen ökologischen Bedingungen und gemeinsamen Merkmalen),

z5) Lebensräume und Biotope (geografische Gebiete mit spezifischen ökologischen Bedingungen, Prozessen, Strukturen und (lebensunterstützenden) Funktionen als physische Grundlage für dort lebende Organismen; dies umfasst auch durch geografische, abiotische und biotische Merkmale gekennzeichnete natürliche oder naturnahe terrestrische und aquatische Gebiete),

z6) Verteilung der Arten (geografische Verteilung des Auftretens von Tier- und Pflanzenarten, zusammengefasst in Gittern, Region, Verwaltungseinheit oder sonstigen analytischen Einheiten),

z7) Energiequellen (Energiequellen wie zum Beispiel Kohlenwasserstofflagerstätten, Wasserkraft, Bioenergie, Sonnen- und Windenergie, gegebenenfalls mit Tiefen- beziehungsweise Höhenangaben zur Ausdehnung der Energiequelle),

z8) mineralische Bodenschätze (mineralische Rohstofflagerstätten wie zum Beispiel Metallerze, Industrieminerale, gegebenenfalls mit Tiefen- beziehungsweise Höhenangaben zur Ausdehnung der Lagerstätten).

(2) Einzelheiten zur Spezifikation der den Themen zugeordneten Geodaten werden durch Rechtsverordnung nach § 15 geregelt.

(3) Sind neben einer Referenzversion mehrere identische Kopien der gleichen Geodaten bei verschiedenen geodatenhaltenden Stellen vorhanden oder werden sie für diese bereitgehalten, so gilt dieses Gesetz nur für die Referenzversion, von der die Kopien abgeleitet sind.

(4) Verfügt die geodatenhaltende Stelle bezogen auf Geodaten und Geodatendienste nicht selbst über die Rechte an geistigem Eigentum, so bleiben diese Rechte von den Vorschriften dieses Gesetzes unberührt.

Abschnitt 3
Anforderungen

§ 5 Bereitstellung von Geodaten

(1) Die amtlichen Daten des Liegenschaftskatasters, der Geotopografie und des geodätischen Raumbezugs sind die fachneutralen Kernkomponenten der nationalen Geodateninfrastruktur. Sie werden für Zwecke dieses Gesetzes durch die hierfür zuständigen Stellen des Bundes und der Länder bereitgestellt.

(2) Die Geodaten nach § 4 Absatz 1 Nummer 4 sind Bestandteil der Datengrundlage der nationalen Geodateninfrastruktur. Sie werden durch die hierfür jeweils ursprünglich zuständigen Stellen bereitgestellt.

(3) Die geodatenhaltenden Stellen haben ihre Geodaten auf der Grundlage der Daten nach Absatz 1 zu erfassen und zu führen.

(4) Soweit Geodaten sich auf einen Standort oder ein geografisches Gebiet beziehen, dessen Lage sich auf das Hoheitsgebiet mehrerer Mitgliedstaaten der Europäischen Gemeinschaft erstreckt, stimmen die zuständigen geodatenhaltenden Stellen mit den jeweils zuständigen Stellen in dem Mitgliedstaat beziehungsweise in den Mitgliedstaaten die Darstellung und die Position des Standorts beziehungsweise des geografischen Gebiets ab.

§ 6 Bereitstellung der Geodatendienste und Netzdienste

(1) Die geodatenhaltenden Stellen stellen sicher, dass für die von ihnen erhobenen, geführten oder bereitgestellten Geodaten und Metadaten mindestens die nachfolgenden Dienste bereitstehen:

1. Suchdienste,
2. Darstellungsdienste,
3. Downloaddienste,

4. Transformationsdienste,
5. Dienste zur Abwicklung eines elektronischen Geschäftsverkehrs.

(2) Die Dienste nach Absatz 1 sollen Nutzeranforderungen berücksichtigen und müssen über elektronische Netzwerke öffentlich verfügbar sein.

(3) Transformationsdienste sind mit den anderen Diensten nach Absatz 1 so zu kombinieren, dass die Geodatendienste und Netzdienste im Einklang mit diesem Gesetz betrieben werden können.

(4) Für Suchdienste sind zumindest folgende Suchkriterien zu gewährleisten:

1. Schlüsselwörter,
2. Klassifizierung von Geodaten und Geodatendiensten,
3. geografischer Standort,
4. Qualitätsmerkmale,
5. Bedingungen für den Zugang zu und die Nutzung von Geodaten und Geodatendiensten,
6. für die Erfassung, Führung und Bereitstellung von Geodaten und Geodatendiensten zuständige geodatenhaltende Stelle.

(5) Einzelheiten zur Spezifikation der Geodatendienste und Netzdienste werden durch Rechtsverordnung nach § 15 geregelt.

§ 7 Bereitstellung von Metadaten

(1) Die geodatenhaltenden Stellen, welche Geodaten und Geodatendienste als Referenzversion im Sinne von § 4 Absatz 3 bereitstellen, haben die zugehörigen Metadaten zu erstellen, zu führen und bereitzustellen sowie in Übereinstimmung mit den Geodaten und Geodatendiensten zu halten.

(2) Als Metadaten zu Geodaten sind mindestens nachstehende Inhalte oder Angaben zu folgenden Aspekten zu führen:

1. Schlüsselwörter,
2. Klassifizierung,
3. geografischer Standort,
4. Qualitätsmerkmale,
5. bestehende Beschränkungen des Zugangs der Öffentlichkeit nach § 12 sowie die Gründe für solche Beschränkungen,
6. Bedingungen für den Zugang und die Nutzung sowie gegebenenfalls entsprechende Geldleistungen,
7. für die Erfassung, Führung und Bereitstellung zuständige geodatenhaltende Stelle.

(3) Als Metadaten zu Geodatendiensten und Netzdiensten sind mindestens Angaben zu folgenden Aspekten zu führen:

1. Qualitätsmerkmale,
2. Bedingungen für den Zugang und die Nutzung sowie gegebenenfalls hiermit verbundene Geldleistungen,
3. für die Erfassung, Führung und Bereitstellung zuständige geodatenhaltende Stelle.

(4) Einzelheiten zur Spezifikation der Metadaten werden durch Rechtsverordnung nach § 15 geregelt.

§ 8 Interoperabilität

(1) Geodaten und Geodatendienste sowie Metadaten sind interoperabel bereitzustellen.

(2) Einzelheiten werden durch Rechtsverordnung nach § 15 geregelt.

Abschnitt 4
Elektronisches Netzwerk

§ 9 Geodateninfrastruktur und Geoportal

(1) Metadaten, Geodaten, Geodatendienste und Netzdienste werden als Bestandteile der nationalen Geodateninfrastruktur über ein elektronisches Netzwerk verknüpft.

(2) Der Zugang zum elektronischen Netzwerk nach Absatz 1 erfolgt auf der Ebene des Bundes durch ein Geoportal.

§ 10 Nationale Anlaufstelle

(1) Die Organisation der nationalen Geodateninfrastruktur erfolgt in der Verantwortung eines nationalen Lenkungsgremiums des Bundes und der Länder.

(2) Das nationale Lenkungsgremium nimmt die Aufgaben der nationalen Anlaufstelle im Sinne des Artikels 19 Absatz 2 der Richtlinie 2007/2/EG wahr.

(3) Die Einzelheiten regeln Bund und Länder in einer Verwaltungsvereinbarung.

Abschnitt 5
Nutzung von Geodaten

§ 11 Allgemeine Nutzung

(1) Geodaten und Geodatendienste, einschließlich zugehöriger Metadaten, sind vorbehaltlich der Vorschrift des § 12 Absatz 1 und 2 öffentlich zur Verfügung zu stellen.

(2) Geodaten und Metadaten sind über Geodatendienste für die kommerzielle und nicht kommerzielle Nutzung geldleistungsfrei zur Verfügung zu stellen, soweit durch besondere Rechtsvorschrift nichts anderes bestimmt ist oder vertragliche oder gesetzliche Rechte Dritter dem nicht entgegenstehen. Geodatenhaltende Stellen des Bundes stellen einander ihre Geodaten und Geodatendienste, einschließlich zugehöriger Metadaten, geldleistungsfrei zur Verfügung, soweit deren Nutzung zur Wahrnehmung öffentlicher Aufgaben erfolgt.

(3) Die Einzelheiten zur Nutzung von Geodaten und Geodatendiensten, einschließlich zugehöriger Metadaten, werden in einer Rechtsverordnung nach § 15 geregelt.

§ 12 Schutz öffentlicher und sonstiger Belange

(1) Der Zugang der Öffentlichkeit zu Geodaten und Geodatendiensten über Suchdienste im Sinne des § 6 Absatz 1 Nummer 1 kann beschränkt werden, wenn er nachteilige Auswirkungen auf die internationalen Beziehungen, bedeutsame Schutzgüter der öffentlichen Sicherheit oder die Verteidigung haben kann.

(2) Für den Zugang der Öffentlichkeit zu Geodaten und Geodatendiensten über die Dienste nach § 6 Absatz 1 Nummer 2 bis 5 gelten die Zugangsbeschränkungen nach § 8 Absatz 1 sowie § 9 des Umweltinformationsgesetzes vom 22. Dezember 2004 (BGBl. I S. 3704) entsprechend.

(3) Gegenüber geodatenhaltenden Stellen mit Ausnahme derjenigen Stellen im Sinne von § 2 Absatz 1 Nummer 2 des Umweltinformationsgesetzes vom 22. Dezember 2004 sowie gegenüber entsprechenden Stellen der Länder, der Kommunen und anderer Mitgliedstaaten der Europäischen Gemeinschaft sowie gegenüber Organen und Einrichtungen der Europäischen Gemeinschaft sowie auf der Grundlage von Gegenseitigkeit und Gleichwertigkeit auch gegenüber Einrichtungen, die durch internationale Übereinkünfte geschaffen wurden, soweit die Europäische Gemeinschaft und ihre Mitgliedstaaten zu deren Vertragsparteien gehören, können der Zugang zu Geodaten und Geodatendiensten sowie der Austausch und die Nutzung von Geodaten beschränkt werden, wenn hierdurch

1. die Durchführung eines laufenden Gerichtsverfahrens,
2. der Anspruch einer Person auf ein faires Verfahren,
3. die Durchführung strafrechtlicher, ordnungswidrigkeitenrechtlicher oder disziplinarrechtlicher Ermittlungen,
4. bedeutsame Schutzgüter der öffentlichen Sicherheit,
5. die Verteidigung oder
6. die internationalen Beziehungen

gefährdet werden können.

Abschnitt 5a
Überwachungs- und Bußgeldvorschriften

§ 13 Überwachung

(1) Die zuständigen Stellen der öffentlichen Verwaltung, die die Kontrolle im Sinne des § 2 Absatz 2 des Umweltinformationsgesetzes für den Bund oder eine unter der Aufsicht des Bundes stehende juristische Person des öffentlichen Rechts ausüben, überwachen die geodatenhaltenden Stellen im Sinne des § 3 Absatz 8 dieses Gesetzes in Verbindung mit § 2 Absatz 1 Nummer 2 des Umweltinformationsgesetzes (private geodatenhaltende Stellen) bei deren Aufgabenwahrnehmung.

(2) Die privaten geodatenhaltenden Stellen haben den zuständigen Stellen der öffentlichen Verwaltung auf Verlangen alle Informationen herauszugeben, die diese zur Wahrnehmung ihrer Aufgaben nach Absatz 1 benötigen.

(3) Die zuständigen Stellen der öffentlichen Verwaltung können die zur Wahrnehmung ihrer Aufgaben nach diesem Gesetz erforderlichen Maßnahmen treffen. Sie können insbesondere gegenüber privaten geodatenhaltenden Stellen anordnen:

1. die Bereitstellung von Geodaten, Geodatendiensten und Netzdiensten sowie Metadaten gemäß den §§ 5 bis 7,
2. die Herstellung von Interoperabilität gemäß § 8 oder
3. die Gewährleistung der allgemeinen Nutzung gemäß § 11.

§ 14 Bußgeldvorschriften

(1) Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig einer vollziehbaren Anordnung nach § 13 Absatz 3 Satz 2 zuwiderhandelt.

(2) Die Ordnungswidrigkeit kann mit einer Geldbuße bis zu zehntausend Euro geahndet werden.

Abschnitt 6
Schlussbestimmungen

§ 15 Verordnungsermächtigung

Die Bundesregierung wird ermächtigt, durch Rechtsverordnung, die nicht der Zustimmung des Bundesrates bedarf,

1. die Verpflichtungen aus den Durchführungsbestimmungen nach Artikel 5 Absatz 4, Artikel 7 Absatz 1, Artikel 16, 17 Absatz 8 sowie Artikel 21 Absatz 4 der Richtlinie 2007/2/EG zu erfüllen, soweit diese den Anwendungsbereich dieses Gesetzes betreffen,
2. die Nutzungsbedingungen nach § 11 Absatz 3, insbesondere zu den Nutzungsrechten, zur Gewährleistung und zum Haftungsausschluss, festzulegen und
3. die Aufgaben nach § 13 Absatz 1 bis 3 abweichend von § 13 Absatz 1 auf andere Stellen der öffentlichen Verwaltung zu übertragen.

§ 16 Inkrafttreten

Dieses Gesetz tritt am Tage nach der Verkündung in Kraft.

Gesetz zur staatlichen geologischen Landesaufnahme sowie zur Übermittlung, Sicherung und öffentlichen Bereitstellung geologischer Daten und zur Zurverfügungstellung geologischer Daten zur Erfüllung öffentlicher Aufgaben (Geologiedatengesetz - GeolDG)

Eingangsformel

Der Bundestag hat mit Zustimmung des Bundesrates das folgende Gesetz beschlossen:

Inhaltsübersicht

Abschnitt 2
Anzeige- und übermittlungsverpflichtete Personen, Frist und Form für die Übermittlung

Kapitel 4
Öffentliche Bereitstellung geologischer Daten und Zurverfügungstellung geologischer Daten zur Erfüllung öffentlicher Aufgaben

Abschnitt 1
Öffentliche Bereitstellung geologischer Daten und Zugang zu bereitgestellten Daten

Unterabschnitt 1
Allgemeine Regeln für die öffentliche Bereitstellung

Unterabschnitt 2
Öffentliche Bereitstellung staatlicher geologischer Daten

Unterabschnitt 3
Öffentliche Bereitstellung nichtstaatlicher geologischer Daten

Kapitel 1
Allgemeine Vorschriften

§ 1 Zweck des Gesetzes

Dieses Gesetz regelt die staatliche geologische Landesaufnahme, die Übermittlung, die dauerhafte Sicherung und die öffentliche Bereitstellung geologischer Daten sowie die Zurverfügungstellung geologischer Daten zur Erfüllung öffentlicher Aufgaben, um den nachhaltigen Umgang mit dem geologischen Untergrund gewährleisten und Geogefahren erkennen und bewerten zu können. Geologische Daten werden insbesondere benötigt

1. zur Aufsuchung und Gewinnung von Bodenschätzen und für weitere Nutzungen des geologischen Untergrunds,
2. zur Erkennung, Untersuchung und Bewertung geogener oder anthropogener Risiken,
3. in der Wasserwirtschaft, der Land- und Forstwirtschaft, der Bauwirtschaft und bei der Planung großer Infrastrukturprojekte sowie
4. für das Standortauswahlverfahren nach dem Standortauswahlgesetz.

§ 2 Sachlicher und räumlicher Anwendungsbereich

(1) Dieses Gesetz ist anzuwenden auf

1. die staatliche geologische Landesaufnahme,
2. die Anzeige geologischer Untersuchungen bei der zuständigen Behörde,
3. die Übermittlung der bei geologischen Untersuchungen gewonnenen geologischen Daten an die zuständige Behörde,
4. die Sicherung geologischer Daten, die
   a) auf Grund der Nummern 1 bis 3 von der zuständigen Behörde gewonnen oder dieser übermittelt werden,
   b) bis zum 30. Juni 2020 auf Grund des Lagerstättengesetzes in der im Bundesgesetzblatt Teil III, Gliederungsnummer 750-1, veröffentlichten bereinigten Fassung, das zuletzt durch Artikel 22 des Gesetzes vom 10. November 2001 (BGBl. I S. 2992) geändert worden ist, oder auf Grund anderer Rechtsvorschriften von der zuständigen Behörde gewonnen oder dieser übermittelt worden sind,
   c) auf Grund des Beitritts der Deutschen Demokratischen Republik zur Bundesrepublik Deutschland am 3. Oktober 1990 von der zuständigen Behörde übernommen worden sind oder
   d) inhaberlos nach § 25 Absatz 1 sind,
5. die öffentliche Bereitstellung gesicherter geologischer Daten nach Nummer 4,
6. die Zurverfügungstellung gesicherter geologischer Daten nach Nummer 4 zur Erfüllung öffentlicher Aufgaben.

(2) Dieses Gesetz ist auch im Bereich der ausschließlichen Wirtschaftszone und des Festlandsockels der Bundesrepublik Deutschland anzuwenden.

(3) Dieses Gesetz ist auf geologische Daten anzuwenden, die im Rahmen geologischer Untersuchungen gewonnen werden. Daten zum Zustand und zur Zusammensetzung der Luft, des Bodens und des Wassers sowie weitere Daten, die nicht zum Zweck geologischer Untersuchungen gewonnen worden sind oder gewonnen werden, sind vom Anwendungsbereich dieses Gesetzes nicht erfasst. Dazu zählen insbesondere Messungen und Aufnahmen der Luft, des Bodens und des Wassers, die sich an geologische Untersuchungen anschließen und die auf Grund fachrechtlicher Vorschriften insbesondere zur Altlastenerfassung und -überwachung sowie zur Grundwasserüberwachung zu erheben sind.

(4) Dieses Gesetz ist auch auf geologische Daten anzuwenden, die im Lauf der Nutzung des geologischen Untergrunds in einer geologischen Untersuchung zur weiteren Erkundung desselben Nutzungsgebietes oder eines angrenzenden Nutzungsgebietes gewonnen werden. Geologische Daten, die nicht zur Erkundung des Nutzungsgebietes, sondern zur Durchführung der Produktion, insbesondere zur Produktions- und Grubensicherung gewonnen werden, sind nicht vom Anwendungsbereich dieses Gesetzes erfasst.

(5) Die Länder können festlegen, dass auf geologische Daten nach Absatz 3 Satz 2 und 3 und Absatz 4 Satz 2 die Vorschriften zur geologischen Landesaufnahme nach § 5 Absatz 1, 2 und 4 sowie nach den §§ 6 und 7, die Vorschriften zur Übermittlung geologischer Daten nach

den §§ 8 bis 16 sowie die Vorschriften zur Zurverfügungstellung von Daten nach § 33 Absatz 1 bis 4 sowie § 33 Absatz 5 erster Halbsatz ganz oder teilweise anzuwenden sind. Die Länder können festlegen, dass sich der Anwendungsbereich des Gesetzes nicht auf geologische Daten aus Bohrungen, Baugrunduntersuchungen oder Rammkernsondierungen erstreckt, die jeweils lediglich eine Tiefe von bis zu 10 Metern erreichen.

(6) Dieses Gesetz ist nicht auf geologische Daten anzuwenden, die als Verschlusssache dem staatlichen materiellen Geheimschutz unterliegen. Der Herausgeber einer Verschlusssache kann festlegen, dass für geologische Daten nach Satz 1 die Vorschriften dieses Gesetzes mit Ausnahme der Vorschriften über die öffentliche Bereitstellung nach den §§ 18 bis 32 sowie 34 und 35 Absatz 1 angewendet werden, wenn die Vorgaben des staatlichen materiellen Geheimschutzes eingehalten werden.

(7) Die bergrechtlichen, wasserrechtlichen, bodenschutzrechtlichen, naturschutzrechtlichen, immissionsschutzrechtlichen, strahlenschutzrechtlichen, landwirtschaftsrechtlichen, forstrechtlichen, bodenschätzungsrechtlichen und baurechtlichen Bestimmungen bleiben unberührt.

§ 3 Begriffsbestimmungen

(1) Staatliche geologische Landesaufnahme im Sinne dieses Gesetzes ist die systematische punkt-, linien-, flächen- und raumbezogene Erfassung, Analyse, Beschreibung, Dokumentation und Darstellung der geologischen Verhältnisse der Erdoberfläche, des geologischen Untergrunds und, soweit im Rahmen einer geologischen Untersuchung erstellt, des Bodens und des Grundwassers.

(2) Eine geologische Untersuchung umfasst

1. alle allgemein geologischen, rohstoffgeologischen, ingenieurgeologischen, geophysikalischen, mineralogischen, geochemischen, bodenkundlichen, geothermischen, hydrogeologischen sowie geotechnischen Messungen und Aufnahmen der Erdoberfläche, des geologischen Untergrunds, des Bodens oder des Grundwassers mit Hilfe von Schürfen, Bohrungen, Feld- oder Bohrlochmessungen und sonstigen Erkundungsmethoden wie der Fernerkundung sowie die Aufbereitung der hierbei gewonnenen Daten mit am Markt verfügbaren technischen Mitteln in vergleichbare und bewertungsfähige Daten, zum Beispiel in Form von Daten- und Gesteinssammlungen, Schichtenverzeichnissen oder grafischen Darstellungen, sowie
2. die Analyse und Bewertung der nach Nummer 1 gewonnenen Fachdaten, zum Beispiel in Form von Gutachten, Studien oder räumlichen Modellen des geologischen Untergrunds einschließlich Vorratsberechnungen oder in Form von Daten zu sonstigen Nutzungspotenzialen des Untersuchungsgebiets.

(3) Geologische Daten im Sinne dieses Gesetzes sind in geologischen Untersuchungen gewonnene Nachweisdaten, Fachdaten und Bewertungsdaten. Dabei sind

1. Nachweisdaten die Daten, die geologische Untersuchungen persönlich, örtlich, zeitlich und allgemein inhaltlich zuordnen,
2. Fachdaten die Daten, die mittels Messungen und Aufnahmen gewonnen worden sind oder die mittels Messungen und Aufnahmen gewonnen und mit am Markt verfügbaren technischen Mitteln in vergleichbare und bewertungsfähige Daten aufbereitet worden sind,

3. Bewertungsdaten die Daten, die Analysen, Einschätzungen und Schlussfolgerungen zu Fachdaten, insbesondere in Form von Gutachten, Studien oder räumlichen Modellen des geologischen Untergrunds einschließlich Vorratsberechnungen oder Daten zu sonstigen Nutzungspotenzialen des Untersuchungsgebiets beinhalten.

(4) Staatliche geologische Daten sind geologische Daten, die

1. von einer Behörde oder im Auftrag einer Behörde bei einer geologischen Untersuchung gewonnen worden sind,
2. von einer natürlichen oder juristischen Person des Privatrechts in Erfüllung einer öffentlichen Aufgabe, die dabei der Kontrolle einer oder mehrerer juristischer Personen des öffentlichen Rechts im Sinne des § 2 Absatz 2 des Umweltinformationsgesetzes in der jeweils geltenden Fassung unterliegt, bei einer geologischen Untersuchung gewonnen worden sind,
3. auf Grund des Beitritts der Deutschen Demokratischen Republik zur Bundesrepublik Deutschland am 3. Oktober 1990 von der zuständigen Behörde übernommen worden sind oder
4. inhaberlos nach § 25 Absatz 1 sind.

Nichtstaatliche geologische Daten sind geologische Daten, die nicht von Satz 1 erfasst sind. Sofern eine natürliche oder juristische Person eine Aufgabe nach Satz 1 Nummer 2 im Wettbewerb mit privaten Anbietern am Markt erfüllt, sind für die öffentliche Bereitstellung der geologischen Daten, die von dieser Person gewonnen worden sind, die Regelungen für nichtstaatliche Daten anzuwenden. Im Übrigen bleiben die Vorschriften dieses Gesetzes unberührt.

(5) Datensicherung im Sinne dieses Gesetzes ist die Erfassung, Bearbeitung, Systematisierung, Digitalisierung und Archivierung geologischer Daten zum Zweck des dauerhaften Erhalts und der dauerhaften Verfügbarkeit, Lesbarkeit und Verständlichkeit dieser Daten.

(6) Öffentliche Bereitstellung im Sinne dieses Gesetzes ist die Zugänglichmachung von geologischen Daten für jedermann.

(7) Zurverfügungstellung im Sinne dieses Gesetzes ist die Datenübermittlung geologischer Daten an eine Behörde oder eine natürliche oder juristische Person des Privatrechts, die eine öffentliche Aufgabe erfüllt, die der Kontrolle einer oder mehrerer juristischer Personen des öffentlichen Rechts im Sinne des § 2 Absatz 2 des Umweltinformationsgesetzes in der jeweils geltenden Fassung unterliegt.

§ 4 Anwendung des Geodatenzugangsgesetzes und des Umweltinformationsgesetzes

Auf die Ausführung dieses Gesetzes und der auf Grund des § 38 Absatz 1 erlassenen Rechtsverordnungen sind, soweit in diesem Gesetz nichts anderes bestimmt ist, in der jeweils geltenden Fassung anzuwenden:

1. die Vorschriften des Bundes und der Länder zum Aufbau einer Geodateninfrastruktur, die in Umsetzung der Richtlinie 2007/2/EG des Europäischen Parlaments und des Rates vom 14. März 2007 zur Schaffung einer Geodateninfrastruktur in der Europäischen Gemeinschaft (INSPIRE) (ABl. L 108 vom 25.4.2007, S. 1), die durch die Verordnung (EU) 2019/1010 (ABl. L 170 vom 25.6.2019, S. 115) geändert worden ist, beschlossen worden sind,

2. die Vorschriften des Bundes und der Länder zum Zugang zu Umweltinformationen, die in Umsetzung der Richtlinie 2003/4/EG des Europäischen Parlaments und des Rates vom 28. Januar 2003 über den Zugang der Öffentlichkeit zu Umweltinformationen und zur Aufhebung der Richtlinie 90/313/EWG des Rates beschlossen worden sind.

Kapitel 2
Aufgaben und Befugnisse der zuständigen Behörde

§ 5 Aufgaben der zuständigen Behörde

(1) Die zuständige Behörde nimmt die staatliche geologische Landesaufnahme mittels eigener geologischer Untersuchungen sowie auf der Grundlage geologischer Untersuchungen Dritter vor. Erlangt die zuständige Behörde hierbei Erkenntnisse über dringende Geogefahren, so informiert sie unverzüglich die für die Durchführung der Gefahrenabwehr zuständige Behörde.

(2) Die zuständige Behörde sichert die in § 2 Absatz 1 Nummer 4 genannten für die geologische Landesaufnahme erforderlichen geologischen Daten sowie gegebenenfalls ausgewählte Bohrkerne und Bohr-, Gesteins- und Bodenproben, um deren dauerhafte Verfügbarkeit, Lesbarkeit und Verständlichkeit zu gewährleisten. Bereits bei ihr vorhandene analoge Daten soll die zuständige Behörde im Zuge der Datensicherung digitalisieren, so dass diese Daten nach den Anforderungen der §§ 5 bis 9 des Geodatenzugangsgesetzes vom 10. Februar 2009 (BGBl. I S. 278), das durch Artikel 1 des Gesetzes vom 7. November 2012 geändert worden ist, öffentlich bereitgestellt werden können. Die Pflicht zur Datensicherung ist auch erfüllt, wenn eine nach § 14 Satz 1 Nummer 1, 2 oder Nummer 3 verpflichtete Person die Daten auf Grund von § 11 Absatz 2 vorhält oder auf Grund von § 11 Absatz 3 von der Übermittlung der Daten befreit ist, die sie ansonsten nach den §§ 9, 10 Absatz 1 oder auf Grund von § 10 Absatz 2 übermitteln müsste.

(3) Die zuständige Behörde gewährleistet die öffentliche Bereitstellung der bei ihr vorhandenen geologischen Daten nach den Anforderungen der §§ 5 bis 9 des Geodatenzugangsgesetzes und nach den auf Grund des § 14 des Geodatenzugangsgesetzes erlassenen Rechtsverordnungen oder nach den dem Geodatenzugangsgesetz entsprechenden landesrechtlichen Regelungen, soweit dieses Gesetz oder eine auf Grund des § 38 Absatz 1 erlassene Rechtsverordnung nichts anderes bestimmen. Die zuständige Behörde stellt geologische Daten den Behörden und Personen nach § 33 Absatz 1, die öffentliche Aufgaben des Bundes und der Länder erfüllen, zur Verfügung.

(4) Die zuständige Behörde gewährleistet die Sicherung geologischer Daten, die nicht oder noch nicht öffentlich bereitgestellt werden, vor dem unberechtigten Zugriff Dritter nach dem Stand der Technik und erforderlichenfalls nach den Vorgaben des staatlichen materiellen Geheimschutzes.

(5) Die zuständige Behörde löscht den Teil der Nachweisdaten, der den Namen und die Anschrift einer natürlichen Person enthält, sobald dieser Teil für die Aufgabenerfüllung nach diesem Gesetz nicht mehr erforderlich ist und wenn der Name und die Anschrift nicht gleichlautend sind mit dem Namen und der Anschrift einer anzeigenden Firma. Die zuständige Behörde löscht personenbezogene Daten, insbesondere den Namen und die Anschrift einer natürlichen Person, die mit geologischen Daten verbunden sind, sobald diese für die Aufgabenerfüllung nach diesem Gesetz und die in § 1 genannten Zwecke nicht mehr erfor-

derlich sind. Für die Löschung von Eigennamen in geologischen Daten, die in analoger Form vorliegen, ist § 32 Absatz 2 entsprechend anzuwenden.

§ 6 Betretensrecht für die staatliche geologische Landesaufnahme; Betretensrecht zur Verhütung geologischer Gefahren; Zutritt zu geologischen Untersuchungen Dritter

(1) Die zuständige Behörde und die von ihr beauftragten Personen sind befugt, zum Zweck der staatlichen geologischen Landesaufnahme gemäß § 5 Absatz 1 an Werktagen in der Zeit von 7.00 bis 20.00 Uhr nach vorheriger rechtzeitiger Ankündigung Grundstücke mit Ausnahme der in erkennbarem Wohnzusammenhang stehenden Teile dieser Grundstücke (Wohngrundstücke) zu betreten und die erforderlichen geologischen Untersuchungen durchzuführen. Zur Verhütung gemeiner Gefahren sind die zuständige Behörde und die von ihr beauftragten Personen befugt, Grundstücke einschließlich Wohngrundstücken in der Zeit von 7.00 bis 20.00 Uhr zu betreten und dort die erforderlichen geologischen Untersuchungen vorzunehmen; die gemeine Gefahr ist von der zuständigen Behörde schriftlich zu belegen. Zur Verhütung dringender Gefahren für die öffentliche Sicherheit und Ordnung sind die zuständige Behörde und die von ihr beauftragten Personen befugt, Grundstücke einschließlich Wohngrundstücken jederzeit zu betreten und dort die erforderlichen geologischen Untersuchungen durchzuführen; die dringende Gefahr für die öffentliche Sicherheit und Ordnung ist von der zuständigen Behörde nachträglich schriftlich zu belegen. Die für die geologischen Untersuchungen nach den Sätzen 1 bis 3 erforderlichen Geräte dürfen auch außerhalb der in Satz 1 genannten Uhrzeiten betrieben werden. Das Grundrecht auf Unverletzlichkeit der Wohnung nach Artikel 13 Absatz 1 des Grundgesetzes wird durch die Sätze 2 und 3 eingeschränkt. Liegen die Voraussetzungen der Sätze 1, 2 oder 3 nicht vor, so dürfen Grundstücke nur mit Zustimmung des Eigentümers oder eines sonstigen Nutzungsberechtigten betreten werden. Wohn-, Betriebs- und Geschäftsgebäude dürfen nur mit Zustimmung des Eigentümers oder eines sonstigen Nutzungsberechtigten betreten werden. Landesrechtliche Betretensrechte zum Zweck der staatlichen geologischen Landesaufnahme bleiben unberührt.

(2) Der zuständigen Behörde und den von ihr beauftragten Personen steht zum Zweck der geologischen Landesaufnahme der Zutritt zu allen Standorten geologischer Untersuchungen, insbesondere zu Anlagen und Einrichtungen für Bohrungen sowie zu Steinbrüchen, Kiesgruben und sonstigen der Nutzung des geologischen Untergrunds dienenden Betrieben, im städtischen Bereich auch zu Baugruben, und die Inaugenscheinnahme der bei den geologischen Untersuchungen gewonnenen Ergebnisse im Benehmen mit der zuständigen Aufsichtsbehörde und in Abstimmung mit der für die Sicherheit zuständigen Aufsichtsperson des Betriebs innerhalb der Betriebs- und Geschäftszeiten jederzeit offen. Die zuständige Behörde und die von ihr beauftragen Personen sind befugt, Betriebs- und Geschäftsräume an Standorten geologischer Untersuchungen zu den üblichen Betriebs- und Geschäftszeiten zu betreten, wenn dies für den Zutritt zu der geologischen Untersuchung erforderlich ist oder wenn der Eigentümer oder ein sonstiger Nutzungsberechtigter zugestimmt hat. Die zuständige Behörde kann in Abstimmung mit dem Betroffenen auf ihre Kosten eigene geologische Untersuchungen bei geologischen Untersuchungen Dritter vornehmen.

(3) Die Art, den voraussichtlichen Umfang und die geplante Dauer von geologischen Untersuchungen nach den Absätzen 1 und 2, die den Einsatz von Maschinen voraussetzen oder die Dauer von zwei Arbeitstagen überschreiten, hat die zuständige Behörde dem Grundstückseigentümer und dem sonstigen Nutzungsberechtigten mindestens zwei Wochen vor Beginn der geplanten Untersuchung schriftlich, elektronisch oder, wenn mehr als zehn Grundstü-

cke betroffen sind, durch ortsübliche Bekanntmachung in den Gemeinden, in denen die Untersuchung stattfindet, bekannt zu geben.

(4) Geologische Untersuchungen nach Absatz 1 Satz 1 und 2 sowie Absatz 2 Satz 2 sind unzulässig, wenn sie für die betroffene Person unzumutbar, insbesondere mit dem Betriebs- und Geschäftsablauf einer betroffenen Person unvereinbar sind. Soweit öffentlich-rechtliche Beschränkungen der Inanspruchnahme eines Grundstücks entgegenstehen, hat sich die für die staatliche geologische Landesaufnahme zuständige Behörde mit der für die öffentlich-rechtliche Beschränkung zuständigen Behörde vor der Inanspruchnahme ins Benehmen zu setzen.

§ 7 Wiederherstellungspflicht und Haftung

(1) Nach Abschluss einer geologischen Untersuchung gemäß § 6 Absatz 1 oder Absatz 2 stellt die zuständige Behörde bei allen durch die Untersuchung unmittelbar oder mittelbar beeinträchtigten Grundstücken den Zustand wieder her, der vor der Durchführung der Untersuchung bestanden hat, es sei denn, dass

1. die Wiederherstellung des Ausgangszustands ganz oder teilweise unmöglich oder unzumutbar ist oder
2. der Grundstückseigentümer schriftlich oder elektronisch bestätigt hat, dass die Wiederherstellung für ihn nicht von Interesse ist.

Die zuständige Behörde stellt abweichend von Satz 1 einen anderen Zustand her, soweit überwiegende öffentliche Interessen dies erfordern.

(2) Der Eigentümer oder der sonstige Nutzungsberechtigte eines durch die Untersuchung unmittelbar oder mittelbar beeinträchtigten Grundstücks haben Anspruch auf einen angemessenen Ausgleich der Vermögensnachteile, die durch eine geologische Untersuchung nach § 6 Absatz 1 oder Absatz 2 entstanden sind, wenn

1. der Vermögensnachteil durch die Wiederherstellung des Ausgangszustands oder durch eine davon abweichende Wiederherstellung nicht oder nicht ausreichend ausgeglichen worden ist,
2. die Wiederherstellung des Ausgangszustands ganz oder teilweise unmöglich oder unzumutbar ist oder
3. der Ausgangszustand wegen überwiegender öffentlicher Interessen nicht wiederhergestellt worden ist.

Der Ausgleich wird in Geld gewährt. Auf die Verjährung sind die Vorschriften des Bürgerlichen Gesetzbuchs anzuwenden. Der Ausgleichsanspruch unterliegt der regelmäßigen Verjährung nach § 195 des Bürgerlichen Gesetzbuchs. Der Ausgleichsanspruch besteht nicht, wenn der Grundstückseigentümer schriftlich oder elektronisch bestätigt hat, dass die Wiederherstellung für ihn nicht von Interesse ist. Weitergehende Ersatzansprüche bleiben unberührt.

(3) Der Grundstückseigentümer und der sonstige Nutzungsberechtigte haften gegenüber Dritten nicht für Schäden oder sonstige Nachteile, die durch geologische Untersuchungen nach § 6 Absatz 1 oder Absatz 2 entstanden sind.

Kapitel 3
Übermittlung geologischer Daten an die zuständige Behörde

Abschnitt 1
Anzeige geologischer Untersuchungen; Übermittlung geologischer Daten

§ 8 Anzeige geologischer Untersuchungen und Übermittlung von Nachweisdaten an die zuständige Behörde

Spätestens zwei Wochen vor Beginn einer geologischen Untersuchung haben die nach § 14 Satz 1 Nummer 1, 2 und 3 verpflichteten Personen die geologische Untersuchung der zuständigen Behörde unaufgefordert anzuzeigen, unbeschadet der für die Untersuchung einschlägigen Vorschriften anderer Gesetze. Dazu haben sie der zuständigen Behörde, sofern bekannt, die folgenden Nachweisdaten zu übermitteln:

1. die Bezeichnung und den Zweck der geologischen Untersuchung sowie den Namen und die Anschrift der anzeigenden Person sowie der Person, die die Untersuchung in Auftrag gegeben hat; bei juristischen Personen und Personengesellschaften: den Namen und die Anschrift einer nach Gesetz, Satzung oder Gesellschaftsvertrag zur Vertretung berechtigten Person,
2. die Art, die Methode, den voraussichtlichen Umfang und die geplante Dauer der geologischen Untersuchung,
3. bei flächenhaft durchgeführten geologischen Untersuchungen wie geologischen Kartierungen und geophysikalischen oder geochemischen Messungen: die Lage des Untersuchungsgebiets und, soweit möglich, die grafische Darstellung der Messpunkte,
4. bei Bohrungen: die voraussichtliche Bezeichnung der Bohrung, die geplante Lage und Ansatzhöhe des Bohrpunktes, den geplanten Bohrlochverlauf, die geplante Endteufe, die gegebenenfalls prognostizierten Gesteinsschichten, die geplanten Bohrlochmessungen, die Art des Bohrverfahrens sowie den voraussichtlichen künftigen Aufbewahrungsort und die beabsichtigte Aufbewahrungsdauer von Bohrkernen und Bohr-, Gesteins- und Bodenproben,
5. bei geologischen Untersuchungen wie der Aufnahme von geologischen Aufschlüssen, dem Anlegen von Schürfen oder der Beprobung von Bergbauhalden: die Lage der Untersuchungspunkte, die Art der geplanten Untersuchungen, gegebenenfalls die Art des Aufschlussverfahrens und, soweit möglich, die grafische Darstellung dieser Angaben sowie den voraussichtlichen künftigen Aufbewahrungsort und die beabsichtigte Aufbewahrungsdauer von Gesteins- und Bodenproben und
6. bei Neubearbeitungen öffentlich bereitgestellter Fachdaten und Bewertungsdaten: die Nachweisdaten, aus denen die Fachdaten und Bewertungsdaten, die in die geologische Untersuchung einbezogen werden, abgelesen werden können.

Die Anzeige- und Übermittlungspflicht nach den Sätzen 1 und 2 wird auch durch die Übermittlung einer Anzeige oder eines Antrags an die zuständige Behörde erfüllt, wenn die Anzeige oder der Antrag auf Grund anderer Gesetze erstellt worden ist und soweit die Angaben nach Satz 2 darin enthalten sind. Die für ein Vorhaben geplanten geologischen Untersuchungen und die hierfür erforderlichen Daten können im Rahmen einer Anzeige oder eines

Antrags angezeigt und übermittelt werden. Für die Anzeige- und Übermittlungspflicht während des laufenden Betriebs ist § 15 Absatz 2 entsprechend anzuwenden.

§ 9 Übermittlung von Fachdaten geologischer Untersuchungen an die zuständige Behörde

(1) Spätestens drei Monate nach dem Abschluss der geologischen Untersuchung haben die nach § 14 Satz 1 Nummer 1, 2 und 3 verpflichteten Personen die folgenden Fachdaten, sofern sie bei der geologischen Untersuchung gewonnen wurden und unbeschadet der für die Untersuchung einschlägigen Vorschriften anderer Gesetze, unaufgefordert an die zuständige Behörde zu übermitteln:

1. bei flächenhaft durchgeführten geologischen Untersuchungen mittels Messungen:
   a) die Darstellung des Untersuchungsgebiets, die endgültige Lage der Mess- und Probenahmepunkte, die tatsächlich vorgenommenen Messungen und die verwendeten Messmethoden,
   b) die Messdaten sowie
   c) die mit am Markt verfügbaren technischen Mitteln in vergleichbare und bewertungsfähige Daten aufbereiteten Messdaten einschließlich der Dokumentation der angewandten Aufbereitungsschritte,
2. die Beschreibungen von Aufschlüssen, Schürfen und Bergbauhalden, zum Beispiel in Form von lithologischen und gegebenenfalls stratigraphischen Profilen,
3. bei geologischen Untersuchungen mittels Bohrung:
   a) eine Darstellung und Beschreibung der Lage und des Verlaufs der Bohrung, die Angaben zum Bohrkern oder zu Bohrproben sowie das Schichtenverzeichnis der Bohrung,
   b) die Methoden und Ergebnisse der durchgeführten Bohrlochmessungen oder ähnlicher Verfahren sowie die mit am Markt verfügbaren technischen Mitteln in vergleichbare und bewertungsfähige Daten aufbereiteten Bohrlochmessungen einschließlich der Dokumentation der angewandten Aufbereitungsschritte,
   c) eine Beschreibung aller Probenahmen nach Lage und Art der Probe und der jeweiligen Probenmenge sowie den Aufbewahrungsort und die beabsichtigte Aufbewahrungsdauer der Proben,
   d) die Ergebnisse von Pumpversuchen und anderen hydraulischen Tests,
   e) die Angaben zum Bohrverfahren, zur gesamten Bohrtechnik sowie zum Ausbau und zur Verfüllung des Bohrloches,
4. die Art, die Menge, die Koordinaten und die Teufenangaben des aus der geologischen Untersuchung hervorgegangenen Probenmaterials,
5. die Ergebnisse aller Test- und Laboranalysen der aus der geologischen Untersuchung stammenden Materialien wie Gesteins-, Flüssigkeits- und Gasproben mit Ausnahme derjenigen Ergebnisse von Test- und Laboranalysen, die über die Qualität und Menge des Bodenschatzes, auf den die Untersuchung gerichtet ist, Aufschluss geben,

6. bei Neubearbeitungen öffentlich bereitgestellter geologischer Daten: die mit am Markt verfügbaren technischen Mitteln in vergleichbare und bewertungsfähige Daten aufbereiteten Daten.

Bohrkerne sowie Bohr-, Gesteins- und Bodenproben sind von den in § 14 Satz 1 Nummer 1 und 2 verpflichteten Personen mit der Lage, der Teufe und dem Zeitpunkt ihrer Entnahme zu kennzeichnen. Auf Verlangen der zuständigen Behörde ist ihr Zugang zu vorhandenen Bohrkernen sowie Bohr-, Gesteins- und Bodenproben entsprechend § 6 Absatz 3 zu gewähren und ist ihr im Einvernehmen mit einer nach § 14 Satz 1 Nummer 1, 2 oder Nummer 3 verpflichteten Person ein geringfügiger Anteil vorhandener Bohrkerne und Bohr-, Gesteins- und Bodenproben zu übergeben.

(2) Die zuständige Behörde kann festlegen, dass die nach Absatz 1 Satz 1 zu übermittelnden Daten im Rahmen einer schriftlichen Dokumentation der geologischen Untersuchung zu übermitteln sind. Satz 1 ist nicht für kleine und mittlere Unternehmen anzuwenden.

§ 10 Übermittlung von Bewertungsdaten geologischer Untersuchungen an die zuständige Behörde

(1) Spätestens sechs Monate nach dem Abschluss der geologischen Untersuchung haben die nach § 14 Satz 1 Nummer 1, 2 und 3 verpflichteten Personen die Ergebnisse von durchgeführten Test- und Laboranalysen der aus der geologischen Untersuchung stammenden Materialien wie Gesteins-, Flüssigkeits- und Gasproben, die über die Menge und Qualität des Bodenschatzes, auf den die Untersuchung gerichtet ist, Aufschluss geben, unaufgefordert an die zuständige Behörde zu übermitteln.

(2) Die zuständige Behörde kann verlangen, dass ihr die nach § 14 Satz 1 Nummer 1, 2 und 3 verpflichteten Personen die folgenden Bewertungsdaten übermitteln, sofern sie bei der geologischen Untersuchung erstellt wurden und soweit sie für die staatliche geologische Landesaufnahme oder für die Erfüllung öffentlicher Aufgaben, insbesondere zu den in § 1 genannten Zwecken, erforderlich sind:

1. die im Rahmen der geologischen Untersuchung erstellten bewertenden Gutachten, Studien und vergleichbaren Produkte,
2. die im Rahmen der geologischen Untersuchung erstellten räumlichen Modelle einschließlich ihrer Dokumentation,
3. die Daten zu der Art, der Qualität und der Menge von Rohstoffvorkommen (Vorratsberechnung) und die Angaben zu den Verwendungsmöglichkeiten des jeweiligen Rohstoffs sowie
4. die Daten zu sonstigen Nutzungspotenzialen des Untersuchungsgebiets.

Spätestens sechs Monate nach dem Abschluss der geologischen Untersuchung haben die nach § 14 Satz 1 Nummer 1, 2 und 3 verpflichteten Behörden und Personen nach § 3 Absatz 4 Satz 1 Nummer 2 die Bewertungsdaten nach Satz 1 an die zuständige Behörde zu übermitteln.

(3) Die zuständige Behörde kann festlegen, in welchen Fällen ein bewertender Abschlussbericht nach Absatz 2 Satz 1 Nummer 1 verpflichtend zu erstellen ist. Satz 1 ist nicht für kleine und mittlere Unternehmen anzuwenden.

§ 11 Einschränkung von Anzeige- und Übermittlungspflichten; Vorhaltung geologischer Daten bei übermittlungsverpflichteten Personen; Verlängerung von Übermittlungsfristen

(1) Die zuständige Behörde kann die Anzeige- und Übermittlungspflichten nach den §§ 8 bis 10 Absatz 1 einschränken, sofern die geologische Untersuchung mangels ihrer räumlichen Ausbreitung oder ihres inhaltlichen Umfangs keine Bedeutung für die staatliche geologische Landesaufnahme, die Datensicherung, die öffentliche Bereitstellung oder die Zurverfügungstellung erwarten lässt. Bei der Entscheidung nach Satz 1 berücksichtigt die zuständige Behörde auch die Belastungen für kleine und mittlere Unternehmen. Die zuständige Behörde hat die Einschränkung nach Satz 1 unter Angabe der Entscheidungsgründe im jeweils einschlägigen Verkündungsorgan und im Internet öffentlich bekannt zu machen.

(2) Die zuständige Behörde kann auf die Übermittlung von Fachdaten nach § 9 Absatz 1 Satz 1 und Bewertungsdaten nach § 10 Absatz 1 verzichten, wenn

1. die Vorhaltung bei einer nach § 14 Satz 1 Nummer 1, 2 oder Nummer 3 verpflichteten Person sachlich begründet ist und
2. sich die nach § 14 Satz 1 Nummer 1, 2 oder Nummer 3 verpflichtete Person schriftlich oder elektronisch dazu bereit erklärt hat, die Daten vorzuhalten und der zuständigen Behörde den im Rahmen der üblichen Betriebs- und Geschäftszeiten jederzeitigen und, soweit möglich, elektronischen Zugang zu den vorgehaltenen Daten zu gewähren.

Solange die zuständige Behörde auf die Übermittlung verzichtet und die schriftliche oder elektronische Erklärung der nach § 14 Satz 1 Nummer 1, 2 oder Nummer 3 verpflichteten Person gültig ist, ruht die Übermittlungspflicht für die Daten nach § 9 Absatz 1 Satz 1 und § 10 Absatz 1.

(3) Die zuständige Behörde befreit eine nach § 14 Satz 1 Nummer 1, 2 oder Nummer 3 verpflichtete Behörde oder Person nach § 3 Absatz 4 Satz 1 Nummer 2 von den Übermittlungspflichten nach den §§ 9 und 10, wenn diese Behörde oder Person die geologischen Daten nach den §§ 18 bis 32 sowie 34 und 35 Absatz 1 öffentlich bereitstellt. Die zuständige Behörde weist nach § 22 Nummer 3 in den von ihr zu pflegenden Geodatendiensten auf die öffentliche Bereitstellung durch die von den Übermittlungspflichten nach den §§ 9 und 10 befreite Behörde oder Person nach § 3 Absatz 4 Satz 1 Nummer 2 hin.

(4) Die zuständige Behörde kann die in § 9 Absatz 1 Satz 1 und in § 10 Absatz 1 und 2 Satz 2 genannten Fristen im Einzelfall auf Antrag oder von Amts wegen verlängern, wenn dies im Hinblick auf den Umfang der geologischen Untersuchung, insbesondere im Hinblick auf die Anzahl oder den Umfang von Bohrungen, geboten erscheint.

§ 12 Nachträgliche Anforderung nichtstaatlicher Fachdaten

Die zuständige Behörde kann die Übermittlung von nichtstaatlichen Fachdaten, die vor dem 30. Juni 2020 in einer geologischen Untersuchung gewonnen worden sind und die bei einer nach § 14 Satz 1 verpflichteten Person noch vorhanden sind, entsprechend § 9 Absatz 1 oder Absatz 2 Satz 1 verlangen, wenn die Erfüllung öffentlicher Aufgaben zu den in § 1 genannten Zwecken oder andere überwiegende öffentliche Interessen die nachträgliche Übermittlung erfordern.

§ 13 Pflichten vor Entledigung von Proben und Löschung von Daten

Die nach § 14 Satz 1 verpflichteten Personen haben der zuständigen Behörde sämtliche in geologischen Untersuchungen gewonnenen Proben und geologische Daten vor deren Entledigung oder Löschung anzubieten, insbesondere:

1. sämtliche Bohrkerne sowie Bohr-, Gesteins- und Bodenproben sowie
2. solche geologische Daten,
   a) die der zuständigen Behörde nach § 3 des Lagerstättengesetzes hätten übermittelt werden müssen,
   b) die der zuständigen Behörde nach § 8 Satz 2, § 9 Absatz 1 Satz 1 und § 10 Absatz 1 hätten übermittelt werden müssen,
   c) die auf Grund einer Erklärung nach § 11 Absatz 2 bei einer nach § 14 Satz 1 Nummer 1, 2 oder Nummer 3 verpflichteten Person verblieben sind oder
   d) die auf Grund einer Befreiung nach § 11 Absatz 3 bei der nach § 14 Satz 1 Nummer 1, 2 oder Nummer 3 verpflichteten Behörde oder Person nach § 3 Absatz 4 Satz 1 Nummer 2 verblieben sind.

Vor der Verbringung von Bohrkernen sowie Bohr-, Gesteins- und Bodenproben an einen Ort außerhalb des Geltungsbereichs dieses Gesetzes sind diese Bohrkerne sowie Bohr-, Gesteins- und Bodenproben der zuständigen Behörde nach Satz 1 anzubieten. Die zuständige Behörde entscheidet spätestens zwei Monate nach dem Angebot nach Satz 1 oder Satz 2, ob die Proben oder geologischen Daten an sie zu übermitteln sind. Proben oder geologische Daten zu potenziellen Wirtsgesteinen gemäß Standortauswahlgesetz, die nach Mitteilung durch den Vorhabenträger nach dem Standortauswahlgesetz für das Standortauswahlverfahren benötigt werden können, müssen von der zuständigen Behörde übernommen werden. Die Kosten für die Übermittlung der Proben oder geologischen Daten trägt die zuständige Behörde.

Abschnitt 2
Anzeige- und übermittlungsverpflichtete Personen, Frist und Form für die Übermittlung

§ 14 Anzeige- und übermittlungsverpflichtete Personen

Zur Anzeige geologischer Untersuchungen nach § 8 Satz 1, zur Übermittlung der Nachweisdaten nach § 8 Satz 2 und der Fachdaten nach § 9 Absatz 1 Satz 1, zur Kennzeichnung von Bohrkernen und Proben nach § 9 Absatz 1 Satz 2, zur Gewährung des Zugangs zu Bohrkernen und Bohr-, Gesteins- und Bodenproben nach § 9 Absatz 1 Satz 3, zur Übermittlung von Bewertungsdaten nach § 10 Absatz 1 sowie zur Übermittlung von Bewertungsdaten auf Grund von § 10 Absatz 2 und von geologischen Fachdaten auf Grund von § 12 ist verpflichtet:

1. wer selbst oder als Beauftragter eine geologische Untersuchung vornimmt,
2. der Auftraggeber einer geologischen Untersuchung,
3. der Rechtsnachfolger einer nach Nummer 1 oder Nummer 2 verpflichteten Person oder

4. im Fall einer nachträglichen Übermittlung von nichtstaatlichen geologischen Fachdaten gemäß § 12: wer zum Zeitpunkt der Übermittlungsforderung Inhaber der geologischen Daten ist.

Die Anzeige oder Übermittlung der Daten durch einen Mitverpflichteten befreit die übrigen Verpflichteten von der Anzeigepflicht oder der Übermittlungspflicht. Der Rechtsnachfolger einer nach Satz 1 Nummer 1 und 2 anzeige- und übermittlungspflichtigen Person haftet nicht für die Verstöße gegen dieses Gesetz durch den Rechtsvorgänger.

§ 15 Abschluss einer geologischen Untersuchung; Beginn der Übermittlungsfrist; Einhaltung der Anzeige- und Übermittlungsfristen

(1) Eine geologische Untersuchung gilt mit dem Ablauf der nach § 8 Satz 2 Nummer 2 jeweils angegebenen Dauer als abgeschlossen, es sei denn, die Fortdauer der Untersuchung ist gegenüber der zuständigen Behörde innerhalb des jeweils ursprünglich angegebenen Zeitraums rechtzeitig angezeigt worden.

(2) Bei geologischen Untersuchungen, die ein Jahr oder länger dauern oder die im Lauf der Nutzung des geologischen Untergrunds zur weiteren Erkundung nach § 2 Absatz 4 durchgeführt werden, sind die Daten nach § 9 Absatz 1 Satz 1 und § 10 Absatz 1 der zuständigen Behörde jeweils jährlich zu übermitteln, erstmals mit dem Ablauf des ersten Jahres nach der Erteilung der Genehmigung oder nach der Anzeige der Untersuchung.

(3) Ist die geologische Untersuchung auf Grund anderer Gesetze anzeige- oder genehmigungspflichtig, so sind die Anzeige- und Übermittlungsfristen nach den §§ 8 bis 10 Absatz 1 auch eingehalten durch die fristgerechte Anzeige und die vollständige Übermittlung der geologischen Daten an die Behörde, die für die Anzeige oder Genehmigung der geologischen Untersuchung auf Grund anderer Gesetze zuständig ist. Diese Behörde übermittelt die geologischen Daten unverzüglich an die nach § 37 zuständige Behörde. Die nach § 37 zuständige Behörde kann geologische Daten von den nach § 14 Satz 1 verpflichteten Personen nachfordern, wenn die übermittelten Daten nicht vollständig sind.

§ 16 Datenformat

(1) In den Fällen der §§ 8 bis 10 sind die Daten der zuständigen Behörde, soweit möglich und gegebenenfalls in Absprache mit der zuständigen Behörde, in einem von ihr benannten interoperablen Format elektronisch zu übermitteln. Unbeschadet des Satzes 1 sind für die Interoperabilität raumbezogener Daten die Durchführungsbestimmungen nach Artikel 5 Absatz 4, Artikel 7 Absatz 1 und Artikel 16 der Richtlinie 2007/2/EG zu beachten.

(2) Im Fall des § 12 sind die Daten der zuständigen Behörde, soweit möglich, elektronisch zu übermitteln.

(3) Für die Übermittlung des Namens und der Anschrift einer anzeigenden natürlichen Person sowie deren Auftraggeber nach § 8 Satz 2 Nummer 1 sind die Anforderungen an die Sicherheit der Datenverarbeitung gemäß den Artikeln 32 bis 34 der 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; L 314 vom 22.11.2016, S. 72; L 127 vom 23.5.2018, S. 2) zu beachten.

§ 17 Kennzeichnung von Daten

(1) Die nach § 14 Satz 1 verpflichteten Personen kennzeichnen die zu übermittelnden geologischen Daten als

1. Nachweisdaten nach § 8,
2. Fachdaten nach § 9 oder
3. Bewertungsdaten nach § 10.

(2) Die nach § 14 Satz 1 verpflichteten Personen geben an,

1. ob Fachdaten zum Zweck einer gewerblichen Tätigkeit gewonnen wurden und
2. ob und für welchen Zeitraum Beschränkungen für die öffentliche Bereitstellung nach den §§ 31 und 32 sowie nach spezialgesetzlichen Veröffentlichungsvorschriften bestehen könnten.

(3) Die zuständige Behörde setzt die Datenkategorie fest und berücksichtigt dabei die Kennzeichnung und die Angaben nach den Absätzen 1 und 2. Die Festsetzung ist ein Verwaltungsakt. Die zuständige Behörde gibt die Festsetzungen der Datenkategorien in regelmäßigen Abständen öffentlich bekannt. Sie veröffentlicht die Bekanntgabe im Internet sowie nach Möglichkeit in den nach § 6 Absatz 1 des Geodatenzugangsgesetzes vorgeschriebenen Geodatendiensten. Zusätzlich zu der öffentlichen Bekanntgabe nach Satz 4 kann die zuständige Behörde die Festsetzung denjenigen Personen, die die Daten übermittelt haben, oder deren Rechtsnachfolgern schriftlich oder elektronisch bekannt geben.

Kapitel 4
Öffentliche Bereitstellung geologischer Daten und Zurverfügungstellung geologischer Daten zur Erfüllung öffentlicher Aufgaben

Abschnitt 1
Öffentliche Bereitstellung geologischer Daten und Zugang zu bereitgestellten Daten

Unterabschnitt 1
Allgemeine Regeln für die öffentliche Bereitstellung

§ 18 Öffentliche Bereitstellung geologischer Daten; anderweitige Ansprüche auf Informationszugang

(1) Die zuständige Behörde stellt geologische Daten nach den §§ 23 bis 27 sowie 29 vorbehaltlich der Beschränkungen nach den §§ 31 und 32 sowie nach spezialgesetzlichen Veröffentlichungsvorschriften öffentlich bereit. Weder die nach § 14 Satz 1 verpflichteten Personen noch die zuständige Behörde haften für die Aktualität, Vollständigkeit und Richtigkeit dieser öffentlich bereitgestellten geologischen Daten.

(2) Der Anspruch auf Zugang zu Umweltinformationen sowie die Pflicht zur aktiven Unterrichtung der Öffentlichkeit nach dem Umweltinformationsgesetz oder nach den entsprechenden landesrechtlichen Regelungen und die Bereitstellung von Geodaten nach dem Geodatenzugangsgesetz oder nach den entsprechenden landesrechtlichen Regelungen bleiben unberührt.

§ 19 Öffentliche Bereitstellung nach den Anforderungen des Geodatenzugangsgesetzes; analoge Bereitstellung

(1) Die zuständige Behörde stellt geologische Daten, die gemäß § 4 Absatz 1 Nummer 2 des Geodatenzugangsgesetzes in elektronischer Form vorliegen, nach den Anforderungen der §§ 5 bis 9 des Geodatenzugangsgesetzes oder nach den Anforderungen der entsprechenden landesrechtlichen Regelungen für den Zugang öffentlich bereit.

(2) Solange und soweit geologische Daten zum Zeitpunkt der öffentlichen Bereitstellung nach diesem Gesetz die Voraussetzungen des § 4 Absatz 1 Nummer 2 des Geodatenzugangsgesetzes oder die Anforderungen der entsprechenden landesrechtlichen Regelungen nicht erfüllen, werden diese Daten und die vorhandenen Bohrkerne sowie Bohr-, Gesteins- und Bodenproben am Standort der zuständigen Behörde oder am amtlichen Aufbewahrungsort zu den geschäftsüblichen Zeiten in analoger Form öffentlich bereitgestellt. Die öffentliche Bereitstellung nach Satz 1 muss die Einsichtnahme und, soweit die Beschaffenheit der Daten, der Bohrkerne sowie Bohr-, Gesteins- und Bodenproben es gestattet, die Vervielfältigung oder eine andere Form der beständigen Kenntnisnahme ermöglichen.

§ 20 Zugang zu öffentlich bereitgestellten geologischen Daten im Rahmen gewerblicher Tätigkeiten

(1) Wird der Zugang zu öffentlich bereitgestellten geologischen Daten im Rahmen einer gewerblichen Tätigkeit begehrt, soll die zugangsbegehrende Person, bei juristischen Personen und Personengesellschaften eine nach Gesetz, Satzung oder Gesellschaftsvertrag zur Vertretung berechtigte Person, Folgendes angeben:

1. ihren Namen und den Namen eines etwaigen Auftraggebers,
2. die Lage des Gebiets, für das geologische Daten begehrt werden, und
3. den Zweck, der dem Zugangsbegehren zu Grunde liegt.

(2) Mit dem Zugang zu öffentlich bereitgestellten geologischen Daten soll die Person nach Absatz 1 erklären, von den Anzeige- und Übermittlungspflichten nach den §§ 8, 9 Absatz 1 Satz 1 und § 10 Absatz 1 und etwaigen Übermittlungspflichten auf Grund von § 10 Absatz 2 und 3 Kenntnis genommen zu haben.

§ 21 Öffentliche Bereitstellung geologischer Daten in analoger Form anlässlich eines Zugangsbegehrens

(1) Hat die zuständige Behörde zu dem Zeitpunkt, zu dem sie analoge Daten öffentlich bereitstellen müsste, noch nicht geprüft, ob Beschränkungsgründe nach den §§ 31 und 32 oder nach spezialgesetzlichen Veröffentlichungsvorschriften vorliegen, und kann sie deshalb lediglich analog vorhandene geologische Daten anlässlich eines Zugangsbegehrens nicht öffentlich bereitstellen, so hat die zuständige Behörde die Prüfung innerhalb eines Monats nach dem Zugangsbegehren nachzuholen und die Daten, für die keine Beschränkungsgründe nach den §§ 31 und 32 oder nach spezialgesetzlichen Veröffentlichungsvorschriften vorliegen, öffentlich bereitzustellen. Satz 1 ist entsprechend für geologische Fach- und Bewertungsdaten anzuwenden, auf deren Übermittlung die zuständige Behörde nach § 11 Absatz 2 verzichtet hat.

(2) Soweit die analogen Daten derart umfangreich und komplex sind, dass die Frist des Absatzes 1 nicht eingehalten werden kann, kann der Zeitraum für die Prüfung mit Zustim-

mung der zuständigen Aufsichtsbehörde auf insgesamt zwei Monate verlängert werden. Die zugangsbegehrende Person ist über die Geltung der längeren Frist innerhalb eines Monats ab ihrem Zugangsbegehren zu unterrichten; dabei sind die Gründe für die Verlängerung der Frist anzugeben.

§ 22 Hinweise auf geologische Daten in Geodatendiensten

In den nach § 6 Absatz 1 des Geodatenzugangsgesetzes vorgeschriebenen Geodatendiensten muss die zuständige Behörde darauf hinweisen,

1. welche Fach- und Bewertungsdatenbestände lediglich analog vorhanden sind,
2. welche Fachdatenbestände nach § 11 Absatz 2 bei Dritten vorgehalten werden,
3. welche Fach- und Bewertungsdatenbestände nach § 11 Absatz 3 von Behörden oder Personen nach § 3 Absatz 4 Satz 1 Nummer 2 nach den §§ 18 bis 32 sowie 34 und 35 Absatz 1 öffentlich bereitgestellt werden sowie
4. dass Fach- und Bewertungsdaten, die von Dritten bereitgestellt wurden, nicht der Gewährleistung der zuständigen Behörde auf Aktualität, Vollständigkeit und Richtigkeit unterliegen.

Unterabschnitt 2
Öffentliche Bereitstellung staatlicher geologischer Daten

§ 23 Öffentliche Bereitstellung staatlicher geologischer Daten der zuständigen Behörde

(1) Nachweisdaten einer eigenen geologischen Untersuchung der zuständigen Behörde werden unverzüglich öffentlich bereitgestellt, davon ausgenommen sind der Name und die Anschrift natürlicher Personen.

(2) Fach- und Bewertungsdaten, die die zuständige Behörde bei einer eigenen geologischen Untersuchung gewonnen hat, werden spätestens sechs Monate nach Abschluss der geologischen Untersuchung öffentlich bereitgestellt. Für die öffentliche Bereitstellung von Fach- und Bewertungsdaten geologischer Untersuchungen, die ein Jahr oder länger dauern, ist § 15 Absatz 2 entsprechend anzuwenden.

(3) Geologische Daten, die die zuständige Behörde vor dem 30. Juni 2020 in einer eigenen geologischen Untersuchung gewonnen hat, sowie die aus anderen Gründen bei ihr vorhandenen staatlichen geologischen Daten werden spätestens nach dem Ablauf von sechs Monaten nach dem 30. Juni 2020 öffentlich bereitgestellt.

§ 24 Öffentliche Bereitstellung übermittelter staatlicher geologischer Daten

(1) Nachweisdaten einer anderen Behörde als der zuständigen Behörde oder einer Person nach § 3 Absatz 4 Satz 1 Nummer 2 werden spätestens drei Monate nach Ablauf der Anzeige- und Übermittlungsfrist nach § 8 öffentlich bereitgestellt. Die zuständige Behörde aktualisiert die Nachweisdaten anhand der nach § 9 Absatz 1 Satz 1 übermittelten Fachdaten. Der Name und die Anschrift natürlicher Personen werden nicht öffentlich bereitgestellt, es sei denn, sie sind gleichlautend mit dem Namen oder der Anschrift einer anzeigenden Firma.

(2) Fach- und Bewertungsdaten, die eine andere Behörde als die zuständige Behörde oder eine Person nach § 3 Absatz 4 Satz 1 Nummer 2 gewonnen hat, werden spätestens sechs Mona-

te nach Ablauf der Übermittlungsfrist nach § 9 Absatz 1 Satz 1 und § 10 Absatz 1 und 2 Satz 2 öffentlich bereitgestellt.

§ 25 Inhaberlose Daten

(1) Die zuständige Behörde kann ein Aufgebotsverfahren einleiten, wenn sie den Inhaber geologischer Daten mit den ihr zu Gebote stehenden Mitteln nicht ermitteln kann. Hierzu gibt die zuständige Behörde die für die geologischen Fach- und Bewertungsdaten maßgeblichen Nachweisdaten im jeweils einschlägigen Verkündungsorgan und im Internet bekannt und fordert den Inhaber auf, sich bei ihr zu melden; ist die Angabe der Nachweisdaten zu umfangreich, gibt sie die Lage und, sofern bekannt, den Gewinnungszeitpunkt der Daten sowie den Endzeitpunkt der Aufgebotsfrist bekannt. Meldet sich innerhalb eines Jahres nach der Veröffentlichung der Aufforderung der Inhaber nicht, erlässt die zuständige Behörde einen Ausschlussbescheid. Wenn erforderlich, kann zuvor eine angemessene Frist gesetzt werden. Der Ausschlussbescheid ist nach § 10 des Verwaltungszustellungsgesetzes öffentlich zuzustellen. Mit dem bestandskräftigen Ausschlussbescheid sind die Daten inhaberlos.

(2) Inhaberlose Daten sind staatliche geologische Daten des Landes, auf dessen Gebiet sich die Daten beziehen. Bei grenzübergreifenden Datensätzen ist das Land Dateninhaber, dessen Gebiet von der Mehrheit der Daten erfasst wird, es sei denn, die Länder einigen sich anderweitig über die Inhaberschaft.

Unterabschnitt 3
Öffentliche Bereitstellung nichtstaatlicher geologischer Daten

§ 26 Öffentliche Bereitstellung nichtstaatlicher Nachweisdaten nach § 8

Nichtstaatliche Nachweisdaten, die der zuständigen Behörde gemäß § 8 Satz 2 übermittelt worden sind, werden spätestens drei Monate nach Ablauf der Anzeige- und Übermittlungsfrist nach § 8 Satz 1 öffentlich bereitgestellt. Die zuständige Behörde aktualisiert die Nachweisdaten anhand der nach § 9 Absatz 1 Satz 1 übermittelten Fachdaten. Der Name und die Anschrift natürlicher Personen werden nicht öffentlich bereitgestellt, es sei denn, sie sind gleichlautend mit dem Namen oder der Anschrift einer anzeigenden Firma.

§ 27 Öffentliche Bereitstellung nichtstaatlicher Fachdaten nach § 9

(1) Nichtstaatliche Fachdaten, die der zuständigen Behörde nach § 9 Absatz 1 Satz 1 übermittelt worden sind, werden nach Ablauf von fünf Jahren nach Ablauf der Übermittlungsfrist öffentlich bereitgestellt, es sei denn, sie dienen wie die Daten des § 9 Absatz 1 Satz 1 Nummer 1 lediglich der Aktualisierung der Nachweisdaten.

(2) Nichtstaatliche Fachdaten, die der zuständigen Behörde nach § 9 Absatz 1 Satz 1 zum Zweck einer gewerblichen Tätigkeit auf Grund einer Bergbauberechtigung oder auf Grund eines anderweitig genehmigten oder anzeigepflichtigen Vorhabens für die Untersuchung des geologischen Untergrunds, die Gewinnung von Bodenschätzen oder die Nutzung des geologischen Untergrunds übermittelt worden sind, werden abweichend von Absatz 1 nach Ablauf von zehn Jahren nach Ablauf der Übermittlungsfrist öffentlich bereitgestellt.

(3) Nichtstaatlich gewonnene Bohrkerne sowie nichtstaatlich gewonnene Bohr-, Gesteins- und Bodenproben werden entsprechend Absatz 1 oder Absatz 2 nach § 19 Absatz 2 öffentlich bereitgestellt; die öffentliche Bereitstellung beschränkt sich auf die Möglichkeit der Ein-

sichtnahme. Sind die Voraussetzungen des § 34 Absatz 2 erfüllt und gestattet es die Beschaffenheit von Bohrkernen und Bohr-, Gesteins- und Bodenproben, so kann eine beständige Form der Kenntnisnahme ermöglicht werden.

§ 28 Schutz nichtstaatlicher Bewertungsdaten nach § 10 sowie nachträglich angeforderter nichtstaatlicher Fachdaten nach § 12

Nichtstaatliche Bewertungsdaten nach § 10 und die von der zuständigen Behörde nachträglich angeforderten nichtstaatlichen Fachdaten nach § 12 werden nicht öffentlich bereitgestellt.

§ 29 Öffentliche Bereitstellung nichtstaatlicher geologischer Daten, die vor dem 30. Juni 2020 an die zuständige Behörde übermittelt worden sind

(1) Auf nichtstaatliche Nachweisdaten entsprechend § 8 Satz 2, die vor dem 30. Juni 2020 auf Grund des Lagerstättengesetzes oder auf Grund anderer Rechtsvorschriften an die zuständige Behörde übermittelt worden sind, ist § 26 anzuwenden.

(2) Auf nichtstaatliche Fachdaten entsprechend § 9 Absatz 1 Satz 1 und nichtstaatlich gewonnene Bohrkerne und Bohr-, Gesteins- und Bodenproben entsprechend § 9 Absatz 1 Satz 3, die vor dem 30. Juni 2020 auf Grund des Lagerstättengesetzes oder auf Grund anderer Rechtsvorschriften an die zuständige Behörde übermittelt oder übergeben worden sind, ist § 27 anzuwenden. Ist die Frist für die öffentliche Bereitstellung nichtstaatlicher Fachdaten nach Satz 1 am 30. Juni 2020 bereits abgelaufen oder liefe die Frist innerhalb zweier Monate nach dem 30. Juni 2020 ab, so werden diese Daten nach dem Ablauf von sechs Monaten nach dem 30. Juni 2020 öffentlich bereitgestellt.

(3) Auf nichtstaatliche Bewertungsdaten entsprechend § 10, die vor dem 30. Juni 2020 auf Grund des Lagerstättengesetzes oder auf Grund anderer Rechtsvorschriften an die zuständige Behörde übermittelt worden sind, ist § 28 anzuwenden.

(4) In den Fällen der Absätze 1 und 2 ist für die Berechnung der Frist für die öffentliche Bereitstellung auf das jeweilige Übermittlungsdatum oder, wenn dieses nicht feststellbar ist, auf das letzte Datum der jeweiligen geologischen Untersuchung abzustellen. Ist beides nicht ermittelbar, beginnt die Frist am 30. Juni 2020.

(5) Die zuständige Behörde setzt die Datenkategorie der Daten fest, die vor dem 30. Juni 2020 auf Grund des Lagerstättengesetzes oder auf Grund anderer Rechtsvorschriften an die zuständige Behörde übermittelt oder übergeben worden sind. Die Festsetzung ist ein Verwaltungsakt. Die zuständige Behörde gibt die Festsetzungen der Datenkategorien spätestens einen Monat vor der öffentlichen Bereitstellung öffentlich bekannt. Sie veröffentlicht die Bekanntgabe im Internet sowie nach Möglichkeit in den nach § 6 Absatz 1 des Geodatenzugangsgesetzes vorgeschriebenen Geodatendiensten. Zusätzlich zu der öffentlichen Bekanntgabe nach Satz 4 kann die zuständige Behörde die Festsetzung denjenigen Personen, die die Daten übermittelt haben, oder deren Rechtsnachfolgern schriftlich oder elektronisch bekannt geben.

(6) Den Absätzen 1 bis 4 entgegenstehende Abreden zwischen dem Dateninhaber und der zuständigen Behörde zur Vertraulichkeit geologischer Daten können der öffentlichen Bereitstellung nach diesem Gesetz oder auf Grund dieses Gesetzes nicht entgegengehalten werden.

§ 30 Einwilligung des Dateninhabers

Soweit eine nach § 14 Satz 1 verpflichtete Person in die öffentliche Bereitstellung der von ihr übermittelten nichtstaatlichen geologischen Daten eingewilligt hat, ist § 24 entsprechend anzuwenden.

Abschnitt 2
Beschränkung der öffentlichen Bereitstellung geologischer Daten

§ 31 Schutz öffentlicher Belange

Die zuständige Behörde hat sicherzustellen, dass geologische Daten nicht oder nicht innerhalb eines von ihr benannten Zeitraums öffentlich bereitgestellt werden, wenn oder solange die öffentliche Bereitstellung nachteilige Auswirkungen hätte auf

1. die internationalen Beziehungen oder die Verteidigung,
2. bedeutsame Schutzgüter der öffentlichen Sicherheit, insbesondere kritische Infrastrukturen,
3. die Vertraulichkeit der Beratungen von Behörden und natürlichen oder juristischen Personen des Privatrechts, soweit sie öffentliche Aufgaben wahrnehmen, oder
4. die Durchführung eines laufenden Gerichtsverfahrens, den Anspruch einer Person auf ein faires Verfahren oder die Durchführung strafrechtlicher, ordnungswidrigkeitenrechtlicher oder disziplinarrechtlicher Ermittlungen.

Geologische Daten dürfen entgegen Satz 1 öffentlich bereitgestellt werden, wenn das öffentliche Interesse an der öffentlichen Bereitstellung die nachteiligen Auswirkungen überwiegt. Die Entscheidung, ob und inwieweit die öffentliche Bereitstellung der geologischen Daten nachteilige Auswirkungen gemäß Satz 1 hat oder ob nach Satz 2 das öffentliche Interesse an der Bereitstellung überwiegt, trifft die zuständige Behörde im Benehmen mit derjenigen Behörde oder Person nach § 3 Absatz 4 Satz 1 Nummer 2, deren Aufgabenbereich durch die geologischen Daten nach den Sätzen 1 und 2 betroffen ist.

§ 32 Schutz sonstiger Belange bei verbundenen Daten

(1) Abgesehen von den nach diesem Gesetz oder auf Grund dieses Gesetzes öffentlich bereitzustellenden geologischen Daten dürfen die folgenden mit diesen verbundenen weiteren Daten nicht öffentlich bereitgestellt werden:

1. personenbezogene Daten,
2. Daten, soweit der Schutz von Betriebs- und Geschäftsgeheimnissen entgegensteht,
3. Daten, soweit der Schutz geistigen Eigentums entgegensteht, sowie
4. Informationen, die dem Steuergeheimnis oder dem Statistikgeheimnis unterliegen.

Die Daten werden entgegen Satz 1 öffentlich bereitgestellt, wenn das öffentliche Interesse an der öffentlichen Bereitstellung überwiegt. Die Entscheidung, welche Daten als verbundene Daten gemäß Satz 1 nicht bereitgestellt werden oder ob nach Satz 2 das öffentliche Interesse an der Bereitstellung der verbundenen Daten überwiegt, trifft die zuständige Behörde.

(2) Bei Vorliegen eines öffentlichen Interesses an der öffentlichen Bereitstellung ist der Schutz von Eigennamen der mit der geologischen Untersuchung beauftragten Personen bei geologischen Daten in analoger Form in der Regel nachrangig, wenn die Unkenntlichmachung des Namens für die mit der Untersuchung beauftragten Personen wegen Zeitablaufs voraussichtlich nicht mehr von Interesse ist.

Abschnitt 3
Zurverfügungstellung geologischer Daten zur Erfüllung öffentlicher Aufgaben

§ 33 Zurverfügungstellung geologischer Daten für öffentliche Aufgaben

(1) Die nach § 37 zuständige Behörde stellt die bei ihr vorhandenen geologischen Daten, die zur Erfüllung einer öffentlichen Aufgabe des Bundes oder der Länder, insbesondere zu einem der in § 1 genannten Zwecke, erforderlich sind, der Behörde oder Person nach § 3 Absatz 4 Satz 1 Nummer 2, die für die Erfüllung der öffentlichen Aufgaben des Bundes oder der Länder zuständig ist, auf deren Anfrage hin unentgeltlich zur Verfügung.

(2) Die in Absatz 1 genannten Behörden und Personen stellen die bei ihnen vorhandenen geologischen Daten der nach § 37 zuständigen Behörde für die Erfüllung der Aufgaben nach § 5 auf deren Anfrage hin unentgeltlich zu Verfügung. Die §§ 8 bis 17 bleiben unberührt.

(3) Die Absätze 1 und 2 können auch auf die mit geologischen Daten verbundenen Daten, insbesondere auf technische Daten, die zu einem der in § 1 genannten Zwecke benötigt werden, angewendet werden. Die nach § 37 zuständige Behörde und die in Absatz 1 genannten Behörden und Personen können einander geologische Daten und die mit ihnen verbundenen Daten, die zu einem der in § 1 genannten Zwecke benötigt werden, elektronisch unentgeltlich zur Verfügung stellen, die geologischen Daten und die mit ihnen verbundenen Daten nutzen sowie diese Daten verarbeiten.

(4) Die Pflichten nach den Absätzen 1 und 2 bestehen unabhängig vom Status der Datensicherung und der öffentlichen Bereitstellung der geologischen Daten sowie der sonstigen Rechte Dritter. § 18 Absatz 1 Satz 2 ist entsprechend anzuwenden. Die Daten nach den Absätzen 1 und 2 sind in dem nach dem Geodatenzugangsgesetz oder nach den entsprechenden landesrechtlichen Regelungen festgelegten Format oder, soweit die Daten in diesem Format nicht vorliegen, in ihrem aktuellen Format zur Verfügung zu stellen. Die Zurverfügungstellung kann auch in der Bereitstellung von digitalen Daten mittels einer internetbasierten Einrichtung wie einem Download-Link oder in der Bereitstellung von analogen Daten bestehen.

(5) Über die Erforderlichkeit geologischer Daten nach Absatz 1 setzt sich die nach § 37 zuständige Behörde mit der für die Erfüllung der öffentlichen Aufgabe zuständigen Behörde oder Person nach Absatz 1 ins Benehmen; abweichend hiervon richtet sich die Zurverfügungstellung von Daten für die Zwecke des Standortauswahlverfahrens nach § 12 Absatz 3 Satz 2 des Standortauswahlgesetzes in der jeweils geltenden Fassung.

(6) Die für eine öffentliche Aufgabe zuständige Behörde oder Person nach Absatz 1 gewährleistet die öffentliche Bereitstellung geologischer Daten nach den §§ 18 bis 32 sowie 34 und 35 Absatz 1, wenn die öffentliche Bereitstellung zur Erfüllung einer öffentlichen Aufgabe des Bundes oder der Länder zu den in § 1 genannten Zwecken erforderlich ist, es sei denn, die beteiligten Behörden haben sich einvernehmlich darauf geeinigt, dass die nach § 37 zuständige Behörde die öffentliche Bereitstellung nach den §§ 18 bis 32 sowie 34 und 35 Absatz 1 gewährleistet.

(7) Soweit die geologischen Daten von der Behörde oder Person nach Absatz 1 öffentlich bereitgestellt werden, übermittelt die nach § 37 Absatz 1 zuständige Behörde die Entscheidung über die Datenkategorisierung sowie das Prüfungsergebnis nach den §§ 31 und 32 und nach spezialgesetzlichen Veröffentlichungspflichten mit der Zurverfügungstellung der Daten an die Behörde oder Person nach Absatz 1. Widerspruch und Anfechtungsklage gegen die Entscheidung über die Kategorisierung von geologischen Daten, die für das Standortauswahlverfahren benötigt werden und entscheidungserheblich sind, haben keine aufschiebende Wirkung.

(8) Für geologische Daten, die dem Vorhabenträger am 30. Juni 2020 bereits zur Verfügung gestellt worden sind, reicht die nach § 37 zuständige Behörde die Entscheidung über die Datenkategorisierung und das Prüfungsergebnis nach den §§ 31 und 32 sowie den spezialgesetzlichen Veröffentlichungsfristen innerhalb zweier Monate nach, nachdem der Vorhabenträger nach dem Standortauswahlgesetz ihr für die für das Standortauswahlverfahren benötigten und entscheidungserheblichen Daten einen Vorschlag zur Entscheidung über die Datenkategorisierung unterbreitet hat. Abweichend von § 29 Absatz 2 Satz 2 werden diese Daten nach dem Ablauf von drei Monaten nach dem 30. Juni 2020 öffentlich bereitgestellt.

§ 34 Erweiterte öffentliche Bereitstellung geologischer Daten

(1) Die für die Erfüllung einer öffentlichen Aufgabe des Bundes oder der Länder, insbesondere zu einem der in § 1 genannten Zwecke, zuständige Behörde oder Person nach § 33 Absatz 1 kann, wenn die öffentliche Bereitstellung für die Aufgabenerfüllung erforderlich ist und das öffentliche Interesse an der öffentlichen Bereitstellung gegenüber dem privatrechtlichen Interesse an der Geheimhaltung überwiegt, entscheiden, dass

1. nichtstaatliche Fachdaten nach § 9 vor Ablauf der Fristen nach § 27 Absatz 1 und 2 und § 29 Absatz 2 in Verbindung mit § 27 Absatz 1 und 2 öffentlich bereitgestellt werden sowie
2. nachgeforderte nichtstaatliche Fachdaten nach § 12 entgegen § 28 öffentlich bereitgestellt werden.

Für Verfahren nach den §§ 14 bis 20 des Standortauswahlgesetzes ist in der Regel davon auszugehen, dass die Gründe des Allgemeinwohls für die öffentliche Bereitstellung überwiegen. Bei der Abwägung berücksichtigt die Behörde oder Person nach § 35 Absatz 1 die Erkenntnisse aus der Anhörung nach § 34 Absatz 3.

(2) Die für die Erfüllung einer öffentlichen Aufgabe des Bundes oder der Länder, insbesondere zu einem der in § 1 genannten Zwecke, zuständige Behörde oder Person nach § 33 Absatz 1 kann entscheiden, dass nichtstaatliche Bewertungsdaten nach § 10 entgegen § 28 oder entgegen § 29 Absatz 3 in Verbindung mit § 28 öffentlich bereitgestellt werden, wenn die öffentliche Bereitstellung für die Aufgabenerfüllung erforderlich ist und

1. der Bergbaubetrieb oder das Vorhaben zur Gewinnung von Bodenschätzen oder zur Nutzung des geologischen Untergrunds, das auf Grund anderer Vorschriften genehmigt oder angezeigt worden ist, tatsächlich eingestellt worden ist und das öffentliche Interesse an der öffentlichen Bereitstellung gegenüber dem privatrechtlichen Interesse an der Geheimhaltung überwiegt,
2. nach dem Ablauf von 15 Jahren nach der Übermittlung von Bewertungsdaten kein Bergbaubetrieb auf Grund des Bundesberggesetzes oder kein anderweitiges Vorhaben zur Gewinnung von Bodenschätzen oder zur Nutzung des geologischen Un-

tergrunds errichtet und betrieben wurde und das öffentliche Interesse an der Bereitstellung gegenüber dem privatrechtlichen Interesse an der Geheimhaltung überwiegt oder

3. die Gründe des Allgemeinwohls für die öffentliche Bereitstellung aus anderen Gründen gegenüber dem privatrechtlichen Interesse an der Geheimhaltung wesentlich überwiegen.

Für Verfahren nach den §§ 14 bis 20 des Standortauswahlgesetzes ist in der Regel davon auszugehen, dass die Gründe des Allgemeinwohls für die öffentliche Bereitstellung wesentlich überwiegen. Nach Ablauf von 30 Jahren nach deren Übermittlung werden nichtstaatliche Bewertungsdaten öffentlich bereitgestellt, wenn sie für das Standortauswahlverfahren benötigt werden und entscheidungserheblich sind und ein Bergbaubetrieb auf Grund des Bundesberggesetzes oder ein anderweitiges Vorhaben zur Gewinnung von Bodenschätzen oder zur Nutzung des geologischen Untergrunds zum Zeitpunkt der öffentlichen Bereitstellung nicht im Antragsverfahren ist, keine Genehmigung hat, nicht betrieben wird oder eingestellt worden ist und keine überwiegenden Investitionsinteressen entgegenstehen. Bei der Abwägung nach Satz 1 und 2 sowie der Entscheidung über die Erforderlichkeit nichtstaatlicher Bewertungsdaten für das Standortauswahlverfahren nach Satz 3 berücksichtigt die Behörde oder Person nach § 35 Absatz 1 die Erkenntnisse aus der Anhörung nach § 34 Absatz 3.

(3) Vor der Entscheidung über die öffentliche Bereitstellung nach den Absätzen 1, 2 oder § 35 Absatz 1 sind die betroffenen, nach § 14 Satz 1 verpflichteten Personen anzuhören. Die Entscheidung nach den Absätzen 1 und 2 oder § 35 Absatz 1 ist der Person nach § 14 Satz 1, die angehört wurde, sechs Wochen vor der öffentlichen Bereitstellung zuzustellen. Dabei ist die Erforderlichkeit der öffentlichen Bereitstellung für die Aufgabenerfüllung schriftlich oder elektronisch darzulegen. Die nach § 37 zuständige Behörde ist über die öffentliche Bereitstellung nach den Absätzen 1 und 2 oder § 35 Absatz 1 zu informieren; sie unterstützt die Behörde oder Person nach § 33 Absatz 1 bei der Ermittlung der nach Satz 1 anzuhörenden Personen, soweit ihr diese bekannt sind.

§ 35 Erweiterte öffentliche Bereitstellung geologischer Daten im Standortauswahlverfahren; wissenschaftliche Beratung zur Einsicht in nicht öffentlich bereitgestellte Daten, Bereitstellung und Einsicht im Datenraum

(1) Bei geologischen Daten nach § 34 Absatz 1 und 2, die für das Standortauswahlverfahren benötigt werden und entscheidungserheblich sind, entscheiden der Vorhabenträger nach dem Standortauswahlgesetz und das Bundesamt für die Sicherheit der nuklearen Entsorgung jeweils im Rahmen ihrer Zuständigkeit über die öffentliche Bereitstellung. Der Bund überträgt dem Vorhabenträger nach dem Standortauswahlgesetz durch Beleihung die hoheitliche Befugnis, Entscheidungen nach § 34 Absatz 1 und 2 zu treffen; § 9a Absatz 3 Satz 3 bis 5, 8 und 11 des Atomgesetzes ist entsprechend anzuwenden.

(2) Widerspruch und Anfechtungsklage gegen die Entscheidung zur öffentlichen Bereitstellung geologischer Daten nach Absatz 1 in Verbindung mit § 34 Absatz 1 oder 2, die im Standortauswahlverfahren benötigt werden und entscheidungserheblich sind, haben keine aufschiebende Wirkung. Mit der Zustellung des Antrags auf Anordnung der aufschiebenden Wirkung des Widerspruchs gegen die Entscheidung nach Absatz 1 in Verbindung mit § 34 Absatz 1 oder 2, der innerhalb der Frist des § 34 Absatz 3 Satz 2 gestellt worden ist, stellt der Vorhabenträger nach dem Standortauswahlgesetz die von dem Antrag erfassten geologischen Daten in dem nach Absatz 5 einzurichtenden Datenraum bereit, bis der Antrag nach §

80 Absatz 5 der Verwaltungsgerichtsordnung rechtskräftig abgelehnt oder die Klage im Hauptsacheverfahren rechtskräftig abgewiesen wird.

(3) Für staatliche 3D-Modelle des Untergrunds, die über nichtstaatliche Fachdaten oder nichtstaatliche Bewertungsdaten Aufschluss geben könnten, ist davon auszugehen, dass die Voraussetzungen des § 34 Absatz 1 und 2 erfüllt sind, wenn die 3D-Modelle für das Standortauswahlverfahren benötigt werden und entscheidungserheblich sind. Dies gilt auch für die von dem Vorhabenträger nach dem Standortauswahlgesetz zur Erstellung oder Spezifizierung der staatlichen 3D-Modelle herangezogenen Schichtenverzeichnisse nach § 9 Absatz 1 Satz 1 Nummer 3 Buchstabe a. In den Fällen der Sätze 1 und 2 ist § 34 Absatz 3 nicht anzuwenden.

(4) Das Nationale Begleitgremium kann sich nach § 8 Absatz 4 Satz 3 zweiter Halbsatz des Standortauswahlgesetzes im Hinblick auf geologische Daten, die nach Absatz 1 für das Standortauswahlverfahren benötigt werden und entscheidungserheblich sind und die nach diesem Gesetz nicht oder noch nicht öffentlich bereitgestellt werden, wissenschaftlich beraten lassen und hierfür bis zu fünf externe Sachverständige mit der Einsicht in die Daten beauftragen. Die Beauftragten nach Satz 1 müssen über die für die wissenschaftliche Beratung notwendige fachliche Expertise verfügen und dürfen keine eigenen wirtschaftlichen Interessen oder wirtschaftliche Interessen der nach § 14 Satz 1 verpflichteten Personen verfolgen. Die Beauftragten unterstützen das Nationale Begleitgremium bei der Begleitung des Standortauswahlverfahrens, indem sie die geologischen Daten nach Satz 1 sichten, bewerten und gegenüber dem Nationalen Begleitgremium Stellungnahmen abgeben, ob diese Daten im Standortauswahlverfahren zutreffend bewertet und sachgerecht berücksichtigt worden sind. Das Nationale Begleitgremium kann die Beauftragten für weitere Fragestellungen zur Berücksichtigung geologischer Daten im Standortauswahlverfahren hinzuziehen. Die Regelungen des Standortauswahlgesetzes bleiben unberührt.

(5) Der Vorhabenträger nach dem Standortauswahlgesetz richtet einen gesonderten Datenraum für die geologischen Daten nach Absatz 4 Satz 1 ein und stellt insbesondere die geologischen Daten nach Absatz 4 Satz 1 sowie die für das Standortauswahlverfahren nicht entscheidungserheblichen Daten, die bei ihm vorhanden sind, dort bereit. Die Beauftragten nach Absatz 4 Satz 1 haben Zugang zu allen Daten, die in dem gesonderten Datenraum bereitgestellt werden. Die Beauftragten nach Absatz 4 Satz 1 sind zur Geheimhaltung über die Inhalte der geologischen Daten im gesonderten Datenraum, die nach diesem Gesetz nicht oder noch nicht öffentlich bereitgestellt werden, verpflichtet und dürfen die Ergebnisse der Dateneinsicht nur für die Aufgaben nach Absatz 4 Satz 3 und 4 nutzen. Der Vorhabenträger gewährleistet die Sicherung der im Datenraum bereitgestellten Daten vor dem unberechtigten Zugriff Dritter nach dem Stand der Technik.

Kapitel 5
Schlussbestimmungen

§ 36 Anordnungsbefugnis

Die zuständige Behörde kann im Einzelfall Anordnungen treffen, die zur Durchführung dieses Gesetzes und zur Durchführung der auf Grund dieses Gesetzes erlassenen Rechtsverordnungen erforderlich sind.

§ 37 Zuständige Behörden; Überwachung

(1) Die Zuständigkeit für den Vollzug dieses Gesetzes richtet sich vorbehaltlich der Absätze 2 und 3 nach Landesrecht.

(2) Für die Überwachung der Einhaltung dieses Gesetzes sind

1. § 13 Absatz 1 des Umweltinformationsgesetzes in der jeweils geltenden Fassung oder
2. Bestimmungen der Länder, die inhaltsgleich zu Nummer 1 sind,

entsprechend anzuwenden.

(3) Die für den Vollzug dieses Gesetzes im Bereich der ausschließlichen Wirtschaftszone und des Festlandsockels zuständige Behörde ist die Bundesanstalt für Geowissenschaften und Rohstoffe.

§ 38 Verordnungsermächtigung; Ausschluss abweichenden Landesrechts

(1) Die Landesregierungen können durch Rechtsverordnung Folgendes bestimmen:

1. die Festlegung, welche der in § 2 Absatz 5 Satz 1 genannten Vorschriften auf die vom Anwendungsbereich dieses Gesetzes ausgeschlossenen Daten nach § 2 Absatz 3 Satz 2 und 3 oder § 2 Absatz 4 Satz 2 anzuwenden sind,
2. die Festlegung, dass sich der Anwendungsbereich des Gesetzes nicht auf geologische Daten aus den in § 2 Absatz 5 Satz 2 genannten Untersuchungen erstreckt,
3. die näheren Anforderungen an die Anzeige und Übermittlung geologischer Daten nach den §§ 8 bis 10 einschließlich der Konkretisierung der nach § 14 Satz 1 verpflichteten Personen,
4. die Tatsachen, die eine eingeschränkte Anzeige- und Übermittlungspflicht begründen, sowie die näheren Anforderungen an die eingeschränkte Anzeige- und Übermittlungspflicht nach § 11 Absatz 1,
5. die näheren Anforderungen an die Vorhaltung geologischer Daten bei einer nach § 14 Satz 1 Nummer 1, 2 und 3 verpflichteten Behörde oder Person nach § 11 Absatz 2 sowie die näheren Anforderungen an die Befreiung einer nach § 14 Satz 1 Nummer 1, 2 und 3 verpflichteten Behörde oder Person nach § 11 Absatz 3,
6. die näheren Anforderungen an die Entledigung und Löschung von Proben und Daten nach § 13,
7. die näheren Anforderungen an die interoperablen Formate geologischer Daten nach § 16 Absatz 1 sowie die näheren Anforderungen an die elektronische Übermittlung nach § 16 Absatz 2,
8. die näheren Anforderungen an das Verfahren und die Formvorschriften für die Kennzeichnung von Nachweisdaten, Fachdaten und Bewertungsdaten nach § 17 Absatz 1,
9. die näheren Anforderungen an die öffentliche Bereitstellung geologischer Daten nach § 19 Absatz 2 oder an den Zugang zu öffentlich bereitgestellten geologischen Daten nach § 20,

10. die näheren Anforderungen an die Zurverfügungstellung geologischer Daten zur Erfüllung öffentlicher Aufgaben nach § 33, insbesondere zu den in § 1 genannten Zwecken.

(2) Von den in diesem Gesetz getroffenen Regelungen des Verwaltungsverfahrens kann durch Landesrecht nicht abgewichen werden.

§ 39 Bußgeldvorschriften

(1) Ordnungswidrig handelt, wer im Rahmen einer gewerblichen Tätigkeit vorsätzlich oder fahrlässig

1. entgegen § 8 Satz 1, auch in Verbindung mit einer Rechtsverordnung nach § 38 Absatz 1 Nummer 3, eine Anzeige nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig erstattet,
2. entgegen § 9 Absatz 1 Satz 1 oder § 10 Absatz 1, jeweils auch in Verbindung mit einer Rechtsverordnung nach § 38 Absatz 1 Nummer 3, dort genannte Daten nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig übermittelt,
3. einer vollziehbaren Anordnung nach § 9 Absatz 2 Satz 1, § 10 Absatz 2 Satz 1 oder Absatz 3 Satz 1 oder § 12 zuwiderhandelt oder
4. entgegen § 13 Satz 1 oder 2, jeweils auch in Verbindung mit einer Rechtsverordnung nach § 38 Absatz 1 Nummer 6, eine dort genannte Probe oder dort genannte Daten nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig anbietet.

(2) Die Ordnungswidrigkeit kann mit einer Geldbuße bis zu dreißigtausend Euro geahndet werden.

§ 40 Inkrafttreten, Außerkrafttreten

(1) Dieses Gesetz tritt am Tag nach der Verkündung in Kraft.

(2) Gleichzeitig treten das Lagerstättengesetz in der im Bundesgesetzblatt Teil III, Gliederungsnummer 750-1, veröffentlichten bereinigten Fassung, das zuletzt durch Artikel 22 des Gesetzes vom 10. November 2001 (BGBl. I S. 2992) geändert worden ist, und die Verordnung zur Ausführung des Gesetzes über die Durchforschung des Reichsgebiets nach nutzbaren Lagerstätten (Lagerstättengesetz) in der im Bundesgesetzblatt Teil III, Gliederungsnummer 750-1-1, veröffentlichten bereinigten Fassung außer Kraft.

(3) Das Gesetz wird zum 31. Dezember des Jahres evaluiert, in dem sich dessen Inkrafttreten zum vierten Mal jährt.

Gesetz über die Verkündung von Gesetzen und Rechtsverordnungen und über Bekanntmachungen (Verkündungs- und Bekanntmachungsgesetz – VkBkmG)

Abschnitt 1
Allgemeine Vorschriften

§ 1 Verkündungs- und Bekanntmachungsorgane des Bundes

(1) Das Bundesgesetzblatt ist das Verkündungsorgan des Bundes für Gesetze und Rechtsverordnungen. Das Bundesgesetzblatt ist außerdem das Bekanntmachungsorgan des Bundes, wenn durch Rechtsvorschrift die amtliche Bekanntmachung im Bundesgesetzblatt vorgeschrieben ist.

(2) Der Bundesanzeiger ist ein Bekanntmachungsorgan des Bundes. Er hat einen amtlichen Teil. Dieser ist bestimmt für

1. andere als die in Absatz 1 Satz 2 genannten amtlichen Bekanntmachungen der Behörden des Bundes, einschließlich Ausschreibungen und Hinweise, und
2. amtliche Bekanntmachungen der Behörden der Länder, sofern die Bekanntmachung im amtlichen Teil des Bundesanzeigers durch Bundesgesetz oder Rechtsverordnung des Bundes vorgeschrieben ist.

Der Bundesanzeiger kann weitere Teile für andere Bekanntmachungen enthalten.

(3) Das Bundesgesetzblatt und der Bundesanzeiger werden vom Bundesministerium der Justiz herausgegeben.

§ 2 Ausgabe und dauerhafte Bereithaltung im Internet

(1) Das Bundesgesetzblatt wird vom Bundesamt für Justiz auf der Internetseite www.recht.bund.de ausgegeben. Es wird dort vollständig und dauerhaft bereitgehalten.

(2) Der Bundesanzeiger wird vom Betreiber des Bundesanzeigers auf der Internetseite www.bundesanzeiger.de ausgegeben. Er wird dort vollständig und dauerhaft bereitgehalten.

(3) § 7 des Datennutzungsgesetzes vom 16. Juli 2021 (BGBl. I S. 2941, 2942, 4114) in der jeweils geltenden Fassung ist anzuwenden.

§ 3 Verkündung und amtliche Bekanntmachung

(1) Die Verkündung von Gesetzen und Rechtsverordnungen erfolgt jeweils durch die Ausgabe einer Nummer des Bundesgesetzblatts. Amtliche Bekanntmachungen im Bundesgesetzblatt erfolgen jeweils durch die Ausgabe einer Nummer des Bundesgesetzblatts. Jede Nummer des Bundesgesetzblatts trägt das Datum ihrer Ausgabe.

(2) Die amtlichen Bekanntmachungen im Bundesanzeiger erfolgen jeweils durch Ausgabe einer Nummer des amtlichen Teils des Bundesanzeigers. Absatz 1 Satz 3 gilt entsprechend.

§ 4 Freier Zugang

(1) Das Bundesgesetzblatt ist jederzeit frei zugänglich. Es kann unentgeltlich gelesen, ausgedruckt, gespeichert und verwertet werden.

(2) Der amtliche Teil des Bundesanzeigers ist jederzeit frei zugänglich. Er kann unentgeltlich gelesen, ausgedruckt und gespeichert werden.

§ 5 Benachrichtigungsdienste

Für das Bundesgesetzblatt ist ein unentgeltlicher elektronischer Benachrichtigungsdienst bereitzustellen, der über jede Ausgabe einer neuen Nummer und deren Inhalt informiert. Gleiches gilt für den amtlichen Teil des Bundesanzeigers.

§ 6 Änderungsverbot; Löschung personenbezogener Daten; Berichtigungen

(1) Änderungen des Bundesgesetzblatts auf der Internetseite www.recht.bund.de und des amtlichen Teils des Bundesanzeigers auf der Internetseite www.bundesanzeiger.de sind vorbehaltlich des Absatzes 2 unzulässig.

(2) Müssen personenbezogene Daten aus Gründen ihres Schutzes gelöscht werden, so werden in der betreffenden Nummer des Bundesgesetzblatts oder des amtlichen Teils des Bundesanzeigers diese Daten unkenntlich gemacht und wird ein Hinweis auf Datum und Grund der Löschung angebracht.

(3) Die Berichtigung von offenbaren Unrichtigkeiten im Bundesgesetzblatt ist dort bekannt zu machen. Satz 1 gilt für den Bundesanzeiger entsprechend.

§ 7 Sicherung der Echtheit und Unverfälschtheit

(1) Jede Nummer des Bundesgesetzblatts, die nach § 3 Absatz 1 oder nach § 8 Absatz 1 ausgegeben wird, und jede Nummer des amtlichen Teils des Bundesanzeigers trägt ein qualifiziertes elektronisches Siegel nach Artikel 3 Nummer 27 der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG (ABl. L 257 vom 28.8.2014, S. 73; L 23 vom 29.1.2015, S. 19; L 155 vom 14.6.2016, S. 44).

(2) Wird die Urschrift eines Gesetzes elektronisch zur Gegenzeichnung und Ausfertigung vorgelegt, so erfolgen diese jeweils durch qualifizierte elektronische Signatur nach Artikel 3 Nummer 12 der Verordnung (EU) Nr. 910/2014. Gleiches gilt auch für die Ausfertigung von Rechtsverordnungen und amtlichen Bekanntmachungen.

Abschnitt 2
Verkündung und Bekanntmachung in besonderen Fällen

§ 8 Ersatzverkündungen und -bekanntmachungen des Bundesgesetzblatts

(1) Ist die Ausgabe einer Nummer des Bundesgesetzblatts auf der Internetseite www.recht.bund.de nicht nur kurzfristig unmöglich, so erfolgt die Verkündung oder amtliche Bekanntmachung durch Ausgabe der Nummer des Bundesgesetzblatts auf der Internetseite www.bundesanzeiger.de. Auf Anordnung des Bundesamtes für Justiz hat der Betreiber des Bundesanzeigers diese Nummer des Bundesgesetzblatts auf der Internetseite www.bundesanzeiger.de öffentlich bereitzustellen und sie dort bis zur nachträglichen Bereitstellung auf der Internetseite www.recht.bund.de bereitzuhalten.

(2) Ist die Ausgabe einer Nummer des Bundesgesetzblatts auch auf der Internetseite www.bundesanzeiger.de nicht nur kurzfristig unmöglich, so erfolgt die Verkündung oder amtliche Bekanntmachung durch Ausgabe einer gedruckten Nummer des Bundesgesetzblatts. Die gedruckte Nummer des Bundesgesetzblatts ist nach einem zuvor vom Bundesministerium der Justiz im Bundesanzeiger bekannt gemachten Verteiler an Bibliotheken und Behörden auszugeben.

§ 9 Vereinfachte Verkündungen und vereinfachte amtliche Bekanntmachungen

Ist die Ausgabe einer Nummer des Bundesgesetzblatts weder nach § 3 Absatz 1 noch nach § 8 rechtzeitig möglich, so findet sie in den folgenden Fällen als vereinfachte Verkündung oder vereinfachte amtliche Bekanntmachung statt:

1. Verkündung der Feststellung des Verteidigungsfalles (Artikel 115a Absatz 3 Satz 2 des Grundgesetzes),
2. Bekanntgabe des Zeitpunktes des Eintritts des Verteidigungsfalles (Artikel 115a Absatz 4 Satz 2 des Grundgesetzes),
3. Verkündung von Bundesgesetzen im Verteidigungsfall (Artikel 115d Absatz 3 des Grundgesetzes),
4. Verkündung von Rechtsverordnungen des Bundes im Verteidigungsfall und in den Fällen des Artikels 80a Absatz 1 und 3 des Grundgesetzes,
5. Bekanntmachung von Beschlüssen des Bundestages nach Artikel 80a Absatz 1 des Grundgesetzes und
6. Bekanntmachung von Beschlüssen internationaler Organe im Rahmen eines Bündnisvertrages und der Zustimmung der Bundesregierung bei der Anwendung des Artikels 80a Absatz 3 Satz 1 des Grundgesetzes.

§ 10 Arten der vereinfachten Verkündung und der vereinfachten amtlichen Bekanntmachung

(1) Eine vereinfachte Verkündung oder vereinfachte amtliche Bekanntmachung nach § 9 erfolgt durch die Ausgabe der Nummer des Bundesgesetzblatts

1. im Rundfunk oder Fernsehen,
2. in der gedruckten oder digitalen Tagespresse,
3. als Aushang an den für amtliche Bekanntmachungen vorgesehenen Stellen bei den Verwaltungen der Gemeinden und Landkreise oder durch eine andere amtliche Bekanntmachung für das Gebiet einer Gemeinde oder eines Landkreises oder
4. in sozialen Netzwerken über die vom Presse- und Informationsamt der Bundesregierung betriebenen Profile.

(2) Die für die vereinfachte Verkündung oder vereinfachte amtliche Bekanntmachung zuständige Stelle hat den Zeitpunkt und den Wortlaut der Ausgabe der Nummer des Bundesgesetzblatts zu dokumentieren.

(3) Werden mehrere der in Absatz 1 genannten Medien genutzt, so wird die Verkündung oder amtliche Bekanntmachung durch diejenige Ausgabe bewirkt, die zuerst erfolgt ist.

(4) Die Befugnis der Bundespräsidentin oder des Bundespräsidenten, für ihren oder seinen Zuständigkeitsbereich andere Arten der vereinfachten Verkündung oder der vereinfachten amtlichen Bekanntmachung vorzusehen, bleibt unberührt.

§ 11 Duldungs- und Mitwirkungspflichten; Ausschluss der aufschiebenden Wirkung des Widerspruchs und der Klage

(1) Die für die Verkündung oder die amtliche Bekanntmachung zuständige Stelle kann

1. anordnen, dass der Betreiber eines sozialen Netzwerks eine vereinfachte Verkündung oder eine vereinfachte amtliche Bekanntmachung (§§ 9 und 10 Absatz 1 Nummer 4) duldet,
2. dem Betreiber eines sozialen Netzwerks untersagen, die vereinfachte Verkündung oder vereinfachte amtliche Bekanntmachung zu löschen oder ihre öffentliche Sichtbarkeit einzuschränken,
3. anordnen, dass der Betreiber eines sozialen Netzwerks einen Hinweis auf eine bereits erfolgte vereinfachte Verkündung oder vereinfachte amtliche Bekanntmachung duldet.

(2) Wer eines der in § 10 Absatz 1 Nummer 1 und 2 genannten Medien betreibt, hat auf Anordnung der für die Verkündung oder amtliche Bekanntmachung zuständigen Stelle eine vereinfachte Verkündung oder vereinfachte amtliche Bekanntmachung unverzüglich vorzunehmen. Die zuständige Stelle kann in der Anordnung auch Folgendes bestimmen:

1. bei vereinfachter Verkündung oder vereinfachter amtlicher Bekanntmachung in der digitalen Tagespresse (§ 10 Absatz 1 Nummer 2):
   a) den Zeitpunkt der Verkündung oder amtlichen Bekanntmachung und
   b) die Dauer, für die der Wortlaut der Verkündung oder Bekanntmachung auf der Startseite des jeweiligen Internetauftritts angezeigt werden muss, sowie
2. bei vereinfachter Verkündung oder vereinfachter amtlicher Bekanntmachung im Rundfunk oder Fernsehen (§ 10 Absatz 1 Nummer 1):
   a) den Zeitpunkt der Verkündung oder Bekanntmachung und
   b) die Anzahl der zu sendenden Wiederholungen.

(3) Ist eine vereinfachte Verkündung oder vereinfachte amtliche Bekanntmachung bereits erfolgt, so kann die zuständige Stelle gegenüber Betreibern von Medien nach § 10 Absatz 1 Nummer 1 und 2 anordnen, auf diese Verkündung oder amtliche Bekanntmachung hinzuweisen.

(4) Verantwortlich für die Umsetzung der Anordnungen nach den Absätzen 2 und 3 sind

1. bei Rundfunkanstalten die Intendantinnen und Intendanten,
2. in Verlagsunternehmen die Verlegerinnen und Verleger, die Herausgeberinnen und Herausgeber sowie die Chefredakteurinnen und Chefredakteure.

(5) Widerspruch und Anfechtungsklage gegen Anordnungen nach den Absätzen 1 bis 3 haben keine aufschiebende Wirkung.

§ 12 Nachträgliche Bereitstellung

Sobald die Ausgabe des Bundesgesetzblatts auf der Internetseite www.recht.bund.de wieder möglich ist, werden dort die nach den §§ 8 und 9 ausgegebenen Nummern des Bundesgesetzblatts unverzüglich bereitgestellt.

§ 13 Aufwendungsersatz

Wer zur Ausführung folgender Anordnungen verpflichtet wurde, kann von der Bundesrepublik Deutschland nach Maßgabe des § 670 des Bürgerlichen Gesetzbuchs den Ersatz der Aufwendungen verlangen:

1. zur Durchführung der Ersatzverkündung oder -bekanntmachung im Bundesgesetzblatt (§ 8 Absatz 1 Satz 2),
2. zur Durchführung der vereinfachten Verkündung oder vereinfachten amtlichen Bekanntmachung (§ 11 Absatz 2 Satz 1) oder
3. zu einem Hinweis auf eine vereinfachte Verkündung oder vereinfachte amtliche Bekanntmachung (§ 11 Absatz 3).

§ 14 Ersatzbekanntmachungen des Bundesanzeigers

(1) Ist die Ausgabe des Bundesanzeigers auf der Internetseite www.bundesanzeiger.de nicht nur kurzfristig unmöglich, so erfolgen Bekanntmachungen durch Ausgabe des Bundesanzeigers in gedruckter Form. Die gedruckte Ausgabe des Bundesanzeigers ist nach einem zuvor vom Bundesministerium der Justiz im Bundesanzeiger bekannt gemachten Verteiler an Bibliotheken und Behörden auszugeben. Bekanntmachungen in weiteren Teilen des Bundesanzeigers (§ 1 Absatz 2 Satz 4) können in den Fällen des Satzes 1 auch in einer anderen dauerhaft allgemein zugänglichen Form erfolgen.

(2) Im Fall der Ersatzbekanntmachung nach Absatz 1 Satz 1 ist, sofern diese nicht nach Absatz 1 Satz 3 erfolgt, im Bundesgesetzblatt unverzüglich bekannt zu machen,

1. dass der Bundesanzeiger in gedruckter Form ausgegeben wird,
2. wann die Unmöglichkeit eingetreten ist, den Bundesanzeiger auf der Internetseite www.bundesanzeiger.de auszugeben, und
3. an welche Bibliotheken und Behörden der gedruckte Bundesanzeiger ausgegeben wird.

(3) Sobald die Ausgabe des Bundesanzeigers auf der Internetseite www.bundesanzeiger.de wieder möglich ist, werden dort die zuvor gedruckten Bekanntmachungen (Absatz 1 Satz 1) und sonstigen Ersatzbekanntmachungen (Absatz 1 Satz 3) unverzüglich elektronisch bereitgestellt.

Abschnitt 3
Bekanntmachungen von Beschlüssen nach Artikel 80a des Grundgesetzes

§ 15 Zuständige Stelle für die amtliche Bekanntmachung von Beschlüssen nach Artikel 80a des Grundgesetzes

Zuständige Stelle für die amtliche Bekanntmachung der Beschlüsse nach Artikel 80a Absatz 1 und 3 Satz 1 des Grundgesetzes ist die Bundesregierung oder ein von ihr bestimmtes Mitglied der Bundesregierung.

§ 16 Verfahren der amtlichen Bekanntmachung von Beschlüssen nach Artikel 80a des Grundgesetzes

Beschlüsse nach Artikel 80a Absatz 1 und 3 Satz 1 des Grundgesetzes sind unverzüglich im Bundesgesetzblatt bekannt zu machen. In der amtlichen Bekanntmachung ist der Zeitpunkt der Beschlussfassung anzugeben. Beschlüsse internationaler Organe nach Artikel 80a Absatz 3 Satz 1 des Grundgesetzes müssen nicht in ihrem vollen Wortlaut, jedoch zusammen mit der zugehörigen Zustimmung der Bundesregierung in einem Umfang bekannt gemacht werden, aus dem sich eindeutig ergibt, welche Rechtsvorschriften nach Maßgabe dieser Beschlüsse anwendbar sind. Die anwendbaren Rechtsvorschriften sind jeweils genau zu bezeichnen.

Abschnitt 4
Archivierung

§ 17 Dauerhafte Aufbewahrung

(1) Jede Nummer des Bundesgesetzblatts ist zusammen mit einem Nachweis über den Verkündungs- oder Bekanntmachungszeitpunkt zur dauerhaften Aufbewahrung an das digitale Zwischenarchiv (nach § 8 Absatz 1 Satz 2 des Bundesarchivgesetzes) abzugeben. Im Falle des § 8 Absatz 2 Satz 1 ist die gedruckte Nummer des Bundesgesetzblatts zu digitalisieren sowie mit einem qualifizierten Siegel gemäß § 7 Absatz 1 zu versehen und in dieser Form zusammen mit einem Nachweis über den Verkündungs- oder Bekanntmachungszeitpunkt zur dauerhaften Aufbewahrung an das digitale Zwischenarchiv abzugeben. Im Falle des § 9 sind die Dokumente nach § 10 Absatz 2 zu digitalisieren sowie mit einem qualifizierten Siegel gemäß § 7 Absatz 1 zu versehen und zur dauerhaften Aufbewahrung an das digitale Zwischenarchiv abzugeben. In den Fällen des § 12 ist auch die auf der Internetseite www.recht.bund.de bereitgestellte Nummer des Bundesgesetzblatts, sofern noch nicht geschehen, mit einem qualifizierten Siegel gemäß § 7 Absatz 1 zu versehen und zusammen mit einem Nachweis über den Bereitstellungszeitpunkt zur dauerhaften Aufbewahrung an das digitale Zwischenarchiv abzugeben.

(2) Elektronisch ausgefertigte Urschriften der im Bundesgesetzblatt vorzunehmenden Verkündungen und amtlichen Bekanntmachungen sind zusammen mit der zugehörigen Nummer des Bundesgesetzblatts zur dauerhaften Aufbewahrung an das digitale Zwischenarchiv abzugeben.

(3) Jede Nummer des amtlichen Teils des Bundesanzeigers ist zusammen mit einem Nachweis über den Bekanntmachungszeitpunkt zur dauerhaften Aufbewahrung an das digitale Zwischenarchiv abzugeben. Im Falle des § 14 Absatz 1 Satz 1 ist die gedruckte Nummer des amtlichen Teils des Bundesanzeigers zu digitalisieren sowie mit einem qualifizierten Siegel

gemäß § 7 Absatz 1 zu versehen und in dieser Form zusammen mit einem Nachweis über den Bekanntmachungszeitpunkt zur dauerhaften Aufbewahrung an das digitale Zwischenarchiv abzugeben. Im Falle des § 14 Absatz 3 ist auch die auf der Internetseite www.bundesanzeiger.de bereitgestellte Nummer des amtlichen Teils des Bundesanzeigers, sofern noch nicht geschehen, mit einem qualifizierten Siegel gemäß § 7 Absatz 1 zu versehen und zusammen mit einem Nachweis über den Bereitstellungszeitpunkt zur dauerhaften Aufbewahrung an das digitale Zwischenarchiv abzugeben.

§ 18 Erhaltung des Beweiswerts

Enthalten die nach § 17 Absatz 1 und 3 dauerhaft aufzubewahrenden Dokumente ein qualifiziertes elektronisches Siegel, eine qualifizierte elektronische Signatur oder einen qualifizierten elektronischen Zeitstempel, sind sie im digitalen Zwischenarchiv durch geeignete Maßnahmen nach dem Stand der Technik neu zu schützen, bevor der Sicherheitswert des vorhandenen Siegels, der vorhandenen Signatur oder des vorhandenen Zeitstempels durch Zeitablauf geringer wird und ein nach dem Stand der Technik angemessenes Schutzniveau nicht mehr gewährleistet ist.

Abschnitt 5
Straf- und Bußgeldvorschriften

§ 19 Strafvorschriften

Mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe wird bestraft, wer einer vollziehbaren Anordnung nach § 11 Absatz 1 Nummer 1 oder 2 oder Absatz 2 Satz 1 zuwiderhandelt.

§ 20 Bußgeldvorschriften

(1) Ordnungswidrig handelt, wer eine in § 19 bezeichnete Handlung fahrlässig begeht.

(2) Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig einer vollziehbaren Anordnung nach § 11 Absatz 1 Nummer 3 oder Absatz 3 zuwiderhandelt.

(3) Die Ordnungswidrigkeit kann mit einer Geldbuße bis zu hunderttausend Euro geahndet werden.

VERORDNUNG (EU) 2022/868 DES EUROPÄISCHEN PARLAMENTS UND DES RATES

vom 30. Mai 2022

über europäische Daten-Governance und zur Änderung der Verordnung (EU) 2018/1724 (Daten-Governance-Rechtsakt)

(Text von Bedeutung für den EWR)

Inhaltsübersicht

KAPITEL IV
Datenaltruismus

KAPITEL V
Zuständige Behörden und Verfahrensvorschriften

KAPITEL VI
Europäischer Dateninnovationsrat

KAPITEL VII
Internationaler Zugang und internationale Übertragung

KAPITEL VIII
Delegierung und Ausschussverfahren

KAPITEL IX
Schluss- und Übergangsbestimmungen

[Vom Abdruck der Erwägungsgründe wurde abgesehen]

KAPITEL I
Allgemeine Bestimmungen

Artikel 1
Gegenstand und Anwendungsbereich

(1) In dieser Verordnung wird Folgendes festgelegt:

a) Bedingungen für die Weiterverwendung von Daten bestimmter Datenkategorien, die im Besitz öffentlicher Stellen sind, innerhalb der Union;

b) ein Anmelde- und Aufsichtsrahmen für die Erbringung von Datenvermittlungsdiensten;

c) ein Rahmen für die freiwillige Eintragung von Einrichtungen, die für altruistische Zwecke zur Verfügung gestellte Daten erheben und verarbeiten und

d) ein Rahmen für die Einsetzung eines Europäischen Dateninnovationsrats.

(2) Diese Verordnung begründet weder eine Verpflichtung für öffentliche Stellen, die Weiterverwendung von Daten zu erlauben, noch befreit sie öffentliche Stellen von ihren Geheimhaltungspflichten nach dem Unionsrecht oder dem nationalen Recht.

Von dieser Verordnung unberührt bleiben

a) besondere Bestimmungen des Unionsrechts oder des nationalen Rechts über den Zugang zu bestimmten Kategorien von Daten oder deren Weiterverwendung, insbesondere in Bezug auf die Zugangsgewährung zu amtlichen Dokumenten und deren Offenlegung, und

b) die nach dem Unionsrecht oder dem nationalen Recht geltenden Verpflichtungen öffentlicher Stellen, die Weiterverwendung von Daten zu erlauben, oder die Anforderungen in Bezug auf die Verarbeitung nicht personenbezogener Daten.

Müssen öffentliche Stellen, Anbieter von Datenvermittlungsdiensten oder anerkannte Einrichtungen, die Datenaltruismus-Dienste erbringen, aufgrund sektorspezifischen Unionsrechts oder nationalen Rechts bestimmte zusätzliche technische, administrative oder organisatorische Anforderungen einhalten, einschließlich durch Genehmigungs- oder Zertifizierungsverfahren, so finden auch diese Bestimmungen des sektorspezifischen Unionsrechts oder nationalen Rechts Anwendung. Etwaige spezifische zusätzliche Anforderungen müssen nichtdiskriminierend, verhältnismäßig und objektiv gerechtfertigt sein.

(3) Das Unionsrecht und das nationale Recht über den Schutz personenbezogener Daten gelten für alle personenbezogenen Daten, die im Zusammenhang mit der vorliegenden Verordnung verarbeitet werden. Insbesondere gilt die vorliegende Verordnung unbeschadet der

Verordnungen (EU) 2016/679 und (EU) 2018/1725 und der Richtlinien 2002/58/EG und (EU) 2016/680, einschließlich im Hinblick auf die Befugnisse der Aufsichtsbehörden. Im Fall eines Konflikts zwischen der vorliegenden Verordnung und dem Unionsrecht über den Schutz personenbezogener Daten oder dem entsprechend diesem Unionsrecht erlassenen nationalen Recht soll das einschlägige Unionsrecht bzw. das nationale Recht über den Schutz personenbezogener Daten Vorrang haben. Die vorliegende Verordnung schafft keine Rechtsgrundlage für die Verarbeitung personenbezogener Daten, noch berührt es die in den Verordnungen (EU) 2016/679 oder (EU) 2018/1725 oder den Richtlinien 2002/58/EG oder (EU) 2016/680 festgelegten Rechte und Pflichten.

(4) Die Anwendung des Wettbewerbsrechts bleibt von dieser Verordnung unberührt.

(5) Diese Verordnung lässt die Zuständigkeiten der Mitgliedstaaten für Tätigkeiten im Bereich der öffentlichen Sicherheit, der Landesverteidigung und der nationalen Sicherheit unberührt.

Artikel 2
Begriffsbestimmungen

Für die Zwecke dieser Verordnung bezeichnet der Ausdruck

1. „Daten“ jede digitale Darstellung von Handlungen, Tatsachen oder Informationen sowie jede Zusammenstellung solcher Handlungen, Tatsachen oder Informationen auch in Form von Ton-, Bild- oder audiovisuellem Material;
2. „Weiterverwendung“ die Nutzung von Daten, die im Besitz öffentlicher Stellen sind, durch natürliche oder juristische Personen für kommerzielle oder nichtkommerzielle Zwecke, die sich von dem ursprünglichen Zweck im Rahmen des öffentlichen Auftrags, für den die Daten erstellt wurden, unterscheiden, abgesehen vom Austausch von Daten zwischen öffentlichen Stellen ausschließlich im Rahmen der Erfüllung ihres öffentlichen Auftrags;
3. „personenbezogene Daten“ personenbezogene Daten im Sinne des Artikels 4 Nummer 1 der Verordnung (EU) 2016/679;
4. „nicht personenbezogene Daten“ Daten, die keine personenbezogenen Daten sind;
5. „Einwilligung“ eine Einwilligung im Sinne des Artikels 4 Nummer 11 der Verordnung (EU) 2016/679;
6. „Erlaubnis“, dass Datennutzern das Recht auf Verarbeitung nicht personenbezogener Daten eingeräumt wird;
7. „betroffene Person“ eine betroffene Person im Sinne von Artikel 4 Nummer 1 der Verordnung (EU) 2016/679;
8. „Dateninhaber“ eine juristische Person, einschließlich öffentlichen Stellen und internationalen Organisationen oder natürlichen Person, die in Bezug auf die betreffenden Daten keine betroffene Person ist, welche nach geltendem Unionsrecht oder geltendem nationalen Recht berechtigt ist, Zugang zu bestimmten personenbezogenen Daten oder nicht personenbezogenen Daten zu gewähren oder diese Daten weiterzugeben;

9. „Datennutzer“ eine natürliche oder juristische Person, die rechtmäßig Zugang zu bestimmten personenbezogenen oder nicht personenbezogenen Daten hat und im Fall personenbezogener Daten, unter anderem nach der Verordnung (EU) 2016/679, berechtigt ist, diese Daten für kommerzielle oder nichtkommerzielle Zwecke zu nutzen;

10. „gemeinsame Datennutzung“ die entgeltliche oder unentgeltliche Bereitstellung von Daten durch eine betroffene Person oder einen Dateninhaber an einen Datennutzer für die gemeinschaftliche oder individuelle Nutzung dieser Daten auf der Grundlage freiwilliger Vereinbarungen, des Unionsrechts oder des nationalen Rechts, sowohl direkt als auch über einen Mittler, etwa im Rahmen von gebührenpflichtigen oder gebührenfreien offenen oder kommerziellen Lizenzen;

11. „Datenvermittlungsdienst“ einen Dienst, mit dem durch technische, rechtliche oder sonstige Mittel Geschäftsbeziehungen zwischen einer unbestimmten Anzahl von betroffenen Personen oder Dateninhabern einerseits und Datennutzern andererseits hergestellt werden sollen, um die gemeinsame Datennutzung, auch für die Zwecke der Ausübung der Rechte betroffener Personen in Bezug auf personenbezogene Daten, zu ermöglichen, und die zumindest folgendes nicht umfassen:

    a) Dienste, in deren Rahmen Daten von Dateninhabern eingeholt und aggregiert, angereichert oder umgewandelt werden, um deren Wert erheblich zu steigern, und Lizenzen für die Nutzung der resultierenden Daten an die Datennutzer vergeben werden, ohne eine Geschäftsbeziehung zwischen Dateninhabern und Datennutzern herzustellen;

    b) Dienste, deren Schwerpunkt auf der Vermittlung urheberrechtlich geschützter Inhalte liegt;

    c) Dienste, die ausschließlich von einem Dateninhaber genutzt werden, um die Verwendung von im Besitz dieses Dateninhabers befindlichen Daten zu ermöglichen, oder die von mehreren juristischen Personen in einer geschlossenen Gruppe, einschließlich Lieferanten- oder Kundenbeziehungen oder vertraglich festgelegter Kooperationen, genutzt werden, insbesondere wenn deren Hauptziel darin besteht, Funktionen von Gegenständen und Geräten im Zusammenhang mit dem Internet der Dinge sicherzustellen;

    d) Datenvermittlungsdienste, die von öffentlichen Stellen ohne die Absicht der Herstellung von Geschäftsbeziehungen angeboten werden;

12. „Verarbeitung“ die Verarbeitung im Sinne von Artikel 4 Nummer 2 der Verordnung (EU) 2016/679 im Hinblick auf personenbezogene Daten oder Artikel 3 Nummer 2 der Verordnung (EU) 2018/1807 im Hinblick auf nicht personenbezogene Daten;

13. „Zugang“ die Datennutzung im Einklang mit bestimmten technischen, rechtlichen oder organisatorischen Anforderungen, ohne dass Daten hierzu zwingend übertragen oder heruntergeladen werden müssen;

14. „Hauptniederlassung“ einer juristischen Person den Ort, an dem sich ihre Hauptverwaltung in der Union befindet;

15. „Dienste von Datengenossenschaften“ Datenvermittlungsdienste, die von einer Organisationsstruktur angeboten werden, welche sich aus betroffenen Personen,

Ein-Personen-Unternehmen oder KMU, die in dieser Struktur Mitglied sind, zusammensetzt, und deren Hauptzwecke in der Unterstützung ihrer Mitglieder bei der Ausübung ihrer Rechte in Bezug auf bestimmte Daten bestehen, unter anderem beim Treffen einer sachkundigen Entscheidung vor der Einwilligung zur Datenverarbeitung, beim Meinungsaustausch über die den Interessen ihrer Mitglieder im Zusammenhang mit ihren Daten am besten entsprechenden Zwecke und Bedingungen der Datenverarbeitung und beim Aushandeln der Bedingungen der Datenverarbeitung im Namen der Mitglieder, bevor die Erlaubnis zur Verarbeitung nicht personenbezogener Daten erteilt oder in die Verarbeitung personenbezogener Daten eingewilligt wird;

16. „Datenaltruismus" die freiwillige gemeinsame Nutzung von Daten auf der Grundlage der Einwilligung betroffener Personen zur Verarbeitung der sie betreffenden personenbezogenen Daten oder einer Erlaubnis anderer Dateninhaber zur Nutzung ihrer nicht personenbezogenen Daten, ohne hierfür ein Entgelt zu fordern oder zu erhalten, das über eine Entschädigung für die ihnen durch die Bereitstellung ihrer Daten entstandenen Kosten hinausgeht, für Ziele von allgemeinem Interesse gemäß dem nationalen Recht, wie die Gesundheitsversorgung, die Bekämpfung des Klimawandels, die Verbesserung der Mobilität, die einfachere Entwicklung, Erstellung und Verbreitung amtlicher Statistiken, die Verbesserung der Erbringung öffentlicher Dienstleistungen, die staatliche Entscheidungsfindung oder die wissenschaftliche Forschung im allgemeinen Interesse;

17. „öffentliche Stelle" den Staat, Gebietskörperschaften, Einrichtungen des öffentlichen Rechts oder Verbände, die aus einer oder mehreren dieser Körperschaften oder einer oder mehreren dieser Einrichtungen des öffentlichen Rechts bestehen;

18. „Einrichtungen des öffentlichen Rechts" Einrichtungen, die die folgenden Eigenschaften aufweisen:

    a) sie wurden zu dem besonderen Zweck gegründet, im allgemeinen Interesse liegende Aufgaben zu erfüllen, und haben keinen gewerblichen oder kommerziellen Charakter,

    b) sie besitzen Rechtspersönlichkeit,

    c) sie werden überwiegend vom Staat, von Gebietskörperschaften oder von anderen Einrichtungen des öffentlichen Rechts finanziert, unterstehen hinsichtlich ihrer Leitung der Aufsicht dieser Körperschaften oder Einrichtungen, oder haben ein Verwaltungs-, Leitungs- beziehungsweise Aufsichtsorgan, das mehrheitlich aus Mitgliedern besteht, die vom Staat, von Gebietskörperschaften oder von anderen Einrichtungen des öffentlichen Rechts ernannt worden sind;

19. „öffentliches Unternehmen" ein Unternehmen, auf das öffentliche Stellen aufgrund ihres Eigentums, ihrer finanziellen Beteiligung oder der für das Unternehmen geltenden Bestimmungen unmittelbar oder mittelbar einen beherrschenden Einfluss ausüben können; von einem beherrschenden Einfluss der öffentlichen Stellen ist im Sinne dieser Begriffsbestimmung in jedem der folgenden Fälle auszugehen, in denen diese Stellen unmittelbar oder mittelbar

    a) die Mehrheit des gezeichneten Kapitals des Unternehmens halten,

b) über die Mehrheit der mit den Anteilen am Unternehmen verbundenen Stimmrechte verfügen,

c) mehr als die Hälfte der Mitglieder des Verwaltungs-, Leitungs- oder Aufsichtsorgans des Unternehmens ernennen können;

20. „sichere Verarbeitungsumgebung" die physische oder virtuelle Umgebung und die organisatorischen Mittel, mit denen die Einhaltung der Anforderungen des Unionsrechts, wie der Verordnung (EU) 2016/679, insbesondere im Hinblick auf die Rechte der betroffenen Personen, der Rechte des geistigen Eigentums und der geschäftlichen und statistischen Vertraulichkeit, der Integrität und der Verfügbarkeit, sowie des geltenden Unionsrechts und des nationalen Rechts gewährleistet wird und die es der Einrichtung, die die sichere Verarbeitungsumgebung bereitstellt, ermöglichen, alle Datenverarbeitungsvorgänge zu bestimmen und zu beaufsichtigen, darunter auch das Anzeigen, Speichern, Herunterladen und Exportieren von Daten und das Berechnen abgeleiteter Daten mithilfe von Rechenalgorithmen;

21. „gesetzlicher Vertreter" eine in der Union niedergelassene natürliche oder juristische Person, die ausdrücklich benannt wurde, um im Auftrag eines nicht in der Union niedergelassenen Anbieters von Datenvermittlungsdiensten oder einer Einrichtung, die von natürlichen oder juristischen Personen auf der Grundlage des Datenaltruismus für Ziele von allgemeinem Interesse zur Verfügung gestellte Daten erhebt, zu handeln, und an die sich die für die Datenvermittlungsdienste zuständigen Behörden und die für die Registrierung datenaltruistischer Organisationen zuständigen Behörden hinsichtlich der Verpflichtungen nach dieser Verordnung ausschließlich oder zusätzlich zu den betreffenden Anbietern von Datenvermittlungsdiensten bzw. den betreffenden Einrichtungen, wenden auch um gegen einen nicht in der Union niedergelassenen Anbieter von Datenvermittlungsdiensten oder eine nicht in der Union niedergelassene Einrichtung, der bzw. die die Vorschriften nicht einhält, Durchsetzungsverfahren einzuleiten.

KAPITEL II
Weiterverwendung bestimmter Kategorien geschützter Daten im Besitz öffentlicher Stellen

Artikel 3
Datenkategorien

(1) Dieses Kapitel gilt für Daten, die sich im Besitz öffentlicher Stellen befinden und aus folgenden Gründen geschützt sind:

a) geschäftliche Geheimhaltung, einschließlich Betriebsgeheimnissen, Berufsgeheimnissen, Unternehmensgeheimnissen;

b) statistische Geheimhaltung,

c) der Schutz geistigen Eigentums Dritter oder

d) der Schutz personenbezogener Daten, soweit diese Daten nicht in den Anwendungsbereich der Richtlinie (EU) 2019/1024 fallen.

(2) Dieses Kapitel gilt nicht für

a) Daten, die im Besitz öffentlicher Unternehmen sind,

b) Daten, die im Besitz öffentlich-rechtlicher Rundfunkanstalten und ihrer Zweigstellen oder anderer Stellen und deren Zweigstellen sind und der Wahrnehmung eines öffentlichen Sendeauftrags dienen,

c) Daten, die im Besitz von Kultureinrichtungen und Bildungseinrichtungen sind,

d) Daten, die im Besitz öffentlicher Stellen sind und aus Gründen der öffentlichen Sicherheit, der Landesverteidigung oder der nationalen Sicherheit geschützt sind, oder

e) Daten, deren Bereitstellung nicht unter den im betreffenden Mitgliedstaat gesetzlich oder anderweitig verbindlich festgelegten öffentlichen Auftrag der betreffenden öffentlichen Stellen fällt oder, in Ermangelung solcher Rechtsvorschriften, nicht unter den durch allgemeine Verwaltungspraxis in dem Mitgliedstaat festgelegten öffentlichen Auftrag fällt, vorausgesetzt, dass der Umfang der öffentlichen Aufträge transparent ist und regelmäßig überprüft wird.

(3) Dieses Kapitel berührt nicht:

a) Das Unionsrecht und das nationale Recht oder völkerrechtliche Übereinkünfte, denen die Union oder die Mitgliedstaaten beigetreten sind, in Bezug auf den Schutz der in Absatz 1 genannten Datenkategorien und

b) das Unionsrecht und das nationale Recht über den Zugang zu Dokumenten.

Artikel 4
Verbot von Ausschließlichkeitsvereinbarungen

(1) Vereinbarungen oder sonstige Praktiken in Bezug auf die Weiterverwendung von Daten, die im Besitz öffentlicher Stellen sind und Daten der in Artikel 3 Absatz 1 genannten Datenkategorien enthalten, sind verboten, soweit sie ausschließliche Rechte gewähren oder aber zum Gegenstand haben oder bewirken, dass solche ausschließlichen Rechte gewährt werden oder die Verfügbarkeit von Daten zur Weiterverwendung durch andere Einrichtungen als die Parteien solcher Vereinbarungen oder sonstigen Praktiken eingeschränkt wird.

(2) Abweichend von Absatz 1 kann ein ausschließliches Recht auf Weiterverwendung der in dem Absatz genannten Daten gewährt werden, soweit dies für die Erbringung eines Dienstes oder die Bereitstellung eines Produkts im allgemeinen Interesse erforderlich ist, die andernfalls nicht möglich gewesen wären.

(3) Ein ausschließliches Recht nach Absatz 2 wird durch einen Verwaltungsakt oder eine vertragliche Vereinbarung gemäß dem geltenden Unionsrecht oder dem nationalen Recht sowie im Einklang mit den Grundsätzen der Transparenz, der Gleichbehandlung und der Nichtdiskriminierung gewährt.

(4) Die Dauer des ausschließlichen Rechts auf Weiterverwendung von Daten darf 12 Monate nicht überschreiten. Wird ein Vertrag abgeschlossen, so ist dessen Dauer die gleiche wie die des ausschließlichen Rechts.

(5) Die Gewährung eines ausschließlichen Rechts nach den Absätzen 2, 3 und 4, einschließlich der Begründung, warum die Gewährung eines solchen Rechts erforderlich ist, ist transparent und wird in einer Form, die dem einschlägigen Unionsrecht für die Vergabe öffentlicher Aufträge entspricht, im Internet öffentlich zugänglich gemacht.

(6) Vereinbarungen oder andere Praktiken, die unter das in Absatz 1 genannte Verbot fallen und die in den Absätzen 2 und 3 festgelegten Bedingungen nicht erfüllen, die aber vor dem 23. Juni 2022 bereits bestanden haben, werden zum Ende des anwendbaren Vertrags, auf jeden Fall aber zum 24. Dezember 2024 beendet.

Artikel 5
Bedingungen für die Weiterverwendung

(1) Öffentliche Stellen, die nach nationalem Recht dafür zuständig sind, den Zugang zur Weiterverwendung von Daten einer oder mehrerer der in Artikel 3 Absatz 1 genannten Datenkategorien zu gewähren oder zu verweigern, machen die Bedingungen für das Erlauben einer solchen Weiterverwendung und das Verfahren für die Beantragung einer solchen Weiterverwendung über die zentrale Informationsstelle nach Artikel 8 öffentlich zugänglich. Bei der Gewährung oder Verweigerung des Zugangs zur Weiterverwendung können sie von den in Artikel 7 Absatz 1 genannten zuständigen Stellen unterstützt werden.

Die Mitgliedstaaten stellen sicher, dass die öffentlichen Stellen über die notwendigen Ressourcen verfügen und den vorliegenden Artikel einhalten.

(2) Die Bedingungen für die Weiterverwendung müssen in Bezug auf die Datenkategorien, die Zwecke der Weiterverwendung und die Art der Daten, deren Weiterverwendung erlaubt wird, nichtdiskriminierend, transparent, verhältnismäßig und objektiv gerechtfertigt sein. Diese Bedingungen dürfen nicht der Behinderung des Wettbewerbs dienen.

(3) Öffentliche Stellen sorgen gemäß dem Unionsrecht und dem nationalen Recht dafür, dass die Daten geschützt bleiben. Sie können folgende Anforderungen vorschreiben:

a) Den Zugang zur Weiterverwendung von Daten nur zu gewähren, wenn die öffentliche Stelle oder die zuständige Stelle nach Eingang des Antrags auf Weiterverwendung sichergestellt hat, dass die Daten

   i) im Falle personenbezogener Daten anonymisiert wurden und

   ii) im Falle von vertraulichen Geschäftsinformationen, einschließlich Geschäftsgeheimnisse oder durch Rechte des geistigen Eigentums geschützte Inhalte, nach einer anderen Methode der Offenlegungskontrolle verändert, aggregiert oder aufbereitet wurden,

b) der Zugang zu den Daten und deren Weiterverwendung erfolgt durch Fernzugriff in einer von der öffentlichen Stelle bereitgestellten oder kontrollierten sicheren Verarbeitungsumgebung,

c) der Zugang zu den Daten und deren Weiterverwendung erfolgt unter Einhaltung hoher Sicherheitsstandards innerhalb der physischen Räumlichkeiten, in denen sich die sichere Verarbeitungsumgebung befindet, sofern ein Fernzugriff nicht erlaubt werden kann, ohne die Rechte und Interessen Dritter zu gefährden.

(4) Die öffentlichen Stellen erlegen im Falle einer erlaubten Weiterverwendung gemäß Absatz 3 Buchstaben b und c Bedingungen auf, mit denen die Integrität des Betriebs der technischen Systeme der verwendeten sicheren Verarbeitungsumgebung gewahrt wird. Die öffentliche Stelle behält sich das Recht vor, das Verfahren, die Mittel und die Ergebnisse der vom Weiterverwender durchgeführten Datenverarbeitung zu überprüfen, um die Integrität des Datenschutzes zu wahren, und sie behält sich das Recht vor, die Verwendung der Ergebnisse zu verbieten, wenn darin Informationen enthalten sind, die die Rechte und Interessen

Dritter gefährden. Die Entscheidung, die Verwendung der Ergebnisse zu verbieten, muss für den Weiterverwender verständlich und transparent sein.

(5) Sofern im nationalen Recht für die Weiterverwendung von Daten gemäß Artikel 3 Absatz 1 keine besonderen Schutzvorkehrungen bezüglich geltender Geheimhaltungspflichten vorgesehen sind, macht die öffentliche Stelle die Nutzung der gemäß Absatz 3 des vorliegenden Artikels bereitgestellten Daten davon abhängig, ob der Weiterverwender einer Geheimhaltungspflicht nachkommt, wonach ihm die Offenlegung von Informationen, die er möglicherweise trotz der getroffenen Schutzvorkehrungen erlangt hat, untersagt ist, wenn dadurch die Rechte und Interessen Dritter verletzt würden. Weiterverwendern ist es untersagt, betroffene Personen, auf die sich die Daten beziehen, erneut zu identifizieren, und sie ergreifen technische und operative Maßnahmen, um eine erneute Identifizierung zu verhindern und der öffentlichen Stelle etwaige Datenschutzverletzungen, die zu einer erneuten Identifizierung der betroffenen Personen führen könnten, mitzuteilen. Im Falle der unbefugten Weiterverwendung nicht personenbezogener Daten unterrichtet der Weiterverwender unverzüglich, gegebenenfalls mit Unterstützung der öffentlichen Stelle, die juristischen Personen, deren Rechte und Interessen beeinträchtigt werden könnten.

(6) Kann die Weiterverwendung von Daten gemäß den in den Absätzen 3 und 4 des vorliegenden Artikels festgelegten Verpflichtungen nicht erlaubt werden und es keine andere Rechtsgrundlage für die Übermittlung der Daten gemäß der Verordnung (EU) 2016/679 gibt, bemüht sich die öffentliche Stelle, gemäß dem Unionsrecht und dem nationalen Recht, nach besten Kräften, mögliche Weiterverwender dabei zu unterstützen, die Einwilligung der betroffenen Personen oder die Erlaubnis der Dateninhaber einzuholen, deren Rechte und Interessen durch eine solche Weiterverwendung beeinträchtigt werden könnten, sofern dies ohne einen unverhältnismäßig hohen Aufwand für die öffentliche Stelle machbar ist. In den Fällen, in denen die öffentliche Stelle eine solche Unterstützung leistet, kann sie von den in Artikel 7 Absatz 1 genannten zuständigen Stellen unterstützt werden.

(7) Die Weiterverwendung von Daten ist nur unter Wahrung der Rechte des geistigen Eigentums zulässig. Öffentliche Stellen nehmen das in Artikel 7 Absatz 1 der Richtlinie 96/9/EG vorgesehene Recht der Hersteller von Datenbanken nicht in Anspruch, um dadurch die Weiterverwendung von Daten zu verhindern oder diese Weiterverwendung über die in dieser Verordnung festgelegten Beschränkungen hinaus einzuschränken.

(8) Werden angeforderte Daten nach den Bestimmungen des Unionsrechts oder des nationalen Rechts über die geschäftliche oder die statistische Geheimhaltung als vertraulich angesehen, so stellen die öffentlichen Stellen sicher, dass die vertraulichen Daten infolge der Erlaubnis einer solchen Weiterverwendung nicht offengelegt werden, es sei denn, die Weiterverwendung ist gemäß Absatz 6 zulässig.

(9) Beabsichtigt ein Weiterverwender nach Artikel 3 Absatz 1 geschützte nicht personenbezogene Daten in ein Drittland zu übertragen, so hat er die öffentliche Stelle zum Zeitpunkt der Beantragung der Weiterverwendung solcher Daten von seiner Absicht, solche Daten zu übertragen, und dem Zweck dieser Übertragung zu unterrichten. Im Falle einer Weiterverwendung gemäß Absatz 6 des vorliegenden Artikels unterrichtet der Weiterverwender, gegebenenfalls mit Unterstützung der öffentlichen Stelle, die juristische Person, deren Rechte und Interessen beeinträchtigt werden können, über diese Absicht, den Zweck und die angemessenen Schutzvorkehrungen. Die öffentliche Stelle gestattet die Weiterverwendung nur, wenn die juristische Person die Erlaubnis für die Übertragung erteilt.

(10) Öffentliche Stellen übermitteln nicht personenbezogene vertrauliche Daten oder durch Rechte des geistigen Eigentums geschützte Daten nur dann an einen Weiterverwender, der beabsichtigt, diese Daten in ein nicht gemäß Absatz 12 benanntes Drittland zu übertragen, wenn der Weiterverwender sich vertraglich dazu verpflichtet,

a) die gemäß den Absätzen 7 und 8 auferlegten Verpflichtungen auch nach der Übertragung der Daten in das Drittland weiterhin zu erfüllen und

b) die Zuständigkeit der Gerichte des Mitgliedstaats der übermittelnden öffentlichen Stelle für alle Streitigkeiten im Zusammenhang mit der Einhaltung der Absätze 7 und 8 anzuerkennen.

(11) Öffentliche Stellen bieten den Weiterverwendern gegebenenfalls und im Rahmen ihrer Möglichkeiten Beratung und Unterstützung, indem sie den in Absatz 10 des vorliegenden Artikels genannten Verpflichtungen nachkommen.

Zur Unterstützung der öffentlichen Stellen und der Weiterverwender kann die Kommission Durchführungsrechtsakte mit Mustervertragsklauseln für die Erfüllung der in Absatz 10 des vorliegenden Artikels genannten Verpflichtungen erlassen. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 33 Absatz 3 genannten Prüfverfahren erlassen.

(12) Wenn dies aufgrund der Vielzahl unionsweit gestellter Anträge auf Weiterverwendung nicht personenbezogener Daten in bestimmten Drittländern gerechtfertigt ist, kann die Kommission Durchführungsrechtsakte erlassen, in denen sie erklärt, dass die Rechts-, Aufsichts- und Durchsetzungsmechanismen eines Drittlands

a) den Schutz geistigen Eigentums und von Geschäftsgeheimnissen in einer Weise gewährleisten, die im Wesentlichen dem durch das Unionsrecht gewährleisteten Schutz gleichwertig ist,

b) wirksam angewendet und durchgesetzt werden und

c) wirksame gerichtliche Rechtsbehelfe vorsehen.

Diese Durchführungsrechtsakte werden gemäß dem in Artikel 33 Absatz 3 genannten Prüfverfahren erlassen.

(13) Nach besonderen Gesetzgebungsakten der Union können bestimmte Kategorien nicht personenbezogener Daten, die im Besitz öffentlicher Stellen sind, für die Zwecke dieses Artikels als hochsensibel gelten, wenn die Übertragung dieser Daten in Drittländer Ziele des Gemeinwohls der Union, beispielsweise in den Bereichen Sicherheit und öffentliche Gesundheit, gefährden könnte oder die Gefahr einer erneuten Identifizierung anhand nicht personenbezogener, anonymisierter Daten birgt. Wird ein solcher Rechtsakt erlassen, so erlässt die Kommission gemäß Artikel 32 delegierte Rechtsakte zur Ergänzung dieser Verordnung durch Festlegung besonderer Bedingungen für die Übertragung dieser Daten in Drittländer.

Diese besonderen Bedingungen richten sich nach der Art der Kategorien der nicht personenbezogenen Daten, die in dem besonderen Gesetzgebungsakt der Union aufgeführt werden, und den Gründen, aus denen diese Kategorien als hochsensibel gelten, wobei sie die Risiken einer erneuten Identifizierung anhand anonymisierter Daten berücksichtigen. Sie sind nichtdiskriminierend und auf das erforderliche Maß zur Erreichung der in diesem Gesetzgebungsakt der Union festgelegten Ziele des Gemeinwohls der Union beschränkt; sie stehen im Einklang mit den internationalen Verpflichtungen der Union.

Wenn dies nach besonderen Gesetzgebungsakt der Union gemäß Unterabsatz 1 erforderlich ist, können diese besonderen Bedingungen Vorgaben für die Übertragung oder diesbezügliche technische Vorkehrungen, Beschränkungen bezüglich der Weiterverwendung von Daten in Drittländern oder Kategorien von Personen, die berechtigt sind, solche Daten in Drittländer zu übertragen, oder – in Ausnahmefällen – Beschränkungen für Übertragungen in Drittländer umfassen.

(14) Die natürliche oder juristische Person, der das Recht auf Weiterverwendung nicht personenbezogener Daten gewährt wurde, darf die Daten nur in solche Drittländer übertragen, die die Anforderungen der Absätze 10, 12 und 13 erfüllen.

Artikel 6
Gebühren

(1) Öffentliche Stellen, die eine Weiterverwendung von Daten der in Artikel 3 Absatz 1 genannten Datenkategorien erlauben, können Gebühren für die Erlaubnis der Weiterverwendung dieser Daten erheben.

(2) Gemäß Absatz 1 erhobene Gebühren müssen transparent, nichtdiskriminierend, verhältnismäßig und objektiv gerechtfertigt sein und dürfen den Wettbewerb nicht einschränken.

(3) Öffentliche Stellen müssen gewährleisten, dass alle Gebühren auch online über weithin verfügbare grenzüberschreitende Zahlungsdienste ohne Diskriminierung aufgrund des Niederlassungsorts des Zahlungsdienstleisters, des Ausstellungsorts des Zahlungsinstruments oder des Standorts des Zahlungskontos in der Union bezahlt werden können.

(4) Erheben die öffentlichen Stellen Gebühren, so ergreifen sie Maßnahmen, um – gemäß den Vorschriften über staatliche Beihilfen – Anreize für die Weiterverwendung von Daten der in Artikel 3 Absatz 1 genannten Datenkategorien zu nichtkommerziellen Zwecken wie der wissenschaftlichen Forschung und durch KMU und Start-up-Unternehmen zu schaffen. In diesem Zusammenhang können öffentliche Stellen die Daten insbesondere KMU, Start-up-Unternehmen, der Zivilgesellschaft und Bildungseinrichtungen auch gegen eine ermäßigte Gebühr oder unentgeltlich zur Verfügung stellen. Öffentliche Stellen können zu diesem Zweck eine Liste der Kategorien von Weiterverwendern aufstellen, denen Daten für die Weiterverwendung gegen eine ermäßigte Gebühr oder unentgeltlich zur Verfügung gestellt werden. Diese Liste wird zusammen mit den Kriterien, die bei ihrer Aufstellung verwendet wurden, veröffentlicht.

(5) Gebühren werden aus den Kosten abgeleitet, die mit der Durchführung des Antragsverfahrens auf Weiterverwendung von Daten der in Artikel 3 Absatz 1 genannten Datenkategorien verbunden sind, und auf die für das Folgende erforderlichen Kosten beschränkt:

a) die Vervielfältigung, Bereitstellung und Verbreitung der Daten,

b) die Freigabe der Urheberrechte,

c) die Anonymisierung oder sonstigen Aufbereitung personenbezogener oder vertraulicher Geschäftsinformationen gemäß Artikel 5 Absatz 3,

d) die Instandhaltung einer sicheren Verarbeitungsumgebung,

e) der Erwerb des Rechts auf Erlaubnis der Weiterverwendung gemäß diesem Kapitel von Dritten außerhalb des öffentlichen Sektors und

f) der Unterstützung von Weiterverwendern bei der Einholung der Einwilligung der betroffenen Personen und der Erlaubnis der Dateninhaber, deren Rechte und Interessen durch eine solche Weiterverwendung beeinträchtigt werden könnten.

(6) Die Kriterien und die Methode für die Gebührenberechnung werden von den Mitgliedstaaten festgelegt und veröffentlicht. Die öffentliche Stelle veröffentlicht eine Beschreibung der wichtigsten Kostenarten und die Regeln der Kostenzuweisung.

Artikel 7
Zuständige Stellen

(1) Für die Durchführung der in diesem Artikel genannten Aufgaben benennt jeder Mitgliedstaat eine oder mehrere zuständige Stellen, die für bestimmte Sektoren zuständig sein können, welche die öffentlichen Stellen, die Zugang zur Weiterverwendung von Daten der in Artikel 3 Absatz 1 genannten Datenkategorien gewähren oder verweigern, unterstützen. Die Mitgliedstaaten können entweder eine oder mehrere neue zuständige Stellen einrichten oder sich auf bestehende öffentliche Stellen oder interne Dienste öffentlicher Stellen stützen, die die in dieser Verordnung festgelegten Bedingungen erfüllen.

(2) Die zuständigen Stellen können nach dem Unionsrecht oder dem nationalen Recht, wenn darin eine solche Zugangsgewährung vorgesehen ist, befugt werden, den Zugang zur Weiterverwendung von Daten der in Artikel 3 Absatz 1 genannten Datenkategorien zu gewähren. In den Fällen, in denen sie den Zugang zur Weiterverwendung gewähren oder verweigern, finden die Artikel 4, 5, 6 und 9 auf diese zuständigen Stellen Anwendung.

(3) Die zuständigen Stellen müssen zur Erfüllung der ihnen übertragenen Aufgaben über angemessene rechtliche, finanzielle, technische und personelle Mittel, einschließlich der erforderlichen technischen Sachkenntnis, verfügen, damit sie in der Lage sind, das einschlägige Unionsrecht bzw. nationale Recht in Bezug auf die Regelungen für den Zugang zu Daten der in Artikel 3 Absatz 1 genannten Datenkategorien einzuhalten.

(4) Soweit erforderlich, beinhaltet die Unterstützung nach Absatz 1 Folgendes:

a) Leistung technischer Unterstützung durch Bereitstellung einer sicheren Verarbeitungsumgebung für die Gewährung des Zugangs zur Weiterverwendung von Daten;

b) Beratung und technische Unterstützung bei der bestmöglichen Strukturierung und Speicherung von Daten, um diese Daten leicht zugänglich zu machen;

c) Leistung technischer Unterstützung bei der Pseudonymisierung und Sicherstellung, dass die Datenverarbeitung in einer Weise erfolgt, bei der die Privatsphäre, die Vertraulichkeit, die Integrität und die Zugänglichkeit in Bezug auf die Informationen in den Daten, deren Weiterverwendung erlaubt wird, effektiv gewahrt bleiben; dazu gehören auch Techniken zur Anonymisierung, Generalisierung, Unterdrückung und Randomisierung personenbezogener Daten oder andere dem Stand der Technik entsprechende Methoden zur Wahrung der Privatsphäre sowie die Löschung vertraulicher Geschäftsinformationen, wie Handelsgeheimnisse oder durch Rechte des geistigen Eigentums geschützte Inhalte;

d) gegebenenfalls Unterstützung der öffentlichen Stellen, um Weiterverwender bei der Einholung der Einwilligung der betroffenen Personen zur Weiterverwendung oder der Erlaubnis der Dateninhaber entsprechend ihrer besonderen Festlegungen zu unterstützen, auch im Hinblick auf das Hoheitsgebiet, in dem die Datenverar-

beitung stattfinden soll, und Unterstützung der öffentlichen Stellen bei der Einrichtung technischer Mechanismen, mit denen Einwilligungsanfragen oder die Erlaubnis der Weiterverwender übermittelt werden können, soweit dies praktikabel ist;

e) Unterstützung öffentlicher Stellen bei der Beurteilung, ob die von einem Weiterverwender nach Artikel 5 Absatz 10 eingegangenen vertragliche Zusagen angemessen sind.

(5) Jeder Mitgliedstaat teilt der Kommission bis zum 24. September 2023 die Namen der nach Absatz 1 benannten zuständigen Stellen mit. Jeder Mitgliedstaatteilt der Kommission auch alle späteren Änderungen des Namens dieser benannten zuständigen Stellen mit.

Artikel 8
Zentrale Informationsstellen

(1) Die Mitgliedstaaten gewährleisten, dass alle einschlägigen Informationen in Bezug auf die Anwendung der Artikel 5 und 6 über eine zentrale Informationsstelle erhältlich und leicht zugänglich sind. Als Informationsstelle können die Mitgliedstaaten entweder eine neue Stelle oder Organisation einrichten oder eine vorhandene Stelle oder Organisation benennen. Die zentrale Informationsstelle kann mit sektoralen, regionalen oder lokalen Informationsstellen verknüpft sein. Die Funktionen der zentralen Informationsstelle können automatisiert werden, sofern die öffentliche Stelle für angemessene Unterstützung sorgt.

(2) Die zentrale Informationsstelle ist befugt, Anfragen oder Anträge in Bezug auf die Weiterverwendung von Daten der in Artikel 3 Absatz 1 genannten Datenkategorien entgegenzunehmen, und übermittelt diese – sofern möglich und angebracht durch automatisierte Verfahren – an die zuständigen öffentlichen Stellen oder gegebenenfalls an die in Artikel 7 Absatz 1 genannten zuständigen Stellen. Die zentrale Informationsstelle stellt auf elektronischem Wege eine durchsuchbare Bestandsliste mit einer Übersicht aller verfügbaren Datenressourcen, gegebenenfalls einschließlich der bei sektoralen, regionalen oder lokalen Informationsstellen verfügbaren Datenressourcen, und einschlägige Informationen mit einer Beschreibung der verfügbaren Daten bereit, die mindestens das Datenformat und den Datenumfang und die Bedingungen für ihre Weiterverwendung umfasst.

(3) Die zentrale Informationsstelle kann einen gesonderten, vereinfachten und gut dokumentierten Informationskanal für KMU und Start-up-Unternehmen einrichten, der auf deren Bedarf und Kapazitäten mit Blick auf die Beantragung der Weiterverwendung von Daten der in Artikel 3 Absatz 1 genannten Datenkategorien abstellt.

(4) Die Kommission richtet ein europaweites zentrales Zugangsportal ein, über das ein durchsuchbares elektronisches Verzeichnis der bei den zentralen nationalen Informationsstellen verfügbaren Daten sowie weitere Informationen darüber bereitgestellt werden, wie über die zentralen nationalen Informationsstellen Daten angefordert werden können.

Artikel 9
Verfahren für Anträge auf Weiterverwendung

(1) Sofern nicht gemäß dem nationalen Recht kürzeren Fristen festgelegt sind, treffen die zuständigen öffentlichen Stellen oder die in Artikel 7 Absatz 1 genannten zuständigen Stellen eine Entscheidung über den Antrag auf Weiterverwendung von Daten der in Artikel 3 Absatz 1 genannten Datenkategorien innerhalb von zwei Monaten nach Eingang des Antrags.

Bei außergewöhnlich umfangreichen und komplexen Anträgen auf Weiterverwendung kann diese Frist von zwei Monaten um bis zu 30 Tage verlängert werden. In solchen Fällen teilen die zuständigen öffentlichen Stellen oder die in Artikel 7 Absatz 1 genannten zuständigen Stellen dem Antragsteller möglichst bald mit, dass für die Durchführung des Verfahrens mehr Zeit benötigt wird, zusammen mit den Gründen für die Verzögerung.

(2) Jede natürliche oder juristische Person, die von einer Entscheidung gemäß Absatz 1 direkt betroffen ist, hat in dem Mitgliedstaat, in dem die betreffende Stelle ihren Sitz hat, einen wirksamen Rechtsbehelfsanspruch. Dieser Rechtsbehelfsanspruch ist durch das nationale Recht geregelt und umfasst die Möglichkeit der Überprüfung durch eine unparteiische Stelle mit entsprechender Sachkenntnis, wie die nationale Wettbewerbsbehörde, die für den Zugang zu Dokumenten zuständige Behörde, die gemäß der Verordnung (EU) 2016/679 errichtete Aufsichtsbehörde oder ein nationales Gericht, deren Entscheidungen für die betreffende öffentliche Stelle oder die zuständige Stelle bindend sind.

KAPITEL III
Anforderungen an Datenvermittlungsdienste

Artikel 10
Datenvermittlungsdienste

Die Erbringung der folgenden Datenvermittlungsdienste erfolgt gemäß Artikel 12 und unterliegt einem Anmeldeverfahren:

a) Vermittlungsdienste zwischen Dateninhabern und potenziellen Datennutzern, einschließlich Bereitstellung der technischen oder sonstigen Mittel als Voraussetzung solcher Dienste; zu diesen Diensten können auch der zwei- oder mehrseitige Austausch von Daten oder die Einrichtung von Plattformen oder Datenbanken, die den Austausch oder die gemeinsame Nutzung von Daten ermöglichen, sowie die Einrichtung anderer spezieller Infrastrukturen für die Vernetzung von Dateninhabern mit Datennutzern gehören;

b) Vermittlungsdienste zwischen betroffenen Personen, die ihre personenbezogenen Daten zugänglich machen wollen, oder natürlichen Personen, die nicht personenbezogene Daten zugänglich machen wollen, und potenziellen Datennutzern, einschließlich Bereitstellung der technischen oder sonstigen Mittel als Voraussetzung dieser Dienste, sowie insbesondere Ermöglichung der Ausübung der in der Verordnung (EU) 2016/679 verankerten Rechte betroffener Personen;

c) Dienste von Datengenossenschaften.

Artikel 11
Anmeldung der Anbieter von Datenvermittlungsdiensten

(1) Jeder Anbieter von Datenvermittlungsdiensten, der beabsichtigt, die in Artikel 10 genannten Datenvermittlungsdienste zu erbringen, muss sich bei der für Datenvermittlungsdienste zuständigen Behörde anmelden.

(2) Unbeschadet unionsrechtlicher Bestimmungen zur Regelung grenzübergreifender Schadenersatzklagen und damit zusammenhängender Verfahren gilt für die Zwecke dieser Verordnung, dass ein Anbieter von Datenvermittlungsdiensten, der in mehreren Mitgliedstaa-

ten niedergelassen ist, der rechtlichen Zuständigkeit des Mitgliedstaats unterliegt, in dem er seine Hauptniederlassung hat.

(3) Ein Anbieter von Datenvermittlungsdiensten, der nicht in der Union niedergelassen ist, aber die in Artikel 10 genannten Datenvermittlungsdienste in der Union anbietet, benennt einen gesetzlichen Vertreter in einem der Mitgliedstaaten, in denen diese Dienste angeboten werden.

Um die Einhaltung dieser Verordnung sicherzustellen, beauftragt der Anbieter der Datenvermittlungsdienste den gesetzlichen Vertreter, neben ihm oder an seiner Stelle für Datenvermittlungsdienste zuständigen Behörden oder betroffenen Personen und Dateninhabern bei Fragen im Zusammenhang mit den erbrachten Datenvermittlungsdiensten als Anlaufstelle zu dienen. Der gesetzliche Vertreter arbeitet mit den für Datenvermittlungsdienste zuständigen Behörden zusammen und legt ihnen auf Verlangen umfassend dar, welche Maßnahmen und Vorkehrungen der Anbieter von Datenvermittlungsdiensten getroffen hat, um die Einhaltung dieser Verordnung sicherzustellen.

Es gilt, dass der Anbieter von Datenvermittlungsdiensten der rechtlichen Zuständigkeit des Mitgliedstaats unterliegt, in dem sich der gesetzliche Vertreter befindet. Die Benennung eines gesetzlichen Vertreters durch den Anbieter von Datenvermittlungsdiensten erfolgt unbeschadet etwaiger rechtlicher Schritte gegen den Anbieter von Datenvermittlungsdiensten.

(4) Sobald er die Anmeldung vorgenommen hat, kann der Anbieter von Datenvermittlungsdiensten gemäß Absatz 1 die Tätigkeit unter den in diesem Kapitel festgelegten Bedingungen aufnehmen.

(5) Die in Absatz 1 genannte Anmeldung berechtigt den Anbieter von Datenvermittlungsdiensten zur Erbringung von Datenvermittlungsdiensten in allen Mitgliedstaaten.

(6) Die in Absatz 1 genannte Anmeldung muss folgende Angaben enthalten:

a) den Namen des Anbieters von Datenvermittlungsdiensten,

b) den Rechtsstatus, die Rechtsform, die Eigentümerstruktur, die relevanten Tochtergesellschaften und, sofern der Anbieter von Datenvermittlungsdiensten in einem Handelsregister oder einem anderen vergleichbaren öffentlichen nationalen Register eingetragen ist, die Registernummer des Anbieters von Datenvermittlungsdiensten,

c) die Anschrift der Hauptniederlassung des Anbieters von Datenvermittlungsdiensten in der Union, falls zutreffend, und die Anschrift einer etwaigen Zweigniederlassung in einem anderen Mitgliedstaat oder des gesetzlichen Vertreters,

d) eine öffentliche Website mit vollständigen und aktuellen Informationen über den Anbieter von Datenvermittlungsdiensten und seine Tätigkeiten, einschließlich mindestens der Informationen gemäß den Buchstaben a, b, c und f,

e) die Kontaktpersonen und Kontaktangaben des Anbieters von Datenvermittlungsdiensten,

f) eine Beschreibung des Datenvermittlungsdienstes, den der Anbieter von Datenvermittlungsdiensten zu erbringen beabsichtigt, und Angaben dazu, unter welche der in Artikel 10 genannten Kategorien dieser Datenvermittlungsdienst fällt,

g) den voraussichtlichen Tag der Aufnahme der Tätigkeit, falls dies ein anderer als der Tag der Anmeldung ist.

(7) Die für Datenvermittlungsdienste zuständige Behörde stellt sicher, dass das Anmeldeverfahren nichtdiskriminierend ist und zu keinen Wettbewerbsverzerrungen führt.

(8) Auf Antrag des Anbieters von Datenvermittlungsdiensten gibt die für Datenvermittlungsdienste zuständige Behörde innerhalb einer Woche nach einer ordnungsgemäß und vollständig abgeschlossenen Anmeldung eine standardisierte Erklärung ab, in der sie bestätigt, dass der Anbieter von Datenvermittlungsdiensten die in Absatz 1 genannte Anmeldung vorgenommen hat und dass die Anmeldung die in Absatz 6 genannten Informationen enthält.

(9) Auf Antrag des Anbieters von Datenvermittlungsdiensten bestätigt die für Datenvermittlungsdienste zuständige Behörde, dass der Anbieter von Datenvermittlungsdiensten die Anforderungen dieses Artikels und des Artikels 12 erfüllt. Nach Erhalt einer solchen Bestätigung kann der Anbieter von Datenvermittlungsdiensten bei der schriftlichen und mündlichen Kommunikation den das Label „in der Union anerkannter Anbieter von Datenvermittlungsdiensten" führen und ein gemeinsames Logo verwenden.

Damit in der Union anerkannte Anbieter von Datenvermittlungsdiensten in der gesamten Union leicht erkennbar sind, legt die Kommission im Wege von Durchführungsrechtsakten die Ausgestaltung eines gemeinsamen Logos fest. In der Union anerkannte Anbieter von Datenvermittlungsdiensten verwenden das gemeinsame Logo deutlich gut sichtbar auf jeder mit ihren Datenvermittlungsdiensten verbundenen Online- und Offline-Veröffentlichung.

Die Durchführungsrechtsakte werden nach dem in Artikel 33 Absatz 2 genannten Beratungsverfahren erlassen.

(10) Die für Datenvermittlungsdienste zuständige Behörde teilt der Kommission jede neue Anmeldung unverzüglich auf elektronischem Wege mit. Die Kommission führt ein Register aller Anbieter von Datenvermittlungsdiensten, die ihre Dienste in der Union erbringen, und aktualisiert dieses Register regelmäßig. Die Informationen gemäß Absatz 6 Buchstaben a, b, c, d, f und g werden in einem öffentlichen Register veröffentlicht.

(11) Die für Datenvermittlungsdienste zuständige Behörde kann nach Maßgabe des nationalen Rechts Gebühren für die Anmeldung erheben. Diese Gebühren sind verhältnismäßig und objektiv und beruhen auf den Verwaltungskosten, die durch die Überwachung der Einhaltung der Vorschriften und andere Marktkontrolltätigkeiten der für Datenvermittlungsdienste zuständigen Behörden in Bezug auf Anmeldungen von Anbietern von Datenvermittlungsdiensten entstehen. Im Falle von KMU und Start-up-Unternehmen kann die für Datenvermittlungsdienste zuständige Behörde eine ermäßigte Anmeldegebühr verlangen oder auf die Gebühr verzichten.

(12) Anbieter von Datenvermittlungsdiensten teilen der für Datenvermittlungsdienste zuständigen Behörde jede Änderung der gemäß Absatz 6 übermittelten Angaben innerhalb von 14 Tagen ab dem Tag der Änderung mit.

(13) Stellt ein Anbieter von Datenvermittlungsdiensten seine Tätigkeiten ein, so meldet er dies der nach den Absätzen 1, 2 und 3 bestimmten für Datenvermittlungsdienste zuständigen Behörde innerhalb von 15 Tagen.

(14) Die für Datenvermittlungsdienste zuständige Behörde teilt der Kommission jede der in den Absätzen 12 und 13 genannten Abmeldung unverzüglich auf elektronischem Wege mit.

Die Kommission aktualisiert das öffentliche Register der Anbieter von Datenvermittlungsdiensten in der Union entsprechend.

Artikel 12
Bedingungen für die Erbringung von Datenvermittlungsdiensten

Die Erbringung von Datenvermittlungsdiensten nach Artikel 10 unterliegt folgenden Bedingungen:

a) Der Anbieter von Datenvermittlungsdiensten verwendet die Daten, für die er Datenvermittlungsdienste erbringt, für keine anderen Zwecke, als sie den Datennutzern zur Verfügung zu stellen, und stellt die Datenvermittlungsdienste über eine gesonderte juristische Person bereit;

b) die kommerziellen Bedingungen, einschließlich der Preisgestaltung, für die Erbringung von Datenvermittlungsdiensten für einen Dateninhaber oder Datennutzer sind nicht davon abhängig, ob der Dateninhaber oder Datennutzer andere Dienste desselben Anbieters von Datenvermittlungsdiensten oder eines verbundenen Unternehmens nutzt, und wenn dies der Fall ist, in welchem Umfang der Dateninhaber oder Datennutzer diese anderen Dienste nutzt;

c) die Daten, die in Bezug auf Tätigkeiten einer natürlichen oder juristischen Person zur Erbringung des Datenvermittlungsdienstes erhoben werden, einschließlich Datum, Uhrzeit und Geolokalisierungsdaten, Dauer der Tätigkeit sowie Verbindungen zu anderen natürlichen oder juristischen Personen, die von der den Datenvermittlungsdienst nutzenden Person hergestellt werden, werden nur für die Entwicklung dieses Datenvermittlungsdienstes verwendet, was die Nutzung von Daten für die Aufdeckung von Betrug oder im Interesse der Cybersicherheit umfassen kann, und sie sind den Dateninhabern auf Anfrage zur Verfügung zu stellen;

d) der Anbieter von Datenvermittlungsdiensten ermöglicht den Austausch der Daten in dem Format, in dem er diese von einer betroffenen Person oder vom Dateninhaber erhält, wandelt die Daten nur in bestimmte Formate um, um die Interoperabilität innerhalb und zwischen Sektoren zu verbessern, oder wenn der Datennutzer dies verlangt, oder wenn das Unionsrecht dies vorschreibt oder wenn dies der Harmonisierung mit internationalen oder europäischen Datennormen dient und bietet betroffenen Personen oder Dateninhabern die Möglichkeit an, auf diese Umwandlungen zu verzichten („opt out“), sofern sie nicht durch das Unionsrecht vorgeschrieben sind;

e) Datenvermittlungsdienste können ein Angebot zusätzlicher spezifischer Werkzeuge und Dienste für Dateninhaber oder betroffene Personen umfassen, insbesondere um den Datenaustausch zu erleichtern, z. B. vorübergehende Speicherung, Pflege, Konvertierung, Anonymisierung und Pseudonymisierung; diese Werkzeuge werden nur auf ausdrücklichen Antrag oder mit Zustimmung des Dateninhabers oder der betroffenen Person verwendet, und die in diesem Zusammenhang angebotenen Werkzeugen Dritter werden für keine anderen Zwecke verwendet;

f) der Anbieter von Datenvermittlungsdiensten stellt sicher, dass das Verfahren für den Zugang zu seinem Dienst sowohl für betroffene Personen als auch für Dateninhaber sowie für Datennutzer – auch in Bezug auf die Preise und die Geschäftsbedingungen – fair, transparent und nichtdiskriminierend ist;

g) der Anbieter von Datenvermittlungsdiensten verfügt über Verfahren, um betrügerische oder missbräuchliche Praktiken in Bezug auf Parteien zu verhindern, die über seine Datenvermittlungsdienste Zugang zu erlangen suchen;

h) der Anbieter von Datenvermittlungsdiensten gewährleistet im Falle seiner Insolvenz eine angemessene Weiterführung der Erbringung seiner Datenvermittlungsdienste und richtet, sofern dieser Datenvermittlungsdienst die Speicherung von Daten sicherstellt, Mechanismen ein, die es Dateninhabern und Datennutzern ermöglichen, Zugang zu ihren Daten zu erhalten, diese zu übertragen oder abzurufen und im Fall der Erbringung von Datenvermittlungsdiensten zwischen betroffenen Personen und Datennutzern, ihre Rechte auszuüben;

i) der Anbieter von Datenvermittlungsdiensten trifft geeignete Maßnahmen, um unter anderem mithilfe von allgemein verwendeten offenen Standards in dem Sektor, in dem der Anbieter von Datenvermittlungsdiensten tätig ist, die Interoperabilität mit anderen Datenvermittlungsdiensten zu gewährleisten;

j) der Anbieter von Datenvermittlungsdiensten ergreift angemessene technische, rechtliche und organisatorische Maßnahmen, um die Übertragung nicht personenbezogener Daten oder den Zugang zu diesen Daten zu verhindern, die nach Maßgabe des Unionsrechts oder des nationalen Rechts des jeweiligen Mitgliedstaats rechtswidrig sind;

k) die Dateninhaber werden vom Anbieter von Datenvermittlungsdiensten im Falle einer unbefugten Übertragung, des unbefugten Zugriffs oder der unbefugten Nutzung der von ihm geteilten nicht personenbezogenen Daten unverzüglich unterrichtet;

l) der Anbieter von Datenvermittlungsdiensten trifft die notwendigen Maßnahmen, um ein angemessenes Sicherheitsniveau bei der Speicherung, Verarbeitung und Übermittlung nicht personenbezogener Daten zu gewährleisten, und der Anbieter von Datenvermittlungsdiensten stellt ferner das höchste Sicherheitsniveau bei der Speicherung und Übermittlung sensibler wettbewerbsrelevanter Informationen sicher;

m) der Anbieter von Datenvermittlungsdiensten, der Dienste für betroffene Personen anbietet, handelt bei der Erleichterung der Rechteausausübung durch die betroffenen Personen im besten Interesse der betroffenen Personen; insbesondere informiert und –soweit erforderlich – berät er betroffene Personen in prägnanter, transparenter, verständlicher und leicht zugänglicher Weise über die beabsichtigte Nutzung der Daten durch Datennutzer und die üblichen Geschäftsbedingungen für solche Nutzungen, bevor die betroffenen Personen ihre Einwilligung erteilen;

n) stellt ein Anbieter von Datenvermittlungsdiensten Werkzeuge zur Einholung der Einwilligung betroffener Personen oder der Erlaubnis zur Verarbeitung der von Dateninhabern zur Verfügung gestellten Daten bereit, so gibt er gegebenenfalls das Hoheitsgebiet des Drittlandes an, in dem die Datennutzung stattfinden soll, und stellt den betroffenen Personen Werkzeuge zur Erteilung und zum Widerruf der Einwilligung sowie Dateninhabern Werkzeuge zur Erteilung und zum Widerruf der Erlaubnis zur Verarbeitung von Daten zur Verfügung;

o) der Anbieter von Datenvermittlungsdiensten führt ein Protokoll über die Datenvermittlungstätigkeit.

Artikel 13
Zuständige Behörden für Datenvermittlungsdienste

(1) Jeder Mitgliedstaat benennt eine oder mehrere zuständige Behörden für die Wahrnehmung der Aufgaben im Zusammenhang mit dem Anmeldeverfahren für Datenvermittlungsdienste, und teilt der Kommission bis zum 24. September 2023 die Namen dieser zuständigen Behörden mit. Jeder Mitgliedstaat teilt der Kommission auch alle späteren Änderungen der Namen dieser zuständigen Behörden mit.

(2) Die für Datenvermittlungsdienste zuständigen Behörden müssen den Anforderungen des Artikels 26 genügen.

(3) Die Befugnisse der für Datenvermittlungsdienste zuständigen Behörden lassen die Befugnisse der Datenschutzbehörden, der nationalen Wettbewerbsbehörden, der für Cybersicherheit zuständigen Behörden und anderer einschlägiger Fachbehörden unberührt. Nach Maßgabe ihrer jeweiligen Befugnisse im Rahmen des Unionsrechts und des nationalen Rechts begründen diese Behörden eine enge Zusammenarbeit, tauschen Informationen aus, die für die Wahrnehmung ihrer Aufgaben in Bezug auf Anbieter von Datenvermittlungsdiensten erforderlich sind, und bemühen sich darum, dass die Entscheidungen, die bei der Anwendung der Verordnung getroffen werden, konsistent sind.

Artikel 14
Überwachung der Einhaltung

(1) Die für Datenvermittlungsdienste zuständigen Behörden überwachen und beaufsichtigen die Einhaltung der Anforderungen dieses Kapitels durch die Anbieter von Datenvermittlungsdiensten. Auf Antrag einer natürlichen oder juristischen Person kann die für Datenvermittlungsdienste zuständige Behörde auch die Einhaltung der Rechtsvorschriften durch Anbieter von Datenvermittlungsdiensten überwachen und beaufsichtigen.

(2) Die für Datenvermittlungsdienste zuständigen Behörden sind befugt, von den Anbietern von Datenvermittlungsdiensten oder ihren gesetzlichen Vertretern alle Informationen anzufordern, die nötig sind, um die Einhaltung der Anforderungen dieses Kapitels zu überprüfen. Jede Anforderung von Informationen muss in angemessenem Verhältnis zur Wahrnehmung dieser Aufgabe stehen und mit Gründen versehen sein.

(3) Stellt die für Datenvermittlungsdienste zuständige Behörde fest, dass ein Anbieter von Datenvermittlungsdiensten gegen eine oder mehrere Anforderungen dieses Kapitels verstößt, teilt sie dies dem betreffenden Anbieter von Datenvermittlungsdiensten mit und gibt ihm Gelegenheit, innerhalb von 30 Tagen nach Erhalt der Mitteilung dazu Stellung zu nehmen.

(4) Die für Datenvermittlungsdienste zuständige Behörde ist befugt, die Beendigung des in Absatz 3 genannten Verstoßes innerhalb einer angemessenen Frist oder im Fall eines schwerwiegenden Verstoßes unverzüglich zu verlangen, und ergreift angemessene und verhältnismäßige Maßnahmen, um die Einhaltung sicherzustellen. In dieser Hinsicht müssen die für Datenvermittlungsdienste zuständigen Behörden gegebenenfalls dazu befugt sein,

a) im Rahmen von Verwaltungsverfahren abschreckende Geldstrafen, die Zwangsgelder und Zwangsgelder mit Rückwirkung umfassen können, zu verhängen gerichtliche Verfahren zur Verhängung von Geldbußen einzuleiten, oder beides zu tun;

b) eine Verschiebung des Beginns oder eine Aussetzung der Erbringung des Datenvermittlungsdienstes bis zu den von der für Datenvermittlungsdienste zuständigen Behörde geforderten Änderungen seiner Bedingungen anzuordnen oder

c) die Einstellung der Bereitstellung des Datenvermittlungsdienstes anzuordnen, falls schwere oder wiederholte Verstöße trotz der vorherigen Mitteilung gemäß Absatz 3 nicht behoben wurden.

Die für Datenvermittlungsdienste zuständige Behörde fordert die Kommission auf, den Anbieter des Datenvermittlungsdienstes aus dem Register der Anbieter von Datenvermittlungsdiensten zu streichen, sobald sie die Einstellung der Bereitstellung von Datenvermittlungsdiensten gemäß Unterabsatz 1 Buchstabe c angeordnet hat.

Wenn ein Anbieter von Datenvermittlungsdiensten die Verstöße beseitigt, teilt dieser Anbieter von Datenvermittlungsdiensten dies erneut der für Datenvermittlungsdienste zuständigen Behörde mit. Die für Datenvermittlungsdienste zuständige Behörde teilt der Kommission jede erneute Mitteilung mit.

(5) Wenn ein Anbieter von Datenvermittlungsdiensten, der nicht in der Union niedergelassen ist, keinen gesetzlichen Vertreter benennt oder der gesetzliche Vertreter es versäumt, auf Verlangen der für Datenvermittlungsdienste zuständigen Behörde die erforderlichen Informationen vorzulegen, durch die die Einhaltung dieser Verordnung umfassend belegt wird, ist die für Datenvermittlungsdienste zuständige Behörde befugt, den Beginn der Erbringung des Datenvermittlungsdienstes zu verschieben oder diese auszusetzen, bis der gesetzliche Vertreter benannt wurde oder die erforderlichen Informationen vorgelegt wurden.

(6) Die für Datenvermittlungsdienste zuständigen Behörden teilen dem betreffenden Anbieter der Datenvermittlungsdienste unverzüglich die gemäß den Absätzen 4 und 5 auferlegten Maßnahmen, die Gründe dafür sowie die notwendigen Schritte zur Behebung der entsprechenden Mängel mit und setzen dem Anbieter von Datenvermittlungsdiensten eine angemessene Frist von höchstens 30 Tagen damit der Anbieter von Datenvermittlungsdiensten diesen Maßnahmen nachkommen kann.

(7) Hat ein Anbieter von Datenvermittlungsdiensten für die gemeinsame Datennutzung seine Hauptniederlassung oder seinen gesetzlichen Vertreter in einem Mitgliedstaat, erbringt aber Dienste in anderen Mitgliedstaaten, so arbeiten die für Datenvermittlungsdienste zuständige Behörde des Mitgliedstaats, in dem sich die Hauptniederlassung oder der gesetzliche Vertreter befindet, und die für Datenvermittlungsdienste zuständigen Behörden der betreffenden anderen Mitgliedstaaten zusammen und unterstützen einander. Diese Unterstützung und Zusammenarbeit kann den Informationsaustausch zwischen den betreffenden für Datenvermittlungsdienste zuständigen Behörden für die Zwecke ihrer Tätigkeiten im Rahmen dieser Verordnung und das begründete Ersuchen umfassen, die in diesem Artikel genannten Maßnahmen zu ergreifen.

Ersucht eine für Datenvermittlungsdienste zuständige Behörde in einem Mitgliedstaat um Unterstützung einer für Datenvermittlungsdienste zuständigen Behörden aus einem anderen Mitgliedstaat, so stellt sie ein begründetes Ersuchen. Die für Datenvermittlungsdienste zuständige Behörde antwortet dieses Ersuchen unverzüglich und innerhalb einer Frist, die der Dringlichkeit des Ersuchens angemessen ist.

Alle Informationen, die im Zusammenhang mit einem Amtshilfeersuchen und geleisteter Amtshilfe nach diesem Artikel ausgetauscht werden, dürfen nur zu den Zwecken verwendet werden, für die um sie ersucht wurde.

Artikel 15
Ausnahmen

Dieses Kapitel gilt nicht für anerkannte datenaltruistische Organisationen und andere Einrichtungen ohne Erwerbszweck, soweit deren Tätigkeit darin besteht, für Ziele von allgemeinem Interesse Daten zu erheben, die von natürlichen oder juristischen Personen auf der Grundlage des Datenaltruismus zur Verfügung gestellt werden, es sei denn, diese Organisationen und Einrichtungen sind bestrebt, Geschäftsbeziehungen zwischen einer unbestimmten Zahl von betroffenen Personen und Dateninhabern einerseits und Datennutzern andererseits herzustellen.

KAPITEL IV
Datenaltruismus

Artikel 16
Nationale Regelungen für Datenaltruismus

Die Mitgliedstaaten können organisatorische oder technische Regelungen oder beides festlegen, um Datenaltruismus zu erleichtern. Hierzu können die Mitgliedstaaten nationale Strategien für Datenaltruismus festlegen. Diese nationalen Strategien können insbesondere dazu dienen, betroffene Personen dabei zu unterstützen, sie betreffende personenbezogene Daten im Besitz öffentlicher Stellen freiwillig für den Datenaltruismus zur Verfügung zu stellen, und die erforderlichen Informationen festzulegen, die betroffenen Personen in Bezug auf die Weiterverwendung ihrer Daten im allgemeinen Interesse zur Verfügung gestellt werden müssen.

Entwickelt ein Mitgliedstaat solche nationalen Strategien, so teilt er dies der Kommission mit.

Artikel 17
Öffentliche Register der anerkannten datenaltruistischen Organisationen

(1) Jede für die Registrierung von datenaltruistischen Organisationen zuständige Behörde führt ein öffentliches nationales Register der anerkannten datenaltruistischen Organisationen und aktualisiert dieses regelmäßig.

(2) Die Kommission pflegt zu Informationszwecken ein öffentliches Unionsregister der anerkannten datenaltruistischen Organisationen. Sofern eine gemäß Artikel 18 im öffentlichen nationalen Register der anerkannten datenaltruistischen Organisationen eingetragene Einrichtung registriert ist, darf sie in ihrer schriftlichen und mündlichen Kommunikation die Bezeichnung „in der Union anerkannte datenaltruistische Organisation“ und ein gemeinsames Logo verwenden.

Damit anerkannte datenaltruistische Organisationen in der gesamten Union leicht zu erkennen sind, legt die Kommission im Wege von Durchführungsrechtsakten die Ausgestaltung des gemeinsamen Logos fest. Anerkannte datenaltruistische Organisationen verwenden das gemeinsame Logo gut sichtbar auf jeder Online- und Offline-Veröffentlichung, die mit ihren datenaltruistischen Tätigkeiten in Zusammenhang steht. Das gemeinsame Logo erscheint gemeinsam mit einem QR-Code mit Link zum öffentlichen Unionsregister der anerkannten datenaltruistischen Organisationen.

Die Durchführungsrechtsakte werden nach dem in Artikel 33 Absatz 2 genannten Beratungsverfahren erlassen.

Artikel 18
Allgemeine Eintragungsanforderungen

Um für eine Eintragung in ein öffentliches nationales Register anerkannter datenaltruistischer Organisationen infrage zu kommen, muss eine Einrichtung

a) datenaltruistische Tätigkeiten durchführen;

b) gemäß nationalem Recht Rechtspersönlichkeit haben, um gegebenenfalls gemäß dem nationalen Recht Ziele von allgemeinem Interesse zu erreichen;

c) selbst ohne Erwerbszweck tätig sein und rechtlich unabhängig von jeder Organisation, die Erwerbszwecke verfolgt, handeln;

d) die Datenaltruismus-Tätigkeiten über eine Struktur ausüben, die von ihren anderen Tätigkeiten funktionell getrennt ist;

e) dem in Artikel 22 Absatz 1 genannten Regelwerk entsprechen, und zwar spätestens 18 Monate nach dem Tag des Inkrafttretens der delegierten Rechtsakte, auf die in jenem Absatz Bezuggenommen wird.

Artikel 19
Eintragung anerkannter datenaltruistischer Organisationen

(1) Eine Einrichtung, die die Anforderungen des Artikels 18 erfüllt, kann einen Antrag auf Eintragung in das nationale öffentliche Register der anerkannten datenaltruistischen Organisationen in dem Mitgliedstaat stellen, in dem sie niedergelassen ist.

(2) Eine Einrichtung, die die Anforderungen des Artikels 18 erfüllt und in mehreren Mitgliedstaaten niedergelassen ist, kann einen Antrag zur Eintragung in das nationale öffentliche Register der anerkannten datenaltruistischen Organisationen in dem Mitgliedstaat beantragen, in dem sie ihre Hauptniederlassung hat.

(3) Eine Einrichtung, die die Anforderungen des Artikels 18 erfüllt, aber nicht in der Union niedergelassen ist, benennt einen gesetzlichen Vertreter in einem der Mitgliedstaaten, in dem diese datenaltruistischen Dienste angeboten werden.

Um die Einhaltung dieser Verordnung sicherzustellen, beauftragt die Einrichtung den gesetzlichen Vertreter, neben ihr oder an ihrer Stelle für die Registrierung datenaltruistischer Organisationen den zuständigen Behörden oder betroffenen Personen und Dateninhabern bei Fragen im Zusammenhang mit diesen Einrichtungen als Anlaufstelle zu dienen. Der gesetzliche Vertreter arbeitet mit den für die Registrierung datenaltruistischer Organisationen zuständigen Behörden zusammen und legt ihnen auf Verlangen umfassend dar, welche Maßnahmen und Vorkehrungen die Einrichtung getroffen hat, um die Einhaltung dieser Verordnung sicherzustellen.

Die Einrichtung gilt als in der Zuständigkeit des Mitgliedstaats liegend, in dem der gesetzliche Vertreter niedergelassen ist. Die Einrichtung kann einen Antrag zur Registrierung in das nationale öffentliche Register der anerkannten datenaltruistischen Organisationen in diesem Mitgliedstaat beantragen. Die Benennung eines gesetzlichen Vertreters durch die Einrichtung erfolgt unbeschadet etwaiger rechtlicher Schritte gegen die Einrichtung.

(4) Der Eintragungsantrag gemäß den Absätzen 1, 2 und 3 muss folgende Angaben enthalten:

a) den Namen der Einrichtung,

b) Rechtsstatus, Rechtsform und, sofern die Einrichtung in einem öffentlichen nationalen Register eingetragen ist, Registernummer der Einrichtung,

c) die Satzung der Einrichtung, falls zutreffend,

d) die Einnahmequellen der Einrichtung,

e) die Anschrift der Hauptniederlassung der Einrichtung in der Union, falls vorhanden, und die Anschrift einer etwaigen Zweigniederlassung in einem anderen Mitgliedstaat oder des gesetzlichen Vertreters,

f) eine öffentliche Website mit vollständigen und aktuellen Informationen über die Einrichtung und ihre Tätigkeiten, einschließlich mindestens der Informationen gemäß den Buchstaben a, b, d, e und h,

g) die Kontaktpersonen und Kontaktangaben der Einrichtung,

h) die Ziele von allgemeinem Interesse, die sie mit der Erhebung der Daten fördern will,

i) die Art der Daten, die die Einrichtung überprüfen oder verarbeiten will, sowie, im Fall von personenbezogenen Daten, die Kategorien von personenbezogenen Daten,

j) alle sonstigen Nachweise, die belegen, dass die Anforderungen des Artikels 18 erfüllt werden.

(5) Nachdem die Einrichtung alle erforderlichen Informationen gemäß Absatz 4 übermittelt hat und die für die Registrierung datenaltruistischer Organisationen zuständige Behörde den Eintragungsantrag bewertet hat und zu dem Schluss gekommen ist, dass die Einrichtung die Anforderungen des Artikels 18 erfüllt, nimmt die Behörde innerhalb von 12 Wochen nach Eingang des Antrags auf Registrierung die Eintragung der Einrichtung in das öffentliche nationale Register der anerkannten datenaltruistischen Organisationen vor. Die Eintragung gilt in allen Mitgliedstaaten.

Die für die Registrierung von datenaltruistischen Organisationen zuständige Behörde teilt der Kommission jede Registrierung mit. Die Kommission nimmt diese Registrierung in das öffentliche Unionsregister der anerkannten datenaltruistischen Organisationen auf.

(6) Die in Absatz 4 Buchstaben a, b, f, g und h genannten Angaben werden im einschlägigen öffentlichen nationalen Register der anerkannten datenaltruistischen Organisationen veröffentlicht.

(7) Eine anerkannte datenaltruistische Organisation teilt der entsprechenden für die Registrierung von datenaltruistischen Organisationen zuständigen Behörde jede Änderung der gemäß Absatz 4 übermittelten Angaben innerhalb von 14 Tagen ab dem Tag der Änderung mit.

Die für die Registrierung datenaltruistischer Organisationen zuständigen Behörde teilt der Kommission unverzüglich jede solche Mitteilung auf elektronischem Wege mit. Auf der

Grundlage einer solchen Meldung aktualisiert die Kommission unverzüglich das öffentliche Unionsregister der anerkannten datenaltruistischen Organisationen.

Artikel 20
Transparenzanforderungen

(1) Eine anerkannte datenaltruistische Organisation führt vollständige und genaue Aufzeichnungen über Folgendes:

a) alle natürlichen oder juristischen Personen, denen die Möglichkeit zur Verarbeitung der im Besitz dieser anerkannten datenaltruistischen Organisation befindlichen Daten gegeben wurde, sowie deren Kontaktdaten,

b) den Zeitpunkt oder die Dauer der Verarbeitung personenbezogener Daten oder der Nutzung nicht personenbezogener Daten,

c) den Zweck der Verarbeitung entsprechend der Erklärung der natürlichen oder juristischen Person, der die Möglichkeit zur Verarbeitung gegeben wurde,

d) etwaige Gebühren, die von den die Daten verarbeitenden natürlichen oder juristischen Personen gezahlt wurden.

(2) Eine anerkannte datenaltruistische Organisation erstellt einen jährlichen Tätigkeitsbericht und übermittelt ihn der entsprechenden für die Eintragung von datenaltruistischen Organisationen zuständigen Behörde; dieser Bericht enthält mindestens Folgendes:

a) Informationen über die Tätigkeiten der anerkannten datenaltruistischen Organisation,

b) eine Beschreibung, in welcher Weise die Zwecke von allgemeinem Interesse, zu denen die Daten gesammelt wurden, in dem betreffenden Geschäftsjahr gefördert wurden,

c) eine Liste aller natürlichen und juristischen Personen, denen erlaubt wurde, die in ihrem Besitz befindlichen Daten zu verarbeiten, einschließlich einer zusammenfassenden Beschreibung der Zwecke von allgemeinem Interesse, die mit dieser Datenverarbeitung verfolgt wurden, und einer Beschreibung der hierzu herangezogenen technischen Mittel, die auch eine Beschreibung der zur Wahrung der Privatsphäre und des Datenschutzes eingesetzten Techniken umfasst,

d) gegebenenfalls eine Zusammenfassung der Ergebnisse der von der anerkannten datenaltruistischen Organisationerlaubten Datenverarbeitung,

e) Informationen über die Einnahmequellen der anerkannten datenaltruistischen Organisation, insbesondere alle Einnahmen aus der Zugänglichmachung der Daten, sowie über die Ausgaben.

Artikel 21
Besondere Anforderungen zum Schutz der Rechte und Interessen betroffener Personen und Dateninhaber im Hinblick auf ihre Daten

(1) Eine anerkannte datenaltruistische Organisation informiert betroffene Personen oder Dateninhaber vor der Verarbeitung ihrer Daten auf klare und leicht verständliche Weise über Folgendes:

a) die Ziele von allgemeinem Interesse und gegebenenfalls den angegebenen, ausdrücklichen und rechtmäßigen Zweck der Verarbeitung personenbezogener Daten, für die sie die Verarbeitung ihrer Daten durch einen Datennutzer erlaubt;

b) den Standort und die Ziele von allgemeinem Interesse, für die sie eine etwaige Verarbeitung in einem Drittland erlaubt, sofern die Verarbeitung von der anerkannten datenaltruistischen Organisation vorgenommen wird.

(2) Die anerkannte datenaltruistische Organisation verwendet die Daten nicht für andere als die Ziele von allgemeinem Interesse, für die die betroffene Person oder der Dateninhaber die Verarbeitung erlaubt hat. Die anerkannte datenaltruistische Organisation darf keine irreführenden Vermarktungspraktiken verwenden, um Daten zu erhalten.

(3) Die anerkannte datenaltruistische Organisation stellt Werkzeuge zur Einholung der Einwilligung betroffener Personen oder der Erlaubnis zur Verarbeitung der von Dateninhabern zur Verfügung gestellten Daten bereit. Die anerkannte datenaltruistische Organisation stellt ferner Werkzeuge zum einfachen Widerruf einer solchen Einwilligung oder Erlaubnis zur Verfügung.

(4) Die anerkannte datenaltruistische Organisation ergreift Maßnahmen, um ein angemessenes Sicherheitsniveau für die Speicherung und Verarbeitung der nicht personenbezogenen Daten sicherzustellen, die sie auf der Grundlage von Datenaltruismus erhoben hat.

(5) Die Dateninhaber werden von der anerkannten datenaltruistischen Organisation im Falle einer unbefugten Übertragung, des unbefugten Zugriffs oder der unbefugten Nutzung der von ihm geteilten nicht personenbezogenen Daten unverzüglich unterrichtet.

(6) Ermöglicht die anerkannte datenaltruistische Organisation die Datenverarbeitung durch Dritte, einschließlich durch die Bereitstellung von Werkzeugen zur Einholung der Einwilligung betroffener Personen oder der Erlaubnis zur Verarbeitung der von Dateninhabern zur Verfügung gestellten Daten bereit, so gibt sie gegebenenfalls das Hoheitsgebiet des Drittlandes an, in denen die Datennutzung stattfinden soll.

Artikel 22
Regelwerk

(1) Die Kommission erlässt gemäß Artikel 32 delegierte Rechtsakte zur Ergänzung der vorliegenden Verordnung durch die Ausarbeitung eines Regelwerks, das Folgendes enthält:

a) angemessene Informationsanforderungen, um sicherzustellen, dass betroffene Personen und Dateninhaber vor Erteilung einer Einwilligung oder Erlaubnis für Datenaltruismus ausreichend detaillierte, klare und transparente Informationen über die Datennutzung, die Werkzeuge zur Erteilung und zum Widerruf der Einwilligung oder Erlaubnis und über die Maßnahmen erhalten, die ergriffen werden, um

einen Missbrauch der mit der datenaltruistischen Organisation ausgetauschten Daten zu verhindern,

b) geeignete technische Anforderungen und Sicherheitsanforderungen, um ein angemessenes Sicherheitsniveau für die Speicherung und Verarbeitung von Daten sowie für die Werkzeuge zur Erteilung und zum Widerruf der Einwilligung oder der Erlaubnis,

c) Kommunikationsfahrpläne, bei denen ein multidisziplinärer Ansatz verfolgt wird, um das Bewusstsein für Datenaltruismus, die Bezeichnung als „in der Union anerkannte datenaltruistische Organisation" und das Regelwerk unter den einschlägigen Interessenträgern, insbesondere Dateninhabern und betroffenen Personen, die möglicherweise ihre Daten austauschen würden, zu schärfen,

d) Empfehlungen zu einschlägigen Interoperabilitätsnormen.

(2) Das in Absatz 1 genannte Regelwerk wird in enger Zusammenarbeit mit datenaltruistischen Organisationen und einschlägigen Interessenträgern erstellt.

Artikel 23
Für die Registrierung von datenaltruistischen Organisationen zuständige Behörden

(1) Jeder Mitgliedstaat benennt eine oder mehrere zuständige Behörden, die für das öffentliche nationale Register der anerkannten datenaltruistischen Organisationen zuständig sind.

Die für die Registrierung von datenaltruistischen Organisationen zuständigen Behörden müssen den Anforderungen gemäß Artikel 26 entsprechen.

(2) Jeder Mitgliedstaat teilt der Kommission den Namen seiner für die Registrierung von datenaltruistischen Organisationen zuständigen Behörden bis zum 24. September 2023 mit. Jeder Mitgliedstaat teilt der Kommission auch alle späteren Änderungen der Namen dieser zuständigen Behörden mit.

(3) Die für die Eintragung von datenaltruistischen Organisationen zuständige Behörde nimmt ihre Aufgaben in Bezug auf die Verarbeitung personenbezogener Daten in Zusammenarbeit mit der einschlägigen Datenschutzbehörde sowie mit den einschlägigen sektoralen Behörden desselben Mitgliedstaats wahr.

Artikel 24
Überwachung der Einhaltung

(1) Die für die Registrierung von datenaltruistischen Organisationen zuständigen Behörden überwachen und beaufsichtigen die Einhaltung der in diesem Kapitel festgelegten Anforderungen durch die anerkannten datenaltruistischen Organisationen. Die für die Eintragung von datenaltruistischen Organisationen zuständige Behörde kann die Einhaltung der Rechtsvorschriften durch diese datenaltruistischen Organisationen auch auf Antrag einer natürlichen oder juristischen Person überwachen und beaufsichtigen.

(2) Die für die Registrierung von datenaltruistischen Organisationen zuständigen Behörden sind befugt, von den anerkannten datenaltruistischen Organisationen alle Informationen zu verlangen, die nötig sind, um die Einhaltung der Anforderungen dieses Kapitels zu überprüfen. Jede Anforderung von Informationen muss in angemessenem Verhältnis zur Wahrnehmung dieser Aufgabe stehen und begründet sein.

(3) Stellt die für die Registrierung von datenaltruistischen Organisationen zuständige Behörde fest, dass eine anerkannte datenaltruistische Organisation gegen eine oder mehrere Anforderungen dieses Kapitels verstößt, teilt sie dies der anerkannten datenaltruistischen Organisation mit und gibt ihr Gelegenheit, innerhalb von 30 Tagen nach Erhalt der Meldung dazu Stellung zu nehmen.

(4) Die für die Registrierung von datenaltruistischen Organisationen zuständige Behörde ist befugt, die Beendigung des in Absatz 3 genannten Verstoßes entweder unverzüglich oder innerhalb einer angemessenen Frist zu verlangen, und ergreift angemessene und verhältnismäßige Maßnahmen, um die Einhaltung sicherzustellen.

(5) Erfüllt eine anerkannte datenaltruistische Organisation eine oder mehrere der Anforderungen dieses Kapitels auch dann nicht, nachdem sie von der für die Registrierung von datenaltruistischen Organisationen zuständigen Behörde gemäß Absatz 3 davon unterrichtet wurde, so

a) verliert sie ihr Recht, in ihrer schriftlichen und mündlichen Kommunikation die Bezeichnung „in der Union anerkannte datenaltruistische Organisation“ zu führen,

b) wird sie aus dem einschlägigen öffentlichen nationalen Register der anerkannten datenaltruistischen Organisationen und dem öffentlichen Unionsregister der anerkannten datenaltruistischen Organisationen gestrichen.

Jede Entscheidung gemäß Unterabsatz 1 Buchstabe a, die das Recht widerruft, die Bezeichnung „in der Union anerkannte datenaltruistische Organisation“ zu führen, wird durch die für die Registrierung von datenaltruistischen Organisationen zuständige Behörde öffentlich zugänglich gemacht.

(6) Hat eine anerkannte datenaltruistische Organisation ihre Hauptniederlassung oder ihren gesetzlichen Vertreter in einem Mitgliedstaat, betätigt sich aber in anderen Mitgliedstaaten, so arbeiten die für die Registrierung von datenaltruistischen Organisationen zuständige Behörde des Mitgliedstaats, in dem sich die Hauptniederlassung oder der gesetzliche Vertreter befindet, und die für die Registrierung von datenaltruistischen Organisationen zuständigen Behörden der betreffenden anderen Mitgliedstaaten zusammen und unterstützen einander. Diese Unterstützung und Zusammenarbeit kann den Informationsaustausch zwischen den betreffenden für die Registrierung von datenaltruistischen Organisationen zuständigen Behörden für die Zwecke ihrer Tätigkeiten im Rahmen dieser Verordnung und begründete Ersuchen umfassen, die in diesem Artikel genannten Maßnahmen zu ergreifen.

Ersucht eine für die Registrierung von datenaltruistischen Organisationen zuständige Behörde in einem Mitgliedstaat um Unterstützung durch eine für die Registrierung von datenaltruistischen Organisationen zuständige Behörde in einem anderen Mitgliedstaat, so stellt sie ein begründetes Ersuchen. Nach einem solchen Ersuchen antwortet die für die Registrierung von datenaltruistischen Organisationen zuständige Behörde unverzüglich und innerhalb eines Zeitrahmens, der der Dringlichkeit des Ersuchens angemessen ist.

Alle Informationen, die im Zusammenhang mit einem Amtshilfeersuchen und geleisteter Amtshilfe nach diesem Artikel ausgetauscht werden, dürfen nur zu den Zwecken des Ersuchens verwendet werden.

Artikel 25
Europäisches Einwilligungsformular für Datenaltruismus

(1) Um die Erhebung von Daten auf der Grundlage des Datenaltruismus zu erleichtern, erlässt die Kommission nach Konsultation des Europäischen Datenschutzausschusses, unter Berücksichtigung der Empfehlungen des Europäischen Dateninnovationsrats sowie unter entsprechender Einbeziehung einschlägiger Interessenträger Durchführungsrechtsakte zur Festlegung und Ausarbeitung eines europäischen Einwilligungsformulars für Datenaltruismus. Das Formular ermöglicht das Einholen von Einwilligungen und Erlaubnissen in allen Mitgliedstaaten in einem einheitlichen Format. Diese Durchführungsrechtsakte werden nach dem in Artikel 33 Absatz 2 genannten Beratungsverfahren erlassen.

(2) Das europäische Einwilligungsformular für Datenaltruismus ist modular aufgebaut, damit es für bestimmte Sektoren und für verschiedene Zwecke angepasst werden kann.

(3) Werden personenbezogene Daten erfasst, so ermöglicht das europäische Einwilligungsformular für Datenaltruismus es, dass betroffene Personen gemäß der Verordnung (EU) 2016/679 damit ihre Einwilligung zu einem bestimmten Datenverarbeitungsvorgang erteilen und widerrufen können.

(4) Das Formular ist leicht verständlich und wird in einer Form bereitgestellt, in der es auf Papier ausgedruckt werden kann, sowie in elektronischer, maschinenlesbarer Form.

KAPITEL V
Zuständige Behörden und Verfahrensvorschriften

Artikel 26
Anforderungen an zuständige Behörden

(1) Die für Datenvermittlungsdienste zuständigen Behörden und die für die Registrierung von datenaltruistischen Organisationen zuständigen Behörden müssen von allen Anbietern von Datenvermittlungsdiensten und allen anerkannten datenaltruistischen Organisationen rechtlich getrennt und funktional unabhängig sein. Die Aufgaben der für Datenvermittlungsdienste zuständigen Behörden und der für die Registrierung von datenaltruistischen Organisationen zuständigen Behörden können von derselben Behörde wahrgenommen werden. Die Mitgliedstaaten können entweder eine oder mehrere neue Behörden für diese Zwecke errichten oder bereits vorhandene Behörden nutzen.

(2) Die für Datenvermittlungsdienste zuständigen Behörden und die für die Registrierung von datenaltruistischen Organisationen zuständigen Behörden nehmen ihre Aufgaben unparteiisch, transparent, kohärent und rechtzeitig wahr. Bei der Wahrnehmung ihrer Aufgaben sorgen sie für einen fairen Wettbewerb und Diskriminierungsfreiheit.

(3) Die oberste Leitungsebene und die Mitarbeiter, die für die Durchführung der in dieser Verordnung vorgesehenen einschlägigen Aufgaben der für Datenvermittlungsdienste zuständigen Behörden und der für die Registrierung von datenaltruistischen Organisationen zuständigen Behörden verantwortlich sind, dürfen weder Konstrukteur, Hersteller, Lieferant, Installateur, Käufer, Eigentümer, Verwender oder Wartungsbetrieb der von ihnen bewerteten Dienste noch bevollmächtigter Vertreter einer dieser Parteien sein. Dies schließt die Verwendung von bewerteten Diensten, die für die Tätigkeit der für Datenvermittlungsdienste zuständigen Behörde und der für die Registrierung von datenaltruistischen Organi-

sationen zuständigen Behörde nötig sind, oder die Verwendung solcher Dienste zum persönlichen Gebrauch nicht aus.

(4) Die oberste Leitungsebene und die Mitarbeiter der für Datenvermittlungsdienste zuständigen Behörden und der für die Registrierung von datenaltruistischen Organisationen zuständigen Behörden dürfen sich nicht mit Tätigkeiten befassen, die ihre Unabhängigkeit bei der Beurteilung oder ihre Integrität im Zusammenhang mit den ihnen übertragenen Bewertungstätigkeiten beeinträchtigen könnten.

(5) Die für Datenvermittlungsdienste zuständigen Behörden und die für die Registrierung von datenaltruistischen Organisationen zuständigen Behörden müssen über angemessene finanzielle und personelle Mittel verfügen, um die ihnen übertragenen Aufgaben erfüllen zu können, einschließlich der erforderlichen Fachkenntnisse und Ressourcen.

(6) Die für Datenvermittlungsdienste zuständigen Behörden und die für die Registrierung von datenaltruistischen Organisationen zuständigen Behörden eines Mitgliedstaats stellen der Kommission und den für Datenvermittlungsdienste zuständigen Behörden und den für die Registrierung von datenaltruistischen Organisationen zuständigen Behörden anderer Mitgliedstaaten auf begründeten Antrag und unverzüglich die Informationen zur Verfügung, die sie zur Wahrnehmung ihrer Aufgaben gemäß dieser Verordnung benötigen. Sieht eine für Datenvermittlungsdienste zuständige Behörden oder eine für die Registrierung von datenaltruistischen Organisationen zuständige Behörde die verlangten Informationen nach den Bestimmungen des Unionsrechts und des nationalen Rechts über das Berufs- und Geschäftsgeheimnis als vertraulich an, so gewährleisten die Kommission und alle anderen für Datenvermittlungsdienste zuständigen Behörden und die für die Registrierung von datenaltruistischen Organisationen zuständigen Behörden eine entsprechende vertrauliche Behandlung.

Artikel 27
Beschwerderecht

(1) Natürliche und juristische Personen haben das Recht, wegen aller in den Anwendungsbereich dieser Verordnung fallenden Angelegenheiten bei der jeweiligen, für die Datenvermittlungsdienste zuständigen Behörde, allein oder gegebenenfalls gemeinsam, Beschwerde gegen einen Anbieter von Datenvermittlungsdiensten oder bei der jeweiligen, für die Registrierung von datenaltruistischen Organisationen gegen eine anerkannte datenaltruistische Organisation einzulegen.

(2) Die für Datenvermittlungsdienste zuständige Behörde und die für die Registrierung von datenaltruistischen Organisationen zuständige Behörde, bei der die Beschwerde eingelegt wurde, unterrichtet den Beschwerdeführer

a) über den Stand des Verfahrens und die getroffene Entscheidung und

b) über die Möglichkeit eines gerichtlichen Rechtsbehelfs nach Artikel 28.

Artikel 28
Recht auf einen wirksamen gerichtlichen Rechtsbehelf

(1) Jede betroffene natürliche oder juristische Person hat unbeschadet eines anderweitigen verwaltungsrechtlichen oder außergerichtlichen Rechtsbehelfs das Recht auf einen wirksamen gerichtlichen Rechtsbehelf gegen rechtsverbindliche Entscheidungen gemäß Artikel 14 durch die für Datenvermittlungsdienste zuständigen Behörden in Bezug auf die Verwal-

tung, Kontrolle und Durchsetzung der Anmeldevorschriften für Anbieter von Datenvermittlungsdiensten und rechtsverbindliche Entscheidungen gemäß Artikel 19 und 24 durch die für die Registrierung von datenaltruistischen Organisationen zuständigen Behörden in Bezug auf die Überwachung von anerkannten datenaltruistischen Organisationen.

(2) Verfahren nach diesem Artikel werden bei den Gerichten des Mitgliedstaats der für Datenvermittlungsdienste zuständigen Behörde und der für die Registrierung von datenaltruistischen Organisationen zuständigen Behörde, gegen die der allein oder gegebenenfalls gemeinsam von den Vertretern einer oder mehrerer natürlicher oder juristischer Personen eingelegte Rechtsbehelf gerichtet ist, eingeleitet.

(3) Bleibt eine für Datenvermittlungsdienste zuständige Behörde oder eine für die Registrierung von datenaltruistischen Organisationen zuständige Behörde auf eine Beschwerde untätig, haben betroffene natürliche und juristische Personen gemäß dem nationalen Recht entweder Anspruch auf einen wirksamen gerichtlichen Rechtsbehelf oder Zugang zur Nachprüfung durch eine unparteiische Stelle mit entsprechender Sachkenntnis.

KAPITEL VI
Europäischer Dateninnovationsrat

Artikel 29
Europäischer Dateninnovationsrat

(1) Die Kommission setzt einen Europäischen Dateninnovationsrat ein, der die Form einer Expertengruppe hat und sich aus Vertretern der für Datenvermittlungsdienste zuständige Behörden und der für die Registrierung von datenaltruistischen Organisationen zuständigen Behörden aller Mitgliedstaaten, des Europäischen Datenschutzausschusses, des Europäischen Datenschutzbeauftragten, der ENISA, der Kommission, dem KMU-Beauftragten der EU oder einem vom Netz der KMU-Beauftragten benannten Vertreter und anderen Vertretern von maßgeblichen Stellen in bestimmten Sektoren und von Stellen mit spezifischen Fachkenntnissen zusammensetzt. Bei der Ernennung einzelner Sachverständiger strebt die Kommission im Hinblick auf die Zusammensetzung der Expertengruppe ein ausgewogenes Geschlechterverhältnis und geografische Ausgewogenheit unter den Mitgliedern der Expertengruppe an.

(2) Der Europäische Dateninnovationsrat besteht aus mindestens den drei folgenden Untergruppen:

a) einer aus den für Datenvermittlungsdienste zuständigen Behörden und den für die Registrierung von datenaltruistischen Organisationen zuständigen Behörden zusammengesetzten Untergruppe für die Aufgaben gemäß Artikel 30 Buchstaben a, c, j und k,

b) einer Untergruppe für technische Beratungen zu Normung, Übertragbarkeit und Interoperabilität gemäß Artikel 30 Buchstaben f und g,

c) einer Untergruppe für die Einbeziehung von Interessenträgern, der einschlägige Vertreter der Wirtschaft, der Forschung, der Wissenschaft, der Zivilgesellschaft, von Normungsgremien, einschlägigen gemeinsamen europäischen Datenräumen und andere einschlägige Interessenträger und Dritte angehören, die den Europäischen Dateninnovationsrat zu Aufgaben gemäß Artikel 30 Buchstaben d, e, f, g und h beraten.

(3) Die Kommission führt den Vorsitz in den Sitzungen des Europäischen Dateninnovationsrats.

(4) Der Europäische Dateninnovationsrat wird von einem Sekretariat unterstützt, das von der Kommission gestellt wird.

Artikel 30
Aufgaben des Europäischen Dateninnovationsrats

Der Europäische Dateninnovationsrat hat folgende Aufgaben:

a) Beratung und Unterstützung der Kommission bei der Entwicklung einer einheitlichen Praxis der öffentlichen Stellen und der in Artikel 7 Absatz 1 genannten zuständigen Stellen für die Bearbeitung von Anträgen auf Weiterverwendung von Daten der in Artikel 3 Absatz 1 genannten Datenkategorien;

b) Beratung und Unterstützung der Kommission bei der Entwicklung einer einheitlichen Praxis für den unionsweiten Datenaltruismus;

c) Beratung und Unterstützung der Kommission bei der Entwicklung einer einheitlichen Praxis der für Datenvermittlungsdienste zuständigen Behörden und der für die Registrierung von datenaltruistischen Organisationen zuständigen Behörden bei der Anwendung der Anforderungen, die jeweils für Anbieter von Datenvermittlungsdiensten und anerkannte datenaltruistische Organisationen gelten;

d) Beratung und Unterstützung der Kommission bei der Entwicklung einheitlicher Leitlinien dazu, wie nicht personenbezogene sensible Geschäftsdaten, vor allem Geschäftsgeheimnisse, aber auch nicht personenbezogene Daten von Inhalten, die durch Rechte des geistigen Eigentums geschützt sind, vor unrechtmäßigem Zugriff, der möglicherweise den Diebstahl geistigen Eigentums oder Industriespionage zur Folge hat, optimal geschützt werden können;

e) Beratung und Unterstützung der Kommission bei der Entwicklung einheitlicher Leitlinien zu Cybersicherheitsanforderungen beim Austausch und der Speicherung von Daten;

f) Beratung der Kommission unter besonderer Berücksichtigung der Beiträge von Normungsgremien bei der Festlegung von Prioritäten für die Verwendung bzw. Entwicklung sektorübergreifender Normen für die Datennutzung und sektorübergreifende gemeinsame Datennutzung durch neue gemeinsame europäische Datenräume sowie für den sektorübergreifenden Vergleich und Austausch bewährter Verfahren in Bezug auf Sicherheitsanforderungen und Zugangsverfahren in bestimmten Sektoren, wobei sektorspezifische Normungstätigkeiten insbesondere bei der Klärung, welche Normen und Praktiken sektorspezifisch und welche sektorübergreifend sind, und bei der diesbezüglichen Differenzierung zu berücksichtigen sind;

g) Unterstützung der Kommission unter besonderer Berücksichtigung der Beiträge von Normungsgremien bei ihren Bemühungen, einer Fragmentierung des Binnenmarkts und der Datenwirtschaft im Binnenmarkt entgegenzuwirken, indem die grenzüberschreitende und die sektorübergreifende Interoperabilität von Daten sowie von Diensten für die gemeinsame Datennutzung zwischen verschiedenen Sektoren und Bereichen auf der Grundlage bestehender europäischer, internationaler

oder nationaler Normen verbessert wird, um unter anderem die Schaffung gemeinsamer europäischer Datenräume zu fördern;

h) Unterbreitung von Leitlinien zu „gemeinsamen europäischen Datenräumen", also zu zweck- oder sektorspezifischen oder auch sektorübergreifenden interoperablen Rahmen mit gemeinsamen Normen und Praktiken für die gemeinsame Nutzung oder Verarbeitung von Daten – unter anderem zur Entwicklung neuer Produkte und Dienste, für die wissenschaftliche Forschung oder für Initiativen der Zivilgesellschaft; solche gemeinsame Normen und Praktiken tragen geltenden Normen Rechnung, entsprechen den Wettbewerbsregeln und gewährleisten den nichtdiskriminierenden Zugang für alle Beteiligten, um die gemeinsame Datennutzung in der Union zu erleichtern und das Potenzial bereits vorhandener und künftiger Datenräume auszuschöpfen; dabei werden folgende Bereiche behandelt:

   i) Verwendung und Entwicklung sektorübergreifender Normen für die Datennutzung und die sektorübergreifende gemeinsame Datennutzung, sektorübergreifender Vergleich und Austausch bewährter Verfahren in Bezug auf sektorale Sicherheitsanforderungen und Zugangsverfahren, wobei sektorspezifische Normungstätigkeiten insbesondere Klärung der Frage, welche Normen und Praktiken sektorspezifisch und welche sektorübergreifend sind, und bei der diesbezüglichen Differenzierung zu berücksichtigen sind,

   ii) Anforderungen bezüglich der Beseitigung von Marktzutrittsbeschränkungen und der Vermeidung von Lock-in-Effekten im Interesse eines fairen Wettbewerbs und der Interoperabilität,

   iii) angemessener Schutz für rechtmäßige Datenübertragungen in Drittländer, einschließlich Schutzvorkehrungen gegen nach Unionsrecht verbotene Datenübertragungen,

   iv) angemessene und nichtdiskriminierende Vertretung der einschlägigen Interessenträger bei der Verwaltung gemeinsamer europäischer Datenräume,

   v) Einhaltung der gemäß dem Unionsrecht geltenden Cybersicherheitsanforderungen.

i) Erleichterung der Zusammenarbeit zwischen den Mitgliedstaaten bezüglich der Festlegung harmonisierter Bedingungen für die Erlaubnis, binnenmarktweit im Besitz öffentlicher Stellen befindliche Kategorien von Daten gemäß Artikel 3 Absatz 1 wiederzuverwenden;

j) Erleichterung der Zusammenarbeit zwischen den für Datenvermittlungsdienste zuständigen Behörden und den für die Registrierung von datenaltruistischen Organisationen zuständigen Behörden mittels Kapazitätsaufbau und Informationsaustausch, insbesondere durch die Festlegung von Methoden für einen effizienten Informationsaustausch über das Anmeldeverfahren für Anbieter von Datenvermittlungsdiensten und die Eintragung und Überwachung anerkannter datenaltruistischer Organisationen, einschließlich der Abstimmung über Gebühren und Sanktionen sowie der Erleichterung der Zusammenarbeit zwischen den für Datenvermittlungsdienste zuständigen Behörden und den für die Registrierung von da-

tenaltruistischen Organisationen zuständigen Behörden beim internationalen Zugang zu Daten und internationale Datenübertragungen;

k) Beratung und Unterstützung der Kommission bei der Prüfung der Frage, ob die Durchführungsrechtsakte gemäß Artikel 5 Absätze 11 und 12 erlassen werden sollen;

l) Beratung und Unterstützung der Kommission bei der Entwicklung des europäischen Einwilligungsformulars für Datenaltruismus gemäß Artikel 25 Absatz 1;

m) Beratung der Kommission bei der Verbesserung des internationalen Regelungsumfelds für nicht personenbezogene Daten einschließlich der Normung.

KAPITEL VII
Internationaler Zugang und internationale Übertragung

Artikel 31
Internationaler Zugang und internationale Übertragung

(1) Die öffentliche Stelle, die natürliche oder juristische Person, der das Recht auf Weiterverwendung von Daten nach Kapitel II gewährt wurde, der Anbieter von Datenvermittlungsdiensten oder die anerkannte datenaltruistische Organisation ergreifen alle angemessenen technischen, rechtlichen und organisatorischen Maßnahmen, einschließlich vertraglicher Vereinbarungen, um die internationale Übertragung in der Union gespeicherter nicht personenbezogener Daten oder den Zugang von Regierungsorganisationen zu diesen Daten zu verhindern, wenn eine solche Übertragung oder ein solcher Zugang im Widerspruch zum Unionsrecht oder dem nationalen Recht des betreffenden Mitgliedstaats stünde; Absatz 2 oder Absatz 3 bleiben davon unberührt.

(2) Entscheidungen und Urteile eines Gerichts eines Drittlands und jegliche Entscheidung einer Verwaltungsbehörde eines Drittlands, mit denen von einer öffentlichen Stelle, einer natürlichen oder juristischen Person, der das Recht auf Weiterverwendung von Daten nach Kapitel II gewährt wurde, einem Anbieter von Datenvermittlungsdiensten oder einer anerkannten datenaltruistischen Organisationen die Übertragung von in der Union gespeicherten nicht personenbezogenen Daten im Anwendungsbereich dieser Verordnung oder der Zugang zu diesen Daten in der Union verlangt wird, werden nur dann anerkannt oder vollstreckbar, wenn sie auf eine in Kraft befindliche völkerrechtliche Übereinkunft wie etwa ein Rechtshilfeabkommen zwischen dem ersuchenden Drittland und der Union oder auf eine solche Vereinbarung zwischen dem ersuchenden Drittland und einem Mitgliedstaat gestützt sind.

(3) Wenn keine völkerrechtliche Übereinkunft gemäß Absatz 2 des vorliegenden Artikels besteht und eine Entscheidung oder ein Urteil eines Gerichts eines Drittlandes oder eine Entscheidung einer Verwaltungsbehörde eines Drittlands, mit der die Übertragung nicht personenbezogener Daten im Anwendungsbereich dieser Verordnung aus der Union oder der Zugang zu diesen Daten in der Union verlangt wird, an eine öffentliche Stelle, eine natürliche oder juristische Person, der das Recht auf Weiterverwendung von Daten nach Kapitel II gewährt wurde, einen Anbieter von Datenvermittlungsdiensten oder eine anerkannte datenaltruistische Organisation gerichtet ist und die Befolgung einer solchen Entscheidung den Adressaten in Widerspruch zum Unionsrecht oder zum nationalen Recht des betreffen-

den Mitgliedstaats bringen würde, erfolgt die Übertragung dieser Daten an die Behörde des Drittlands oder die entsprechende Zugangsgewährung nur dann, wenn

a) das Rechtssystem des Drittlands vorschreibt, dass die Entscheidung oder das Urteil zu begründen ist und verhältnismäßig sein muss, und weiter vorsieht, dass die die Entscheidung oder das Urteil eine hinreichende Bestimmtheit aufweisen muss, indem z. B. darin eine hinreichende Bezugnahme auf bestimmte verdächtige Personen oder Rechtsverletzungen erfolgt,

b) der begründete Einwand des Adressaten von einem zuständigen Gericht des Drittlands überprüft wird und

c) das zuständige Gericht des Drittlands, das die Entscheidung oder das Urteil erlässt oder die Entscheidung einer Verwaltungsbehörde überprüft, nach dem Recht dieses Drittlands befugt ist, die einschlägigen rechtlichen Interessen des Bereitstellers der durch das Unionsrecht oder das nationale Recht des betreffenden Mitgliedstaats geschützten Daten gebührend zu berücksichtigen.

(4) Sind die in Absatz 2 oder 3 festgelegten Bedingungen nicht erfüllt, so überträgt die öffentliche Stelle, die natürliche oder juristische Person, der das Recht auf Weiterverwendung von Daten nach Kapitel II gewährt wurde, der Anbieter von Datenvermittlungsdiensten oder die anerkannte datenaltruistische Organisation aufgrund einer vertretbaren Auslegung des Ersuchens nur die auf das Ersuchen hin zulässige Mindestmenge an Daten.

(5) Bevor die öffentliche Stelle, die natürliche oder juristische Person, der das Recht auf Weiterverwendung von Daten nach Kapitel II gewährt wurde, der Anbieter von Datenvermittlungsdiensten oder die anerkannte datenaltruistische Organisation dem Ersuchen einer Verwaltungsbehörde eines Drittlands auf Zugang zu den Daten eines Dateninhabers nachkommt, unterrichtet sie bzw. er den Dateninhaber über das Vorliegen dieses Ersuchens, es sei denn, das Ersuchen dient Strafverfolgungszwecken, und solange dies zur Wahrung der Wirksamkeit der Strafverfolgungsmaßnahme erforderlich ist.

KAPITEL VIII
Delegierung und Ausschussverfahren

Artikel 32
Ausübung der Befugnisübertragung

(1) Die Befugnis zum Erlass delegierter Rechtsakte wird der Kommission unter den in diesem Artikel festgelegten Bedingungen übertragen.

(2) Die Befugnis zum Erlass delegierter Rechtsakte gemäß Artikel 5 Absatz 13 und Artikel 22 Absatz 1 wird der Kommission auf unbestimmte Zeit ab dem 23. Juni 2022 übertragen.

(3) Die Befugnisübertragung gemäß Artikel 5 Absatz 13 und Artikel 22 Absatz 1 kann vom Europäischen Parlament oder vom Rat jederzeit widerrufen werden. Der Beschluss über den Widerruf beendet die Übertragung der in diesem Beschluss angegebenen Befugnis. Er wird am Tag nach seiner Veröffentlichung im Amtsblatt der Europäischen Union oder zu einem im Beschluss über den Widerruf angegebenen späteren Zeitpunkt wirksam. Die Gültigkeit von delegierten Rechtsakten, die bereits in Kraft sind, wird von dem Beschluss über den Widerruf nicht berührt.

(4) Vor dem Erlass eines delegierten Rechtsakts konsultiert die Kommission die von den einzelnen Mitgliedstaaten benannten Sachverständigen im Einklang mit den in der Interinstitutionellen Vereinbarung vom 13. April 2016 über bessere Rechtsetzung enthaltenen Grundsätzen.

(5) Sobald die Kommission einen delegierten Rechtsakt erlässt, übermittelt sie ihn gleichzeitig dem Europäischen Parlament und dem Rat.

(6) Ein delegierter Rechtsakt, der gemäß Artikel 5 Absatz 13 und Artikel 22 Absatz 1 erlassen wurde, tritt nur in Kraft, wenn weder das Europäische Parlament noch der Rat innerhalb einer Frist von drei Monaten nach Übermittlung dieses Rechtsakts an das Europäische Parlament und den Rat Einwände erhoben haben oder wenn vor Ablauf dieser Frist das Europäische Parlament und der Rat beide der Kommission mitgeteilt haben, dass sie keine Einwände erheben werden. Auf Initiative des Europäischen Parlaments oder des Rates wird diese Frist um drei Monate verlängert.

Artikel 33
Ausschussverfahren

(1) Die Kommission wird von einem Ausschuss unterstützt. Dieser Ausschuss ist ein Ausschuss im Sinne der Verordnung (EU) Nr. 182/2011.

(2) Wird auf diesen Absatz Bezug genommen, so gilt Artikel 4 der Verordnung (EU) Nr. 182/2011.

(3) Wird auf diesen Absatz Bezug genommen, so gilt Artikel 5 der Verordnung (EU) Nr. 182/2011.

KAPITEL IX
Schluss- und Übergangsbestimmungen

Artikel 34
Sanktionen

(1) Die Mitgliedstaaten erlassen Vorschriften über Sanktionen, die bei Verstößen gegen die für die Übertragung nicht personenbezogener Daten in Drittländer gemäß Artikel 5 Absatz 14 und Artikel 31 geltenden Verpflichtungen, die nach Artikel 11 für Anbieter von Datenvermittlungsdiensten geltende Mitteilungspflicht, die gemäß Artikel 12 für die Erbringung von Datenvermittlungsdiensten geltenden Bedingungen und die gemäß den Artikeln 18, 20, 21 und 22 für die Eintragung als anerkannte datenaltruistische Organisation geltenden Bedingungen zu verhängen sind, und treffen alle für die Anwendung der Sanktionen erforderlichen Maßnahmen. Die vorgesehenen Sanktionen müssen wirksam, verhältnismäßig und abschreckend sein. In ihren Sanktionsvorschriften tragen die Mitgliedstaaten den Empfehlungen des Europäischen Dateninnovationsrats Rechnung. Die Mitgliedstaaten teilen der Kommission diese Vorschriften und Maßnahmen bis zum 24. September 2023 mit und melden ihr unverzüglich alle späteren diesbezüglichen Änderungen.

(2) Bei der Verhängung von Sanktionen aufgrund von Verstößen gegen diese Verordnung gegen Anbieter von Datenvermittlungsdiensten und anerkannte datenaltruistische Organisationen berücksichtigen die Mitgliedstaaten, gegebenenfalls die folgenden nicht erschöpfenden und indikativen Kriterien:

a) Art, Schwere, Umfang und Dauer des Verstoßes;

b) Maßnahmen, die der Anbieter von Datenvermittlungsdiensten oder die anerkannte datenaltruistische Organisation zur Minderung oder Behebung des durch den Verstoß bedingten Schadens ergreifen;

c) frühere Verstöße des Anbieters von Datenvermittlungsdiensten oder der anerkannten datenaltruistischen Organisation;

d) die durch den Verstoß bedingten finanziellen Gewinne oder Verluste des Anbieters von Datenvermittlungsdiensten oder der anerkannten datenaltruistischen Organisation, sofern diese Gewinne oder Verluste zuverlässig festgestellt werden können;

e) sonstige erschwerende oder mildernde Umstände im jeweiligen Fall.

Artikel 35
Bewertung und Überprüfung

Bis zum 24. September 2025 führt die Kommission eine Bewertung dieser Verordnung durch und übermittelt dem Europäischen Parlament und dem Rat sowie dem Europäischen Wirtschafts- und Sozialausschuss einen Bericht über ihre wichtigsten Ergebnisse. Dem Bericht werden, soweit erforderlich, Gesetzgebungsvorschläge beigefügt.

Dabei wird in dem Bericht insbesondere Folgendes bewertet:

a) Anwendung und Funktionsweise der von den Mitgliedstaaten gemäß Artikel 34 festgelegten Sanktionsvorschriften;

b) Grad der Einhaltung dieser Verordnung durch die gesetzlichen Vertreter von Anbietern von Datenvermittlungsdiensten und anerkannten datenaltruistischen Organisationen, die nicht in der Union niedergelassen sind, und Grad der Durchsetzbarkeit von verhängten Sanktionen gegen diese Anbieter und Organisationen;

c) Art der gemäß Kapitel IV eingetragenen datenaltruistischen Organisationen und ein Überblick über die mit der gemeinsamen Datennutzung verfolgten Zwecke von allgemeinem Interesse, um diesbezüglich klare Kriterien festzulegen.

Die Mitgliedstaaten übermitteln der Kommission alle zur Ausarbeitung dieses Berichts erforderlichen Informationen.

Artikel 36
Änderung der Verordnung (EU) 2018/1724

[Vom Abdruck wurde abgesehen]

Artikel 38
Inkrafttreten und Geltung

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

Sie gilt ab dem 24. September 2023.

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

Gesetz für die Nutzung von Daten des öffentlichen Sektors (Datennutzungsgesetz – DNG)

§ 1 Grundsatz der offenen Daten

(1) Daten, die in den Anwendungsbereich dieses Gesetzes fallen, sollen, soweit möglich, nach dem Grundsatz „konzeptionell und standardmäßig offen" erstellt werden.

(2) Eine Bereitstellungspflicht oder ein Anspruch auf Zugang zu Daten wird mit diesem Gesetz nicht begründet.

§ 2 Anwendungsbereich

(1) Dieses Gesetz gilt für Daten von Datenbereitstellern nach Absatz 2, die

1. aufgrund eines gesetzlichen Anspruchs auf Zugang bereitgestellt werden,
2. aufgrund einer gesetzlichen Bereitstellungspflicht bereitgestellt werden oder
3. auf sonstige Weise öffentlich oder zur ausschließlichen Nutzung bereitgestellt werden.

(2) Datenbereitsteller im Sinne dieses Gesetzes sind:

1. öffentliche Stellen;
2. Unternehmen der Daseinsvorsorge, die den Vorschriften über die Vergabe von öffentlichen Aufträgen und Konzessionen unterfallen oder öffentliche Personenverkehrsdienste betreiben;
3. in Bezug auf Forschungsdaten, die öffentlich finanziert und bereits über ein institutionelles oder thematisches Repositorium öffentlich bereitgestellt wurden:
   a) Hochschulen, Forschungseinrichtungen und Forschungsfördereinrichtungen,
   b) Forschende, wenn die Forschungsdaten nicht bereits durch andere durch dieses Gesetz verpflichtete Datenbereitsteller bereitgestellt wurden;

   dies gilt nicht, soweit berechtigte Geschäftsinteressen, Wissenstransfertätigkeiten oder bestehende Rechte Dritter an geistigem Eigentum entgegenstehen.

(3) Dieses Gesetz gilt nicht für

1. Daten,
   a) die nicht oder nur eingeschränkt zugänglich sind, wobei eine Einschränkung auch vorliegt, wenn der Zugang nur bei Nachweis eines rechtlichen oder berechtigten Interesses besteht; nicht oder nur eingeschränkt zugänglich sind Daten insbesondere,
      aa) soweit der Schutz personenbezogener Daten entgegensteht,
      bb) soweit der Schutz von Geschäftsgeheimnissen entgegensteht,
      cc) soweit der Schutz der nationalen Sicherheit, der Verteidigung oder der öffentlichen Sicherheit entgegensteht,

dd) soweit die Eigenschaft als vertrauliche Informationen über den Schutz kritischer Infrastrukturen entgegensteht oder

ee) soweit die statistische Geheimhaltung entgegensteht,

b) die geistiges Eigentum Dritter betreffen,

c) die nach den Vorschriften des Bundes oder der Länder über den Zugang der Öffentlichkeit zu Umweltinformationen zugänglich sind und uneingeschränkt, kostenlos, maschinenlesbar und über eine Anwendungsprogrammierschnittstelle nutzbar sind oder

d) deren Bereitstellung nicht unter den durch Rechtsvorschrift festgelegten öffentlichen Auftrag der öffentlichen Stelle fällt;

2. Daten von Unternehmen der Daseinsvorsorge, die außerhalb der Tätigkeit nach § 3 Nummer 2 erstellt wurden;

3. Logos, Wappen und Insignien;

4. Daten von öffentlich-rechtlichen Rundfunkanstalten oder deren Beauftragten, die der Wahrnehmung eines öffentlichen Programm- oder Sendeauftrags dienen;

5. Daten von kulturellen Einrichtungen, außer Bibliotheken, Museen und Archiven; Absatz 2 Nummer 3 findet auf Bibliotheken, Museen und Archive keine Anwendung;

6. Daten von Bildungseinrichtungen der Sekundarstufe und darunter; bei allen sonstigen Bildungseinrichtungen gilt dieses Gesetz nicht für Daten, die keine Forschungsdaten sind.

(4) Die Bestimmungen zum Schutz personenbezogener Daten und weitergehende Anforderungen an die Bereitstellung und Nutzung der Daten von Datenbereitstellern aus anderen Rechtsvorschriften bleiben unberührt.

(5) Öffentliche Stellen berufen sich im Anwendungsbereich dieses Gesetzes nicht auf Rechte des Datenbankherstellers nach § 87b des Urheberrechtsgesetzes.

§ 3 Begriffsbestimmungen

Im Sinne dieses Gesetzes

1. sind öffentliche Stellen

a) Gebietskörperschaften, einschließlich ihrer Sondervermögen,

b) andere juristische Personen des öffentlichen und des privaten Rechts, die zu dem besonderen Zweck gegründet wurden, im Allgemeininteresse liegende Aufgaben nichtgewerblicher Art zu erfüllen, wenn

aa) sie überwiegend von Stellen nach Buchstabe a oder Buchstabe c einzeln oder gemeinsam durch Beteiligung oder auf sonstige Weise finanziert werden,

bb) ihre Leitung der Aufsicht durch Stellen nach Buchstabe a oder Buchstabe c unterliegt oder

cc) mehr als die Hälfte der Mitglieder eines ihrer zur Geschäftsführung oder zur Aufsicht berufenen Organe durch Stellen nach Buchstabe a oder Buchstabe c bestimmt worden sind;

dasselbe gilt, wenn diese juristische Person einer anderen juristischen Person des öffentlichen oder privaten Rechts einzeln oder gemeinsam mit anderen die überwiegende Finanzierung gewährt, über deren Leitung die Aufsicht ausübt oder die Mehrheit der Mitglieder eines zur Geschäftsführung oder Aufsicht berufenen Organs bestimmt hat,

c) Verbände, deren Mitglieder unter Buchstabe a oder Buchstabe b fallen,

2. ist Unternehmen der Daseinsvorsorge ein Unternehmen im Sinne des § 100 Absatz 1 Nummer 2 des Gesetzes gegen Wettbewerbsbeschränkungen, das eine Tätigkeit im Sinne des § 102 des Gesetzes gegen Wettbewerbsbeschränkungen ausübt oder öffentliche Personenverkehrsdienste betreibt,

3. sind Daten vorhandene Aufzeichnungen, unabhängig von der Art ihrer Speicherung,

4. ist Nutzung jede Verwendung von Daten für kommerzielle oder nichtkommerzielle Zwecke, die über die Erfüllung einer öffentlichen Aufgabe oder die Erbringung von Dienstleistungen von allgemeinem Interesse hinausgeht oder die neben der Erfüllung öffentlicher Aufgaben auch zu eigenen kommerziellen Zwecken erfolgt,

5. liegt ein maschinenlesbares Format vor, wenn die Daten durch Software automatisiert ausgelesen und verarbeitet werden können,

6. ist offenes Format ein Dateiformat, das nichtproprietär und plattformunabhängig ist und der Öffentlichkeit ohne Einschränkungen, die der Nutzung von Daten hinderlich wären, zugänglich gemacht wird,

7. ist förmlicher offener Standard ein in Textform niedergelegter Standard, in dem die Anforderungen für die Sicherstellung der Interoperabilität der Software niedergelegt sind,

8. sind dynamische Daten Aufzeichnungen in digitaler Form, die häufig oder in Echtzeit aktualisiert werden, insbesondere aufgrund ihrer Volatilität oder ihres raschen Veraltens,

9. sind hochwertige Datensätze die gemäß den Artikeln 13 und 14 der Richtlinie (EU) 2019/1024 des Europäischen Parlaments und des Rates vom 20. Juni 2019 über offene Daten und die Weiterverwendung von Informationen des öffentlichen Sektors (ABl. L 172 vom 26.6.2019, S. 56) und gemäß den aufgrund dieser Artikel zu erlassenden Durchführungsrechtsakten ausgewiesenen Datensätze,

10. sind Forschungsdaten Aufzeichnungen in digitaler Form, bei denen es sich nicht um wissenschaftliche Veröffentlichungen handelt und die im Laufe von wissenschaftlichen Forschungstätigkeiten erfasst oder erzeugt und als Nachweise im Rahmen des Forschungsprozesses verwendet werden oder die in der Forschungsgemeinschaft allgemein für die Validierung von Forschungsfeststellungen und -ergebnissen als notwendig erachtet werden,

11. ist angemessene Gewinnspanne ein Prozentsatz der Gesamtkosten, der über den zur Deckung der einschlägigen Kosten erforderlichen Betrag hinausgeht, aber

höchstens 5 Prozentpunkte über dem von der Europäischen Zentralbank festgesetzten Zinssatz für Hauptrefinanzierungsgeschäfte liegt,

12. ist Anonymisierung der Prozess, in dessen Verlauf personenbezogene Daten in Daten umgewandelt werden, die sich nicht auf eine identifizierte oder identifizierbare natürliche Person beziehen, oder derart in Daten umgewandelt werden, dass die betroffene Person nicht oder nicht mehr identifiziert werden kann.

§ 4 Grundsatz der uneingeschränkten Datennutzung; Zulässigkeit von Lizenzen

(1) Daten dürfen für jeden kommerziellen oder nichtkommerziellen Zweck genutzt werden.

(2) Für Daten, an denen Bibliotheken, einschließlich Hochschulbibliotheken, Museen und Archive, Urheber- oder verwandte Schutzrechte oder gewerbliche Schutzrechte zustehen, und für Daten von Unternehmen der Daseinsvorsorge gilt Absatz 1 nur, soweit die Einrichtung oder das Unternehmen der Daseinsvorsorge die Nutzung zugelassen hat.

(3) Nutzungsbedingungen (Lizenzen) sind zulässig, soweit sie objektiv, verhältnismäßig, nichtdiskriminierend und durch ein im Allgemeininteresse liegendes Ziel gerechtfertigt sind. Die Lizenz darf nicht zu einer Wettbewerbsverzerrung führen und die Möglichkeiten der Nutzung nicht unnötig einschränken. Öffentliche Stellen sollen nach Möglichkeit offene Lizenzen verwenden.

§ 5 Nichtdiskriminierung

(1) Die Bedingungen für die Datennutzung müssen nichtdiskriminierend sein.

(2) Werden Daten von einer öffentlichen Stelle als Ausgangsmaterial für die eigene Geschäftstätigkeit genutzt, die nicht unter den öffentlichen Auftrag der öffentlichen Stelle fällt, so gelten für die Bereitstellung der Daten für die Geschäftstätigkeit dieselben Entgelte und sonstigen Bedingungen wie für andere Nutzer.

§ 6 Ausschließlichkeitsvereinbarungen

(1) Vereinbarungen öffentlicher Stellen oder Unternehmen der Daseinsvorsorge, die ausschließliche Rechte an der Nutzung von Daten gewähren (Ausschließlichkeitsvereinbarungen), sind unzulässig.

(2) Dies gilt nicht, wenn zur Bereitstellung eines Dienstes im öffentlichen Interesse ein ausschließliches Recht über die Nutzung der Daten erforderlich ist. Der Datenbereitsteller überprüft die Ausschließlichkeitsvereinbarung regelmäßig, mindestens jedoch alle drei Jahre. Der Datenbereitsteller macht nach dem 15. Juli 2019 getroffene Ausschließlichkeitsvereinbarungen spätestens zwei Monate vor ihrem Inkrafttreten im Internet öffentlich zugänglich. Die endgültige Ausschließlichkeitsvereinbarung muss klar und eindeutig sein und im Internet öffentlich zugänglich gemacht werden. Dieser Absatz gilt nicht für die Digitalisierung von Kulturbeständen.

(3) Bezieht sich ein ausschließliches Recht auf die Digitalisierung von Kulturbeständen, darf es für höchstens zehn Jahre gewährt werden. Die Ausschließlichkeitsvereinbarungen müssen klar und eindeutig sein und im Internet öffentlich zugänglich gemacht werden. Der öffentlichen Stelle ist im Rahmen der Ausschließlichkeitsvereinbarung eine Kopie der digitalisierten Kulturbestände unentgeltlich zur Verfügung zu stellen. Die öffentliche Stelle ermöglicht die Nutzung dieser Kopie am Ende des Ausschließlichkeitszeitraums.

(4) Der Datenbereitsteller macht Vereinbarungen über rechtliche oder praktische Vorkehrungen, die nicht ausdrücklich ausschließliche Rechte gewähren, die aber darauf abzielen oder die geeignet sind, die Nutzung von Daten durch andere Einrichtungen als die an der Vereinbarung beteiligten Dritten zu beschränken, spätestens zwei Monate vor ihrem Inkrafttreten im Internet öffentlich zugänglich. Die Auswirkungen solcher rechtlichen oder praktischen Vorkehrungen auf die Verfügbarkeit und Nutzbarkeit von Daten werden regelmäßig, mindestens alle drei Jahre, überprüft. Die endgültige Vereinbarung muss klar und eindeutig sein und im Internet öffentlich zugänglich gemacht werden.

(5) Am 17. Juli 2013 bestehende Ausschließlichkeitsvereinbarungen, die nicht unter die Ausnahmen der Absätze 2 und 3 fallen, enden bei Ablauf der Ausschließlichkeitsvereinbarung, spätestens jedoch am 31. Dezember 2027. Am 16. Juli 2019 bestehende Ausschließlichkeitsvereinbarungen, die von Unternehmen der Daseinsvorsorge getroffen wurden und die nicht unter die Ausnahmen der Absätze 2 und 3 fallen, enden bei Ablauf der Ausschließlichkeitsvereinbarung, spätestens jedoch am 31. Dezember 2033.

§ 7 Verfügbare Formate, Metadaten

(1) Der Datenbereitsteller muss die Nutzung der Daten in allen angefragten und bei ihm vorhandenen Formaten und Sprachen ermöglichen.

(2) Soweit möglich und sinnvoll, sind Daten elektronisch und in nach den anerkannten Regeln der Technik offenen, maschinenlesbaren, zugänglichen, auffindbaren und interoperablen Formaten zusammen mit den zugehörigen Metadaten bereitzustellen. Sowohl die Formate als auch die Metadaten entsprechen, soweit möglich, förmlichen offenen Standards.

(3) Die Absätze 1 und 2 verpflichten öffentliche Stellen und öffentliche Unternehmen nicht, Daten und Metadaten neu zu erstellen oder anzupassen oder Teile von Datensätzen zur Verfügung zu stellen, wenn dies mit unverhältnismäßigem Aufwand verbunden wäre, der über eine einfache Bearbeitung hinausgeht. Öffentliche Stellen und Unternehmen der Daseinsvorsorge sind außerdem nicht verpflichtet, die Erstellung und Speicherung bestimmter Arten von Daten im Hinblick auf deren Nutzung durch eine Organisation des privaten oder öffentlichen Sektors fortzusetzen.

(4) Die Metadaten zu maschinenlesbaren Daten sind, soweit möglich und sinnvoll, über das nationale Metadatenportal GovData zur Verfügung zu stellen.

§ 8 Dynamische Daten

(1) Der Datenbereitsteller muss die Nutzung von dynamischen Daten unmittelbar nach der Erfassung in Echtzeit mithilfe geeigneter Anwendungsprogrammierschnittstellen und, falls technisch erforderlich, als Massen-Download ermöglichen.

(2) Soweit die Anforderungen nach Absatz 1 die finanzielle und technische Leistungsfähigkeit der öffentlichen Stelle oder des Unternehmens der Daseinsvorsorge übersteigen und somit zu einem unverhältnismäßigen Aufwand führen, ist die Nutzung dynamischer Daten vorübergehend mit den zur Verfügung stehenden technischen Mitteln zu ermöglichen. Die Ausschöpfung des wirtschaftlichen und sozialen Potenzials der dynamischen Daten soll dadurch nicht übermäßig beeinträchtigt werden.

§ 9 Hochwertige Datensätze

Öffentliche Stellen und Unternehmen der Daseinsvorsorge müssen die Nutzung hochwertiger Datensätze in maschinenlesbarem Format über geeignete Anwendungsprogrammierschnittstellen und, falls technisch erforderlich, als Massen-Download ermöglichen.

§ 10 Grundsatz der Unentgeltlichkeit

(1) Die Nutzung von Daten ist unentgeltlich. Es ist jedoch zulässig, die Erstattung von verursachten Grenzkosten für die folgenden Tätigkeiten und Maßnahmen zu verlangen:

1. die Reproduktion, Bereitstellung und Verbreitung von Daten,
2. die Anonymisierung personenbezogener Daten und
3. Maßnahmen zum Schutz vertraulicher Geschäftsinformationen.

(2) Abweichend von Absatz 1 Satz 1 dürfen für die Nutzung von Daten Entgelte verlangen:

1. öffentliche Stellen, die ausreichende Einnahmen erzielen müssen, um einen wesentlichen Teil ihrer Kosten im Zusammenhang mit der Erfüllung ihrer öffentlichen Aufträge zu decken;
2. Bibliotheken, einschließlich Hochschulbibliotheken, Museen und Archive;
3. Unternehmen der Daseinsvorsorge.

(3) Absatz 1 Satz 2 und Absatz 2 Nummer 1 und 3 gelten nicht für hochwertige Datensätze sowie Forschungsdaten.

(4) Wenn öffentliche Stellen, die ausreichende Einnahmen erzielen müssen, um einen wesentlichen Teil ihrer Kosten im Zusammenhang mit der Erfüllung ihres öffentlichen Auftrags zu decken, von der Anwendung des Absatzes 1 Satz 1 ausgenommen werden wollen, melden sie die Berufung auf die Ausnahme der Bundesnetzagentur. Die Bundesnetzagentur führt eine Liste der öffentlichen Stellen, die von der Ausnahme Gebrauch machen, und macht die Liste auf ihrer Internetseite zugänglich.

(5) Für öffentliche Stellen, die Einnahmen erzielen müssen, um einen wesentlichen Teil ihrer Kosten bei der Erfüllung ihres öffentlichen Auftrags zu decken, und bei denen sich die unentgeltliche Nutzung hochwertiger Datensätze wesentlich auf ihren Haushalt auswirkt, gilt die Unentgeltlichkeit der Nutzung hochwertiger Datensätze spätestens zwölf Monate nach dem 23. Juli 2021.

§ 11 Bemessung der Entgelthöhe

(1) In den in § 10 Absatz 2 Nummer 1 und 3 genannten Fällen berechnen die öffentlichen Stellen und Unternehmen der Daseinsvorsorge die Entgelte nach von ihnen festzulegenden objektiven, transparenten und nachprüfbaren Kriterien.

(2) Die Entgelte aus der Bereitstellung von Daten und der Gestattung ihrer Nutzung in dem entsprechenden Abrechnungszeitraum dürfen die Kosten ihrer Erfassung, Erstellung, Reproduktion, Verbreitung und Speicherung zuzüglich einer angemessenen Gewinnspanne sowie die Kosten für die Anonymisierung personenbezogener Daten und für Maßnahmen zum Schutz vertraulicher Geschäftsinformationen nicht übersteigen. Im Fall des § 10 Absatz 2 Nummer 2 dürfen zudem die Kosten für Bewahrung und Rechteklärung zur Berechnungsgrundlage hinzugefügt werden.

(3) Die Entgelte werden nach Maßgabe der geltenden Buchführungsgrundsätze berechnet.

§ 12 Transparenz von Entgelten

(1) Wurden für die Nutzung von Daten Entgelte festgelegt, die für die Allgemeinheit gelten (Standardentgelte), sind die Bedingungen und die tatsächliche Höhe der Standardentgelte einschließlich ihrer Berechnungsgrundlage im Internet öffentlich zugänglich zu machen.

(2) Wurden für die Nutzung keine Standardentgelte festgelegt, sind die Faktoren, die bei der Berechnung der Entgelte berücksichtigt werden, anzugeben. Auf Anfrage wird auch die Berechnungsweise dieser Entgelte in Bezug auf einen spezifischen Antrag auf Nutzung angegeben.

§ 13 Rechtsweg

Für Streitigkeiten nach diesem Gesetz ist der Verwaltungsrechtsweg gegeben.

Gesetz zur Nutzung von Gesundheitsdaten zu gemeinwohlorientierten Forschungszwecken und zur datenbasierten Weiterentwicklung des Gesundheitswesens (Gesundheitsdatennutzungsgesetz - GDNG)

§ 1 Zweck des Gesetzes; Anwendungsbereich

(1) Dieses Gesetz dient der Regelung der Nutzung von Gesundheitsdaten zu gemeinwohlorientierten Forschungszwecken und zur datenbasierten Weiterentwicklung des Gesundheitswesens als lernendes System. Das Ziel der Nutzung von Gesundheitsdaten ist, eine sichere, bessere und qualitätsgesicherte Gesundheitsversorgung und Pflege zu gewährleisten, Forschung und Innovation zu fördern und das digitalisierte Gesundheitssystem auf Grundlage einer soliden Datenbasis weiterzuentwickeln.

(2) Dieses Gesetz gilt für die Verarbeitung von Gesundheitsdaten zu Forschungszwecken, zur Verbesserung der Gesundheitsversorgung und Pflege sowie zu weiteren im Gemeinwohl liegenden Zwecken.

(3) Die Vorschriften dieses Gesetzes gehen jenen des Fünften und Elften Buches Sozialgesetzbuch vor, soweit Gesundheitsdaten für wissenschaftliche Forschungszwecke und zu weiteren in diesem Gesetz genannten, im Gemeinwohl liegenden Zwecken verarbeitet werden.

§ 2 Begriffsbestimmungen

Im Sinne dieses Gesetzes sind oder ist

1. „Gesundheitsdaten“ Gesundheitsdaten im Sinne des Artikels 4 Nummer 15 der 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; L 314 vom 22.11.2016, S. 72; L 127 vom 23.5.2018, S. 2; L 74 vom 4.3.2021, S. 35) in der jeweils geltenden Fassung, einschließlich Gesundheitsdaten, die zugleich Sozialdaten nach § 67 des Zehnten Buches Sozialgesetzbuch sind;

2. „personenbezogene Daten“ personenbezogene Daten im Sinne des Artikels 4 Nummer 1 der Verordnung (EU) 2016/679;

3. „datenhaltende Stelle“ natürliche und juristische Personen einschließlich deren Zusammenschlüsse im Sinne von Datenplattformen oder Dateninfrastrukturen, die berechtigt oder verpflichtet sind, Gesundheitsdaten für Forschungszwecke und weitere in diesem Gesetz genannte Zwecke Dritten zur Verfügung zu stellen; dazu gehören insbesondere gesetzlich geregelte datenhaltende Stellen wie das Forschungsdatenzentrum Gesundheit nach § 303d des Fünften Buches Sozialgesetzbuch, das Zentrum für Krebsregisterdaten beim Robert Koch-Institut und die Plattform nach § 64e Absatz 9 des Fünften Buches Sozialgesetzbuch;

4. „Datennutzende“ natürliche und juristische Personen, die Zugang zu Gesundheitsdaten zu Forschungszwecken und weiteren in diesem Gesetz genannten Zwecken begehren oder erhalten haben;

5. „Forschungsvorhaben“ Vorhaben, bei denen Gesundheitsdaten zu den in Artikel 9 Absatz 2 Buchstabe j und Artikel 89 Absatz 1 Satz 1 und Absatz 2 der Verordnung

(EU) 2016/679 genannten wissenschaftlichen Forschungszwecken verarbeitet werden; diese Gesundheitsdaten können auch Sozialdaten nach § 67 des Zehnten Buches Sozialgesetzbuch sein;

6. „Gesundheits- und Versorgungsforschung“ Forschungsvorhaben mit dem Ziel, die Gesundheit zu fördern, Krankheiten vorzubeugen, zu heilen und ihre Folgen zu vermindern, die Gesundheitsversorgung und -prävention zu verbessern sowie das Gesundheitswesen weiterzuentwickeln;

7. „datenverarbeitende Gesundheitseinrichtung“ Einrichtungen, in denen für Zwecke der Gesundheitsvorsorge oder der Arbeitsmedizin, für die Beurteilung der Arbeitsfähigkeit des Beschäftigten, für die medizinische Diagnostik oder für Zwecke der Versorgung oder Behandlung im Gesundheits- oder Sozialbereich Daten von oder unter der Verantwortung von Angehörigen eines Heilberufs verarbeitet werden, der für die Berufsausübung oder die Führung der Berufsbezeichnung eine staatlich geregelte Ausbildung erfordert;

8. „Sekundärdatennutzung“ die Weiterverarbeitung von Gesundheitsdaten zu anderen Zwecken als denjenigen, für die die Daten ursprünglich erhoben wurden.

§ 3 Datenzugangs- und Koordinierungsstelle für Gesundheitsdaten; Verordnungsermächtigung

(1) Beim Bundesinstitut für Arzneimittel und Medizinprodukte wird eine zentrale Datenzugangs- und Koordinierungsstelle für Gesundheitsdaten eingerichtet.

(2) Die Datenzugangs- und Koordinierungsstelle für Gesundheitsdaten unterstützt und berät Datennutzende beim Zugang zu Gesundheitsdaten. Sie hat insbesondere die Aufgabe,

1. einen öffentlichen Metadaten-Katalog barrierefrei zu führen und zu pflegen, in dem zu Transparenzzwecken Informationen über die im deutschen Gesundheitswesen vorhandenen und öffentlich zugänglichen Gesundheitsdaten und über die jeweiligen Halter dieser Daten gesammelt werden,

2. Datennutzende bei der Identifizierung und bei der Lokalisierung der für ihre Zwecke benötigten Gesundheitsdaten zu beraten,

3. bei einer Antragstellung von Datennutzenden auf Zugang zu Gesundheitsdaten bei datenhaltenden Stellen zu beraten,

4. Anträge auf Zugang zu Gesundheitsdaten bei den nach Absatz 3 Satz 1 Nummer 4 zu spezifizierenden datenhaltenden Stellen entgegenzunehmen und im Wege der Weiterleitung an die zuständigen datenhaltenden und mittelnden Stellen zu übermitteln,

5. bei der für die in den Nummern 3 und 4 genannten Antragstellung die erforderliche Kommunikation zwischen den Antragstellenden und den zuständigen Stellen zu unterstützen,

6. die Öffentlichkeit über die Aktivitäten der Datenzugangs- und Koordinierungsstelle für Gesundheitsdaten zu informieren,

7. ein öffentliches Antragsregister mit Informationen zu den über die Datenzugangs- und Koordinierungsstelle für Gesundheitsdaten gestellten Anträgen auf Zugang

zu Gesundheitsdaten, zu den Datennutzenden, zu den Vorhaben, für die Daten beantragt wurden, und zu deren Ergebnissen aufzubauen und zu pflegen,

8. die Bundesregierung im Rahmen von Vorhaben und in Gremien zur Steigerung der Verfügbarkeit von Gesundheitsdaten und beim Aufbau einer vernetzten Gesundheitsdateninfrastruktur auf Bundesebene und in der Europäischen Union zu unterstützen,

9. Konzepte zu erstellen

   a) zur Nutzung von sicheren Verarbeitungsumgebungen als Maßnahme zur Verbesserung des Datenschutzes und der Datensicherheit im Rahmen der Weiterverarbeitung von Gesundheitsdaten zu Forschungszwecken und weiteren im Gemeinwohl liegenden Zwecken,

   b) zur Weiterentwicklung der zentralen Datenzugangs- und Koordinierungsstelle für Gesundheitsdaten als eigenständige Institution unter Einbindung bestehender Dateninfrastrukturen unter Berücksichtigung europäischer Entwicklungen und unter Beteiligung der maßgeblichen Akteure des Gesundheitswesens und der Gesundheitsforschung,

   c) zur Verknüpfung und gemeinsamen Verarbeitung von pseudonymisierten Gesundheitsdaten verschiedener datenhaltender Stellen,

10. die in § 4 für die zentrale Datenzugangs- und Koordinierungsstelle für Gesundheitsdaten vorgesehenen Aufgaben im Antragsverfahren bei der Verknüpfung von Daten des Forschungsdatenzentrums Gesundheit mit Daten der klinischen Krebsregister der Länder nach § 65c des Fünften Buches Sozialgesetzbuch und bei der Verarbeitung dieser Daten wahrzunehmen.

(3) Das Bundesministerium für Gesundheit wird ermächtigt, im Benehmen mit dem Bundesministerium für Bildung und Forschung ohne Zustimmung des Bundesrates durch Rechtsverordnung das Nähere zu regeln zu

1. der Einrichtung und zur Organisation der Datenzugangs- und Koordinierungsstelle für Gesundheitsdaten,

2. den Einzelheiten der Wahrnehmung der Aufgaben der Datenzugangs- und Koordinierungsstelle für Gesundheitsdaten nach Absatz 2 sowie zu den hierbei anzuwendenden Verfahren,

3. den zur Übermittlung der Anträge an die datenhaltenden und datenmittelnden Stellen gemäß Absatz 2 Satz 2 Nummer 4 jeweils notwendigen Arbeitsstrukturen der Datenzugangs- und Koordinierungsstelle für Gesundheitsdaten,

4. Kriterien für die Eignung von datenhaltenden und datenmittelnden Stellen zur Einbeziehung in die Sekundärdatennutzung über die Datenzugangs- und Koordinierungsstelle für Gesundheitsdaten sowie zur Bereitstellung transparenter Informationen über diese Kriterien.

Geplante Regelungen sind im Benehmen mit den Vertretern der jeweiligen datenhaltenden Stellen zu treffen. Soweit die datenhaltenden Stellen dem Recht des Sozialgesetzbuchs unterliegen, ergehen die Regelungen im Benehmen mit dem Bundesministerium für Arbeit und Soziales.

(4) Die Datenzugangs- und Koordinierungsstelle für Gesundheitsdaten richtet im Benehmen mit dem Bundesministerium für Gesundheit und dem Bundesministerium für Bildung und Forschung einen Arbeitskreis zur Gesundheitsdatennutzung ein. Der Arbeitskreis setzt sich aus Vertretern der datenhaltenden Stellen, aus Vertretern der Patientenorganisationen, die in der Patientenbeteiligungsverordnung genannt oder nach dieser Verordnung anerkannt sind, aus Vertretern von Leistungserbringern, aus Vertretern der Gesundheitsforschung sowie aus Vertretern weiterer betroffener Gruppen und Institutionen zusammen. Der Arbeitskreis wirkt beratend an der Ausgestaltung, Weiterentwicklung und Evaluation der Aufgabenwahrnehmung der Datenzugangs- und Koordinierungsstelle für Gesundheitsdaten mit.

(5) Dieser Paragraph gilt nicht für in § 137a Absatz 10 des Fünften Buches Sozialgesetzbuch genannte Anträge auf Auswertung von bei den verpflichtenden Maßnahmen der Qualitätssicherung nach § 136 Absatz 1 Satz 1 Nummer 1 des Fünften Buches Sozialgesetzbuch erhobenen Daten.

§ 4 Verknüpfung von Daten des Forschungsdatenzentrums Gesundheit mit Daten der klinischen Krebsregister der Länder; Verordnungsermächtigung

(1) Die Verknüpfung von pseudonymisierten Daten des Forschungsdatenzentrums Gesundheit nach § 303d des Fünften Buches Sozialgesetzbuch mit pseudonymisierten Daten der klinischen Krebsregister der Länder nach § 65c des Fünften Buches Sozialgesetzbuch sowie die Verarbeitung dieser Daten für Forschungsvorhaben ist nach Maßgabe der folgenden Absätze zulässig.

(2) Für die Verknüpfung und für die Verarbeitung der pseudonymisierten Daten nach Absatz 1 bedarf es einer vorherigen Genehmigung der Datenzugangs- und Koordinierungsstelle für Gesundheitsdaten nach § 3. Die Genehmigung ist auf Antrag zu erteilen, sofern

1. die Verknüpfung der in Absatz 1 genannten Daten für die zu untersuchende Forschungsfrage erforderlich ist,
2. die erforderlichen Anträge auf Zugang zu den zu verknüpfenden Daten in pseudonymisierter Form beim Forschungsdatenzentrum Gesundheit nach § 303e Absatz 3 des Fünften Buches Sozialgesetzbuch sowie bei den zuständigen klinischen Krebsregistern der Länder nach § 65c des Fünften Buches Sozialgesetzbuch nach dem geltenden Landesrecht für den Zugang zu den zu verknüpfenden Daten in pseudonymisierter Form bewilligt worden sind und
3. schutzwürdige Interessen der betroffenen Person nicht beeinträchtigt werden oder das öffentliche Interesse an der Forschung das Geheimhaltungsinteresse der betroffenen Person überwiegt und das spezifische Reidentifikationsrisiko in Bezug auf die beantragten Daten bewertet und unter angemessener Wahrung des angestrebten wissenschaftlichen Nutzens durch geeignete Maßnahmen minimiert worden ist.

(3) In dem Antrag haben die Antragstellenden nachvollziehbar darzulegen, dass Umfang und Struktur der zu verknüpfenden Daten geeignet und erforderlich sind, um die zu untersuchende Forschungsfrage zu beantworten.

(4) Die Datenzugangs- und Koordinierungsstelle für Gesundheitsdaten

1. unterstützt die Antragstellenden im Rahmen des Verfahrens zur Erteilung der Genehmigung nach Absatz 2 Satz 1 bei der Kommunikation mit dem Forschungsdatenzentrum Gesundheit und mit den beteiligten klinischen Krebsregistern der Länder nach § 65c des Fünften Buches Sozialgesetzbuch sowie bei der Stellung der in Absatz 2 Satz 2 Nummer 2 genannten Anträge,

2. stellt für den Antrag auf Genehmigung nach Absatz 2 Satz 1 und für die in Absatz 2 Satz 2 Nummer 2 genannten Anträge einen einheitlichen Antragsprozess im Benehmen mit zwei von den klinischen Krebsregistern der Länder nach § 65c des Fünften Buches Sozialgesetzbuch benannten Vertretern und dem Zentrum für Krebsregisterdaten beim Robert Koch-Institut nach § 1 Absatz 1 des Bundeskrebsregisterdatengesetzes bereit und

3. leitet die in Absatz 2 Satz 2 Nummer 2 genannten Anträge an die zuständigen Stellen weiter.

(5) Wird die Genehmigung nach Absatz 2 Satz 1 erteilt, so werden die im Antrag benannten Daten mit einer von der Datenzugangs- und Koordinierungsstelle für Gesundheitsdaten für den jeweiligen Antrag festzulegenden sicheren Verarbeitungsumgebung einer öffentlichrechtlichen Stelle verknüpft und den Antragstellenden als pseudonymisierte Einzeldatensätze, ohne Sichtbarmachung von Pseudonymen, verfügbar gemacht. In einer sicheren Verarbeitungsumgebung muss durch geeignete technische und organisatorische Maßnahmen sichergestellt sein, dass die Verarbeitung durch die Antragstellenden auf das für den jeweiligen Nutzungszweck erforderliche Maß beschränkt ist und insbesondere ein Kopieren der Daten verhindert werden kann.

(6) Wird die Genehmigung nach Absatz 2 Satz 1 erteilt, übermitteln die klinischen Krebsregister der Länder nach § 65c des Fünften Buches Sozialgesetzbuch an die durch die Datenzugangs- und Koordinierungsstelle für Gesundheitsdaten festgelegte sichere Verarbeitungsumgebung die beantragten Daten in pseudonymisierter Form zusammen mit einer auf Grundlage der Krankenversichertennummer anlassbezogen zu erstellenden Forschungskennziffer unter Mitwirkung der Vertrauensstelle nach § 303c des Fünften Buches Sozialgesetzbuch und nach den Vorgaben der Rechtsverordnung nach Absatz 9. Zur Sicherstellung einer qualitätsgesicherten Datenzusammenführung soll bei der Übermittlung der Daten der klinischen Krebsregister der Länder nach § 65c des Fünften Buches Sozialgesetzbuch ein Datenbereinigungsverfahren genutzt werden.

(7) Wird die Genehmigung nach Absatz 2 Satz 1 erteilt, übermittelt das Forschungsdatenzentrum Gesundheit nach § 303d des Fünften Buches Sozialgesetzbuch an die durch die Datenzugangs- und Koordinierungsstelle für Gesundheitsdaten festgelegte sichere Verarbeitungsumgebung die beantragten Daten in pseudonymisierter Form zusammen mit einer anlassbezogen zu erstellenden Forschungskennziffer unter Mitwirkung der Vertrauensstelle nach § 303c des Fünften Buches Sozialgesetzbuch und nach den Vorgaben der Rechtsverordnung nach Absatz 9.

(8) Die Datennutzenden dürfen die nach Absatz 5 zugänglich gemachten Daten

1. nur für die Zwecke nutzen, für die sie zugänglich gemacht werden, und

2. nicht an Dritte weitergeben.

Die Datennutzenden haben bei der Verarbeitung darauf zu achten, keinen Bezug zu Personen, Leistungserbringern oder Leistungsträgern herzustellen. Im Fall einer unabsichtlichen Herstellung eines Personenbezugs ist die Datenzugangs- und Koordinierungsstelle für Ge-

sundheitsdaten zu informieren. Die Datenzugangs- und Koordinierungsstelle für Gesundheitsdaten leitet die enthaltene Information an das Forschungsdatenzentrum Gesundheit und an die zuständigen klinischen Krebsregister der Länder nach § 65c des Fünften Buches Sozialgesetzbuch weiter.

(9) Das Bundesministerium für Gesundheit wird ermächtigt, durch Rechtsverordnung mit Zustimmung des Bundesrates das Nähere zu regeln zu

1. dem technischen Verfahren zur Verknüpfung der Daten anhand einer anlassbezogen zu erstellenden Forschungskennziffer, einschließlich der hierzu erforderlichen Datenverarbeitung durch
   a) das Forschungsdatenzentrum Gesundheit,
   b) die klinischen Krebsregister der Länder nach § 65c des Fünften Buches Sozialgesetzbuch,
   c) das Zentrum für Krebsregisterdaten beim Robert Koch-Institut nach § 1 des Bundeskrebsregisterdatengesetzes,
   d) die zentrale Antrags- und Registerstelle nach § 10 des Bundeskrebsregisterdatengesetzes sowie
   e) die beteiligten Vertrauensstellen dieser Einrichtungen,
2. den Anforderungen an sichere Verarbeitungsumgebungen nach Absatz 5 und den Kriterien für die Auswahl der Verarbeitungsumgebung durch die Datenzugangs- und Koordinierungsstelle für Gesundheitsdaten,
3. dem einheitlichen Antragsprozess und den weiteren in Absatz 4 genannten unterstützenden Maßnahmen der Datenzugangs- und Koordinierungsstelle für Gesundheitsdaten,
4. dem in Absatz 6 genannten Datenbereinigungsverfahren.

Hinsichtlich des Satzes 1 Nummer 2 erfolgt der Erlass der Rechtsverordnung im Benehmen mit der oder dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit und mit dem Bundesamt für Sicherheit in der Informationstechnik.

§ 5 Datenschutzaufsicht bei länderübergreifenden Gesundheitsforschungsvorhaben

(1) Sind an einem Vorhaben der Versorgungs- oder Gesundheitsforschung, bei dem Gesundheitsdaten verarbeitet werden, eine oder mehrere öffentliche oder nicht öffentliche Stellen als Verantwortliche derart beteiligt, dass mehr als eine Datenschutzaufsichtsbehörde des Bundes oder der Länder nach Kapitel VI der Verordnung (EU) 2016/679 zuständig ist, und sind diese Stellen nicht gemeinsam Verantwortliche gemäß Artikel 26 der Verordnung (EU) 2016/679, so kann dieses Vorhaben den Datenschutzaufsichtsbehörden zur federführenden Datenschutzaufsicht angezeigt werden.

(2) Durch eine Anzeige nach Absatz 1, die von allen Stellen gemeinsam gegenüber allen zuständigen Datenschutzaufsichtsbehörden abzugeben ist, wird die Datenschutzaufsichtsbehörde federführend zuständig, in deren Zuständigkeitsbereich die am Vorhaben nach Absatz 1 beteiligte Stelle fällt, die in dem vorangegangenen Geschäftsjahr den größten Jahresumsatz erzielt hat. In dem Fall, dass nicht alle am Vorhaben nach Absatz 1 beteiligten Stellen einen Jahresumsatz aufweisen, wird stattdessen diejenige Datenschutzaufsichtsbehörde fe-

derführend zuständig, in deren Zuständigkeitsbereich die am Vorhaben nach Absatz 1 beteiligte Stelle fällt, die die meisten Personen beschäftigt, welche ständig personenbezogene Daten automatisiert verarbeiten. Der Anzeige nach Absatz 1 sind die entsprechenden nachweisenden Unterlagen beizufügen.

(3) Die federführend zuständige Datenschutzaufsichtsbehörde hat die Aufgabe, die Tätigkeiten und Aufsichtsmaßnahmen der zuständigen Datenschutzaufsichtsbehörden zu koordinieren; sie fördert eine Zusammenarbeit der zuständigen Aufsichtsbehörden beim Vorhaben nach Absatz 1 und wirkt auf eine gemeinsame Entscheidung hin. Die aufsichtsrechtlichen Befugnisse aller nach Absatz 1 zuständigen Datenschutzaufsichtsbehörden bleiben unberührt. Die zuständigen Datenschutzaufsichtsbehörden stimmen sich untereinander ab, wenn sie in ihrem Zuständigkeitsbereich tätig werden.

(4) Sind an einem Vorhaben der Gesundheits- und Versorgungsforschung, bei dem Gesundheitsdaten verarbeitet werden, eine oder mehrere nicht öffentliche Stellen als Verantwortliche derart beteiligt, dass mehr als eine Datenschutzaufsichtsbehörde der Länder zuständig ist, und sind die beteiligten nicht öffentlichen Stellen gemeinsam Verantwortliche gemäß Artikel 26 der Verordnung (EU) 2016/679, können diese gemeinsam anzeigen, dass sie gemeinsam Verantwortliche sind und deshalb für die von ihnen gemeinsam verantwortete Datenverarbeitung allein die Datenschutzaufsichtsbehörde zuständig sein soll, in deren Zuständigkeitsbereich die nicht öffentliche Stelle fällt, die in dem der Antragstellung vorangegangenen Geschäftsjahr den größten Jahresumsatz erzielt hat. Die gemeinsame Anzeige ist an alle Datenschutzaufsichtsbehörden zu richten, die für die gemeinsam Verantwortlichen zuständig sind, und muss die die umsatzstärkste nicht öffentliche Stelle nachweisenden Unterlagen enthalten. Ab dem Zeitpunkt, zu dem die in den Sätzen 1 und 2 genannte Anzeige bei der für die umsatzstärkste nicht öffentliche Stelle zuständigen Behörde eingegangen ist, wird diese die allein zuständige Datenschutzaufsichtsbehörde. Für nichtöffentliche Stellen, die gemeinsam Verantwortliche gemäß Artikel 26 der Verordnung (EU) 2016/679 sind, jedoch keinen Jahresumsatz erzielen, gelten die Sätze 1 bis 3 entsprechend mit der Maßgabe, dass die Behörde allein zuständig ist, die für den Verantwortlichen zuständig ist, der die meisten Personen beschäftigt, welche ständig personenbezogene Daten automatisiert verarbeiten. § 3 Absatz 3 und 4 des Verwaltungsverfahrensgesetzes findet entsprechende Anwendung.

§ 6 Weiterverarbeitung von Versorgungsdaten zur Qualitätssicherung, zur Förderung der Patientensicherheit und zu Forschungszwecken

(1) Datenverarbeitende Gesundheitseinrichtungen dürfen die bei ihnen gemäß Artikel 9 Absatz 2 Buchstabe h und i der Verordnung (EU) 2016/679 rechtmäßig gespeicherten Daten weiterverarbeiten, soweit dies erforderlich ist

1. zur Qualitätssicherung und zur Förderung der Patientensicherheit,
2. zur medizinischen, zur rehabilitativen und zur pflegerischen Forschung oder
3. zu statistischen Zwecken, einschließlich der Gesundheitsberichterstattung.

Die nach Satz 1 weiterverarbeiteten, personenbezogenen Daten sind zu pseudonymisieren; sie sind zu anonymisieren, sobald dies im Rahmen der Weiterverarbeitung für den jeweiligen Zweck nach Satz 1 möglich ist. Sind mehrere natürliche Personen in der datenverarbeitenden Gesundheitseinrichtung tätig, hat die Gesundheitseinrichtung ein Rechte- und Rollenkonzept zu erstellen, das gewährleistet, dass nur befugte Personen die in Satz 1 genannten Daten weiterverarbeiten können sowie Weiterverarbeitungen protokolliert und unbefugte Verarbeitungen geahndet werden können. Daten, die nach Absatz 1 Satz 1 weiterverarbeitet

werden, sind spätestens 30 Jahre nach Beginn der Weiterverarbeitung nach Absatz 1 Satz 1 zu löschen. § 14 des Transplantationsgesetzes ist zu beachten.

(2) Die Ergebnisse der Weiterverarbeitung von Gesundheitsdaten nach Absatz 1 sind zu anonymisieren, sobald dies nach dem jeweiligen Zweck nach Absatz 1 Satz 1 möglich ist.

(3) Die Weitergabe der personenbezogenen Daten an Dritte ist im Rahmen der Weiterverarbeitung nach Absatz 1 untersagt. Abweichend von Satz 1 ist die Weitergabe von personenbezogenen Daten im Rahmen der Weiterverarbeitung nach Absatz 1 zulässig, soweit die betroffene Person eingewilligt hat oder eine andere gesetzliche Vorschrift des Bundesrechts, des Landesrechts oder unmittelbar geltender Rechtsakte der Europäischen Union dies vorsieht. Die datenverarbeitenden Gesundheitseinrichtungen dürfen die gemäß Artikel 9 Absatz 2 Buchstabe h der Verordnung (EU) 2016/679 rechtmäßig gespeicherten Gesundheitsdaten anonymisieren, um die anonymisierten Daten zu den in Absatz 1 Satz 1 genannten Zwecken an Dritte zu übermitteln. Abweichend von Satz 1 ist eine gemeinsame Nutzung und Verarbeitung der in Absatz 1 Satz 1 genannten Daten zu den in Absatz 1 Satz 1 genannten Zwecken durch öffentlich geförderte Zusammenschlüsse von datenverarbeitenden Gesundheitseinrichtungen einschließlich Verbundforschungsvorhaben und Forschungspraxennetzwerken zulässig, wenn

1. die Verarbeitung zu den in Absatz 1 Satz 1 genannten Zwecken erforderlich ist,
2. die Anforderungen nach den Absätzen 1, 2 und 4 hinsichtlich der Verarbeitung eingehalten werden,
3. die Interessen des datenschutzrechtlich Verantwortlichen an der Verarbeitung die Interessen der betroffenen Person an einem Ausschluss der Verarbeitung erheblich überwiegen und
4. die zuständige Datenschutzaufsichtsbehörde der gemeinsamen Nutzung und Verarbeitung der Daten zugestimmt hat.

Die Datenschutzaufsichtsbehörde soll innerhalb eines Monats über die Zustimmung nach Satz 4 Nummer 4 entscheiden.

(4) Datenverarbeitende Gesundheitseinrichtungen, die nach Absatz 1 Daten verarbeiten, sind verpflichtet, öffentlich und allgemein in präziser, transparenter, leicht verständlicher und zugänglicher Form in einer klaren und einfachen Sprache über die Zwecke, für die nach Absatz 1 Daten weiterverarbeitet werden, zu informieren. Dabei ist auch über laufende Forschungsvorhaben und veröffentlichte Forschungsergebnisse zu informieren, die nach § 8 registriert oder veröffentlicht wurden. Auf Verlangen einer von der Verarbeitung zu den in Absatz 1 Satz 1 Nummer 2 oder 3 genannten Zwecken betroffenen Person ist die datenverarbeitende Gesundheitseinrichtung verpflichtet, über die Art, den Umfang und den konkreten Zweck der Verarbeitung der Daten zu den in Absatz 1 Satz 1 Nummer 2 oder Nummer 3 genannten Zwecken in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu informieren.

§ 7 Geheimhaltungspflichten

(1) Datennutzende dürfen Gesundheitsdaten, die ihnen für wissenschaftliche Forschungszwecke verfügbar gemacht wurden,

1. nur für die Zwecke nutzen, für die sie ihnen zugänglich gemacht wurden, und

2. nicht an Dritte weitergeben, wenn dies nicht nach Absatz 3 oder Absatz 4 zulässig ist.

Satz 1 gilt auch für Gesundheitsdaten einer Person, die bereits verstorben ist.

(2) Bereitgestellte Daten dürfen nicht zum Zwecke der Herstellung eines Personenbezugs oder zum Zwecke der Identifizierung von Leistungserbringern oder Leistungsträgern verarbeitet werden. Dies gilt auch für Gesundheitsdaten einer Person, die bereits verstorben ist.

(3) Personen, denen fremde Gesundheitsdaten zu Forschungszwecken anvertraut oder sonst bekanntgeworden sind, dürfen diese Gesundheitsdaten den bei ihr berufsmäßig tätigen Gehilfen oder den bei ihr zur Vorbereitung auf den Beruf tätigen Personen zum Zwecke der Forschung zugänglich machen. Die Person, der fremde Gesundheitsdaten zu Forschungszwecken anvertraut oder sonst bekanntgeworden sind, darf diese fremden Gesundheitsdaten gegenüber sonstigen Personen offenbaren, die an ihrer beruflichen oder dienstlichen Tätigkeit mitwirken, soweit dies für die Inanspruchnahme der Tätigkeit der sonstigen mitwirkenden Personen erforderlich ist. Satz 2 gilt entsprechend für die dort genannten mitwirkenden Personen, wenn diese sich weiterer Personen bedienen, die an der beruflichen oder dienstlichen Tätigkeit mitwirken.

(4) Entgegen Absatz 1 dürfen Datennutzende Gesundheitsdaten, die ihnen für wissenschaftliche Forschungszwecke verfügbar gemacht wurden, für andere Zwecke weiterverarbeiten oder an Dritte weitergeben, soweit ihnen dies durch Rechtsvorschriften des Bundes oder der Länder oder unmittelbar geltender Rechtsakte der Europäischen Union gestattet ist.

(5) Wenn die zuständige Datenschutzaufsichtsbehörde eine Maßnahme nach Artikel 58 Absatz 2 Buchstabe b bis j der Verordnung (EU) 2016/679 gegenüber den Datennutzenden ergriffen hat, informiert sie den Träger der datenhaltenden Stelle.

§ 8 Registrierungspflicht; Publikationspflicht von Forschungsergebnissen bei Verarbeitung von Gesundheitsdaten im öffentlichen Interesse

Sofern in einem Forschungsvorhaben Gesundheitsdaten auf Grundlage dieses Gesetzes ohne die Einwilligung der betroffenen Personen zu Forschungszwecken verarbeitet werden, sind die für das Forschungsvorhaben Verantwortlichen verpflichtet, das Forschungsvorhaben vor Beginn der Datenverarbeitung in einem von der Weltgesundheitsorganisation anerkannten Primärregister für klinische Studien zu registrieren, sofern ein solches Primärregister die Registrierung des Forschungsvorhabens gestattet. Eine Registrierung nach Satz 1 ist entbehrlich, wenn das Forschungsvorhaben auf Grundlage eines Gesetzes bereits an anderer Stelle registriert wurde. Die für das Forschungsvorhaben Verantwortlichen sind verpflichtet, die Forschungsergebnisse innerhalb von 24 Monaten nach Abschluss des Forschungsvorhabens in anonymisierter Form und in einer für die Allgemeinheit zugänglichen Weise zu veröffentlichen und, sofern das Forschungsvorhaben nach Satz 1 registriert wurde, im jeweiligen Primärregister zu hinterlegen. Behörden können bestimmen, dass Forschungsvorhaben, die sie in Auftrag gegeben haben oder die unter ihrer Rechts- oder Fachaufsicht durchgeführt werden, abweichend von Satz 1 oder Satz 3 nicht registriert werden müssen oder deren Ergebnisse nicht oder erst zu einem späteren Zeitpunkt veröffentlicht werden müssen, sofern dies zum Schutz von besonderen öffentlichen Belangen gemäß § 3 des Informationsfreiheitsgesetzes erforderlich ist.

§ 9 Strafvorschriften

(1) Mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe wird bestraft, wer

1. entgegen § 7 Absatz 1 Gesundheitsdaten nutzt, weitergibt oder
2. entgegen § 7 Absatz 2 die bereitgestellten Daten verarbeitet.

(2) Mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe wird bestraft, wer in den Fällen des Absatzes 1 gegen Entgelt oder in der Absicht handelt, sich oder einen anderen zu bereichern oder einen anderen zu schädigen.

(3) Die Tat wird nur auf Antrag verfolgt. Antragsberechtigt sind der oder die Betroffene, der oder die nach der Verordnung (EU) 2016/679 Verantwortliche, der oder die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit oder die zuständige Datenschutzaufsichtsbehörde.